

# Universidad de Alcalá Escuela Politécnica Superior

## Grado en Ingeniería en Sistemas de Información

### Trabajo Fin de Grado

Tecnología Blockchain: Criptomonedas, legalidad, actividades ilícitas y análisis de las carteras más relevantes

ESCUELA POLITECNICA  
SUPERIOR

**Autor:** Daniel Alonso Arza

**Tutor:** Manuel Sánchez Rubio

2021-2022





# UNIVERSIDAD DE ALCALÁ

ESCUELA POLITÉCNICA SUPERIOR

**Grado en Ingeniería en Sistemas de Información**

**Trabajo Fin de Grado**

**Tecnología Blockchain: Criptomonedas, legalidad, actividades ilícitas y análisis de las carteras más relevantes**

Autor: Daniel Alonso Arza

Tutor: Manuel Sánchez Rubio

**Tribunal**

**Presidente:**

**Vocal 1º:**

**Vocal 2º:**





# Índice

<b>Índice</b> -----	<b>4</b>
<b>Agradecimientos</b> -----	<b>7</b>
<b>Resumen</b> -----	<b>9</b>
<b>Abstract</b> -----	<b>11</b>
<b>Índice de Ilustraciones</b> -----	<b>13</b>
<b>Lista de Acrónimos</b> -----	<b>15</b>
<b>1. Introducción</b> -----	<b>17</b>
1.1 Presentación-----	17
1.2 Objetivos-----	18
<b>2. Blockchain</b> -----	<b>20</b>
2.1 Concepto de Blockchain-----	20
2.2 Historia del Blockchain-----	20
2.3 Funcionamiento del Blockchain-----	24
2.4 Elementos clave del Blockchain-----	26
2.5 Aplicaciones de la tecnología blockchain-----	32
<b>3. Criptomonedas</b> -----	<b>35</b>
3.1 Concepto de Criptomonedas y Ejemplos-----	35
3.2 Cómo obtener Criptomonedas-----	36
3.3 Legalidad de las criptomonedas en España y el resto del mundo-----	37
3.3.1 Introducción-----	37
3.3.2 Legalidad de las criptomonedas en España-----	38
3.3.3 Legalidad de las criptomonedas en Estados Unidos-----	40
3.3.4 Legalidad de las criptomonedas en China-----	41
	4



3.3.5 Legalidad de las criptomonedas en El Salvador -----	42
3.3.6 Cuadro resumen sobre los ejemplos expuestos -----	43
3.4 Caso práctico: las ballenas del bitcoin y seguimiento de estas -----	44
3.4.1 Introducción -----	44
3.4.2 Localización de las principales billeteras y sus movimientos -----	46
3.4.3 Conclusiones del estudio -----	53
3.5 Cajeros de criptomonedas y uso en España -----	55
3.5.1 Concepto de los cajeros de criptomonedas -----	55
3.5.2 Breve historia de los cajeros de criptomonedas -----	56
3.5.3 Cómo funcionan los cajeros de criptomonedas -----	57
3.5.4 Normativa en España de los cajeros de criptomonedas.-----	60
3.5.5 Ventajas e inconvenientes de los cajeros de criptomonedas -----	62
3.6.1 Introducción -----	64
3.6.2 El primer caso: la tienda Silk Road-----	65
3.6.3 El primer caso español: el virus de la policía -----	67
3.6.4 Operación Guatuzo y Kampuzo-----	69
<b>4. Conclusiones -----</b>	<b>74</b>
4.1 Conclusiones -----	74
4.2 Trabajo futuros -----	75
<b>5. Bibliografía -----</b>	<b>77</b>





# Agradecimientos

A mi familia, por todo el apoyo incondicional a lo largo de los años, y, en especial a mis padres, que, sin ellos, no sería quien soy hoy, por todos los sacrificios realizados por y para mi beneficio y no solo ser un apoyo sino por ser una fuente de inspiración para mí. También, quiero agradecerle a Julia, mi pareja, por la paciencia, por estar siempre ahí.

Por último, quiero agradecer a Manuel por aceptar tutorizarme en el presente Trabajo y por sus enriquecedoras clases.







# Resumen

La tecnología blockchain ha ido adquiriendo popularidad con el paso de los años, hasta llegar a nuestros días, que se encuentra en boca de personas relacionadas o no con el mundo de las tecnologías de la información.

En este trabajo, se analizará, desde un punto de vista teórico la evolución de esta tecnología a lo largo de su pequeña historia, lo que es, su funcionamiento y posibles aplicaciones que ya se emplean en nuestros días.

Tras esto, se focalizará en una de estas aplicaciones, las criptomonedas. Desde qué son, cómo obtenerlas y su legalidad en diversos países, pasando por delitos cometidos por estas. A su vez, está incluido en este apartado, un análisis práctico de los principales poseedores de criptomonedas y cómo influyen en el mercado.

**Palabras clave:** Blockchain, Criptomonedas, Bitcoin, Ballenas, Bloque, Billetera.





# Abstract

Blockchain technology has been gaining popularity over the years, until today, which is popular all over the world in people related or not with the world of information technologies.

In this work, the evolution of this technology throughout its brief history will be analysed, from a theoretical point of view, what it is, how it works and possible applications that are already used nowadays.

After this, it will focus on one of these applications, cryptocurrencies. Starting from what they are, how to obtain them and their legality in different countries, going through crimes committed by them. In turn, this section includes a practical analysis of the main cryptocurrency holders and how they influence the market.

**Key words:** Blockchain, Cryptocurrencies, Bitcoin, Whales, Block, Wallet.





# Índice de Ilustraciones

Ilustración 1 – Funcionamiento del Blockchain -----	25
Ilustración 2 - Estructura de 3 bloques del Blockchain-----	27
Ilustración 3 - Bloque de Blockchain 1 -----	29
Ilustración 4 - Bloque de Blockchain 2 -----	29
Ilustración 5 - Wallet de un minero -----	30
Ilustración 6 - Ejemplo de transacción de un bloque -----	31
Ilustración 7 - Resumen de los casos expuestos -----	43
Ilustración 8 - Clasificación de usuarios en función de su cantidad de Bitcoin-----	45
Ilustración 9 – Valor del Bitcoin a cierre del 6 de octubre del 2021 -----	46
Ilustración 10 – Valor del Bitcoin tras la declaraciones gubernamentales de EEUU ---	46
Ilustración 11 - Tweet de Elon Musk -----	47
Ilustración 12 – Evolución del valor del Bitcoin ante prohibiciones mundiales -----	48
Ilustración 13 - Las 15 wallets de Bitcoin con más valor -----	48
Ilustración 14 – Información de la wallet número 1 mundial-----	49
Ilustración 15 – Gráfica de ventas de la mayor wallet de Bitcoin-----	50
Ilustración 16 – Wallet número 4 mundial -----	50
Ilustración 17 – Gráfica con ventas y repercusión del 4º mejor wallet-----	51
Ilustración 18 – Número de transacciones diarias -----	51
Ilustración 19 – Wallet número 5 mundial -----	52
Ilustración 20 – Ventas y repercusión de la 5ª billetera mundial-----	52
Ilustración 21 – Cuenta de Twitter de Whale alert -----	53
Ilustración 22 – Cajeros de Criptomonedas -----	55
Ilustración 23 – Primer BTM de la historia -----	56
Ilustración 24 – Resumen de cómo comprar criptomonedas con un BTM -----	59
Ilustración 25 – Interfaz Gráfica de Silk Road-----	65
Ilustración 26 – Ross Ulbricht Fundador de Silk Road-----	67
Ilustración 27 – Ejemplo del Virus de la Policía -----	68
Ilustración 28 – Funcionamiento de un Hawala -----	70
Ilustración 29 – Proceso de ataque de Carbanak -----	72





# Lista de Acrónimos

BTM Bitcoin Teller Machine

VPN Virtual Private Network

KyC Know your Customer

MB MegaByte

NFT Non Fungible Token

ETF Exchange-Traded Funds







# 1. Introducción

En este primer apartado, se hará una presentación sobre la temática del trabajo, el planteamiento del caso en el cual se basa la parte experimental y los objetivos a lograr en este trabajo final de grado.

## 1.1 Presentación

La tecnología Blockchain ha llegado a nuestras vidas para establecerse como una innovación y modernización de ciertas metodologías poco seguras o fiables.

El Blockchain es sinónimo de seguridad, puesto que, gracias a su inviolabilidad, hace que muchas aplicaciones que requieren ciertas garantías hayan decidido emplear esta tecnología.

Una de estas aplicaciones son las criptomonedas, un activo muy establecido en nuestras vidas recientemente, pero, la gran mayoría del público que las posee o ha oído hablar de ellas desconoce su funcionamiento, su legalidad...

Es por esto por lo que, el presente Trabajo Fin de Grado tiene como objetivo aportar conocimientos una tecnología muy popular en nuestros días y que su popularidad no hará sino aumentar, a su vez de aportar sabiduría sobre una de sus aplicaciones, ya mencionada en estas líneas, las criptomonedas.

En adición a esto, y, para mejorar la comprensión y entender la situación de cualquier interesado o poseedor de estas divisas, se hará un análisis práctico de la tecnología, así como de la influencia de los poseedores de un gran número de estas.



## 1.2 Objetivos

Este Trabajo, el objetivo general que persigue es el de instruir al lector en esta tecnología y en sus diversas posibilidades, haciendo énfasis en las criptomonedas.

Los objetivos específicos que alcanzar son:

- Conocimiento de forma concisa y sencilla sobre lo que es y cómo funciona la tecnología Blockchain.
- Que el lector conozca las amplias posibilidades de esta tecnología.
- Poder realizar un análisis de un bloque de la cadena y comprender todos sus elementos.
- La fiabilidad y transparencia de la tecnología Blockchain.
- Conocimiento más exhaustivo de las criptomonedas y el impacto que la geopolítica tiene en su valor.
- Reflexionar sobre la influencia que posee el lector de este Trabajo, en caso de tener criptomonedas y lo que afectan agentes externos al valor de estas.
- Conocer las posibilidades de adquisición de criptomonedas y sirva de guía en su decisión de adquirirlas.
- La facilidad de cometer delitos de blanqueo con esta tecnología.





## 2. Blockchain

### 2.1 Concepto de Blockchain

Para comenzar, es importante conocer la tecnología de la que hablaremos a lo largo de este trabajo, por lo que debemos partir desde su concepto.

El blockchain o cadena de bloques es una tecnología de libro de contabilidad mayor distribuida en una red pública para los incluidos en ella, protegida criptográficamente hablando, lo cual, citando estos dos aspectos y otros que iremos citando a lo largo de este Trabajo de Fin de Grado, la hace inalterable e imposible de falsificar. En concreto, es inalterable gracias a su diseño en cadenas de bloques que, cada uno de estos, contiene información del bloque anterior y del bloque siguiente cuando se realice otra transacción.

En otras palabras, la tecnología blockchain configura una gran base de datos distribuida y segura (gracias a lo que hemos mencionado anteriormente) que se puede aplicar a todo tipo de transacciones, las cuales no tienen por qué ser necesariamente económicas.

Esta ha sido una definición a grandes rasgos de lo que es la tecnología blockchain, por lo que podemos concluir sobre este punto que es una tecnología compleja, pero que, gracias a su seguridad, garantiza una transacción entre 2 personas, empresas... en la que no sería necesario un intermediario. Esto se presenta como una diferencia fundamental a las transacciones monetarias cotidianas, en las cuales existe la presencia de un intermediario, comúnmente un banco.

### 2.2 Historia del Blockchain

Como dijo en su día el historiador del país galo Pierre Vilar: *‘hay que comprender el pasado para comprender el presente’*, lo que implica que, en lo que a este trabajo respecta, para entender el éxito en nuestros días de la tecnología blockchain, hay que realizar un viaje al pasado y retrotraernos a hace aproximadamente treinta años, que, aunque a priori no dista mucho del año en el que nos encontramos, la tecnología y la forma en la que el ser humano interactúa con ella sí que han cambiado significativamente y está cada vez más presente en nuestro día a día y lo estará en un futuro, queramos o no.

La andadura del blockchain comienza en 1991 y se pueden distinguir 4 fases claramente diferenciadas:



## **1. Etapa primigenia. (1991-2008).**

Esta primera etapa comienza con un trabajo realizado por los científicos Stuart Haber y W. Scott Stornetta en 1991, quienes emplearon un sistema de encriptación de sus archivos mediante cadenas de bloque. Dicho sistema es considerado el principal antecedente de esta tecnología, por lo que puede entenderse que ambos científicos son sus precursores. Su trabajo fue aplicado en su sistema de almacenamiento de documentos, el cual, actuaba como una solución computacionalmente práctica para sus documentos digitales, aplicando una especie de sello de tiempo para así evitar que estos no fueran manipulados ni alterados.

Tras este trabajo, lo mismos Stuart Haber y W. Scott Stornetta pulieron sus sistemas incluyendo árboles de Merkle, estructura de datos que comentaremos más adelante en este trabajo. Su incorporación les permitió almacenar la misma cantidad de documentos en menos bloques, es decir, se convirtió ya no solo en un sistema seguro de almacenamiento, sino que además se logró hacer más eficiente con esta mejora.

Sin embargo, esta tecnología, que fue patentada en su día por los creadores ya citados, no tuvo el éxito que esperaban. Por ello, en el año 2004, al finalizar su patente, caducó y no fue renovada.

Curiosamente, en el mismo año 2004, Harold Thomas Finney II, un programador estadounidense creó, mediante una técnica de la que hablaremos más adelante llamada RPoW (Reusable Proof Of Work) la que podemos denominar la primera criptomoneda.

## **2. Primera Etapa: Aparece Bitcoin. (2008-2013).**

A finales del año 2008, un artículo publicado por un tal Satoshi Nakamoto, del cual se desconoce su identidad e incluso se cree que pueden ser un conjunto de personas, nace la criptomoneda más popular y la que sigue siendo su reina, el Bitcoin.

Al contrario de lo que mucha gente suele pensar sobre la tecnología blockchain, como hemos podido analizar en el apartado anterior, no nace a la par que el



Bitcoin, sino que esta es una de las innumerables aplicaciones que ofrece esta tecnología.

Volviendo al paper que publicó Nakamoto, en él se describe con todo lujo de detalles la red bitcoin como un sistema electrónico peer-to-peer (punto a punto) en el cual, no existirían los grandes obstáculos que existen en las transacciones monetarias cotidianas, los bancos.

El 3 de enero de 2009, Nakamoto minó el primer bloque de bitcoin de la historia, por el cual recibió una cantidad de 50 bitcoins en total. De estas 50 criptomonedas que minó Nakamoto, 10 se utilizaron para realizar la primera transacción de bitcoin de la historia. En tal transacción, Nakamoto envió estas 10 bitcoin a Harold Thomas Finney II, que, como vimos anteriormente, fue el precursor de esta aplicación del blockchain.

Bitcoin fue ganando relevancia, a pesar de que todavía la tecnología del blockchain, y más concretamente su aplicación en el bitcoin, eran, un nicho tecnológico, el día 22 de mayo de 2010, el estadounidense Laszlo Hayneck pagó unas pizzas que costaban 30 dólares en bitcoin, que por aquel entonces equivalían a unos 10000 bitcoin. Esta curiosa compra supuso la primera que se hacía con bitcoin de la historia.

La fama mundial del bitcoin fue escalando hasta tal punto que, Vitalik Buterin, cofundó en el año 2012 la primera revista exitosa de bitcoin, la *Bitcoin Magazine*, cuyos primeros números hoy en día rondan los 1000 dólares.

### **3. Segunda Etapa: Aparece Ethereum y nuevas aplicaciones de la tecnología Blockchain. (2013-2015).**

En el año 2013 Vitalik Buterin, un programador ruso involucrado en el desarrollo de bitcoin que creía en el potencial de la tecnología blockchain y de la propia moneda, propuso expandirla mediante un lenguaje de scripting para crear aplicaciones descentralizadas. Esta propuesta no fue aceptada por el resto de la comunidad, por lo que Buterin, junto a otros desarrolladores, puso en marcha en 2014 un proyecto de creación de otra criptomoneda conocida como Ethereum.

Ethereum fue lanzada en el año 2015 con la diferencia fundamental con respecto al bitcoin de que permitía registrar otros activos, como slogans y contratos. De esta forma y gracias a la red Ethereum, surgieron los Smart contracts, una nueva aplicación para la tecnología blockchain que está llamada a reemplazar a los contratos tradicionales.



#### **4. Tercera Etapa: Aparecen aplicaciones y plataformas basadas en Blockchain. (2015-Actualidad).**

Finalmente, para culminar con la historia de esta tecnología y así poder llegar a la situación en la que nos encontramos actualmente, es necesario hablar en primer lugar de NEO. NEO se trata de una plataforma creada en 2014 en China de aplicaciones descentralizadas de blockchain y de IOTA, una tecnología creada para el registro de datos de código abierto y cuyo objetivo es permitir de forma segura el envío de información y datos en el Internet de las Cosas.

Sin embargo, no fue hasta el año 2015 hasta que tales aplicaciones comenzaron a popularizarse gracias a que grandes empresas tecnológicas, como Microsoft, empezaron a desarrollarlas de forma interna y basándose en emplear de forma privada la tecnología blockchain. Concretamente, fueron creadas para garantizar la privacidad y una muy alta seguridad en ciertos procesos internos que conllevan la realización de grandes transacciones económicas.

De esta etapa, y centrándonos en las transacciones seguras, nace en 2015 de mano de la Linux Foundation la plataforma Hyperledger. Esta plataforma se crea con la idea de ser un lugar común de desarrollo colaborativo centrado en la tecnología blockchain y sus posibles usos en el panorama empresarial y en el industrial. Hyperledger nacía para crear una tecnología que fuera capaz de ser útil en ámbitos como el de las finanzas, la banca, Internet de las Cosas y cadenas de suministros, entre otros. Pese a ello, la parte más importante de todas y en común con todas las iniciativas de la Fundación Linux, se desarrolló con el objetivo de crear un sitio de código abierto donde la creación de proyectos que se servían de esta tecnología estuviera disponible para todos. A esta propuesta, se fueron uniendo grandes empresas de diversos sectores, como J.P Morgan, IBM, Intel, VmWare, Accenture, SWIFT, Mitsubishi UFJ Financial Group y Cisco entre otras. Desde el 2018 impulsan grandes proyectos a nivel mundial, siendo ejemplos una aplicación empleada para la adopción de la tecnología blockchain en pequeñas y medianas empresas o, recientemente, una versión de Hyperledger, la cual está siendo empleada por el Tribunal de Cuentas de Brasil para monitorear el gasto público del país.





## 2.3 Funcionamiento del Blockchain

Llegados a este punto, y conociendo el trasfondo y la historia de la tecnología blockchain desde sus inicios hasta la situación actual, así como lo presente que está y estará de forma creciente en nuestras vidas, es indispensable conocer cómo funciona.

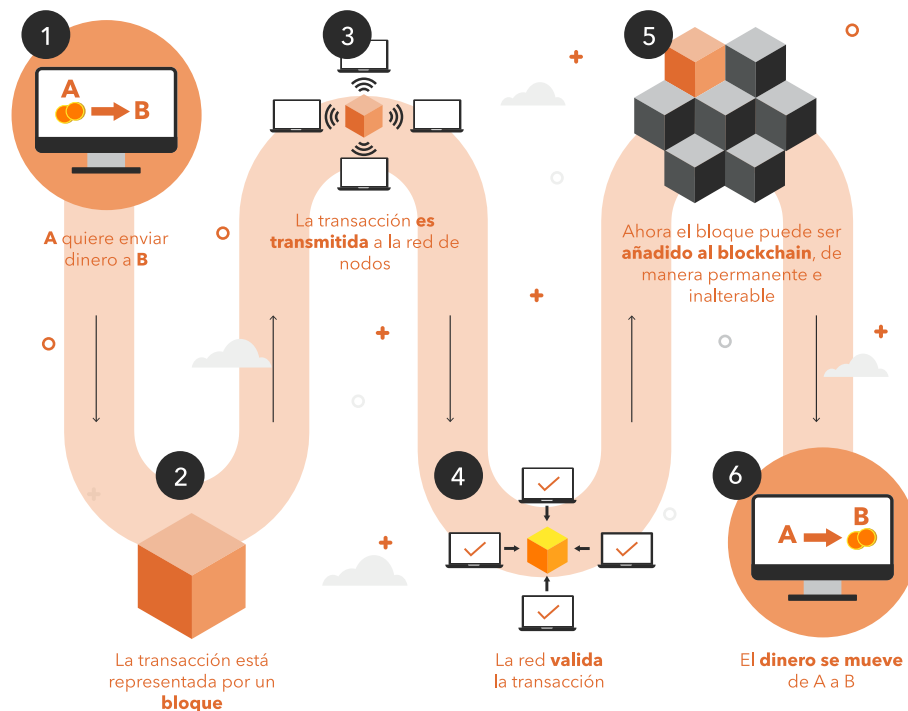
En primer lugar y de forma sencilla, podemos definir el funcionamiento de la tecnología blockchain como un registro público (salvo que se trate de una infraestructura blockchain privada) que almacena todas las transacciones que se realicen en una red, y por la que se van realizando copias de estas a través de sus nodos. Para garantizar la seguridad de las transacciones que se realizan, existen una serie de colaboradores que, comparándolo con algo más cotidiano, realizarían las funciones de los moderadores de un foro. Por lo que, sin la aprobación de estos, la transacción no sería válida, y, por tanto, no sería registrada en la red.

Una vez realizada esta explicación cuyo entendimiento es sencillo, vamos a realizar una exposición algo más compleja y técnica.

Blockchain permite a los usuarios de una red crear un registro o libro de contabilidad en el que no es necesaria la actuación de intermediarios (como la banca u otra entidad reguladora) para garantizar la seguridad e inmutabilidad de la red. Esta red está formada por bloques que se generan mediante las transacciones que se realizan en ella. Cada una de las transacciones equivale a un bloque que contiene toda la información de esta: usuario que realiza la transacción y quién la recibe, qué se envía y cuándo... Para que dicha transacción sea incluida en la cadena de bloques, debe previamente intervenir la figura del minero, el cual pertenece a la red y se encarga de verificar la transacción empleando la potencia de su ordenador. A cambio de verificarla correctamente, el minero es recompensado normalmente mediante criptomonedas y el bloque recibe su hash, elemento por el cual podemos garantizar la autenticidad de los datos de la transacción.

Una vez se valida la transacción, actúan los nodos. Estos no son más que ordenadores conectados a la red blockchain y cuya principal función será transmitir al resto de nodos una copia de la cadena de bloques de transacciones actualizada a tiempo real. De esta manera, se consigue garantizar lo ya citado anteriormente: seguridad y la imposibilidad de modificación por ninguno de los integrantes de la red.

A continuación, se muestra una ilustración que pretende resumir y clarificar todo lo explicado anteriormente en este punto de una forma gráfica y esquemática:



*Ilustración 1 – Funcionamiento del Blockchain*

En la ilustración anterior, podemos ver la tecnología blockchain en funcionamiento, esquematizada en 6 pasos claramente diferenciados:

1. El usuario A envía dinero a B.
2. La transacción que pretenden realizar se forma en un bloque que contendrá todos los detalles de esta.
3. La transacción es transmitida a los nodos de la red en busca de validación y verificación de esta.
4. La transacción, gracias a la colaboración de los mineros de la red, es validada.
5. El bloque que contiene la transacción, una vez ya ha sido validado, es incluido en la cadena de bloques (blockchain) y, por lo tanto, la transacción es registrada, pasa a ser inalterable por ninguno de los miembros de la red.
6. El usuario, tras haberse cumplido con éxito los pasos previos, la transacción es completada y el usuario B recibe el dinero del usuario A.



## 2.4 Elementos clave del Blockchain

En este punto, una vez hemos visto cómo funciona esta tecnología, lo siguiente será analizar cada uno de los elementos que intervienen en esta tecnología de una forma lo más estructurada y concisa posible. El objetivo de este punto es que el lector de estas líneas conozca lo necesario de todos los elementos clave que forman parte de la tecnología que llevamos tratando durante todo este trabajo, el blockchain. A continuación, procedemos a enumerar los elementos sobre los cuales se fundamenta toda esta tecnología.

### 1. Bloque.

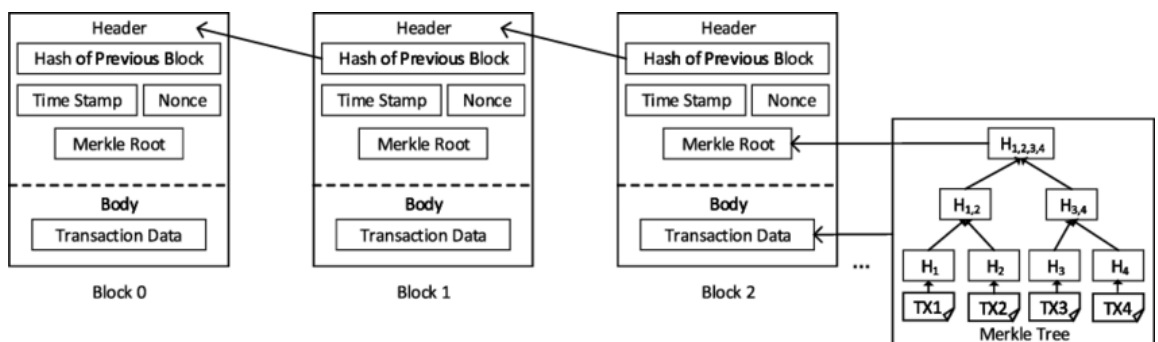
Es el pilar fundamental sobre el que se estructura toda la cadena de bloques. En él, se almacena la siguiente información:

- **Versión:** es el elemento que nos indica el nivel de desarrollo del software en el momento en que el bloque fue minado, para así facilitar la lectura del bloque y que se haga de la manera adecuada.
- **Hash del bloque anterior:** es una cadena de alfanuméricos, que en el caso del bitcoin es de 64 caracteres, que sirve para identificar el bloque que precede al actual.
- **Raíz de Merkle:** como explicaremos a continuación, todas las transacciones del bloque se unen en un solo hash resultante, que es la raíz.
- **Marca de tiempo:** indica, mediante un número, exactamente el momento en el que ha sido minado el bloque. Este número cuenta los segundos desde el 1 de enero de 1970 hasta el momento exacto en el que se ha minado este bloque.
- **Nonce:** viene de la frase “number that can be only used once”, es decir, el número que solo puede ser usado una vez. Es un número que está muy ligado al hash y, sobre todo, a la marca de tiempo, ya que unida a esta garantizamos que no haya repeticiones de este nonce y nuestro bloque sea falsificable o que se puedan repetir hashes anteriores. El cálculo del nonce es posible únicamente mediante la fuerza computacional, o, dicho en otras palabras, se requieren de altas cantidades de recursos de la máquina que se vaya a emplear y también tiempo para que esta obtenga el valor correcto, lo que conlleva que para lograr este número sea necesario lo que se conoce como prueba de trabajo o Proof of Work, concepto el cual trataremos más adelante.



- **Transacciones:** en esta parte se almacenan las transferencias realizadas, indicando quién la emite y quién será su receptor. Una vez han sido validadas en la red, se transmite por esta y se van agrupando de forma ordenada en el bloque. Todas y cada una de estas transacciones componen están englobadas por lo que se conoce como árbol de Merkel. En este árbol se van uniendo todas las transacciones presentes en el bloque, para generar un único hash, algo ya mencionado en este apartado con anterioridad, que es la raíz de Merkle o hash definitivo.
- **Tamaño de bloque:** como su propio nombre indica, es un elemento presente en el bloque, el cual, es un número en bytes para indicar el tamaño de este. En caso de ser un bloque de Bitcoin, este número ocupa 4 bytes.
- **Contador de transacciones:** este elemento, presente en todos los bloques de blockchain, representa mediante una cifra, la cantidad de operaciones que ha habido en el presente bloque.
- **Número mágico:** este número, es el identificador de la red de blockchain en la que nos encontremos. En el caso de la criptomoneda Bitcoin, su valor es el de 0xD9B4BEF9. Sirve para confirmar la veracidad de que el bloque que estamos inspeccionando se encuentra dentro de la red blockchain deseada.

A continuación, y a modo de reunir de forma lo más clara y concisa posible todo lo mencionado en estas líneas, veremos una imagen que resume a la perfección la estructura de tres bloques consecutivos de blockchain:



*Ilustración 2 - Estructura de 3 bloques del Blockchain*



Como se puede observar en la imagen, esta está representando 3 bloques consecutivos de una misma cadena de blockchain. Se pueden observar elementos ya citados con anterioridad, como el hash del bloque anterior, el nonce, la raíz de Merkle y la marca de tiempo. Aparte de estos elementos, encontramos la información de la transacción que, como se puede ver en la parte derecha de la ilustración, parte de esta es el árbol de Merkle, en el cual, todas las transacciones, en este caso son 4 (Tx1, Tx2, Tx3 y Tx4), se van agrupando y formando hashes, hasta llegar a la raíz, el cual es un único hash compuesto por los hashes de todas las transacciones del bloque.

Con respecto a la imagen anterior, cabe destacar que no todos los bloques de blockchain presentan la misma estructura, ya que el primer bloque de una cadena de blockchain no contiene, por ejemplo, el elemento que indica el hash del bloque anterior, puesto que no existe. Este primer bloque de la cadena es el conocido popularmente como bloque génesis. El bloque génesis es el bloque esencial para constituir la cadena de bloques que le seguirá. También es básico para garantizar la seguridad en una red ya que, si se intenta localizar el bloque génesis desde cualquier nodo de la red, en ambos nodos el resultado que obtenga deberá ser el mismo, ya que, si no, nos encontraríamos con una incongruencia no muy recomendable en caso de querer realizar transacciones en esa red, puesto que podría tratarse de una red fraudulenta o de escasa seguridad, porque ha sido modificada. En el caso del bitcoin su bloque génesis data del 3 de enero de 2009, como se ha mencionado anteriormente, el cual, a modo de curiosidad, contiene el titular de la portada del diario británico The Times, que en su día fue: “El Canciller (británico) está considerando un segundo programa de rescate a la banca”. Esto claramente es una reivindicación al sistema blockchain donde no se necesita la intervención de terceros de confianza, como sí ocurre en el sistema monetario internacional (bancos u organismos gubernamentales).

Tras conocer todo esto del bloque de blockchain, vamos a analizar el siguiente bloque elegido al azar de la página Blockchain.com:



### Bloque 740430

USD BTC

Este bloque se minó el día junio 12, 2022 a las 5:21 AM GMT +02:00 por [AntPool](#). En la actualidad tiene 622 confirmaciones en la cadena Bitcoin.

El minador/los minadores de este bloque ganaron una recompensa total de 6.25000000 BTC (131.855,75 US\$). La recompensa consistía en una recompensa base de 6.25000000 BTC (131.855,75 US\$) con una recompensa de 0.05999089 BTC (1265,62 US\$) pagada en calidad de 2625 transacciones que estaban incluidas en el bloque. Las recompensas Block, también llamadas recompensas Coinbase, se enviaron a esta [dirección](#).

Un total de 7,355.64416397 BTC (155.181.436,48 US\$) se enviaron en el bloque, siendo la transacción media 2.80215016 BTC (59.116,74 US\$). Aprende más sobre [cómo funcionan los bloques](#).

Hash	00000000000000000000071945c650e91006f898e09f33ccb2eebf917580bd5ed9
Confirmaciones	622
Sello de tiempo	2022-06-12 05:21
Altura	740430
Minador	<a href="#">AntPool</a>
Número de transacciones	2625
Complejidad	30.283.293.547.736,68
Raíz de merkle	ae010a3a16eb7ccece2a8d855aebcb9032f6c61e1310be428a2a2fed31434b2d
Versión	0x24f02000

Ilustración 3 - Bloque de Blockchain 1

Complejidad	30.283.293.547.736,68
Raíz de merkle	ae010a3a16eb7ccece2a8d855aebcb9032f6c61e1310be428a2a2fed31434b2d
Versión	0x24f02000
Bits	386.485.098
Peso	3.993.570 WU
Tamaño	1.665.399 bytes
Único	2.894.636.353
Volumen de transacciones	7355.64416397 BTC
Recompensa de bloque	6.25000000 BTC
Recompensa de tasa	0.05999089 BTC

### Transacciones de bloque

Comisión 0.00000000 BTC  
(0.000 sat/B - 0.000 sat/WU - 353 bytes)  
(0.000 sat/vByte - 326 virtual bytes)

6.30999089 BTC

Hash 4de63f0a8275a72f4ab3c9b9f9e272170db9421b1f5375ac4aa585087e23b...

2022-06-12 05:21

Ilustración 4 - Bloque de Blockchain 2

Lo primero que observamos, por orden de aparición en la web, es que es el bloque número 740430 de la cadena de Bitcoin. Este bloque, según lo que también podemos ver, contiene un total de 2625 transacciones por lo que, el árbol de Merkle mencionado anteriormente, tiene unas magnitudes bastante grandes.

Pasando a los elementos en sí, podemos ver su hash, el número de confirmaciones por usuarios de la propia red blockchain de Bitcoin, que en este caso son 622, lo cual, proporciona al usuario que quiere participar en esta red para realizar transacciones a otro usuario ciertas garantías. A continuación de este punto,




tenemos la marca de tiempo que, para hacerla más fácil al usuario que quiera consultar el bloque, indica la fecha en la que fue minado este bloque. En este caso, el 12 de junio de 2022. El siguiente elemento es la altura, que es lo mismo que el contador de transacciones citado anteriormente en este trabajo, es decir, indica la posición del bloque en toda la cadena de bloques, en este caso, de bitcoin.

Por otro lado, podemos observar el minador del bloque, un tal AntPool. Podemos acceder a su perfil en la misma página y vemos que es un usuario bastante activo en la red bitcoin con un total de 2368 transacciones:

**Dirección** USD BTC

Esta dirección ha realizado 2,368 transacciones en la cadena Bitcoin. Ha recibido un total de 14,447,598,167,56 BTC (308.237,195,29 US\$) y ha enviado un total de 14,306,286,294,23 BTC (305.222,329,08 US\$). El valor actual de esta dirección es 141.31187333 BTC (3.014.866,21 US\$).



Dirección	38XnPvu9PmonFU9WouPXUjYbW91wa5MerL
Formato	BASE58 (P2SH)
Transacciones	2368
Total recibido	14447.59816756 BTC
Total enviado	14306.28629423 BTC
Saldo final	141.31187333 BTC

**Transacciones**

Comisión	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 356 bytes) (0.000 sat/vByte - 329 virtual bytes)	+6.56695655 BTC 4 confirmaciones
Hash	57b46d2a7c90ca08d492a5b4ca62136a3a3cad1cd674e3d777863e0244a0c99	2022-06-16 19:04
COINBASE (Monedas Generadas Últimamente)	→ 38XnPvu9PmonFU9WouPXUjYbW91wa5MerL OP_RETURN OP_RETURN	6.56695655 0.00000000 0.00000000 BTC

*Ilustración 5 - Wallet de un minero*

Una vez hemos visto el usuario que minó la transacción, podemos ver las transacciones realizadas en el bloque, 2625 como hemos mencionado recientemente. Tras esto, tenemos la complejidad, un número el cual indica lo complejo que ha resultado para el minero encontrar una hash válida. Acto seguido, tenemos la raíz de Merkle ya explicada anteriormente y que no entraremos en más detalles. Seguidamente, tenemos la versión, ya definida y explicada con anterioridad y para finalizar, una serie de valores como son los bits del bloque, el peso de cada transacción en comparación al tamaño total del bloque, el tamaño total del bloque que hemos elegido, en este caso unos 1,5 Mb aproximadamente, también hay un valor llamado único que sirve para indicar el proof of work, del cual hablaremos más adelante. El antepenúltimo elemento que podemos observar en la información que nos aporta el bloque es el del volumen de transacciones, que indica, en este caso, la cantidad de bitcoin total que se ha transferido en este bloque (7355 btc). Tras este, encontramos la recompensa de bloque, que es, como su propio nombre indica, la cantidad en bitcoin que ha percibido el minero por calcular el hash y por último, encontramos unas tasas que también recibirá el minero por el mismo motivo que el anterior.



Una vez visto todos los elementos que nos indica este bloque, también podemos consultar todas las transacciones que se han hecho en este y así verificar la seguridad y fiabilidad de este tipo de transacciones.

Por ejemplo, la última transacción que aparece en este bloque podemos consultarla:

**Resumen** USD BTC

Comisión: 0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 353 bytes) (0.000 sat/vByte - 326 virtual bytes) 6.30999089 BTC

Hash: 4de63f0a8275a72f4ab3c9b9f9e272170db9421b1f5375ac4aa585087e23b04a 2022-06-12 05:21

COINBASE (Monedas Generadas Últimamente) → 38XnPvu9PmonFU9WouPXUjYbW91wa5MerL 6.30999089 BTC

OP\_RETURN: 0.00000000 BTC  
OP\_RETURN: 0.00000000 BTC  
OP\_RETURN: 0.00000000 BTC

Esta transacción se transmitió a la red Bitcoin el día junio 12, 2022 a las 5:21 AM GMT +02:00. La transacción tiene actualmente 882 confirmaciones en la red. En el momento de esta transacción, 6.30999089 BTC se envió con un valor de \$173,385.20. El valor actual de esta transacción ahora es de 119.567,58 US\$. Aprenda más sobre [cómo funcionan las transacciones](#).

**Detalles**

Hash: 4de63f0a8275a72f4ab3c9b9f9e272170db9421b1f5375ac4aa585087e23b04a

Estado: Confirmado

Tiempo recibido: 2022-06-12 05:21

Tamaño: 353 bytes

Peso: 1304 ₿

Incluido en el bloque: 740430

Peso: 1304

Incluido en el bloque: 740430

Confirmaciones: 882

Entradas totales: 0.00000000 BTC

Gastos totales: 6.30999089 BTC

Tarifa: 0.00000000 BTC

Tasa por byte: 0.000 sat/B

Tarifa por vbyte: 0.000 sat/vByte

Tasa por unidad de peso: 0.000 sat/WU

Valor cuando se transacciona: 173.385,20 US\$ ₿

### Ilustración 6 - Ejemplo de transacción de un bloque

Podemos observar que pertenece al mismo bloque, el 74030, el número de confirmaciones por usuarios que forman parte de la red, que asciende a 882 usuarios, la cantidad de bitcoin que se han enviado, que son 6.30999089 BTC. Otros valores que consideramos reseñables son el del tiempo recibido, que indica la fecha exacta en la que esta transacción se transmitió por la red blockchain de bitcoin, el tamaño, que no es otra cosa que el valor en bytes que ocupa esta transacción, 353 bytes, su hash, diferente al hash del bloque en su conjunto, que, como hemos visto ya con anterioridad, es correcto que sea así y por último el estado, que nos indica que esta transacción ha sido realizada con éxito y que el receptor recibió su dinero.





Una vez vista una de las transacciones que posee un bloque de blockchain, hemos finalizado la explicación y las características del que es el elemento clave de todo el blockchain, el bloque. Hemos visto por lo que este está formado, desde un punto de vista teórico, y acto seguido, hemos comprobado cómo es un bloque de forma práctica mediante un ejemplo real.

## 2.5 Aplicaciones de la tecnología blockchain

Estudiada toda la parte teórica necesaria para conocer el funcionamiento de las cadenas de bloques, es imprescindible conocer también algunos ejemplos sobre los que se aplica esta tecnología a fecha de realización de este Trabajo Fin de Grado. Estas aplicaciones se usan en diferentes campos:

- **Criptomonedas:** Una de las principales y, sin duda alguna, la aplicación más famosa de esta tecnología son las criptomonedas, siendo sus principales valedores bitcoin y Ethereum. A pesar de ser la aplicación más conocida, apenas explotan todo el potencial de esta tecnología, aunque, gracias a estas, la tecnología blockchain ha ido desarrollándose para tener más aplicaciones, que se citarán más adelante en este apartado.

Las criptodivisas han ido ganando repercusión desde su creación, desde ser un activo con un uso ínfimo hasta, a día de hoy, ser un activo muy importante en la economía global. Esto se traduce en que son métodos de pago legales en muchos países a lo largo del globo e incluso se han convertido en moneda oficial en algún que otro país. Toda esta información será tratada más adelante en el presente Trabajo Fin de Grado.

- **Logística:** El blockchain en el campo de la logística está suponiendo una gran mejora a la hora de reducir la cantidad de documentación en la cadena de



suministro y aportando a esta una mejor trazabilidad, seguridad y confianza en todos lados de la cadena.

Un claro ejemplo de estas mejoras la ha experimentado la cadena de supermercados Carrefour, implementando la tecnología blockchain en algunos de sus alimentos. Esta implantación supone para el cliente la facilidad de realizar un seguimiento de las fases de la cadena de suministro que ha realizado su producto y le garantiza el origen de estos.

- Comicios y juntas de accionistas: Esta tecnología ha resultado ser muy eficaz de igual forma en sistemas de votación. Prueba de ello ha sido que, en juntas de accionistas del grupo Santander, a la hora de someter a votación cualquier consulta en la reunión, el voto se haría empleando esta tecnología para evitar errores en los resultados. Esto es evitable gracias a la robustez que proporciona la cadena de bloques a ser modificada.

Por otro lado, el pasado 2021, en las elecciones al parlamento catalán, se probó con 1.000 ciudadanos el voto digital empleando tecnología blockchain. La implantación de este método garantiza combatir el fraude electoral, puesto que, la capacidad computacional necesaria para modificar la cadena es muy elevada y, hasta cierto punto, prácticamente inalcanzable con los ordenadores actuales.

- Historiales médicos y de vacunación: Otra aplicación a esta tecnología tiene que ver con el campo de la medicina y, en concreto, con historiales médicos y de vacunación. Desde empresas como IBM o Transcripts, han desarrollado software basado en la blockchain para crear historiales médicos de pacientes en diferentes clínicas y que estos preserven siempre su integridad y no puedan ser modificados, a excepción del personal sanitario autorizado para ello.

Esta aplicación ha servido a organizaciones como Médicos sin Fronteras a crear historiales médicos de niños en países como la India o Bangladesh, en los que el historial médico de la mayoría de ellos no estaba digitalizado o bien no era del todo correcto. Gracias a esta aplicación, se prevé evitar la muerte de cerca de 7.000 niños de forma anual en estos países, ya que tendrán un historial médico más preciso y seguro.

Por otro lado, este software es empleado también por muchos países, por recomendación de la OMS, para los certificados de vacunación contra el COVID-19. Estos certificados, gracias a esta tecnología y su fácil trazabilidad permiten conocer, con total seguridad, si una persona está o no vacunada, ya que, en caso de ser alterados, la detección sería inmediata.



- **Cripto-arte:** El cripto-arte es una de las más recientes y polémicas aplicaciones surgida de esta tecnología. Son también conocidos como NFT (Non Fungible Token) y su principal función es dar fe de que una obra de arte digital, una imagen, un vídeo o cualquier archivo multimedia, es de tu propiedad. Este tipo de aplicaciones existen gracias a las criptomonedas, y más en concreto al Ethereum.

El principal beneficio de estos NFT es que, a diferencia de las obras de arte convencionales donde el autor de la obra sólo obtenía beneficios de la primera venta, con el cripto-arte, el autor recibe una comisión por cada propietario distinto que tenga. Por otro lado, de cara al comprador de estos NFT, este se garantiza mediante un certificado el cual, no puede ser falseado, que posee la obra original del artista.

Por otro lado, una desventaja de esta tecnología, y lo que la convierte, en cierto modo polémica, es que no elimina la especulación que hay detrás del arte tradicional y muchos personajes famosos han obtenido rédito gracias a la especulación con estos tokens.

- **Registro de la propiedad:** Por último, una de las más interesantes aplicaciones de esta tecnología está relacionada con el registro de la propiedad. Esta tecnología ha logrado ya en países como Japón, Reino Unido, Suecia o Emiratos Árabes Unidos un registro de la propiedad seguro y con total transparencia, ya que, como con las anteriores aplicaciones ya mencionadas, cualquier modificación que se produzca en la cadena de bloques es detectada al instante.

En España, el Colegio de Registradores de la propiedad, ya está viendo la manera de implantar esta tecnología, siguiendo los modelos de los países previamente mencionados. Esta tecnología lograría, gracias a su fiabilidad, agilizar muchos trámites en la compraventa de inmuebles, porque se necesitarían menos verificaciones y, por tanto, requeriría menos tiempo cualquier registro de este tipo.

Estos han sido algunos de los ejemplos más reseñables que se pueden hacer mediante el empleo de esta tecnología, pero el arco de posibilidades es infinito. Se cree que el uso de esta tecnología no va a hacer sino aumentar con el paso del tiempo, debido a las garantías de seguridad que ofrece por imposibilidad de ser falseada, como se ha ido viendo en todos y cada uno de ellos ejemplos, y por la seguridad y fiabilidad que facilita a todas las partes implicadas.



## 3. Criptomonedas

### 3.1 Concepto de Criptomonedas y Ejemplos

Una vez examinado el funcionamiento de la tecnología blockchain, sus elementos clave, su historia, el concepto de esta y algunas de sus posibles aplicaciones, haremos énfasis en una de estas últimas en el presente Trabajo Fin de Grado, las criptomonedas.

Para comenzar, una criptomoneda no es más que es un activo intangible, es decir, digital, que, mediante la tecnología blockchain, es cifrado de forma que en la cadena figura su propietario. Este cifrado es imposible modificarlo y gracias a esto, es posible probar la garantía de operar con estos activos y controlar todas las unidades existentes en el mercado. Esto último, evita que terceros falsifiquen estas divisas, ya que serían automáticamente detectadas y nunca podrían entrar en circulación. El poseedor de estos activos los almacena en a wallet o cartera digital.

Algunos ejemplos de criptomonedas conocidas por entusiastas de estas son:

- Bitcoin: fue la primera criptomoneda creada en 2008 por Satoshi Nakamoto, una persona o grupo de personas anónimos. Es la criptomoneda de mayor valor en el mercado, a fecha de realización de este Trabajo Fin de Grado y es la criptodivisa más conocida mundialmente. La red de blockchain de bitcoin y su seguridad fueron, son y serán sus dos mayores pilares, junto con ser la pionera en esta aplicación, frente al resto de criptomonedas.
- Ethereum: la segunda criptomoneda más usada y conocida del mundo. Como se ha mencionado previamente en este Trabajo, pertenece a la segunda generación de criptomonedas, lo que hace de Ethereum algo más que una criptodivisa. Esto es gracias a su versatilidad, gracias a que su red, a diferencia de la de bitcoin, es programable. A pesar de ser más versátil, realizar transacciones en su red es cada vez más difícil y, por consiguiente, más costoso. Esto está provocando que esté en desarrollo Ethereum 2.0 para reducir costes y ser más transformable.
- Dogecoin: la tercera y última criptomoneda que será mencionada a modo de ejemplo surgió en forma de protesta al resto de las criptomonedas. Billy Markus, su creador, en 2014 inventó esta moneda a modo de protesta por el uso delictivo que se le daba a las criptomonedas empleando una imagen de un perro muy conocido mundialmente en redes sociales. Es una moneda muy sencilla de minar y adquirió popularidad gracias a que personas muy influyentes hablaron de ella



elevaron su precio más de un 200% en cuestión de días y a fecha de redacción del presente Trabajo, es una de las criptomonedas más populares y baratas de adquirir.

### 3.2 Cómo obtener Criptomonedas

Una vez se ha observado qué son las criptomonedas y tres de las más populares, a fecha de redacción del presente Trabajo Fin de Grado, el siguiente paso es conocer cómo se pueden adquirir. Las formas de adquirir cualquier criptomoneda son las siguientes:

- **Mediante un Exchange:** Esta forma es la más cómoda para cualquier tipo de persona interesada en adquirir criptomonedas de hacerse con ellas. Un exchange no es más que una plataforma donde cualquier persona, verificando previamente su identidad, puede comprar y vender criptomonedas. Son la alternativa más cómoda para el usuario y es la más usada, ya que, se realiza a través de internet y sin necesidad de poseer un ordenador con especificaciones técnicas muy altas e incluso, algunas de estas empresas permiten realizar estas mismas transacciones desde su propia aplicación de dispositivo móvil.
- **Minería de dicha criptomoneda:** En la explicación de cómo funciona la blockchain, fue introducido el concepto de minero. Este es un individuo que, aprovechando la alta potencia computacional de su ordenador o conjunto de ordenadores en muchos casos, resuelve el un complejo acertijo matemático que únicamente puede ser resuelto por un ordenador. Este problema sirve para aprobar una transacción realizada entre dos personas. El primero que resuelve el problema, se lleva una recompensa, normalmente en forma de la criptomoneda en la que se están realizando las transacciones. Este es el método más complejo de obtener criptomonedas, ya que el minero suele precisar de un ordenador de muy alta gama para realizar estas operaciones. Además de esto, para la minería de bitcoin, puede ser necesaria hasta una gran infraestructura de ordenadores, con el debido consumo eléctrico que esto necesita. Por lo que, con todo lo mencionado, no es un método de hacerse con criptomonedas destinado a cualquier persona promedio que quiere comprar criptomonedas, ya que el costo de optar a ellas es muy elevado y, en el caso de querer minar criptomonedas en España, poco rentable.
- **En un cajero de criptomonedas:** Este último método es el más sencillo para adquirir criptomonedas. Esto es así gracias a que el funcionamiento de los cajeros de criptomonedas se utiliza de forma muy similar a los cajeros automáticos que usamos a diario. El sistema para obtener cualquier criptomoneda es tan sencillo como que el usuario las adquiera criptomonedas insertando efectivo o pagando con su tarjeta bancaria en dicho cajero. Más adelante, en este Trabajo Fin de



Grado, se comentará en profundidad este método de obtener criptomonedas y la legalidad de estos cajeros en España.

## 3.3 Legalidad de las criptomonedas en España y el resto del mundo

### 3.3.1 Introducción

Tras haber revisado el concepto de qué es una criptomoneda, lo íntimamente ligadas a la tecnología en torno a la que gira el presente Trabajo Fin de Grado, el blockchain, que están, enunciados algunos ejemplos de criptomonedas y cómo obtenerlas, es imprescindible conocer la legalidad para realizar operaciones con ellas, minarlas e incluso sobre su posesión como patrimonio.

En los siguientes apartados, se hablará de la legalidad de estas criptomonedas en España y otros países como Estados Unidos, China, El Salvador y ...

Cabe destacar que, la normativa que se aplica en cada uno de los países que se expondrán a continuación, es a fecha de mediados del año 2022, por lo que, es menester señalar que a fecha de que usted como lector esté leyendo estas líneas, esta normativa se haya visto modificada en todos o alguno de los países ya mencionados.

Esto es debido a que, al tratarse de una tecnología emergente, como es la tecnología blockchain, y siendo su aplicación en las criptomonedas un activo que ha ido ganando popularidad con el paso de los años a nivel mundial, la legislación que existe en el mundo sobre esta es, en la mayoría de los casos, testimonial y en otros casos existen ciertas normativas aprobadas en el último lustro, por lo que es de esperar, que, con el paso de los años, exista una normativa a nivel mundial mucho más clara y precisa, ya que las criptomonedas son divisas en las que cada vez más gente poseerá altas cantidades de su patrimonio depositadas y puede llegar a ser un método de pago más en cada vez más comercios y naciones.

Una vez citadas las anteriores premisas, se expondrá, con el mayor lujo de detalles y claridad posible, la normativa en los países previamente mencionados.



### 3.3.2 Legalidad de las criptomonedas en España

El primer país para estudiar es España, país donde se encuentra la universidad en la que se ha realizado este Trabajo Fin de Grado.

Para responder a la pregunta básica de *¿son las criptomonedas legales en España?* La respuesta es SÍ. Las criptodivisas son totalmente legales en España y está permitido operar con ellas en los diferentes exchanges que hay disponibles en la red de Internet para operar con estos, siempre y cuando estés identificado en esta red y no estés siendo forzado por un tercero a realizar operaciones. En cualquiera de los dos casos mencionados, es ilegal operar con criptomonedas, ya que se podría incurrir en diversos delitos como la extorsión, financiación del terrorismo o la ley existente contra el fraude o blanqueo de capitales.

Conocida la legalidad para la posesión y realización de operaciones en exchanges, las siguientes preguntas a formular, que están íntimamente relacionadas son, *¿son consideradas las criptomonedas dinero en nuestro país? ¿puede un negocio aceptar el pago de sus clientes en forma de criptodivisas?* La respuesta a la primera pregunta sería un NO rotundo. Esto es debido a que el estado español considera a las criptomonedas un bien, en lugar de dinero ya que, a fecha de redacción de este Trabajo Fin de Grado, la Unión Europea y España en particular no incluyen a las criptodivisas en sus sistemas monetarios, como indica en España el artículo 3.1 de la Ley 46/1998, del 17 de diciembre, sobre introducción del euro. En adición a esto, las criptomonedas son consideradas un bien puesto que pueden ser compradas, vendidas o permutadas. Una permutación según el Código Civil en su artículo 1.538 (*“La permuta es un contrato por el cual cada uno de los contratantes se obliga a dar una cosa para recibir otra.”*). Esta definición es útil para resolver la segunda pregunta, a la que su respuesta es SÍ, un negocio puede aceptar el pago en criptodivisas si computa todas las operaciones que se realicen mediante este método con una permuta comercial, es decir, que a pesar de ser un intercambio de bienes, el responsable del negocio deberá emitir la factura empleando la conversión de euros a la criptomoneda deseada, incluyendo el correspondiente IVA, ya que las criptomonedas, como previamente se ha mencionado, no es una moneda de curso legal.

La siguiente cuestión que plantear es, *¿es legal en España la minería de criptomonedas?* La respuesta directa sería SÍ, ya que a fecha de redacción de este trabajo no existe legislación alguna sobre esta actividad y, por tanto, es legal hasta que se indique lo contrario. Aunque no hay legislación sobre la minería de criptodivisa en España, sí que la hay sobre las actividades económicas que se realicen en el territorio. Esto se traduce en que, si una persona quiere dedicarse a la minería, deberá declararlo a Hacienda, y, si obtiene un mínimo de ganancias debería darse de alta como autónomo y declarar sus ganancias ante la Agencia Tributaria y tributar los beneficios que haya obtenido como rendimientos de actividades económicas a efectos de IRPF.

Por último y, para terminar con este apartado, y conociendo todo lo relativo a la legalidad de las criptomonedas en España, es necesario formular la última cuestión, *¿es necesario*



*declarar nuestras criptomonedas a la Hacienda española?* La respuesta a esta última pregunta es SÍ. Es obligatorio declarar nuestras criptomonedas si, como mínimo, nuestros ingresos a través de estas, ya sea en forma de intereses, dividendos y ganancias alcanzadas son superiores a los 1.000 euros.

A partir de esa cifra, los tipos impositivos que se aplican funciona por tramos y son los siguientes:

- Desde los 1.000€ hasta los 6000€: es un tipo impositivo del 19%.
- De 6.000€ a los 50.000€: el tipo impositivo es del 21%.
- Entre 50.000€ y 200.000€: corresponde un tipo impositivo del 23%.
- Cifras superiores a los 200.000€ les corresponde un tipo impositivo del 26%.

En caso de poseer el patrimonio mínimo en criptodivisas y no declararlo, el usuario poseedor podría ser multado con sanciones económicas de hasta el 150% de la cuota del IRPF.

Por otro lado, el poseedor de criptomonedas que realice transacciones con países fuera de la Unión Europea también está obligado a incluirlas en su declaración si de ellas ha obtenido un beneficio.





### 3.3.3 Legalidad de las criptomonedas en Estados Unidos

El segundo país que será caso de estudio son los Estados Unidos de América. A diferencia del país estudiado en el punto anterior, Estados Unidos es un estado federal, lo que implica que lo que en algún estado es legal, en otro puede no serlo. Por suerte, como se verá a continuación, la mayoría de sus estados dan completa libertad al ciudadano a operar con criptomonedas. Cabe reseñar que, a pesar de ser legales, no es debido a que expresamente lo sean sino porque apenas existe legislación, pese a que las criptomonedas llevan existiendo más de una década.

El método de estudio será similar al anterior, por lo que, la primera pregunta a formular es, *¿son las criptomonedas legales en Estados Unidos?* La respuesta es un SÍ rotundo a fecha en la que se está redactando este Trabajo Fin de Grado, pero cabe destacar que las criptomonedas son legales en estados como Hawaii desde el 2018, ya que previamente estaban prohibidas. Continuando con el estado de Hawaii, es importante conocer que, cualquier ciudadano residente en el estado, debe poseer una licencia de transmisor de dinero, si desea operar con ellas. En cambio, hay otros estados como Wyoming que han optado por una actitud diametralmente opuesta a la de Hawaii, y es que, han aprobado una amplia cantidad de leyes para favorecer el comercio en su estado con criptomonedas. Tanto es así, que reciben el mismo estatus que el dinero tradicional y, por consiguiente, cualquier ciudadano residente en ese estado puede tener sus criptodivisas en el banco. Otro estado muy favorable para operar con criptomonedas es California, ya que a fecha de 2022 no se ha legislado nada sobre el dinero virtual y es por ello por lo que la mayoría de exchangers poseen su residencia fiscal en el estado californiano.

En definitiva, las criptomonedas son totalmente legales en los Estados Unidos, y ningún ciudadano incumple la ley en caso de estar en posesión de ellas.

Siguiendo la estructura del punto anterior, la pregunta que se plantea es, *¿son consideradas las criptomonedas dinero en los Estados Unidos? ¿puede un negocio aceptar el pago de sus clientes en forma de criptodivisas?* La respuesta a la primera pregunta planteada es NO. Esto se debe a que, como en ocurre en España, las criptomonedas no son consideradas dinero, sino un bien, como lo puede ser el petróleo o el oro. En cambio, la respuesta a la segunda pregunta es SÍ, se puede aceptar el pago mediante criptomonedas, siempre y cuando, el establecimiento posea una licencia de transmisor de dinero. A su vez, estados como Wyoming o Colorado eximen a los negocios de esta licencia para operar y dependerá de ellos si aceptan o no las criptomonedas como método de pago. Cabe reseñar que, recientemente, algunos bancos estadounidenses permiten a sus clientes el pago de impuestos mediante Bitcoin hasta una cantidad máxima de 10.000 dólares.

Para concluir con la legalidad de las criptomonedas en Estados Unidos, la última pregunta a realizar es, *¿es legal en Estados Unidos la minería de criptomonedas?* En este caso, la respuesta es SÍ en cualquier estado. El único problema es que, debido a la caída del valor de las criptomonedas en este 2022, la minería ha dejado de ser rentable para mineros que



poseían su infraestructura de minado en Estados Unidos, debido a la relación ingreso por minado/costo de la electricidad.

### 3.3.4 Legalidad de las criptomonedas en China

El tercer país que analizar acerca de la legalidad de las criptomonedas en su territorio no es otro que el gigante asiático: China. A diferencia de los países analizados previamente, China es un país ciertamente “cerrado” en cuanto a la obtención de información se refiere y, por consiguiente, resulta complicado obtener cierta información que el gobierno chino no desea que obtengas. Lo que implica todo esto al presente Trabajo Fin de Grado no es baladí, ya que es complicado predecir las acciones futuras que se tomarán con las criptomonedas en China y todo está basado en la rumorología, por lo que, en este Trabajo, todo el contenido reflejado son certezas.

Una vez expuestas las anteriores premisas, la primera pregunta a formular es la misma que la realizada en los anteriores dos puntos, *¿son las criptomonedas legales en China?* Desde el año 2021, la respuesta es un rotundo NO. Es totalmente ilegal el uso de cualquier tipo de criptomoneda o token relacionado con la tecnología blockchain. La negativa al uso de estas es según las autoridades chinas, *“intento por ejercer un mayor control sobre la economía, lograr un crecimiento más sostenible, inclusivo e igualitario”*. Para endurecer más esta medida, cualquier persona residente en China que posea u opere con criptomonedas estando en el país, podría incurrir en multas desde los 100.000 yuanes (unos 14.000 euros) hasta los 485.000 yuanes (unos 70.500 euros al cambio) e incluso penas de prisión hasta un máximo de 10 años.

A pesar de todo esto, y, para facilitar una mayor amplitud de vista al lector de estas líneas, es conveniente formular las mismas preguntas formuladas para comparar a la perfección la legalidad de las criptodivisas en diferentes partes del mundo. Por lo que, las siguientes cuestiones son, *¿son consideradas las criptomonedas dinero en China? ¿puede un negocio aceptar el pago de sus clientes en forma de criptodivisas?* Claramente, según lo explicado en el anterior párrafo la respuesta es NO. Desde el año 2013, China comenzó a legislar contra el uso de las criptomonedas, siendo ese mismo año cuando fueron prohibidas en bancos para comercializar con ellas. Se ha continuado legislando contra ellas, como cuando en el año 2017, China prohibió el aceptar el pago con criptomonedas en cualquier establecimiento, para tener así un mayor control sobre la economía nacional y evitar el fraude y blanqueo de capitales. Esto es porque el estado chino considera que, las criptomonedas, al no pertenecer ni estar controladas por ninguna institución gubernamental internacional, no pueden ser consideradas dinero. En definitiva, por todo lo mencionado en este párrafo, la respuesta a la segunda pregunta de este párrafo es NO.

Para finalizar este apartado en el que se ha tratado la legalidad de las criptodivisas en China, la última cuestión pendiente es, *¿es legal en China la minería de criptomonedas?* La respuesta a esta pregunta también es NO. Es ilegal la minería en el país chino desde el



año 2022, puesto que suponía un excesivo consumo de energía y producía apagones a las personas residentes en las proximidades de donde se realizaba esta actividad.

Para concluir con este apartado, es reseñable que, a pesar de estar prohibidas todas las criptomonedas, desde este año 2022, fecha de la celebración en China de los Juegos Olímpicos de Invierno, se lanzó al mercado chino el e-Yuan, una moneda digital basada en la criptografía, es decir, una criptomoneda, promovida por el gobierno chino. Esto justifica todo lo mencionado en los párrafos anteriores de este apartado en cuestión a la prohibición del resto de criptomonedas existentes, ya que así, el gobierno central chino posee el control de todas las criptomonedas en circulación en su país.

### 3.3.5 Legalidad de las criptomonedas en El Salvador

Para concluir con este punto, será objeto de análisis el país latinoamericano El Salvador, ya que presenta algunas peculiaridades que se expondrán a continuación con respecto a los demás países ejemplificados en este Trabajo Fin de Grado.

Sin mayor detenimiento, la primera pregunta a realizar, siguiendo la estructura realizada en los diferentes países estudiados en este punto es, *¿son las criptomonedas legales en El Salvador?* La clara respuesta en este caso es SÍ. Es totalmente legal el uso de criptomonedas en El Salvador, tanto poseerlas como realizar cualquier tipo de intercambio con exchanges o particulares.

Lo que hace peculiar a este país frente al resto de los países estudiados en el presente Trabajo Fin de Grado, son las dos preguntas siguientes, *¿son consideradas las criptomonedas dinero en El Salvador? ¿puede un negocio aceptar el pago de sus clientes en forma de criptodivisas?* La respuesta a la primera pregunta es SÍ, es uno de los pocos países a nivel mundial que aceptan alguna criptomoneda como moneda de curso legal en su territorio. En ambos casos, la criptomoneda que es considerada moneda oficial del país es el bitcoin. El Salvador, junto con la República Centrafricana, han adoptado esta moneda como oficial. En el caso del país salvadoreño, el bitcoin es un método de pago legal, junto con el dólar estadounidense y el colón salvadoreño, esta última en desuso, desde el pasado año 2021. Por otro lado, y como es evidente, la respuesta a la segunda pregunta planteada en este párrafo es también un SÍ. Lo único que cabe reseñar sobre esta segunda pregunta es que todos los empresarios deberán aceptar el bitcoin como método



de pago, salvo en casos aislados en los que, por falta de medios tecnológicos, no le sea posible acceder a estas tecnologías. Sobre esto último, es importante destacar que cerca de un 50% de la población salvadoreña tiene acceso regular a internet, por lo que, empresarios en esta situación, como es lógico, no tienen obligación de aceptar bitcoin como método de pago, si bien es cierto, que el gobierno de El Salvador está tomando medidas para que el acceso a la red de internet llegue a más ciudadanos.

Finalmente, la última pregunta que se ha planteado en todos los países estudiados es, *¿es legal en El Salvador la minería de criptomonedas?* Pregunta a la que, en este caso, es un SÍ. Aunque, por lo comentado en el párrafo anterior, no todos los ciudadanos salvadoreños tienen acceso a una conexión a internet, por lo que, no es una práctica muy habitual en el país, a pesar de que el bitcoin es moneda oficial y estar totalmente permitida por las autoridades de El Salvador.

### 3.3.6 Cuadro resumen sobre los ejemplos expuestos

Una vez expuestos los diferentes casos de legalidad de las criptomonedas en países como España, Estados Unidos, China y El Salvador. A continuación, se muestra una tabla a modo de resumen de la legalidad en estos países:

<b>PAÍS</b>	<b>¿Es legal tener criptomonedas y operar con ellas?</b>	<b>¿Son consideradas dinero?</b>	<b>¿Puedo pagar en un negocio con ellas?</b>	<b>¿Es legal la minería de criptodivisas?</b>
España	SÍ	NO	SÍ, si se considera una permuta comercial	SÍ
Estados Unidos	SÍ	NO	SÍ, con licencia en algunos estados	SÍ
China	NO, salvo que sea e-Yen	NO, salvo que sea e-Yen	NO, salvo que sea e-Yen	NO
El Salvador	SÍ	SÍ	SÍ	SÍ

*Ilustración 7 - Resumen de los casos expuestos*



## 3.4 Caso práctico: las ballenas del bitcoin y seguimiento de estas

### 3.4.1 Introducción

Para comenzar el caso práctico de estudio, es imprescindible conocer qué son las famosas ballenas del bitcoin. Este término es designado por la cantidad de criptomonedas que posee el usuario o grupo de usuarios que poseen una billetera de bitcoin con una cantidad elevada de este. En este caso práctico, el objetivo es estudiar el comportamiento de estos usuarios, las ballenas y las ballenas jorobadas, que controlan un grueso del bitcoin que hay disponible a fecha de realización de este Trabajo Fin de Grado, ver las transacciones que realizan y el impacto que estas tienen en el valor de la criptomoneda y en la criptomoneda en sí.

Una vez realizado este estudio exhaustivo sobre las principales billeteras de bitcoin, se sacarán una serie de conclusiones sobre ello.

Aunque sólo han sido citadas las ballenas, es necesario conocer la demás “fauna” poseedora de criptomonedas y por qué se caracterizan. La siguiente lista irá ordenada de menor a menos posesión de bitcoin:

- **Camarones:** son aquellos usuarios que se encuentran en posesión de menos de 1 bitcoin.
- **Cangrejos:** aquellas personas que poseen bitcoin en un rango de entre 1 a 10 unidades.
- **Pulpos:** usuarios poseedores de bitcoin desde 10 a 50 unidades.
- **Pescado:** son individuos que poseen desde 50 hasta 100 bitcoin.
- **Delfines:** son aquellos usuarios que ostentan una cantidad de bitcoin que oscila entre los 100 y 500 bitcoin.
- **Tiburones:** son aquellas personas que pueden atesorar una cantidad que ronda entre las 500 y 1000 unidades de bitcoin.
- **Ballenas:** uno de los dos grupos de los cuales realizaremos el estudio, ya que tienen en su haber, como mínimo, 1000 bitcoin y como máximo 5000 de estos.



- **Ballenas jorobadas:** el segundo de los grupos que está incluido en el caso práctico. Este, agrupa al grupo en mayor posesión de bitcoin, el cual tiene, como mínimo, a partir de 5000 unidades.

Como una imagen vale más que mil palabras, a continuación, se muestra un gráfico que resume lo citado en la lista anterior:



*Ilustración 8 - Clasificación de usuarios en función de su cantidad de Bitcoin*



### 3.4.2 Localización de las principales billeteras y sus movimientos

El estudio que se hará sobre algunas ballenas será gracias a las páginas <https://blockchain.com/>, la cual, nos proporcionará información sobre el número de transacciones realizadas en fechas de nuestro interés, <https://es.investing.com/crypto/bitcoin/historical-data>, proporcionará a la investigación la información del bitcoin en el intervalo de tiempo deseado, y por último, y no por ello menos importante, <https://bitinfocharts.com/>, esta facilitará el acceso a cualquier billetera y nos permitirá consultar el historial de sus transacciones, ordenarlas por cantidad de bitcoin compradas o vendidas, las fechas en las que realizaron transacciones, para a su vez ordenarlas y ver cómo afectaron al mercado.

Además de lo mencionado en el anterior párrafo, nos serviremos de diferentes medios de información para conocer posibles fluctuaciones de la moneda y sus causas, ya que, en ocasiones, estas se deben a motivos de nivel geopolítico o a carteras de bitcoin que son completamente desconocidas.

En primer lugar, el primer caso de análisis será de las ballenas poseedoras de una billetera desconocida. Esta ballena, de la cual, se desconoce la identidad del comprador, solicitó el día 6 de octubre del año 2021 la compra de 1.600 millones dólares en bitcoin a un exchange. En la imagen que se muestra a continuación, podemos observar que, ese día, gracias a esa compra, el valor del bitcoin incrementó en un 7,49% en cuestión de un día, lo que evidencia que esa compra de una ballena influyó en el valor del mercado:

06.10.2021	55.323,2	51.470,0	55.676,1	50.439,5	116,26K	7,49%
------------	----------	----------	----------	----------	---------	-------

*Ilustración 9 – Valor del Bitcoin a cierre del 6 de octubre del 2021*

Otro caso que influye en el precio de cotización, ya sean de forma alcista o bajista, de las criptomonedas y que es reseñable mencionar antes de entrar en las ballenas conocidas son las noticias geopolíticas que acontezcan.

Un claro ejemplo de esto fue cuando el 30 de septiembre y ratificado el 1 de octubre del año 2021, el gobierno de Estados Unidos, ante las prohibiciones chinas de las criptomonedas y a las posibles prohibiciones rusas, negó de forma contundente que fuera a seguir los pasos de las otras dos grandes potencias mundiales. Esto se tradujo en cuestión de 2 días, en un aumento del precio del bitcoin de cerca del 15%, pasando de tener un valor de 41.000 dólares a llegar a los 48.000:

01.10.2021	48.146,0	43.824,4	48.435,2	43.292,9	94,66K	9,86%
30.09.2021	43.823,3	41.534,5	44.101,2	41.416,7	64,32K	5,50%

*Ilustración 10 – Valor del Bitcoin tras la declaraciones gubernamentales de EEUU*



Otro caso provocado por el gobierno estadounidense ese mismo mes fue cuando el 15 de octubre aprobó la inclusión del ETF de bitcoin. Estos ETF no son más que activos que cotizan en bolsa y que son considerados, desde el punto de vista bursátil, como activos de muy bajo riesgo, como lo son las materias primas o bonos del estado de países con economías robustas. Esta aprobación supuso un incremento del valor del bitcoin del 7,49% situándose en un valor, por segunda vez en su historia, de más de 60.000 dólares al cambio:

15.10.2021	61.672,5	57.348,2	62.892,8	56.874,8	121,48K	7,54%
------------	----------	----------	----------	----------	---------	-------

*Ilustración 9 – Valor del Bitcoin tras la aprobación de los ETF por EEUU*

No todas las noticias geopolíticas afectan de forma positiva al valor de mercado del bitcoin, y este fue el caso por parte del gobierno de China de prohibir las criptomonedas a todos los habitantes de su población. Y ya no solamente fue este hecho que causó la bajada del valor de bitcoin, además, hubo otro actor que influyó y no fue otra persona si no Elon Musk. Este, un entusiasta de las criptomonedas publicó un tweet en el que retiraba el bitcoin como método de pago de sus coches Tesla:



*Ilustración 11 - Tweet de Elon Musk*





Esto, sumado a la prohibición china, se puede ver reflejado en que, en el mes de mayo del 2021, el precio del bitcoin se desplomó de los cerca de 60.000 dólares de valor a principio de mes a valer 34.000 a finales del mismo:

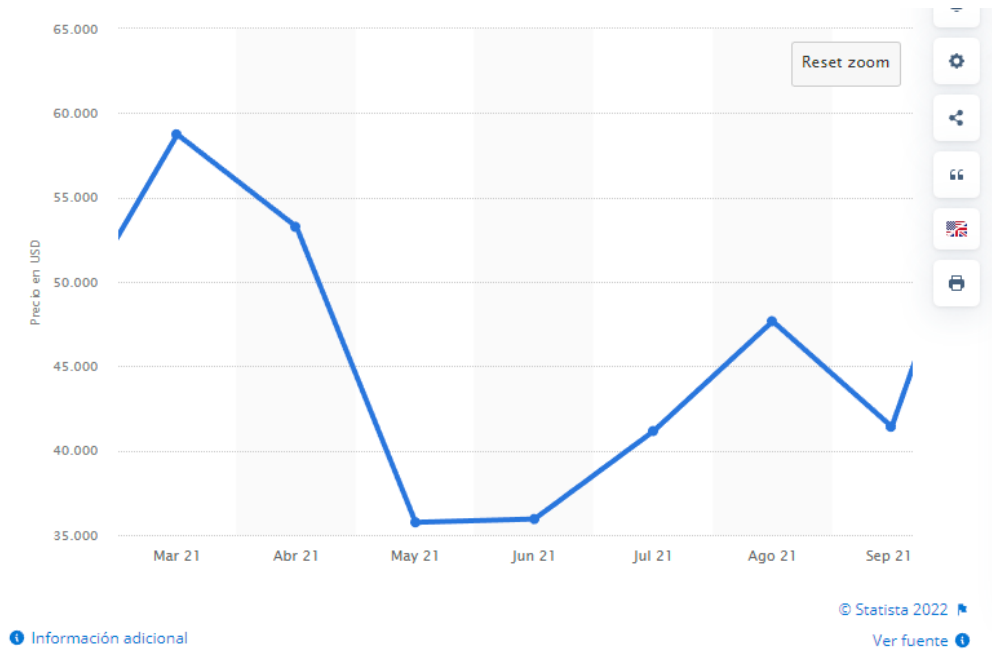


Ilustración 12 – Evolución del valor del Bitcoin ante prohibiciones mundiales

Una vez vistos los agentes externos que afectan al incremento de valor, o, por el contrario, afectan a la depreciación del bitcoin, es momento de ver la influencia de las ballenas, poseedoras de importantes cantidades de bitcoin. La imagen que se muestra seguidamente es posible observar las billeteras de bitcoin más ricas del mundo:

Address	Balance	% of coins	First In	Last In	Ins	First Out	Last Out
1 34xp4VroCGJym3R7yCVPFHOCNv4Ttseo wallet: Binance-coldwallet	252,597 BTC (\$3,360,424,111)	1.32%	2018-10-18 14:59:18	2022-08-19 02:39:18	729	2018-10-18 15:19:26	2022-01-27 20:01:27
2 bc1qgdqv0av3q5jvdb2kdlp7gdp9u8lmgprmv24sq90ecvqjwv97 wallet: Bitfex-coldwallet	168,010 BTC (\$3,565,378,615)	0.8783%	2019-08-16 12:00:29	2022-08-20 06:23:28	98	2020-02-02 18:43:14	2021-11-12 14:40:40
3 1LooVst8KkaUXSPKZHnVeyfEKPHzSsCd	133,517 BTC (\$2,833,390,367) -1834 BTC +4338.87 BTC	0.6990%	2022-06-14 19:31:03	2022-08-20 01:59:28	83	2022-06-15 02:25:24	2022-07-28 23:13:08
4 3LYJfcHPXYJreMtsASk2jIn69LWEYKzxb wallet: Binance-BTCB-Reserve	125,351 BTC (\$2,660,105,389) -0.00331 BTC +0.00331 BTC	0.6553%	2019-06-17 13:52:41	2022-08-19 19:39:03	47		
5 3Mz19KR5vEneNb47ewrPWyb5jQZDjRP6 wallet: Binance-coldwallet	101,266 BTC (\$2,148,989,091)	0.5294%	2018-11-13 15:11:02	2022-07-13 04:29:27	199	2018-11-13 15:11:02	2022-06-16 01:47:31
6 bc1qazcm763858nkq9b86tetajv6wquv8uwxcz2	94,643 BTC (\$2,008,447,353)	0.4948%	2022-02-01 05:14:24	2022-08-20 16:06:33	46		
7 37XUvSEpWW4trkfmvWzegTHQ7BdkSJKUs wallet: 77604498	94,505 BTC (\$2,005,519,615)	0.4941%	2019-09-05 05:30:05	2022-07-31 09:08:17	134	2021-07-04 05:56:36	2021-07-04 06:10:14
8 1FeexV6AHt8lybZpQMjrcCrHG9W9sb6uF	79,957 BTC (\$1,696,790,580)	0.4180%	2011-03-01 11:26:19	2022-08-12 07:37:35	430		
9 bc1qg5wkgaeW2dkv56kVj49D0av5nmI45x9ek9hz6	69,370 BTC (\$1,472,120,483)	0.3627%	2020-11-03 22:31:39	2022-06-17 00:52:05	47		
10 3K2n9qAvWQhEsfQz7ZEQL1EuSx5yNLS <sup>2-of-3</sup> wallet: OKEX-coldwallet	64,769 BTC (\$1,374,480,548) -1401 BTC +1833 BTC	0.3386%	2015-08-25 02:28:20	2022-08-20 02:53:38	1692	2015-08-25 22:44:05	2022-08-20 02:53:38
11 bc1q4y9ezzhmyppwly5dnw7c8nqy5h5mrg0xqsvaef0Qn5kq32vnmwqgv4zr	54,300 BTC (\$1,152,312,782)	0.2839%	2021-10-11 14:39:15	2022-07-22 19:25:55	22	2022-07-15 17:51:57	2022-07-22 19:25:55
12 1LdRcdxBSnmCYYNdeYpUnzIZvZVBEQeC	53,880 BTC (\$1,143,401,199)	0.2817%	2014-05-28 00:49:42	2022-07-09 06:59:27	136		
13 1AC4Mw9Y6j9onSbXEW6H6Zan8QGM5dmtA	51,830 BTC (\$1,099,904,783)	0.2710%	2018-01-07 15:45:18	2022-06-18 09:55:50	109		
14 35PPd9rCSZuqz2S7y9RResHQCVtsYuB3z	50,562 BTC (\$1,072,995,708)	0.2643%	2022-07-09 06:55:53	2022-07-09 06:55:53	1		
15 bc1qmqjefuy06v345v6vwpw105dz2zmx4g3y7wp	49,826 BTC (\$1,057,363,151)	0.2605%	2022-03-25 18:03:13	2022-06-17 00:52:05	8		

Ilustración 13 - Las 15 wallets de Bitcoin con más valor



Como se puede apreciar, en la imagen vemos las 15 billeteras con más bitcoin del mundo. Si hacemos la suma del porcentaje total que tienen esta sobre el global de bitcoin existentes hoy en día, obtenemos que, solo estas 15 billeteras, poseen cerca del 9% de las criptomonedas del mundo.

La que será analizada en primer lugar será la billetera bitcoin número 1 a nivel global, a fecha de realización de este Trabajo Fin de Grado, la correspondiente con la dirección **34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo**:

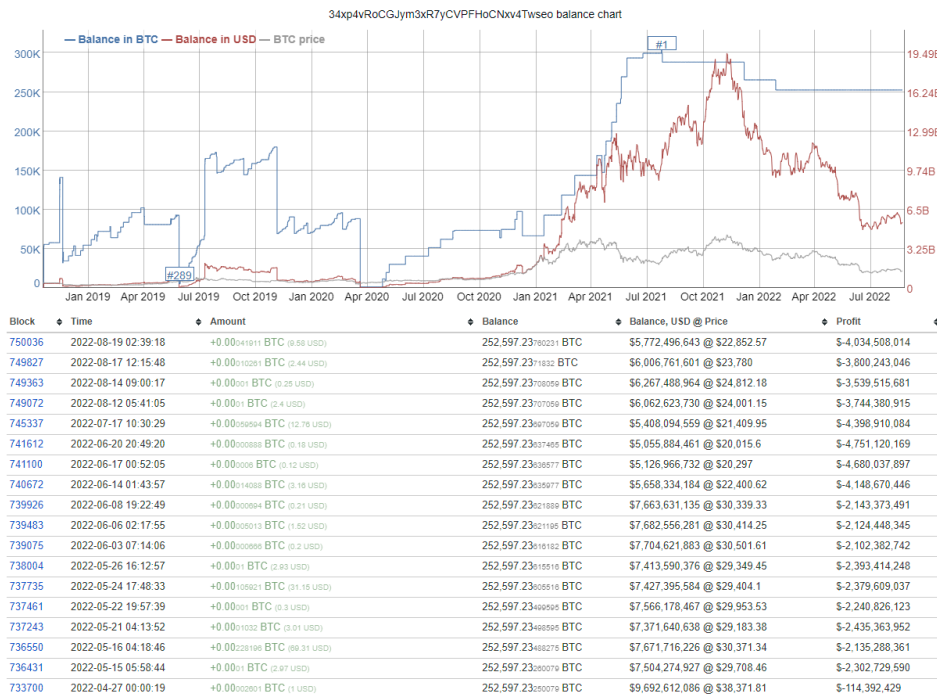
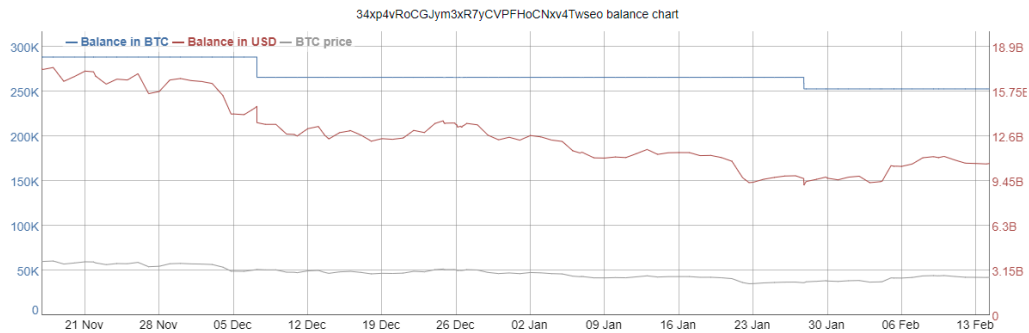


Ilustración 14 - -- Información de la wallet número 1 mundial

La línea azul nos indica el número de bitcoin que tiene, por lo que, si la barra desciende, significa que ha vendido bitcoin y si, por el contrario, aumenta, implica compra por parte de la billetera. Por otro lado, la línea gris nos indica el precio del bitcoin ese día.

Una vez conocido las dos líneas relevantes de la gráfica, el estudio de la mayor billetera de bitcoin se centrará en las últimas ventas y observar el comportamiento del valor del bitcoin ante estas:



*Ilustración 15 – Gráfica de ventas de la mayor wallet de Bitcoin*

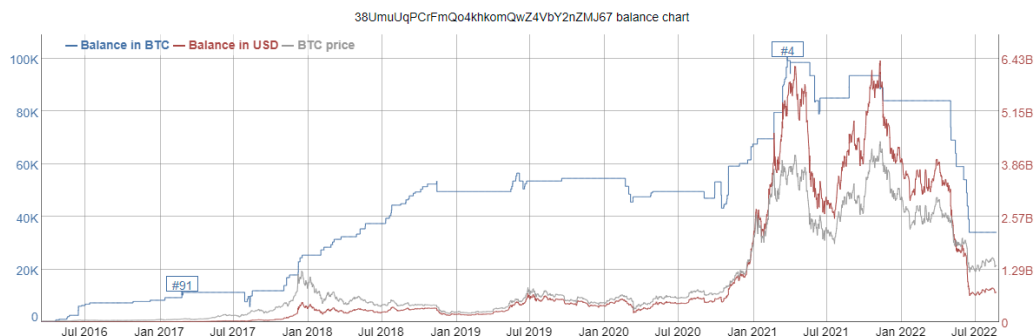
Como se puede observar, según la línea azul, el propietario de esta wallet emitió una orden de venta el día 12 de diciembre del 2021 y otra el 27 de enero de 2022. Como se puede observar en la línea gris, la primera orden de venta tuvo un impacto negativo en el valor del bitcoin, ya que, en cuestión de días, esta criptomoneda pasó a valer de 50.000 dólares a 47.000 dólares.

Centrando la vista en la segunda venta producida, es observable un ligero impacto, pero más insignificante, apenas descendió mil dólares, proporcional a la cantidad de monedas que decidió vender el usuario.

Una vez estudiadas las principales ventas de la mayor cartera de bitcoin del mundo y su impacto en el mercado, el siguiente paso es analizar billeteras que posean una suficiente cantidad de bitcoin como para ser considerada una ballena y una relativa actividad de compraventa de este criptoactivo.

Siguiendo estas premisas, dos billeteras que son aptas para el estudio son 38UmuUqPCrFmQo4khkomQwZ4VbY2nZMJ67 y 3M219KR5vEneNb47ewrPfWYb5jQ2DjxRP6, es decir, la cuarta y quinta carteras más grandes del mundo, respectivamente.

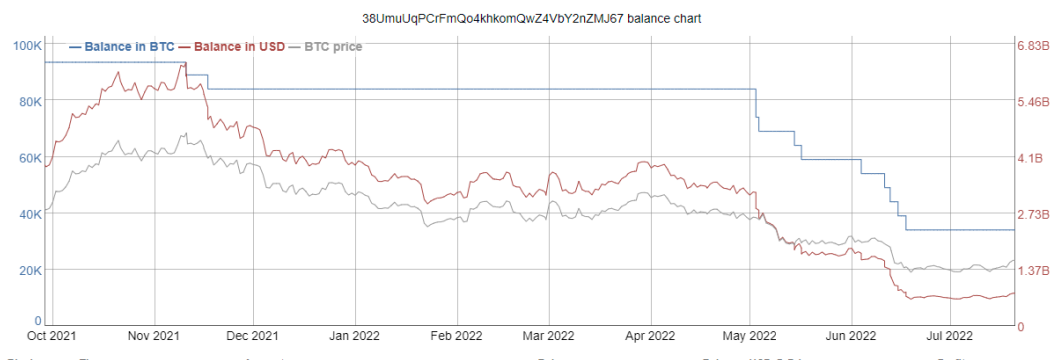
Comenzando con la que ocupa la cuarta posición, es una wallet la cual realiza operaciones menos moderadas, a diferencia de la primera cartera estudiada. Prueba de ello, es la gráfica que se muestra a continuación sobre sus operaciones:



*Ilustración 16 – Wallet número 4 mundial*



Como se observa en la imagen anterior, esta cartera está tendiendo a vender sus bitcoin y, casualmente, cuando realiza ventas, acto seguido la criptomoneda más conocida del mundo de devalúa. Claro ejemplo de esta afirmación es la gráfica siguiente:



*Ilustración 17 – Gráfica con ventas y repercusión del 4º mejor wallet*

Cuando bitcoin alcanzó su máximo histórico el pasado noviembre, llegando a un valor de 68.000 dólares por bitcoin, se puede observar que, esta cartera vende parte de sus activos y al momento, esta criptomoneda pierde valor por ventas como estas, ya que, no ocurrió ningún acontecimiento de índole social o geopolítico que pudiera alterar el valor ese día. Es más, este movimiento tuvo tanta influencia en el mercado que la web blockchain.com registró el mayor número de transacciones de su historia con un total de 345.411.



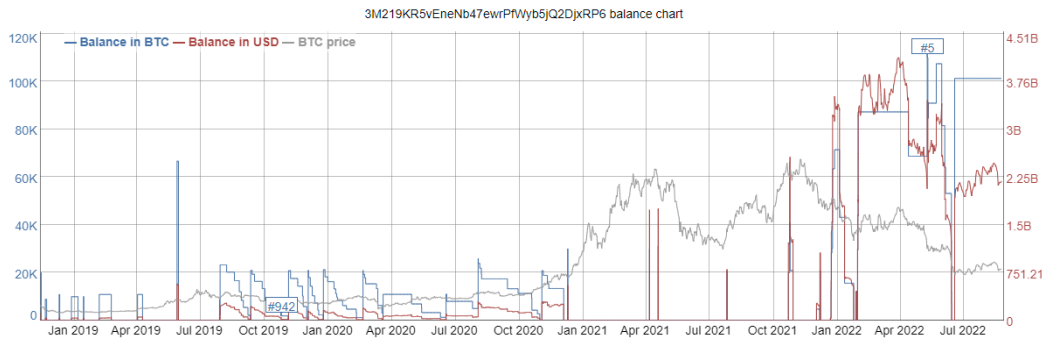
*Ilustración 18 – Número de transacciones diarias*

Para corroborar la influencia de esta y otras carteras, se observa que, en mayo del año 2022, realiza también importantes cesiones de sus activos traduciéndose en el desplome de esta criptomoneda debido a la falta de apoyo por parte de sus principales actores.



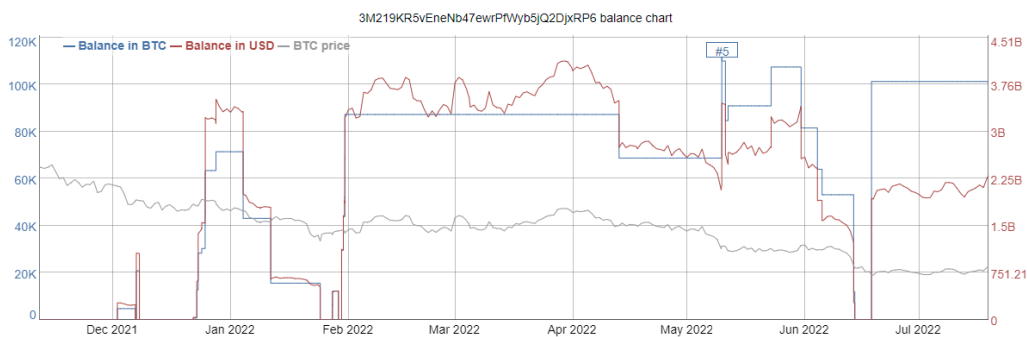
Finalmente, la última cartera analizada será la ya mencionada anteriormente, la que ocupa el puesto número cinco del mundo en cantidad de bitcoin.

Esta billetera, es también muy activa en la compra y venta de bitcoin, llegando en ocasiones a realizar órdenes de venta por valor en el momento realizado de mil quinientos millones de dólares. En la siguiente gráfica es observable este comportamiento:



*Ilustración 19 – Wallet número 5 mundial*

Estos comportamientos, citados en el anterior párrafo, influyeron claramente en muchas ocasiones en el valor de la moneda. Es posible observarlo a finales del año 2021 y comienzos del 2022, cuando tanto sus compras como sus ventas influyeron en el valor de cotización de esta criptomoneda, porque en sus compras de final de año, en cuanto emite la orden, la cotización subió 3.000 dólares inmediatamente después. Y, en el caso de las ventas correspondientes a comienzos de año, concretamente el 4 y el 24 de enero, el precio de esta criptomoneda bajó de 46.000 dólares a 43.000 y de 36.000 a 33.000, respectivamente. Estas tres evidencias demuestran que esta bajada no fue fruto de la casualidad, ni de acontecimientos geopolíticos relevantes con respecto a las criptomonedas.



*Ilustración 20 – Ventas y repercusión de la 5ª billetera mundial*



Por último, si se observan sus movimientos de mayo y junio, vemos también que sus compras evitaron una depreciación más rápida y, sin embargo, las ventas que realizó a lo largo del mes de junio hicieron que se acelerara la depreciación del bitcoin esos meses. Esto es contemplable, concretamente cuando decide liquidar sus criptoactivos el 13 de junio, cuando estos pasan de valer 26.000 dólares a 22.000.

### 3.4.3 Conclusiones del estudio

Tras este estudio realizado en profundidad de las ballenas del bitcoin y la influencia que pueden llegar a obtener en el mercado, es posible sacar conclusiones respecto a ellas. Si bien es cierto que son figuras anónimas que operan con criptomonedas, hay muchos bots en todas las redes sociales que avisan a los usuarios de cuándo y cuánto vende una ballena. Un ejemplo de esto es *Whale alert*, una página de Twitter y un bot de Telegram que notifica a los seguidores de estas acciones de las ballenas:



*Ilustración 21 – Cuenta de Twitter de Whale alert*

Luego, de forma intencionada o no, la actividad de las ballenas influye en la toma de decisiones del resto de animales del espectro que posee bitcoin que mencionamos en la introducción de este punto.



Por otro lado, hemos visto cómo gobiernos de diferentes partes del mundo también influyen en el valor del bitcoin. A su vez, personas con cierta relevancia en el mundo de las redes sociales, como el caso de Elon Musk que hemos estudiado, también impacta positiva y negativamente al precio de las criptomonedas.

Teniendo en cuenta todo esto, es preciso concluir que:

- Las ballenas influyen, en mayor o menor medida en el precio del bitcoin, pero es innegable que tienen una importante influencia en el resto de los usuarios que poseen criptomonedas.
- Las ballenas aprovechan su influencia para comprar o vender en función de sus intereses, ya que, si deprecian mucho el bitcoin o, por el contrario, logran aumentar su valor, estas obtendrán importantes beneficios económicos a costa del resto de usuarios que poseen ínfimas cantidades.
- El impacto de las ballenas en el precio de bitcoin pierde totalmente su relevancia en cuanto estados prohíben o permiten realizar más movimientos económicos con las criptomonedas. Esto se ha visto en este estudio con casos como la ilegalización en China de las criptomonedas o la inclusión por parte del gobierno estadounidense del ETF del bitcoin.
- Las figuras que poseen una amplia relevancia en redes sociales pueden alterar el precio de las criptodivisas, y, en el caso que atañe a este Trabajo Fin de Grado, al bitcoin. Esto hace estas personas, gracias a su influencia, manipulen el mercado en su propio beneficio y quién sabe si alguna de estas personas es alguna de las ballenas estudiadas.
- Un usuario que decida adentrarse en el mundo de las criptomonedas y decida adquirir bitcoin, está expuesto a un mercado de muy alto riesgo y en el que carece de relevancia por sí mismo y, por ende, su dinero queda a merced todas las variables previamente mencionadas.



## 3.5 Cajeros de criptomonedas y uso en España

### 3.5.1 Concepto de los cajeros de criptomonedas

Antes de entrar en materia, es imprescindible comprender en qué consisten los cajeros de criptomonedas y cuál es su funcionamiento. Comúnmente, los cajeros de criptomonedas operan con la criptomoneda con más popularidad mundial, es decir, con Bitcoin. Es por esto que, a estos cajeros, también se les conoce como BTM (Bitcoin Teller Machine).

Los BTM son, en cuanto a su aspecto físico, muy similares a los cajeros automáticos tradicionales. Sin embargo, presentan unas diferencias fundamentales que nos permiten observar un concepto diferente. En primer lugar, mediante los BTM, los usuarios pueden comprar Bitcoin o cualquier criptomoneda que la empresa asociada al cajero acepte (normalmente suelen ser Ethereum, Stellar, Dogecoin...) a cambio de dinero en efectivo o contenido en una cuenta bancaria tradicional. La segunda diferencia es que estos se conectan a un monedero de criptomonedas en lugar de una cuenta bancaria clásica. Además, algunos BTM también permiten a sus clientes la acción contraria, vender Bitcoin o cualquier criptomoneda disponible para operar con la empresa gestora a cambio de efectivo.



*Ilustración 22 – Cajeros de Criptomonedas*





### 3.5.2 Breve historia de los cajeros de criptomonedas

Una vez hemos conocido qué es, a grandes rasgos, un cajero de criptomonedas o BTM, es esencial conocer cómo y cuándo aparecieron en nuestras vidas.

El primer cajero de criptomonedas apareció en el año 2013, concretamente el día 29 de octubre en una cafetería de Vancouver, Canadá, el cual, funcionó hasta el año 2015. En concreto, fue retirado porque numerosos usuarios experimentaban problemas con sus wallets y con Bitstamp, (la empresa encargada de la gestión y el intercambio de divisas en ese cajero).



*Ilustración 23 – Primer BTM de la historia*

Tras esta primera aparición, no tardaría mucho en llegar el primer cajero a Europa (diciembre de 2013) y Estados Unidos (febrero 2014), aunque este último, instalado en Albuquerque, fue retirado de donde se encontraba pasado apenas un mes de su instalación.

A medida que fueron instalados más cajeros de este tipo por todo el mundo, comenzaron a surgir problemas relacionados, en su amplia mayoría, con su legalidad. Por lo que, a fecha de realización del presente trabajo, la normativa que deben seguir en gran parte del mundo es la misma que están obligados a cumplimentar los cajeros automáticos tradicionales. Deben contemplar un número máximo de depósitos y retiradas diarios por persona, además de respetar la normativa contra el blanqueo de capitales y demás delitos financieros.



Esta normativa, apareció debido a que se empezó a emplear estos cajeros con fines delictivos (lo cual continúa ocurriendo), con motivo del anonimato que supone realizar estas transacciones sin una entidad bancaria que la respalde. Es por esto, que las medidas implementadas se han enfocado en que se pierda esa ocultación de identidad y así evitar el uso fraudulento de estas criptomonedas.

En la actualidad, existen unos 28.000 cajeros automáticos de criptomonedas, siendo España el tercer país del mundo con más cajeros BTM, con un total de 100 cajeros repartidos por todo el territorio nacional.

### 3.5.3 Cómo funcionan los cajeros de criptomonedas

Una vez hemos analizado qué son los cajeros de criptomonedas y su origen, es preciso observar cómo funcionan.

En primer lugar, es conveniente conocer que existen dos tipos de cajeros BTM: los cajeros bidireccionales y los cajeros unidireccionales.

- **Cajeros bidireccionales:** Son aquellos que permiten tanto la compra como la venta de estos activos.
- **Cajeros unidireccionales:** Estos cajeros solo admiten, o bien, la compra de criptomonedas, o bien, exclusivamente la venta de estas. Pese a ello, lo más común en este tipo de cajeros es que, si es unidireccional, sea única y exclusivamente para la compra de cryptoactivos, en lugar de venta de estos.

Otro requisito indispensable para entender el funcionamiento de los cajeros de criptomonedas es que estas máquinas precisan de conexión permanente a la red de internet para realizar correctamente las transacciones y, como hemos visto con anterioridad en este trabajo, para que sea incluida dicha transacción en la red blockchain.

A pesar de que detrás de estos cajeros no haya una entidad bancaria tradicional (como las que todos conocemos), sí que existe, en la gran mayoría de países, una normativa que todas las empresas que los gestionen deben acatar para operar en sus países, ya sea la documentación a aportar por el cliente para realizar estas transacciones, así como la cantidad máxima de dinero que se pueden invertir en estos cajeros. Dicha regulación será explicada más adelante en el Trabajo de Fin de Grado.

Una vez sabido esto, podemos apuntar a que lo único necesario para realizar una compra/venta de alguna criptomoneda en uno de estos cajeros es una billetera de



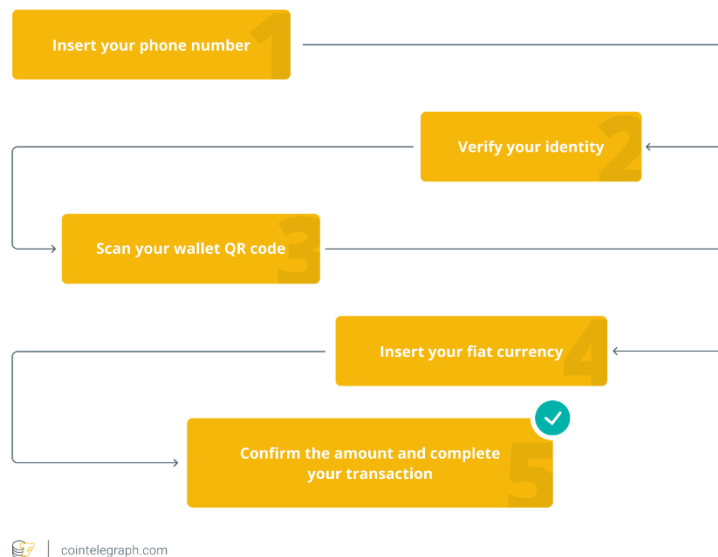
criptomonedas, en la cual sea almacenada la criptomoneda adquirida o en la que se encuentren los activos a vender.

Los pasos a la hora de comprar cualquier criptomoneda en estos cajeros, por norma general, son los siguientes:

1. La verificación del número de teléfono de la persona usuaria: Este primer paso surge para combatir el anonimato del cliente. Para ello, se le solicita un número de móvil para combatir el fraude. Esta medida implementada en muchos países es conocida como *KyC*, es decir, *Know your Customer*, en castellano: *conoce a tu cliente*.
2. El registro en el operador del cajero: en la mayoría de los casos estudiados, gran parte de las operadoras que brindan este servicio solicitan la creación de una cuenta en su sistema. A esta cuenta irá asociado un documento de identidad del cliente que solicite realizar cualquier operación en el cajero. Como ya mencionamos en el anterior paso, esta también es una medida para combatir el fraude y/o blanqueo de capitales. Una vez creada la cuenta y verificada nuestra identidad, podremos seguir con el proceso de compra.
3. Escaneo del código QR correspondiente a nuestra billetera: Una vez el sistema ha verificado la identidad del usuario, solicitará un código QR asociado a su billetera en la que se almacenarán las criptomonedas que compradas. Este paso es imprescindible para que el cajero de criptomonedas conozca, con total exactitud, a qué cartera de criptomonedas enviará el dinero que se ingrese.
4. La inserción del efectivo: A continuación, el cliente lo que debe hacer será ingresar la cantidad de efectivo que desea convertir en la criptomoneda solicitada. Esta cantidad, tiene un valor mínimo y máximo, según el país en el que nos encontremos y las propias normas de la empresa responsable del cajero BTM.
5. La confirmación de la transacción: Una vez realizados todos los pasos anteriores, el cajero solicitará autorización para confirmar dicha compra de criptomonedas para su asignación en la billetera. Una vez confirmada la transacción, esta se anotará en su propia cadena de blockchain y dicho resultado se verá reflejado en la cartera de criptomonedas.



### Steps for exchanging your Fiat currency for BTC using a Bitcoin ATM



*Ilustración 24 – Resumen de cómo comprar criptomonedas con un BTM*

En cuanto a la venta de los cryptoactivos del usuario, las acciones a realizar son similares a los mencionados para realizar la compra. Estos pasos, comúnmente, son los siguientes:

1. La verificación del número de teléfono: Este paso coincide con el de la compra, ya que es esencial para combatir los posibles delitos de fraude y cumplir con la normativa del KyC, por lo que no requiere de una explicación adicional más allá de la dada en el punto 1 del proceso de compra.
2. El registro en el operador del cajero: Al igual que el punto 1, este paso es invariable con respecto al de la compra. Así, será indispensable, en la mayoría de los cajeros, registrarnos aportando nuestra documentación en la plataforma del operador de nuestro cajero.
3. Escaneo del código QR correspondiente a la billetera: Para la venta de los cryptoactivos, será necesario la conexión a la billetera personal de criptomonedas. Una vez conectado el usuario, elegirá entre alguna de las criptomonedas que acepte el cajero de criptomonedas en el que nos encontremos.
4. Escaneo del código QR correspondiente a la billetera del operador del cajero: Una vez elegida la cantidad y la criptomoneda a vender, el cajero mostrará un código QR con la dirección correspondiente a la billetera asociada al cajero en el que se encuentra el cliente. Una vez escaneada, realizará el cambio, aplicando la



comisión que aplique la empresa responsable del cajero y quedará pendiente de nuestra aprobación.

5. Aprobación y retirada del efectivo: Una vez se encuentre conforme con la venta, el usuario deberá aprobar la transacción, la cual, será anotada en la cadena de bloques correspondiente a la criptomoneda que haya deseado vender y podrá retirar el efectivo.

#### 3.5.4 Normativa en España de los cajeros de criptomonedas.

La normativa que han de seguir los cajeros BTM en nuestro país es algo confusa, puesto que las tecnologías avanzan a una velocidad superior a la que lo realiza la legislación. Por ello, no existe una normativa específica que regule los cajeros de criptomonedas, sino que para su estudio deberemos dirigirnos a la de los cajeros convencionales. De esta manera, desde el año 2021, según la ley contra el blanqueo de capitales, la cantidad máxima que puede llevar en efectivo una persona es de un máximo de 1000€.

Los cajeros de criptomonedas más presentes en España son los de la empresa BitBase. Se rigen por una normativa interna para adquirir criptomonedas en sus cajeros, la cual se puede resumir en los siguientes puntos:

- La cantidad máxima que se podrá comprar en un mismo día sin que el usuario aporte su documentación (más allá de un teléfono móvil) es de 995€. Esta cantidad también supone el máximo que se puede comprar con dinero en efectivo. Anteriormente, era posible adquirir hasta 2500€ en efectivo, pero desde que en España se aprobó la Ley 11/2021 de 9 de julio de medidas de medidas de prevención y lucha contra el fraude fiscal, que establece el máximo para pagar en metálico en 1.000 euros, esta cantidad se vio reducida hasta los 995€ mencionados. Para poder comprar más de 995 € en criptomonedas, es posible bien realizar el pago mediante transferencia bancaria o con tarjeta de crédito, o bien registrando el Documento nacional de identidad (en adelante DNI) del



comprador. En este último caso, la cantidad máxima que se permite adquirir en efectivo es de 2.500 €.

- La cantidad máxima mensual que puede adquirir un cliente que no se haya registrado en los cajeros BTM es de un máximo de hasta 5000€ siendo el límite diario el ya especificado en el punto anterior. En caso de que el cliente se hubiera registrado con su DNI, esta limitación no existiría.
- Las personas que se encuentran expuestas políticamente hablando, tienen prohibido utilizar este tipo de cajeros, en el caso de que no estén registrados, para evitar problemas de blanqueo de capitales y/o fraude fiscal.
- Por último y desde la aprobación de la ley 10/2010, del 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, es obligatorio para este tipo de establecimientos de exchange, que conozcan a sus clientes en los términos anteriormente analizados. Además, los empleados deben ser instruidos en la materia y deben contar con un manual adecuado de prevención del blanqueo de capitales y de la financiación del terrorismo, donde estén detalladas las medidas que la empresa ha implantado con el objetivo de evitar e intervenir las operaciones relacionadas con ello. También se impone la obligación de informar a las autoridades en el caso de que se tengan sospechas de que el cliente esté ejerciendo alguna actividad ilícita, ya que, si se llega a la conclusión de que algún cliente realizó un uso indebido del servicio, la empresa gestora podría ser considerada asimismo responsable o incluso cómplice de dichos actos. **La obligación se encuentra en el artículo 18 y se debe hacer ante el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.**
- Siguiendo lo dispuesto en el artículo 1 de la ley 10/2010 del 28 de abril, sobre la prevención del blanqueo de capitales y la financiación del terrorismo, mencionada al inicio de este punto, las actividades que son consideradas ilegales en este ámbito son las siguientes:
  1. La conversión o la transferencia de bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva, con el propósito de ocultar o encubrir el origen ilícito de los bienes o de ayudar a personas que estén implicadas a eludir las consecuencias jurídicas de sus actos.



2. La ocultación o el encubrimiento de la naturaleza, el origen, la localización, la disposición, el movimiento o la propiedad real de bienes o derechos sobre bienes, a sabiendas de que dichos bienes proceden de una actividad delictiva o de la participación en una actividad delictiva.
3. La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de la recepción de los mismos, de que proceden de una actividad delictiva o de la participación en una actividad delictiva.
4. La participación en alguna de las actividades mencionadas en las letras anteriores, la asociación para cometer este tipo de actos, las tentativas de perpetrarlas y el hecho de ayudar, instigar o aconsejar a alguien para realizarlas o facilitar su ejecución.”

La normativa reguladora se encuentra inspirada por el principio mencionado con anterioridad, el *Know your Client*. Esto es observable, por ejemplo, en los artículos 3 y 4 de la ley. La ley obliga a identificar a todas las personas participantes, pero según su artículo 7, esta medida se relaja si se demuestra que no existe un riesgo elevado. En este último artículo es en el que ampararan para imponer su normativa a la hora de operar con cantidades bajas, en las que no tienes por qué identificarte.

Al ser una materia reciente y poco regulada, la normativa puede ser cambiante, es decir, a la fecha de lectura del presente trabajo puede haber sufrido alguna modificación. Así, cabe reseñar, que esta es la normativa actual en España a fecha del año 2022.

### 3.5.5 Ventajas e inconvenientes de los cajeros de criptomonedas

Una vez hemos conocido detenidamente el funcionamiento de los cajeros de criptomonedas desde su origen hasta la actualidad, qué son y cómo podemos emplearlos, además de cuál es su normativa en nuestro país, debemos mencionar las conclusiones extraídas sobre sus ventajas e inconvenientes.

En primer lugar, hablaremos de las ventajas, que se considera que son las siguientes:

- Es una forma rápida y cómoda de comprar criptomonedas en un establecimiento físico.
- Hasta cierto punto, especificado en el apartado anterior, no requiere de cuenta bancaria ni de ninguna tarjeta de crédito, simplemente con efectivo es posible adquirir criptomonedas.
- Algunos cajeros (en países que no requieren KyC) no requieren verificación de identidad, por lo que mantienen el anonimato del cliente.



- Para aquellas personas que quieran introducirse en el mundo de las criptomonedas, en la mayoría de este tipo de cajeros, existen personas que te prestan asesoramiento en caso de dudas, a diferencia de las webs de compra de criptodivisas en las que el cliente se encuentra solo ante la pantalla.

En cuanto a las desventajas de los cajeros BTM, es preciso tener en cuenta las siguientes:

- Estos cajeros aplican un porcentaje de comisión, tanto en la compra/venta, como en el método de pago, que oscila entre un 7%, en las condiciones más optimistas, y hasta un 14% de máximo, algo que puede entenderse, hasta cierto punto, abusivo.
- No son la mejor opción para una persona que quiera realizar grandes inversiones de capital y/o grandes retiradas, ya sea por las comisiones que se aplican, así como las leyes y normas existentes que limitan las transacciones a una cantidad máxima mensual y diaria.
- En cuanto un usuario quiera realizar operaciones de más de una cantidad (la analizada en las páginas anteriores), perderá completamente su anonimato, ya que le será requerido que acredite su identidad y con la pertinente documentación.
- Aunque haya normativas para prevenir el blanqueo de capitales y la financiación del terrorismo, siguen siendo un método muy eficaz para realizar lavados de dinero. El motivo se encuentra en que en ocasiones solo se requiere un número de teléfono como máxima identificación. Así, al ser relativamente sencillo conseguir números de teléfono sin precisar de documentación alguna y al poder una misma persona adquirir tarjetas SIM virtuales, no es un método eficaz de identificación. De esta manera, esto puede propiciar la utilización de estos cajeros de forma ilimitada sin documentación. Por ello, se considera que actualmente la normativa para impedir el empleo de dicho medio para realizar este tipo de actividades ilegales está regulada de forma insuficiente y, para poder evitarlo, sería necesario exigir, sea cual sea la cantidad a retirar, documentación al cliente.





## 3.6 Ejemplos reales de blanqueo de criptomonedas

### 3.6.1 Introducción

Antes de analizar los casos reales ocurridos en el mundo relacionados con el blanqueo de criptomonedas (los cuales se tratarán en los siguientes apartados), debemos comprender que estos son derivados de grandes estafas a nivel mundial. Es por ello por lo que diversos países han decidido crear su propia unidad policial contra el uso ilícito de las distintas criptodivisas existentes.

En el caso español, el Cuerpo Nacional de Policía instruyó en marzo del año 2018 a unos 400 agentes de policía que empezaron a formar parte de un cuerpo especializado en perseguir este tipo de actividades fraudulentas. Si bien es cierto que en un inicio las criptomonedas podían serles útiles a los ciberdelincuentes, debido al auge de las criptodivisas, han captado el interés de otro tipo de delincuentes para ocultar sus delitos, por lo que esta práctica se ha extendido en los diferentes ámbitos delictivos. Esto es debido, en gran parte, al anonimato que proporcionan a su titular y la dificultad que supone identificar quiénes son realmente los propietarios.

La utilización de las criptomonedas con fines delictivos ha supuesto un aliciente para la Unión Europea para idear un conjunto de preceptos a seguir por los países miembros, de tal forma que para luchen contra el anonimato en el mercado de las criptomonedas. Estas medidas continúan actualizándose hasta la fecha en la que se está redactando el presente Trabajo de Fin de Grado. Las más recientes obligan a las entidades que operan con criptomonedas en los países miembros a recopilar cierta información del ordenante y del beneficiario de la transacción, sea cual sea su importe. De esta manera, se pretende asegurar la trazabilidad de las transferencias de criptomonedas para facilitar así la detección y el bloqueo de aquellas que puedan ser susceptibles de incurrir en un delito.

Además de las medidas empleadas por las diversas organizaciones gubernamentales, distintas organizaciones policiales internacionales, como la Europol o la Interpol, han creado una división especializada contra los delitos relacionados con blanqueo de criptomonedas. Sin embargo, los delitos siguen incrementándose y lo seguirán haciendo a menos que en un futuro exista una regulación armonizada a nivel mundial contra el anonimato de los titulares de las criptodivisas en sus transacciones. El gran inconveniente de dicha idea es que se sitúa diametralmente en contra de la razón de ser de las criptodivisas, que nacieron para no ser reguladas por organizaciones gubernamentales o grandes bancos centrales. Pese a ello, se entiende que estas regulaciones son necesarias para proteger tanto a los titulares de criptodivisas como al resto de usuarios, pues se está demostrando que son eficaces. La lucha contra el crimen organizado está obteniendo grandes resultados, con transacciones que han finalizado en intervenciones e incautaciones de monederos virtuales valorados en millones de euros obtenidos de manera fraudulenta



Una vez expuesto lo anterior, realizaremos un gran repaso a lo largo de los delitos de blanqueo de criptomonedas más importantes hasta nuestros días.

### 3.6.2 El primer caso: la tienda Silk Road

El primer caso del que hablaremos será el de Silk Road, una página web la cual, solo estaba presente en la dark web, y que se encargaba de realizar de mediadora entre el vendedor y el comprador interesado en productos ilícitos, ya fueran drogas, armas, software pirateado, productos robados como tarjetas de crédito, dispositivos electrónicos...

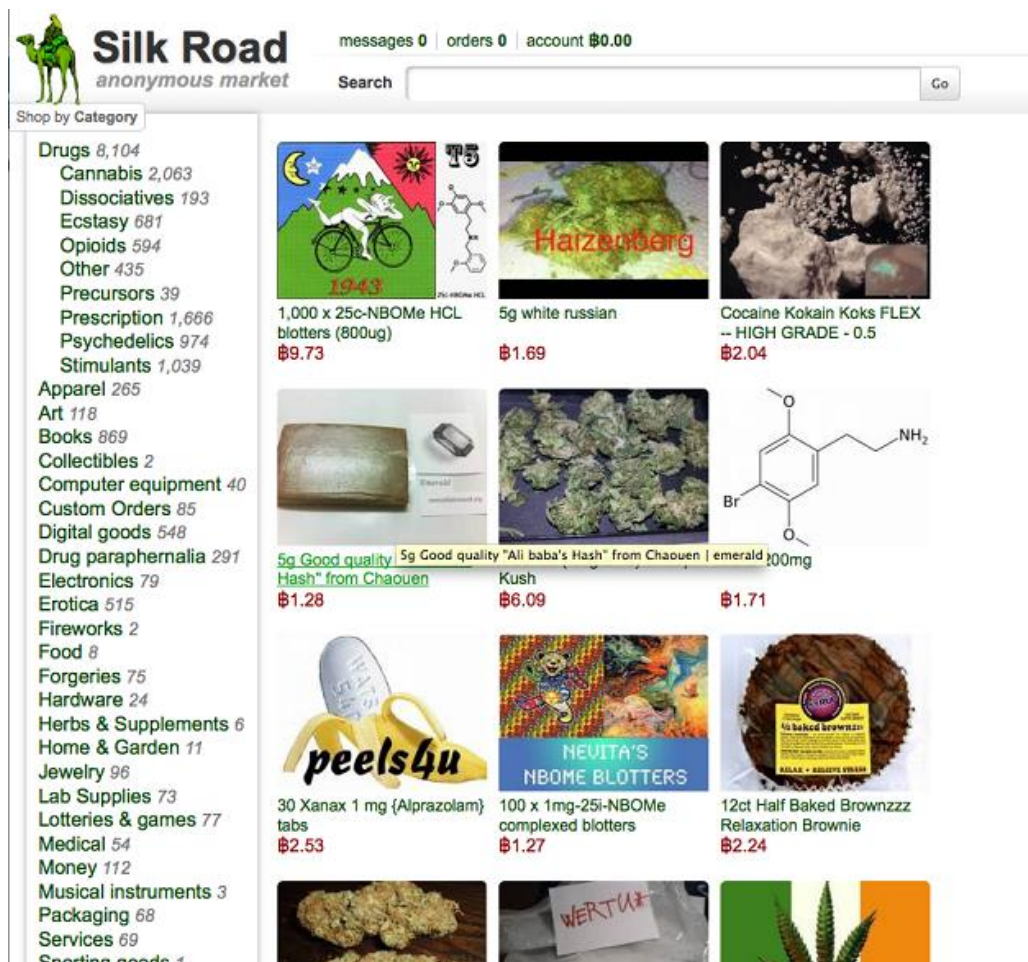


Ilustración 25 – Interfaz Gráfica de Silk Road

Esta web fue creada por el estadounidense Ross Ulbricht y el intercambio entre vendedor y consumidor se realizaba mediante la red TOR y con el Bitcoin como medio de pago. De haber permitido otros métodos tradicionales (como tarjetas de crédito, PayPal y/o



transferencia bancaria) y de haber empleado una web tradicional, es decir, un dominio que no fuera .onion; hubiera sido muy sencillo el rastreo y captura tanto de Ross como de los traficantes, así como de los compradores.

Tras observar el libro de contabilidad de Ross, se pudo determinar que, mediante esta combinación de pago y navegación anónima, Silk Road había ingresado cerca de 600.000 bitcoin en ingresos, un equivalente a unos 80 millones de dólares en la fecha en la que su fundador fue detenido.

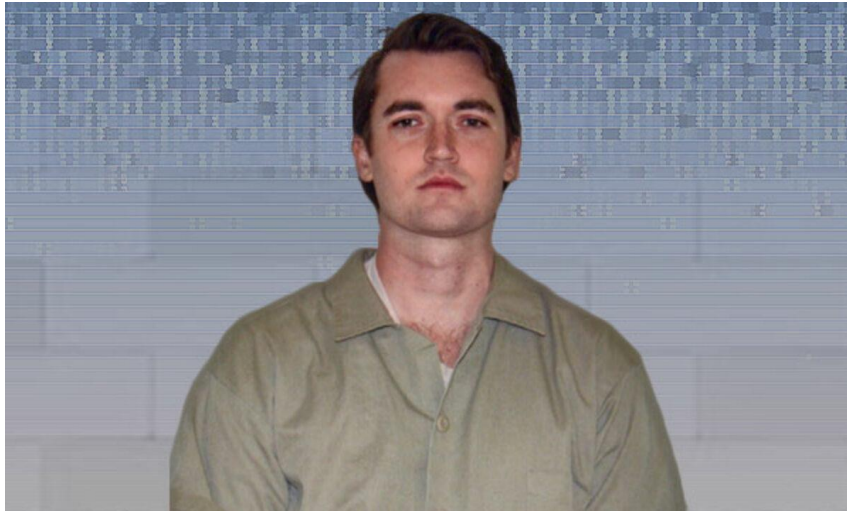
Todo funcionaba correctamente para él, hasta que un empleado suyo de confianza, Curtis Clark Green (un vendedor drogas en Utah) se puso en contacto con un potencial gran comprador que usaba el alias “Nob”. Detrás de este alias se escondían agentes del Departamento de Seguridad Nacional de Estados Unidos y agentes de la DEA. “Nob”, hizo un gran encargo de cocaína y, tras ganarse la confianza de Curtis Green, se ofreció a recibirle en su domicilio. En cuanto lo recibió, fue detenido. Pese a ello, se fingió que se había completado la transacción a los ojos de Ross, el cual utilizaba el alias “Dreadful Pirate Roberts” en Silk Road.

Debido a la detención de Curtis, Ross no recibió la comisión prevista, por lo que pensó que Curtis le estaba traicionando. Por ello, ordenó a “Nob” que contratase a sicarios para asesinarle antes de que este le delatara, así que, con este comportamiento había evidencias de que Ross podría haber usado estos servicios previamente.

Finalmente, lo que hizo que fuera detenido fue ponerle un nombre al fundador de Silk Road. Esto fue gracias a que en un foro un usuario con el alias de “Altoid” hizo mención por primera vez en 2011 de Silk Road. Meses después, un usuario con el mismo alias en otro blog quería contratar a un informático que le escribiera a una dirección de email que contenía su nombre, Ross Ulbricht.

Tras conocer su nombre, se le siguió el rastro, hasta que un día en una biblioteca de San Francisco fue detenido por las autoridades sin que previamente hubiera cerrado su ordenador portátil. De haberlo hecho, se habrían eliminado todas las posibles pruebas de las que se sospechaba que era culpable.

Finalmente, Ross fue juzgado y condenado a cadena perpetua por diversos delitos, entre los que se incluía el blanqueo de capitales por un valor de unos 80 millones de dólares, aproximadamente.



*Ilustración 26 – Ross Ulbricht Fundador de Silk Road*

### 3.6.3 El primer caso español: el virus de la policía

El primer caso que se detectó en España y del cual se incautaron criptodivisas es la famosa estafa conocida como “el virus de la policía”. La policía nacional fue el primer cuerpo de policía europeo en combatir contra el crimen y el uso de las criptomonedas de forma fraudulenta. Fue en el año 2013, cuando el cuerpo detuvo a dos informáticos de origen ucraniano en posesión de cerca de 55.000€ en diferentes monederos virtuales y diferentes criptoactivos.

Este virus, de tipo ransomware, antes de la detención de los informáticos responsables, llegó a infectar máquinas de alrededor de 1.500 empresas españolas y se calcula que 21.000 a nivel mundial. La estafa era realizada al completo por internet y se estima que llegaban a blanquear, mediante el empleo de criptomonedas, unos 10.000€ de forma diaria.

El método que empleaban se basaba en bloquear el ordenador o dispositivo móvil que empleaba la víctima a través de cierta información y un logo de la policía nacional, que podía llegar a impactar y resultar creíble al usuario al que le aparecía. Para que el ransomware fuera eliminado, exigía al usuario el abono de una multa que rondaba desde los 10€ hasta los 100€ (en caso de que el usuario no pagase). Además, para añadirle credibilidad a la estafa, el virus rastreaba la IP del usuario y mostraba por pantalla su ubicación aproximada, lo que hacía que muchos accedieran al pago para evitar “multas” en nombre de la policía nacional superiores.



**DIRECCIÓN GENERAL DE LA POLICIA Y DE LA GUARDIA CIVIL**  
**CUERPO NACIONAL DE POLICIA**

**Atención!**

Fue detectado un caso de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España. Fue detectada la siguiente infracción:  
Desde su dirección IP bajo el número [REDACTED] fue efectuado un acceso a páginas de internet que contienen pornografía, pornografía infantil, zoofilia, así como violencia sobre los menores. En su ordenador asimismo fueron encontrados archivos de vídeo que contienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo se realizaba envío de spam con subtítulo de terrorismo. El bloqueo del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.

Tour details: IP: [REDACTED]  
Location: [REDACTED]  
ISP: [REDACTED]

Para quitar el bloqueo del ordenador, usted debe pagar una multa de 100 euro.

Usted tiene uno formas de pago:

1) Realizar el pago a través de Ukash:  
Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).  
Si el sistema le genera un error, usted deberá enviar el código al correo electrónico [deposito@ryber-police.net](mailto:deposito@ryber-police.net).

2) Realizar el pago a través de Paysafecard:  
Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).  
Si el sistema le genera un error, usted deberá enviar el código al correo electrónico [deposito@ryber-police.net](mailto:deposito@ryber-police.net).

**Ukash Donde conseguir Ukash?**  
Puedes adquirir Ukash en cientos de miles de establecimientos en todo el mundo, en línea, a partir de carteras, en quioscos y cajeros. A continuación encontrarás dónde puedes adquirir Ukash en tu país.

- cajamar** - A partir de ahora esta disponible Ukash en todos los cajeros de Cajamar.
- Caixa Galicia** - A partir de ahora Ukash esta disponible en todos los cajeros de Caixa Galicia.
- Telefonica** - Ahora, Ukash esta disponible en las 80.000 cabinas de Telefonica.
- Cuponesprepago** - Consiga tu Ukash online a través de su Internet Bank o utilizando tu tarjeta de credito.

**paysafecard Donde conseguir Paysafecard?**  
Puedes adquirir tu paysafecard en las siguientes redes:  
epay (anteriormente Movicarga y Telerecarga), Correos, Cabinas de Telefonica, Teletor, Opencor, Novocaogalicia, Cajamar, Dixa, GMVending, gasolineras Repsol, Campsa, Petrolor, BP, GALP, adheridos a H24, kioscos de Red 30.000, y Canal Recargas de Telefonica.

Ilustración 27 – Ejemplo del Virus de la Policía

Una vez lograban estafar a los usuarios, los hackers responsables de la estafa movían todo el dinero a páginas en las que se intercambiaban por criptomonedas, para lavar todo ese efectivo sin ser identificados y sin necesidad de declararlo. Para identificarse en estas webs muchas veces empleaban datos personales y documentación robada de los ordenadores de sus víctimas para lograr blanquear mayores cantidades de dinero en el mismo tiempo. Además, para asegurarse de no ser descubiertos, repetían este proceso repetidas veces para dificultar la trazabilidad de todas las transacciones y así nunca averiguar la procedencia inicial del montante sustraído.

Hoy en día, esta estafa sigue existiendo y por ello, el cuerpo nacional de policía ha sido la responsable de poner en conocimiento de todos los cuerpos de policía a nivel mundial de la existencia de este ransomware, ya que se ha reproducido en otros países, principalmente en Latinoamérica. A su vez, se ha informado a las diversas empresas que sufrieron estos hackeos de servidores. En el ámbito internacional, más allá de la región latina, esta comunicación se realizó a través de servicios policiales tales como Europol e Interpol.

Tras obtener la policía la experiencia necesaria para solventar esta estafa a nivel nacional, presentaron una serie de medidas para prevenir este tipo de infecciones en los servidores de las empresas:



1. Conexión al servidor de la empresa de formas remotas y siempre empleando VPN.
2. Contraseñas de acceso a los escritorios remotos fuertes y que se modifiquen con cierta periodicidad.
3. Políticas de bloqueo de acceso en caso de intentos fallidos de conexión de forma repetida.

Por último, para el resto de los usuarios, la policía recomienda que se sigan las siguientes directrices:

1. Mantener actualizados constantemente tanto ordenadores como dispositivos móviles.
2. Uso de antivirus fiables en los dispositivos. Esto implica que estos antivirus reciban constante soporte y actualización de los posibles riesgos y amenazas en la red por parte del fabricante de este.
3. Realizar copias de seguridad en los dispositivos en caso de que sea necesario un formateo de este para evitar perder información valiosa en caso de ataque.

### 3.6.4 Operación Guatuzo y Kampuzo

El siguiente ejemplo de blanqueo de criptomonedas tuvo lugar en España y Colombia, por lo que fue vital la colaboración de la Guardia Civil y la Dijin de Colombia.

Este delito se produjo gracias a ocho personas que trabajaban en un locutorio en la ciudad de Madrid, en el cual, había instalados dos cajeros de criptodivisas. Estos cajeros no sólo servían para aquellos usuarios del locutorio que quisieran emplear estos cajeros de forma lícita, sino que también servían a estas ocho personas, integrantes de una organización criminal, ya citadas para blanquear el dinero y financiar a sus redes criminales fuera de Colombia, ubicadas en las ciudades españolas de Madrid, Barcelona y Málaga.

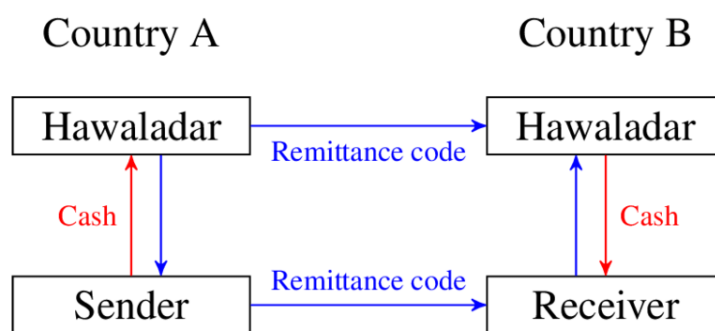
Gracias a la colaboración de la Dijin, la Guardia Civil y la Interpol, se calcula que esta banda lavaba 3 millones de euros mensuales. Esto es posible conocerlo gracias a la intervención de los dos cajeros de criptomonedas, previamente mencionados. Asimismo, fueron intervenidas 4 cold wallets ("billeteras frías") y otros 20 monederos en los que habían sido detectados dichos movimientos por un valor aproximado de 9 millones de euros.



Esta detención supuso el fin de una larga investigación, ya que, en el año 2017, fueron detenidas otras 23 personas implicadas en otras operaciones fraudulentas con criptomonedas. Estas detenciones pertenecían a la operación Guatuzo, la cual, la organización criminal hispano-colombiana, se servían de otros locutorios ubicados en España para recibir dinero y enviar dinero mediante transacciones ilícitas de criptomonedas y así financiar su organización.

En ambas operaciones, el patrón que usaban para delinquir era el mismo:

- Creación de empresas de las cuales contrataban sus servicios una vez obtenidos el efectivo de la compraventa de criptomonedas.
- Suplantaron la identidad de los clientes ajenos a la investigación policial, que hacían un uso lícito de los cajeros de criptomonedas de sus locutorios para seguir blanqueando dinero sin, a priori, ser detectados.
- Uso de Hawala para el lavado de cierto dinero: Usaban este sistema de siglos de antigüedad, consistente en el intercambio de divisas entre dos personas, en los cuales aparecen dos intermediarios, llamados hawaladars. Este sistema permite enviar grandes cantidades de dinero, ya que hace que se desconozcan las cantidades de la transacción, la identidad de quienes manejan esas cantidades, ya que, una de las principales premisas de este método, es la de que los hawaladars nunca dejan registro ni de las transacciones ni de los usuarios que emplean este método. A continuación, se muestra una imagen que resume de forma clara y concisa el funcionamiento del hawala:



*Ilustración 28 – Funcionamiento de un Hawala*

- Transferencia de importantes cantidades monetarias a cuentas bancarias de empresas creadas por la organización, procedentes de empresas dirigidas por bandas criminales cercanas. Estas cantidades llegaban a su destino en forma de criptomoneda, normalmente Bitcoin, y se transferían entre las diferentes wallets que poseían para dificultar la trazabilidad de estos activos.



Estas dos operaciones se relacionaron gracias a los lazos familiares que presentaban los implicados en ambas. Cuando se les detuvo, fueron incautadas 9 millones de euros en criptomonedas, las cuales, habían sido transferidas numerosas ocasiones para evitar ser descubiertos. Esta cifra es de las mayores cantidades de dinero en criptomonedas, a fecha de la realización de este trabajo, requisadas por actividades ilícitas por un cuerpo de seguridad en España. A su vez, fueron sustraídos, además de las billeteras ya mencionadas, 11 vehículos y cerca de 17.000€ en metálico.

### 3.6.5 Operación Carbanak

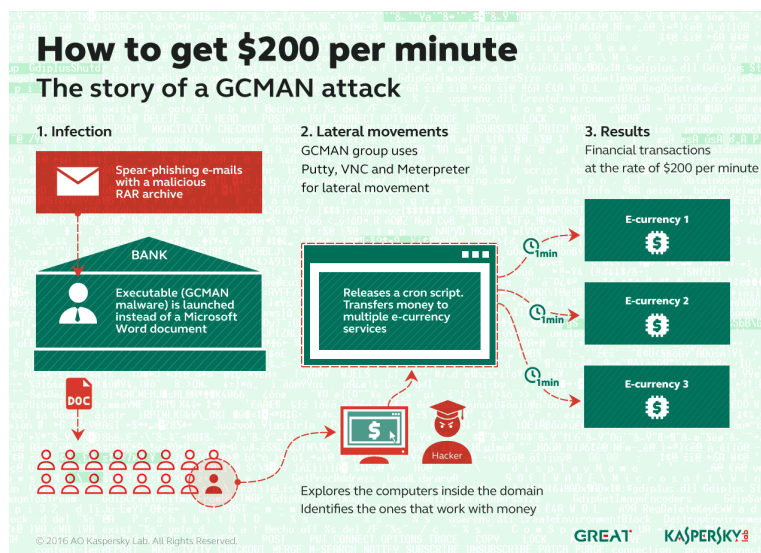
Para concluir con este punto, hablaremos del caso Carbanak, un caso en el que el principal causante del fraude era un hacker informático llamado Denis Tokarenko, aunque también se hacía llamar Denis Katana y en los Pandora Papers, un entramado policial que destapó, mediante un documento, que miles de personalidades en todo el mundo tenían gran parte de su riqueza en corporaciones inexistentes o en cuentas en el extranjero, el sujeto poseía el sobrenombre del zar de Bitcoin.

Esta operación estaba basada en un software informático malicioso que infectaba a miles de cajero en todo el mundo y estos se vaciaban de todo el efectivo que poseían en su interior. En estos casos, Denis tenía a sus “mulas” que acudían a dichos cajeros a recoger todo el efectivo y estos se encargaban de transformar todo este efectivo en Bitcoin en diversas cajas de cambio que poseían en los distintos países en ellos que operaban, como por ejemplo Alemania, España, Ucrania, Taiwán, Estados Unidos... entre otros muchos países afectados. Pero el principal afectado fue Rusia, ya que sus cajeros automáticos se encontraban con softwares de seguridad y antivirus muy desactualizados, lo que facilitaba la penetración de este tipo de virus informático, además de la peculiaridad que poseen los cajeros automáticos en este país, y es que suelen contener mucho más efectivo de lo que suele ser común en el resto del mundo.

Lo que lograba este software malicioso era penetrar en la red informática de la entidad bancaria en cuestión y enviar emails a los empleados de esta con archivos adjuntos, entre los que estaba el ransomware. Una vez alguno de los empleados se descargaba el archivo en su máquina, el virus buscaba en la red la máquina correspondiente al cajero automático. En el momento en que había accedido al cajero automático, todo esto tras pasar barreras de seguridad que se creían inalcanzables para las entidades, accedía al control del dispensador de efectivo y simplemente, cuando uno de los colaboradores de



Denis se encontrara presencialmente en el cajero, dicha máquina comenzaría a expulsar el dinero hasta llegar a vaciarse. Se estima que, al día, podían llegar a sacar alrededor de medio millón de dólares. A continuación, se muestra una imagen con el proceso de extracción del dinero de una forma esquematizada:



*Ilustración 29 – Proceso de ataque de Carbanak*

Para entender la magnitud de este caso, cabe mencionar que este caso fue archivado por la Interpol como un caso APT, que en castellano se traduce como Amenaza Persistente y Avanzada, un rango de amenaza que hasta la fecha solo se había empleado para estados, nunca para organizaciones criminales. Hablando de las cifras estimadas oficiales que se tasan que fueron sustraídas de los cajeros y, posteriormente, blanqueadas gracias a las criptomonedas son de unos 1.000 millones de dólares, e incluso algún portal especializado en ciberseguridad estima que esta cifra debería ser multiplicada hasta por diez veces la cifra oficial.

La policía nacional logró detener al supuesto jefe de la operación gracias a fallos en los procedimientos del blanqueo de criptomonedas por sus colaboradores, ya que, gracias al fallo de uno de estos, la policía logró obtener la dirección de su billetera de Bitcoin y, finalmente, fue detenido en la localidad de Alicante en el año 2018 en posesión de varias billeteras de bitcoin con una suma total de 15.000 bitcoin entre ellas, coches de lujo, varios inmuebles, joyas y un efectivo de varios millones de euros.





## 4. Conclusiones

En este apartado, se va a proceder con un resumen de todas y cada una de las conclusiones obtenidas en la realización de este Trabajo Fin de Grado. En adición a esto, se propone una posible continuación de esta investigación.

### 4.1 Conclusiones

Tras la realización de este proyecto, en el que se ha abarcado muchas facetas de la tecnología blockchain así como de las criptomonedas, por lo que, da pie a obtener las siguientes conclusiones:

- La tecnología blockchain es una tecnología muy robusta y fiable que no va a hacer sino evolucionar y estará cada vez más presente en diferentes aplicaciones en nuestras vidas. Por ejemplo, en documentos oficiales, en los que tener una prueba como la cadena de bloques de que dicho documento no ha sido modificado por agentes externos garantizará que se eviten muchos fraudes y falsificaciones.
- Las criptomonedas han cambiado el sistema financiero mundial. A pesar de que nacieran con el propósito de poseer dinero virtual y realizar operaciones con él de forma anónima, sin regulaciones de estados ni bancos mundiales, debido al uso delictivo que se les dan a las criptodivisas, es necesario que se implanten medidas más fuertes para combatir la delincuencia de forma anónima.
- La legalidad en España con los cajeros de criptomonedas necesita remodelarse y exigir, en cualquier caso, identificación por parte del usuario que quiere operar en BTM. Considero esta casuística porque la normativa actual resulta muy sencilla esquivarla y blanquear grandes cantidades de dinero sin ser descubierto.
- Las billeteras que poseen una mayor cantidad de criptomonedas de un tipo, como bitcoin, pueden llegar a influir en el valor que estas tienen. Por lo que, es importante seguir sus movimientos en caso de poseer criptoactivos para evitar perder dinero.
- Un usuario estándar que compra pequeñas cantidades de criptomonedas está a merced de las ballenas, pero, sobre todo, de los movimientos legales que hagan los gobiernos del mundo en el campo de las criptodivisas y de lo que publiquen en redes sociales personas muy influyentes en la sociedad, por lo que, no es muy



recomendable depositar porcentajes muy elevados del patrimonio total de un individuo.

- Es relativamente sencillo, a nada que se tengan unos conocimientos mínimos en informática, y, en concreto, programación, cometer actividades delictivas relacionadas con el mundo de las criptomonedas y lucrarse a costa de desconocidos y pasar desapercibido gracias a estafas o minado ilegal de criptomonedas.
- Será imprescindible conocer cómo funciona la tecnología blockchain y deberá ser implementado su estudio en enseñanzas superiores, ya que, gracias a la seguridad que aporta, se irá implementando en más sectores y se requerirá de personas expertas en el campo, ya que, a día de hoy, son insuficientes teniendo en cuenta el potencial de esta tecnología.
- Son necesarias más publicaciones y papers por parte de la comunidad mundial, si se quiere conseguir lo citado en el punto anterior. Esto es debido a que existen muy pocas publicaciones de relevancia al respecto y, por ende, es hasta cierto punto complejo obtener contenido de calidad, y esto se agrava en el caso de contenidos y publicaciones en castellano.

## 4.2 Trabajo futuros

Uno de los posibles trabajos futuros a plantear sería realizar un estudio mucho más avanzado de la tecnología blockchain, contando con la ayuda de expertos en el campo, y redactar un libro mucho más técnico y que suponga para la tecnología de la cadena de bloques lo que el libro de William Stallings *Sistemas operativos: aspectos internos y principios de diseño* supuso para los estudiantes y expertos en los sistemas operativos.

Por último, otro posible trabajo sería la creación de un bot que operara con tus criptomonedas por ti, en función de unas variables, las cuales pueden ser, menciones a las criptomonedas con las que se opera por parte de gente influyente, legislaciones y/o comunicados de entidades monetarias o gubernamentales con respecto a las criptomonedas y por último, y no por ello menos importante, los movimientos que realicen las grandes billeteras que operan con tus mismas criptodivisas. El objetivo de este bot sería que operara de forma independiente y nos evitara perder grandes cantidades de dinero e, incluso, que obtengamos ciertos beneficios.





## 5. Bibliografía

[1] Detectives Madrid, (2018, agosto 23), Historia de la informática forense.

<https://detectives-madrid.es/historia-informatica-forense-aplicacion/>

[2] Alonso, Rodrigo. (2022, abril 11). ¿Qué diferencias hay entre la memoria RAM y la memoria ROM?

<https://hardzone.es/tutoriales/componentes/memoria-ram-rom-diferencias/>

### **Bibliografía:**

Preukschat, A. *Blockchain: la revolución industrial de internet*. Ediciones 1ª Ed. Barcelona: Gestión 2000, 2017.

libro: Blockchain quick reference.

### **Enlaces:**

#### **Concepto blockchain.**

(1) IBM, ¿Qué es el blockchain?, Temas de Blockchain.

<https://www.ibm.com/es-es/topics/what-is-blockchain>

(2) Pastor, Javier. (2017, noviembre, 17, actualizado 2018, septiembre, 23). Qué es el blockchain: la explicación definitiva para la tecnología más de moda.

<https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda>

(3) Sáez Hurtado, Javier. (2022, marzo, 4). Qué es el blockchain y cómo funciona la tecnología blockchain.

<https://www.iebschool.com/blog/blockchain-cadena-bloques-revolucionaria-sector-financiero-finanzas/>

#### **Historia del blockchain:**

(4) Navarro, Wladimiro. Historia del blockchain, la solución a un problema.

<https://blog.addalia.com/historia-del-blockchain>



(5) Rodríguez, Nelson, (2018, diciembre, 3), Historia de la tecnología Blockchain: la Guía definitiva.

<https://101blockchains.com/es/historia-de-la-blockchain/>

(6) Academy Binance. (2018, diciembre, 6, actualizado 2021, agosto, 24). La Historia de Blockchain.

<https://academy.binance.com/es/articles/history-of-blockchain>

(7) Ámbito. (2021, mayo, 22). La primera compra con Bitcoin: 2 pizzas que hoy valdrían casi u\$s400 millones

<https://academy.binance.com/es/articles/history-of-blockchain>

(8) No me deja acceder a este link:

<https://academy.bit2me.com/que-es-hyperledger/>

### **Funcionamiento**

(9) No me deja acceder:

<https://academy.bit2me.com/como-funciona-blockchain-cadena-de-bloques/>

(10) Matesanz, Vanea, (2022, agosto, 4). Qué es el blockchain, cómo funciona y cuál es su relación con las criptos [Guía Fácil]

<https://www.finect.com/usuario/vanesamatesanz/articulos/que-blockchain-criptomonedas-guia-facil#:~:text=El%20blockchain%20es%20un%20ecosistema%20de%20cadenas%20de%20bloques.&text=B%20C3%A1sicamente,%20blockchain%20es%20una%20tecnologia%20C3%ADa,forma%20segura,%20r%20C3%A1pida%20y%20descentralizada>

### **Elementos.**

(11) No puedo acceder a este link:

<https://academy.horizen.io/es/technology/beginner/the-elements-of-a-blockchain/>

(12) Perez, Isabel, Blockchain: bloques, transacciones, firmas digitales y hashes

(13) <https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/>

(14) Bit2Me Academy, ¿Qué es un nonce?



<https://academy.bit2me.com/que-es-nonce/>

(15) Bit2Me Academy, ¿Qué es el bloque génesis? (Genesis block).

<https://academy.bit2me.com/que-es-bloque-genesis/>

### **Qué es un cajero bitcoin:**

(16) Deer, Marcel, (2022, abril, 23). Cómo usar un cajero automático de Bitcoin

<https://es.cointelegraph.com/news/how-to-use-a-bitcoin-atm>

(17) Cointelegraph, Cajeros automáticos de Bitcoin: Guía para principiantes sobre los cajeros de Bitcoin.

<https://es.cointelegraph.com/bitcoin-for-beginners/bitcoin-atms-a-beginners-guide-to-bitcoin-teller-machines>

(18) El Español, (2022, enero, 13). España será el tercer país del mundo con más cajeros de bitcoin al acabar el año

[https://www.elespanol.com/invertia/mercados/criptomonedas/20220113/espana-tercer-pais-mundo-cajeros-bitcoin-acabar/642186046\\_0.html](https://www.elespanol.com/invertia/mercados/criptomonedas/20220113/espana-tercer-pais-mundo-cajeros-bitcoin-acabar/642186046_0.html)

(19) Campillo, Rafael (2018, diciembre, 13). ¿Qué es KYC (Know Your Customer)? ¿y AML (Anti-money Laundering)?

<https://www.mobbeel.com/blog/que-es-kyc-know-your-customer-y-aml-anti-money-laundering/#:~:text=Normativas%20KYC%20/%20AML&text=Es%20una%20directiva%20dirigida%20al,de%20la%20financiaci%C3%B3n%20del%20terrorismo>

(20) Ramírez, Adrián, (2022, julio, 7). Este el límite de dinero que puedes ingresar en el banco sin dar explicaciones

<https://www.laopiniondemalaga.es/economia/2022/07/12/cuanto-dinero-puede-ingresar-maximo-banco-sin-justificar-dv-59590382.html>

### **Legalidad Bitcoin:**

(21) Bit2me Academia. Impuestos: Hacienda y Bitcoin ¿qué declarar en España por tener criptomonedas?

<https://academy.bit2me.com/hacienda-espana-bitcoin-criptomonedas-impuestos/>

(22) Cuentas claras, by Abanca, (2022, abril, 25) ¿Es obligatorio declarar criptomonedas?





<https://www.cuentasclaras.es/actualidad/declarar-criptomonedas/>

(23) N26, (2022, marzo, 27) La legislación del minado de criptomonedas en España.

<https://n26.com/es-es/blog/minar-criptomonedas-espana#:~:text=Las%20criptomonedas%20son%20legales%20en,Tributaria%20en%20su%20declaraci%C3%B3n%20sobre>

(24) Ius & Lex Abogados. Bitcoin en España. ¿Es legal el Bitcoin en España?

<https://www.iuslexabogadosmadrid.com/bitcoin-situacion-legal-en-espana/>

(25) Estrategias de inversión, (2022, julio, 28). ¿Es rentable ser minero de Bitcoin al precio actual?

<https://www.estrategiasdeinversion.com/actualidad/noticias/bolsa-eeuu/es-rentable-ser-minero-de-bitcoin-al-precio-actual-n-545575>

(26) Pysnoticias, (2022, abril, 5) ¿Las criptomonedas son legales en estados unidos?

<https://pysnoticias.com/las-criptomonedas-son-legales-en-estados-unidos/>

(27) González, Glenda (2022, abril, 29) Ya es posible pagar facturas e impuestos con bitcoin en EE. UU.

[criptonoticias.com/comunidad/adopcion/ya-posible-pagar-facturas-impuestos-bitcoin-traves-bitrefill-eeuu/](https://criptonoticias.com/comunidad/adopcion/ya-posible-pagar-facturas-impuestos-bitcoin-traves-bitrefill-eeuu/)

(28) Vozpópuli, (2022, julio, 28) ¿Es rentable ser minero de Bitcoin al precio actual?

<https://www.estrategiasdeinversion.com/actualidad/noticias/bolsa-eeuu/es-rentable-ser-minero-de-bitcoin-al-precio-actual-n-545575>

(29) La Vanguardia, (2022, marzo, 1) China castigará hasta con 10 años de prisión cualquier intercambio de criptomonedas

<https://www.lavanguardia.com/tecnologia/actualidad/20220301/8089408/china-castigara-10-anos-prision-intercambio-criptomonedas-pmv.html>

(30) Maestre Abogados, () Cajeros Bitcoin y el Blanqueo de capitales

<https://www.maestreabogados.com/cajeros-bitcoins-blanqueo-capitales/>

(31) Nives, Vicente, (2021, septiembre, 24) China asesta el golpe definitivo a las criptomonedas: "Bitcoin o ethereum son ilegales y no deben usarse"

<https://www.eleconomista.es/mercados-cotizaciones/noticias/11404958/09/21/China-asesta-el-golpe-definitivo-a-las-criptomonedas-Bitcoin-o-ethereum-son-ilegales-y-no-deben-usarse.html>



### Casos de delitos:

- (32) Pérez, Hannah, (2021, octubre, 5) Pandora Papers mencionan a un “zar de Bitcoin” sentenciado  
<https://www.diariobitcoin.com/criptomonedas/pandora-papers-mencionan-zar-de-bitcoin-sentenciado/>
- (33) Alsedo, Quico, (2018, marzo, 27) Cae en España el 'hacker' de los 10.000 millones, el ciberladrón más importante del mundo: Carbanak  
<https://www.elmundo.es/espana/2018/03/26/5ab8bdeb268e3ed01d8b4636.html>
- (34) González, Daniel, (2021, octubre, 2) Cómo funciona la hawala, el sistema financiero informal con siglos de historia que mueve millones de dólares en el mundo  
<https://www.bbc.com/mundo/noticias-58735962>
- (35) Pastor, Javier, (2019, mayo, 10) La Guardia Civil detiene a una banda en España que blanqueó 9 millones de euros a través de las criptodivisas  
<https://www.xataka.com/criptomonedas/guardia-civil-detiene-a-banda-que-blanqueaba-dinero-a-traves-criptodivisas>
- (36) Pérez, Enrique, (2019, diciembre, 9) De Silk Road a la operación "Kampuzo": las incautaciones de criptomonedas más importantes para perseguir al crimen organizado  
<https://www.xataka.com/criptomonedas/silk-road-a-operacion-kampuzo-incautaciones-criptomonedas-importantes-para-perseguir-al-crimen-organizado>
- (37) Policía Nacional,(,), Desarticulada la rama económica responsable del 'virus de la Policía' y que había comprometido la seguridad de 1.500 empresas en España  
[https://www.policia.es/\\_es/comunicacion\\_prensa\\_detalle.php?ID=6790](https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=6790)
- (38) Segal, David, (2014, enero, 30) Ross Ulbricht, el joven detrás de Silk Road  
[https://elpais.com/tecnologia/2014/01/30/actualidad/1391077921\\_678889.html](https://elpais.com/tecnologia/2014/01/30/actualidad/1391077921_678889.html)
- (39) Esparragoza, Luis, (2021, enero, 27) Hace 10 años nació Silk Road, primer mercado de la dark web que aceptó bitcoin  
<https://www.criptonoticias.com/comunidad/10-anos-nacio-silk-road-primer-mercado-darkweb-acepto-bitcoin/>
- (40) Policía Nacional, (2018, marzo, 16) La Policía Nacional se especializa en la lucha contra el ilícito uso de las criptomonedas y el dinero virtual  
[https://policia.es/\\_es/comunicacion\\_prensa\\_detalle.php?ID=4573](https://policia.es/_es/comunicacion_prensa_detalle.php?ID=4573)
- (41) Consejo de Europa, (2022, junio, 29) Lucha contra el blanqueo de capitales: se alcanza un acuerdo provisional sobre la transparencia de las transferencias de cryptoactivos



<https://www.consilium.europa.eu/es/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/>

### **Aplicaciones Blockchain:**

- (42) Blanco, Luis Jesús,(2021, febrero,13) Elecciones catalanas con blockchain: un test piloto de voto digital con Vocdoni  
<https://es.beincrypto.com/elecciones-catalanas-blockchain-test-piloto-voto-digital-vocdoni/>
- (43) Criptomoneda Ninja,( ), Aplicaciones, utilidad y casos de uso del blockchain con ejemplos de 2022  
<https://criptomoneda.ninja/aplicaciones-blockchain/>
- (44) Cuadrado, Carlos, 2020. Octubre, 14) Aplicaciones de blockchain – 11 usos de blockchain que no conocías  
<https://www.armadilloamarillo.com/blog/aplicaciones-de-blockchain-11-usos-de-blockchain-que-no-conocias/>

### **Criptomonedas:**

- (45) Banco Santander, (2022, mayo, 24) Guía para saber qué son las criptomonedas  
<https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas>
- (46) Sáez, Javier, (2022, mayo, 4) Las 10 criptodivisas (o criptomonedas) con más futuro  
<https://www.iebschool.com/blog/criptodivisas-criptomonedas-invertir-finanzas/>
- (47) Bit2meAcademy,( ), ¿Qué es un exchange de criptomonedas?  
<https://academy.bit2me.com/que-es-exchange-criptomonedas/>

### **Caso Práctico:**

- (48) La Mastra, Sebastián,(2021, marzo,17) ¿Camarón, pulpo o ballena?: cómo se los llama a quienes tienen bitcoin y por qué el precio sube y baja tan de golpe  
<https://www.iproup.com/economia-digital/20838-bitcoin-que-son-las-ballenas-y-como-impactan-en-el-precio>
- (49) Cairo, Ariana, (2022, agosto, 18) Las últimas 24 horas de las ballenas Bitcoin (BTC) ¿Qué sabemos al respecto?



<https://criptotendencia.com/2022/08/18/las-ultimas-24-horas-de-las-ballas-bitcoin-btc-que-sabemos-al-respecto/>

- (50) Cairo, Ariana, (2021, octubre, 11) ¿Las ballenas Bitcoin influenciaron el alza de BTC?

<https://criptotendencia.com/2021/10/11/las-ballas-bitcoin-influenciaron-el-alza-de-btc-2/>

- (51) Blackler, Brandie, (2022, julio, 14) ¿Qué es un ETF de Bitcoin? Ventajas y desventajas | Cómo invertir en ellos

<https://admiralmarkets.com/es/education/articles/criptocurrencies/que-es-un-etf-de-bitcoin>

- (52) Caridi, Valentino, (2021, octubre, 15) Bitcoin (BTC), Ethereum (ETH). Análisis del 15 de octubre de 2021

<https://www.cointribune.com/es/criptomercados/bitcoin-btc-ethereum-eth-analisis-del-15-de-octubre-de-2021/>

# Universidad de Alcalá Escuela Politécnica Superior



ESCUELA POLITECNICA  
SUPERIOR



Universidad  
de Alcalá