Explorando las huellas digitales de los criptoactivos mediante fuentes abiertas

Exploring Cryptoasset Fingerprinting through Open Sourcing

Ana Díaz Bernardos[1]
Policía Nacional.
ana.diaz.bernardos@gmail.com

DOI: https://doi.org/10.14201/cp.31816
Recibido: 21-02-23 | Aceptado: 10-04-24

Resumen

El uso de los criptoactivos ha experimentado un notorio aumento en los últimos años, introduciendo consigo una serie de conceptos novedosos en la economía española. Este fenómeno ha permitido a los usuarios operar de nuevas formas, lo que entraña una serie de ventajas y riesgos inherentes que deberían conocer. Las ventajas asociadas a estos activos financieros han supuesto un reclamo que ha hecho que cada vez más individuos hagan uso de los mismos. Esta atracción se ha traducido en una mayor presencia de los criptoactivos en las investigaciones policiales, utilizados como medio de pago, promocionados como inversiones con rendimientos rápidos e incluso utilizados en operativas de blanqueo de capitales procedentes de todo tipo de delitos. La versatilidad en su utilización y su cada vez más marcada presencia en la sociedad plantea desafíos significativos para las autoridades, que deben, sin limitar las oportunidades legítimas que los criptoactivos pueden ofrecer, adaptar su legislación para salvaguardar a la población frente a los posibles riesgos asociados a los criptoactivos y fomentar su uso responsable y seguro. En este sentido, las Fuerzas y Cuerpos de Seguridad están en la obligación de proteger a los ciudadanos en este nuevo ámbito virtual que se presenta.

---

1. Graduada en Derecho y máster en Justicia Criminal. Policía investigadora en la Brigada Central de Delincuencia Económica y Fiscal, de la Unidad Central de Delincuencia Económica y Fiscal, Comisaría General de Policía Judicial de la Policía Nacional.

Palabras clave
Criptoactivos; Trazabilidad; Blockchain; Bitcoin; Cluster; Ethereum; Token; Herramientas; Billetera; Exchange.

Abstract
The use of cryptoassets has experienced a notable increase in recent years, introducing a series of new concepts into the Spanish economy. This phenomenon has allowed users to operate in new ways, which comes with a number of inherent advantages and risks that they should be aware of. The advantages associated with these financial assets have created a demand that has caused more and more individuals to make use of them. This attraction has translated into a greater presence of cryptoassets in police investigations as they are increasingly used as a means of payment, promoted as investments with quick returns and even used in money laundering operations from all types of crimes. The versatility in their use and their increasingly marked presence in society poses significant challenges for authorities, who must, without limiting the legitimate opportunities that cryptoassets can offer, adapt their legislation to safeguard the population against the possible associated risks and promote their responsible and safe use. In this sense, the Security Forces are obliged to protect citizens in this new virtual environment presented to us.

Keywords
Cryptoassets; Traceability; Blockchain; Bitcoin; Cluster; Ethereum; Token; Tools; Wallet; Exchange.

1 Interés por los criptoactivos

La Comisión Nacional del Mercado de Valores (CNMV), organismo nacional competente para la supervisión de los mercados, afirmó en el año 2021 que «los criptoactivos, incluyendo las criptomonedas y la tecnología que les da soporte, pueden ser elementos que dinamicen y modernicen el sistema financiero en los próximos años» (Comunicado conjunto de la CNMV y

del Banco de España sobre el riesgo de las criptomonedas como inversión, 2021, p. 1). Finalizando el año 2023, podríamos afirmar que es una realidad que estos elementos están en vías de hacerlo.

Si esto sucede es fundamental dotar a los ciudadanos de información válida y veraz sobre las ventajas y los riesgos que presenta operar con ellos, así como dotar a las Fuerzas y Cuerpos de Seguridad de los conocimientos necesarios para enfrentarse al uso indebido que los delincuentes puedan hacer de los mismos. En este sentido, el presente artículo pretende aportar ciertos conocimientos básicos al lector que le permitan dar respuesta a la realidad actual e intentar eliminar, o al menos disipar, la creencia de que la operativa con criptoactivos llevada a cabo por los delincuentes es demasiado compleja para enfrentarla.

Han sido varias instituciones, y no solo nacionales, las que han advertido desde hace algunos años de los riesgos de operar con criptoactivos, hecho que se ha visto incentivado por el interés, cada vez más creciente, de la sociedad mundial por estos activos financieros. Son dos los motivos principales que convierten a los criptoactivos en un producto de alto riesgo para el inversor minorista y que coinciden en destacar muchas de las entidades e instituciones financieras: su extrema volatilidad y la complejidad para el inversor minorista.

En este sentido, las autoridades europeas supervisoras (ESA), entre las que se encuentra la Autoridad Europea de Valores y Mercados (ESMA), advierten a los inversores minoristas de que muchos criptoactivos no son adecuados como inversión ni medio de pago o intercambio, ya que revisten un marcado carácter especulativo. Así mismo, les instan a preguntarse si podrían permitirse perder todo el dinero invertido, asumir un alto riesgo debido al alta volatilidad de estos activos, si han consultado si los bróker o empresas con las que operan están advertidas por los organismos nacionales competentes para ello o si disponen de medidas adecuadas para proteger los dispositivos que utilizan para operar con criptoactivos, ya que todos ellos son riesgos específicos asociados a estos activos financieros.

En el caso de España, el organismo nacional competente para la supervisión de los mercados es la CNMV; en el año 2018 informó en un comunicado conjunto con el Banco de España de los riesgos asociados a estos activos de la siguiente manera:

> La CNMV y el Banco de España tienen entre sus prioridades ofrecer información al público para que los inversores y usuarios de servicios financieros estén en condiciones de afrontar con confianza la creciente complejidad del entorno financiero. En consecuencia, ambas autoridades creen oportuno publicar este comunicado, dirigido a inversores y en general a usuarios financieros minoristas. Es esencial que quien decida comprar este tipo de activos digitales o invertir en productos relacionados con ellos considere todos los riesgos asociados y valore si tiene la información suficiente para entender lo que se le está ofreciendo. En este tipo de inversiones existe un alto riesgo de pérdida o fraude. (Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «de ofertas iniciales de criptomonedas» [ICO], 2018, pp. 2 y 3)

Aunque los criptoactivos llevan más de una década en el panorama mundial, fue en el año 2021 cuando varios criptoactivos, principalmente el *bitcoin* y el e*ther*, experimentaron una elevada volatilidad en sus precios, lo que llevó a que aumentase de manera muy significativa su publicidad, encaminada a atraer inversores, lo que impulsó a más personas a operar con ellos. Como consecuencia ha llevado aparejado un aumento de los delitos relacionados con las inversiones en criptoactivos, también favorecido por la escasa cultura de inversión.

Este hecho habría sido uno de los motivos que ha generado la necesidad de muchos países de ponerse al día en materia de criptoactivos, colocándolos en una posición preferente en la agenda normativa de esos. En España, en el año 2022, la institución supervisora de los mercados dispuso la Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores, relativa a la publicidad sobre criptoactivos presentados

como objeto de inversión, que tiene por objeto desarrollar las normas, principios y criterios a los que debe estar sujeta la actividad publicitaria de los criptoactivos. Además, en su informe anual publicado recientemente, informó que, en aplicación de esta cCircular, gestionó más de cien expedientes informativos y analizó casi mil piezas publicitarias.

Más recientemente, y en el mismo sentido, la Unión Europea ha aprobado el Reglamento de Mercados de Criptoactivos (MICA) [Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos], que se ha convertido en el primer instrumento regulador de estos activos, pero que no será de aplicación hasta el 30 de diciembre de 2024, como dice su artículo 149. Esta norma ha dado cobertura jurídica a los criptoactivos y establecido unas reglas comunes a todos los operadores en la Unión Europea, pero por el momento ha dejado fuera de esta cobertura a los llamados NFT (*tokens* no fungibles) y las DeFi (operadores descentralizados).

Para dar por finalizado este apartado, que, entre los riesgos descritos y la carrera de las instituciones financieras por dotar de un marco jurídico y de protección al inversor de criptoactivos, puede generar en el lector una alarma social que quedaría bastante lejos de la realidad. Cabe decir que la tecnología *Blockchain* y los criptoactivos no tienen por qué constituir un problema para la sociedad española ni mundial. Estos elementos tienen el potencial de optimizar las transacciones que todo ciudadano realiza regularmente, otorgándoles mayor transparencia y seguridad al estar respaldadas por una base de datos compartida y descentralizada.

Así, adquirir conocimientos sobre trazabilidad resulta de gran utilidad no solo desde la perspectiva policial, sino también como ciudadano inmerso en una sociedad donde la tecnología *Blockchain* y los criptoactivos ganan cada vez más terreno. De esta manera, las Fuerzas y Cuerpos de Seguridad pueden rastrear fondos fraudulentos y localizar a los criminales que abusan de estos elementos y, al mismo tiempo, los ciudadanos pueden verificar el estado de sus transacciones mediante esta tecnología, que ha llegado para quedarse.

2 Aproximación conceptual

Los siguientes conceptos tienen como objetivo proporcionar al lector las capacidades básicas para comprender la operativa con criptoactivos. Estos conceptos esenciales se presentan de manera sucinta, ya que la intención del presente artículo no es formar expertos en inversión de criptoactivos, sino brindar al lector de unas nociones básicas e introducirlo en este interesante mundo digital.

2.1 ¿Qué es una criptomoneda?

Las criptomonedas son monedas virtuales, intercambiables y descentralizadas, basadas en la criptografía, lo que les permite garantizar su titularidad y asegurar la integridad de las transacciones.

No existen de forma física y tampoco están identificadas físicamente con una cifra o código, queda constatada su existencia a través de un registro de transacciones, contenido dentro de la llamada cadena de bloqueos o *blockchain*.

En la actualidad existen multitud de criptomonedas; las más populares son *bitcoin* y *ether*.

2.2 ¿Qué es un *token*?

Al igual que las criptomonedas, los *tokens* son activos digitales criptográficos, que pueden ser creados por cualquier usuario privado, intercambiados y también funcionan usando la tecnología *Blockchain*.

Los *tokens* necesitan una *blockchain* y una criptomoneda que permita su desarrollo, es decir, los *tokens* no tienen su propia *blockchain* o cadena de bloques, sino que circulan por aquellas que permitan su registro; también necesitan un contrato que los defina.

2.3 ¿Qué es la *blockchain* o cadena de bloques?

La *blockchain* o cadena de bloques es un tipo de base de datos descentralizada, en la que los datos se registran, comparten y sincronizan a través de una red distribuida de ordenadores llamados nodos. Estos nodos interactúan entre sí, sin necesidad de un servidor central, lo que permite el mantenimiento de la *blockchain* sin necesidad de intermediación de terceros.

Existen diferentes tipos de *blockchain* o cadenas de bloques:

- Pública: son aquellas que son accesibles desde Internet. Un ejemplo serían la *Blockchain* de *Bitcoin*, *Ethereum* o *Tron*.

  El funcionamiento de esta red es abierto, esto significa que todos los datos registrados en la *blockchain* pública están disponibles y cualquier usuario puede revisarlos.

- Privada o permisionada: con la evolución de la tecnología *blockchain* se crearon las redes privadas o permisionadas, cuya principal diferencia con las públicas es que las *blockchain* privadas o permisionadas dependen de un servidor central que controla todas las acciones y no son accesibles a todas las personas.

2.4 ¿Qué es un monedero de criptoactivos, billetera o *wallet*?

Un monedero de criptoactivos, también llamado billetera o *wallet* en inglés, es una herramienta que permite al usuario almacenar las claves públicas y privadas, que son las que controlan el acceso a sus criptoactivos y le permiten enviar y recibir pagos.

Es importante señalar que los monederos o *wallet* no contienen criptoactivos. Los monederos lo que contienen son las claves privadas que permiten al usuario operar con sus activos y que están asociadas a la clave pública correspondiente y esta a la dirección.

Para una mejor comprensión se explican los siguientes conceptos:

- Clave privada: es una clave de dominio privado, a la que solo debe tener acceso el propietario de los criptoactivos. La clave privada le va a otorgar la propiedad al usuario y el acceso a sus activos. Funciona como un pin o una contraseña.

- Clave pública: asegura la propiedad de la dirección, que no del monedero, y se puede compartir sin riesgo a que accedan a los fondos del usuario. Esta se deriva de la clave privada y sirve para verificar la autenticidad de las transacciones.

- Dirección o *address* en inglés: es un código compuesto por números y letras, que presentará un formato según el criptoactivo con el que se opere, por lo que no es posible enviar *ether* (ETH) a una dirección *bitcoin* (BTC) y viceversa.

  La dirección indica el origen o destino de un pago del criptoactivo en el que se esté operando y es el código visible en la *blockchain*.

  Desde un monedero se pueden crear varias direcciones a las que enviar y recibir fondos.

  Si el usuario opera con el criptoactivo *bitcoin* (BTC) las direcciones presentarían el siguiente formato comenzando por bc1, 1 o 3. Los siguientes ejemplos se han obtenido aleatoriamente de fuentes abiertas; ejemplos:

  - bc1qc026d7ght3cdjd0ugwvc23mfqsag0q2hvw0l3x
  - 1AdFdaGhGmNQiobrvdnKHPyN9yMuGgfHiF
  - 3EuMyVyv9M1yShgsUscPqT6MZmFZiFN2LGQ

  Si opera con la criptomoneda *ether* (ETH) o los *tokens* que operan en la Red *Ethereum*, el inicio de las direcciones sería siempre 0x, por ejemplo:

  - 0xAe6aEEbfC0E060F992010D596F4A7276f182D444

Si lo hace con la criptomoneda *tron* (TRX) se vería así:

- TYnNCewqZXmsVB6t8NMtYdGYtC38Sc250N

Y así, según el criptoactivo con el que se opere.

- Frase semilla o *seed* en inglés: en la actualidad muchos monederos de criptoactivos derivan sus claves de una única, conocida como frase semilla o *seed*. El propietario de la frase semilla puede reconstruir las claves privadas, desde las que se derivan las claves públicas y de estas las direcciones, y así disponer de los fondos.

  La frase semilla está formada por una lista de palabras en inglés, de 12 a 36 palabras en inglés, que incluye toda la información necesaria para recuperar un monedero o *wallet* de criptoactivos.

2.5 Formas de depósito de los criptoactivos

Pueden ser un dispositivo físico de *hardware*, un programa informático o un servicio que alberga las claves. La principal diferencia es la forma de custodiar la clave privada del monedero de criptoactivos.

- *Exchanges*: las claves privadas están en manos de un tercero que es una institución financiera o una plataforma de intercambio de criptoactivos llamada *exchange*. Las exchanges no son monederos, sino que el usuario posee una cuenta que les brinda una descripción general de sus transacciones y tiene la capacidad para recibir y enviar fondos. Algunos ejemplos de Exchange son *Kraken*, *Binance*, *Coinbase* o *Huobi*.

- Monederos con custodia: al igual que ocurre con las exchanges, en los monederos con custodia también la clave privada está en manos de un tercero. Algunos ejemplos son los llamados monederos *online* o en línea que serían calificados como monederos calientes o *hot wallet* porque están conectados a Internet, y que son páginas web que se asimilan al banco online. Por ejemplo, *Xapo, Bitpay* o *Blockchain.com*.

- Monedero sin custodia o con custodia propia: permite a los usuarios conservar y utilizar sus criptoactivos ya que son ellos mismos quienes custodian sus claves privadas. Algunos ejemplos serían:

    - Los monederos fríos: son monederos que no están conectados a Internet. Son los monederos de papel, en el que el propietario escribe sus claves privadas en un papel y las custodia. El principal problema de este tipo de monederos es que, si se pierde el apunte, el propietario perdería el acceso y el control de sus criptoactivos.

    - Los monederos mixtos: son los monederos *hardware* como *Trezor, Ledger* o *Keepkey*, entre otros; estos dispositivos físicos albergan las claves del monedero del usuario, pero es este quien custodia el dispositivo. Hablamos de monederos mixtos y no fríos porque para realizar una transacción es necesario conectarlos a Internet.

    - Los monederos calientes o *hot wallet*: son aquellos que están conectados a Internet de manera continua. Por ejemplo, *Electrum, Jaxx, Bitcoin Core* o *Atomic*, que son aplicaciones que el usuario instala en su dispositivo móvil, *tablet* u ordenador y puede operar con sus criptoactivos a través de ellos.

2.6 ¿Qué es una transacción de criptoactivos?

Una transacción es la transferencia de fondos entre usuarios en el ecosistema de los criptoactivos, que queda registrado en la cadena de bloques o *blockchain*.

Una transacción incluye:

- La identificación (*ID*) de la transacción o *hash*, como se puede observar en la Figura 1.

Figura 1: Identificación de la transacción o *hash*, término informático que se refiere a la huella digital. El *hash* permite verificar el contenido de una transacción.

Nota. Recorte aleatorio de un *hash* tomando del buscador público *Blockchair* (*Blockchair* 2023).

- El número de criptoactivos enviados; un ejemplo sería el recogido en la Figura 2.

Figura 2: Cantidad de criptoactivos enviados y su equivalencia en dólares.

Nota. Recorte aleatorio del valor de los activos enviados del buscador público *Etherscan* (*Etherscan*, 2023a).

- La comisión pagada por la transacción (*fee* en inglés), como se observa en la Figura 3.

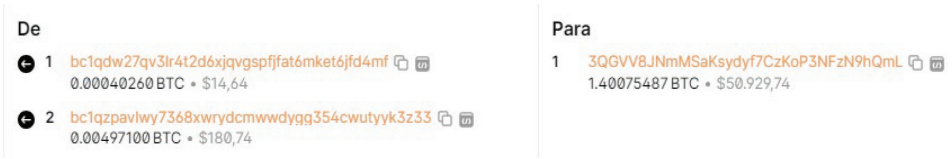
Figura 3: Comisión o *fee* cobrado por la transacción operada.

Nota. Recorte aleatorio de la comisión de la transacción del buscador público *Etherscan* (*Etherscan*, 2023a).

- Entradas o dirección de remitente.

  En el caso de las transacciones operadas con *Bitcoin* puede haber más de una entrada o dirección de remitente, como se observa en la Figura 4.

Figura 4: Direcciones de *Bitcoin* que indican el origen (las que se encuentran a la derecha de la imagen) y destino (las que se encuentran a la izquierda de la imagen) de un pago de *bitcoin*, y son el código visible en la *blockchain*.



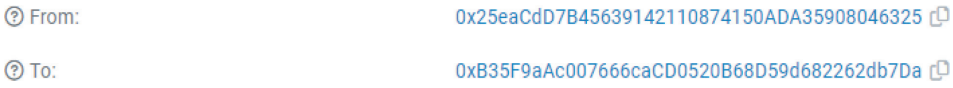
Nota. Recorte aleatorio de una transacción del buscador público *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Esto se debe a que la cantidad de fondos no es suficiente para enviar el pago o a que el remitente ha decidido usar varias

direcciones para enviar el pago. Se explica más detenidamente en el apartado de trazabilidad de *Bitcoin*.

En las transacciones operadas en la Red *Ethereum* solo figura una dirección de entrada o de remitente por transacción *(From)*, como se observa en la Figura 5:

Figura 5: Dirección remitente y dirección de destino de la transacción.



Nota. Recorte aleatorio de una transacción tomado del buscador público *Etherscan* (*Etherscan*, 2023a).

- Salidas o dirección del destinatario.

  En el caso de las transacciones operadas con *Bitcoin* puede haber más de una salida o dirección de destinatario, como se puede observar en la Figura 6.

Figura 6: Direcciones de *Bitcoin*.

Nota. Recorte aleatorio de una transacción del buscador *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Podría tratarse de dos envíos o pagos, o que una salida se correspondiese al pago y otra al cambio (sobrante).

Bitcoin utiliza una tercera dirección llamada dirección de cambio, que se genera porque no se envía la cantidad exacta de *bitcoin* al destinatario, dando lugar a un sobrante que se envía a la dirección de cambio, que también pertenece al remitente. Se explica detenidamente más adelante.

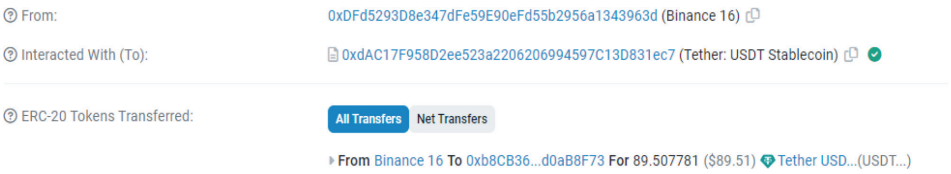
En las transacciones operadas en la Red *Ethereum* solo hay una dirección de salida o de destinatario *(To)* por transacción, como se observa en la Figura 7.

Figura 7: Dirección remitente y dirección de destino de la transacción.

Nota. Recorte aleatorio de una transacción tomado del buscador público *Etherscan* (*Etherscan*, 2023a).

Caso especial es cuando las transacciones se realizan con el activo *tether* (USDT) ya que va a figurar la dirección del contrato o *smart contract* de *Tether* (*tether:* USDT *Stablecoin*). En este caso la dirección de destino es la que se contiene en el apartado *ERC-20 Tokens Transferred*, señalada en la Figura 8.

Figura 8: Transacción operada en la Red *Ethereum* con el activo *tether* (USDT).



Nota. Recorte aleatorio de una transacción con USDT tomado del buscador público *Etherscan* (*Etherscan*, 2023b).

3 Trazabilidad por fuentes abiertas

A continuación, se presentan algunas herramientas de código abierto que permiten al usuario rastrear criptoactivos, junto con algunos trucos que facilitarán esta tarea. Además, se explican qué son los *exchanges*, elementos importantes para obtener información.

3.1 Propuesta de herramientas

Existen diferentes herramientas o buscadores de código abierto, accesibles a través de Internet, que sirven para realizar la trazabilidad de transacciones con criptoactivos. Algunas de ellas son las siguientes:

- *Blockchain Explorer*. Esta herramienta sirve para trazar las transacciones de varios criptoactivos como *bitcoin* (BTC) o *ether* (ETH). También permite ver la capitalización de estos activos, entre otras funcionalidades.

- *Blockchair*. Este buscador permite trazar transacciones de la Red *Bitcoin* de manera muy similar a *Blockchain Explorer*.

- *Wallet Explorer*. Esta herramienta permite descubrir los flujos en la Red *Bitcoin* e indica si la dirección que se ha introducido pertenece a un *cluster*, el resto de direcciones asociadas al mismo y si se trata de una cartera dentro de algún servicio identificado como una exchange o proveedor de criptoactivos.

  Esta herramienta resulta de utilidad para conocer a qué exchange se debe dirigir el investigador para solicitar más información sobre las transacciones de interés, pero se ha de tener en cuenta que está desactualizada por lo que no listará algunas direcciones pertenecientes a proveedores de servicios de criptoactivos.

- *Etherscan*. Esta herramienta permite trazar todas las transacciones dentro de la Red *Ethereum*, entre las que están las operadas con el activo *ether* (ETH) y los *tokens* ERC-20, como *tether* (USDT).

- *Tronscan*. Esta herramienta permite trazar las transacciones operadas en la Red *Tron*, entre las que están las operadas con la criptomoneda *tron* (TRX) y también las operadas con *tokens* que utilicen esta red. Este buscador permite trazar transacciones de la Red *Tron* de manera muy similar a *Etherscan*.

3.2 Las *exchanges*

Las *exchanges* o casas de cambio son proveedores de servicios de criptoactivos que permiten operar con estos activos de forma sencilla, por este motivo son muchos los usuarios que hacen uso de ellos. «Estos exchanges son necesarios en el mundo electrónico, ya que son la manera más sencilla de cambiar criptomonedas

y hacer trading con ellas, o lo que es lo mismo, comprar y vender estos activos cotizados» (Callejo y Ronco, 2020, p. 89).

Existen varios tipos de *exchange*. Los e*xchanges* centralizados son entidades que ofrecen servicios financieros con criptoactivos y se establecen como intermediarios entre los usuarios que operan con ellos ya que facilitan la compra de criptoactivos con dinero fiat a través de una simple transferencia o pago con tarjeta de crédito. Además, disponen de liquidez y un alto número de paridades entre criptoactivos y dinero fiat. Algunos de ellos son *Binance*, *Kraken*, *Houbi, OKX* o *Coinbase*.

Una alternativa a este tipo de *exchanges* son los llamados *exchanges* descentralizados o DEX, que son plataformas de código abierto que únicamente ofrecen el espacio digital donde se produce el intercambio de criptoactivos sin intermediarios, es decir, no hacen de intermediarios entre los usuarios. De esta manera los criptoactivos no se depositan en estas entidades en ningún momento, como sí sucede en los centralizados. Son menos los usuarios que hacen uso de este tipo de *exchanges* debido a que su planteamiento resulta más complejo que el de los *exchanges* centralizados. Algunos de ellos son *SusiSwap*, *PancakeSwap* o *Uniswap*.

3.3 Bitcoin y la Red *Ethereum*

A continuación, se explica cómo rastrear por fuentes abiertas las redes *Bitcoin* y *Ethereum*.

3.3.1 Bitcoin

Bitcoin es un activo, un protocolo, un *software* de código y una red entre pares (P2P) creada en 2009. Su *White paper*, o documento técnico que explica el funcionamiento de esta red, se puede consultar a través de Internet. Como ya se ha indicado, una herramienta de consulta de las transacciones operadas con esta criptomoneda es *Blockchain Explorer*.

Cabe introducir aquí el concepto de *altcoins* o monedas alternativas, que son todas aquellas que no son *bitcoin*; existen

multitud de ellas y se pueden consultar en sitios web como *CoinMarketCap*, que también aporta información sobre el valor de cotización de los criptoactivos.

Bitcoin para validar las transacciones en su *Blockchain* o cadena de bloques utiliza el sistema llamado *Proof of Work*, en el cual los usuarios, llamados mineros, a través de sus ordenadores, validan las transacciones y obtienen una recompensa por ello.

Para empezar a trazar los investigadores deben conocer los diferentes formatos que puede presentar una dirección de *Bitcoin*. Estas comienzan con el número 1 o 3 y tiene entre 26 y 35 caracteres. También son válidos el llamado formato de dirección *bech32*, que comienza con bc1q y tiene más caracteres, y el formato *Taproot*, que comienza con bc1p, ambos introducidos más recientemente.

Ejemplos de direcciones *Bitcoin* obtenidas aleatoriamente del buscador *Blockchain Explorer*:

- bc1qv8HySZ9aPq1xw51GmGQhp4fnydj201AFdt
- bc1qc026d7ght3cdjd0ugwvc23mfqsag0q2hvw0l3x
- 1AdFdaGhGmNQiobrvdnKHPyN9yMuGgfHiF
- 3EuMyVyv9M1yShgsUscPqT6MZmFZiFN2LGQ

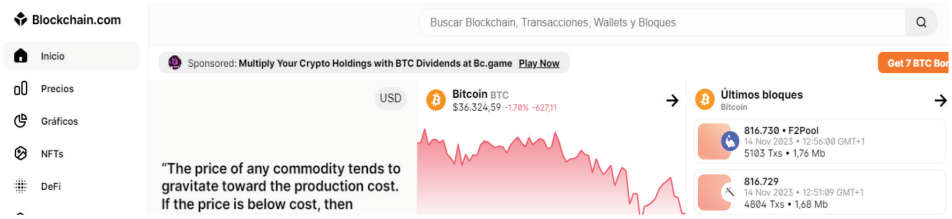
También se deben conocer los formatos de las claves privadas ya que será indispensable para realizar la incautación de los fondos depositados en los monederos. En *Bitcoin* la clave privada tiene entre 51 o 52 dígitos y empieza por 5, 6, K o L.

A continuación, se propone cómo realizar la trazabilidad de transacciones *Bitcoin*:

Si se utiliza la herramienta *Blockchain Explorer*, los pasos a seguir serían los siguientes:

1) Introducir el *hash*, la dirección o el bloque que se quiere trazar en el buscador que se puede observar en la Figura 9.

Figura 9: Imagen del buscador *Blockchain Explorer*, donde introducir el *hash*, dirección o bloque para obtener información del mismo.



Nota. Recorte del buscador público *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Si, al introducir una dirección o *hash*, la herramienta indica que no se han encontrado resultados, puede ser que se trate de una dirección *Bitcoin* o *hash* con un formato incorrecto y pueda pertenecer a otra criptomoneda o se haya escrito incorrectamente.

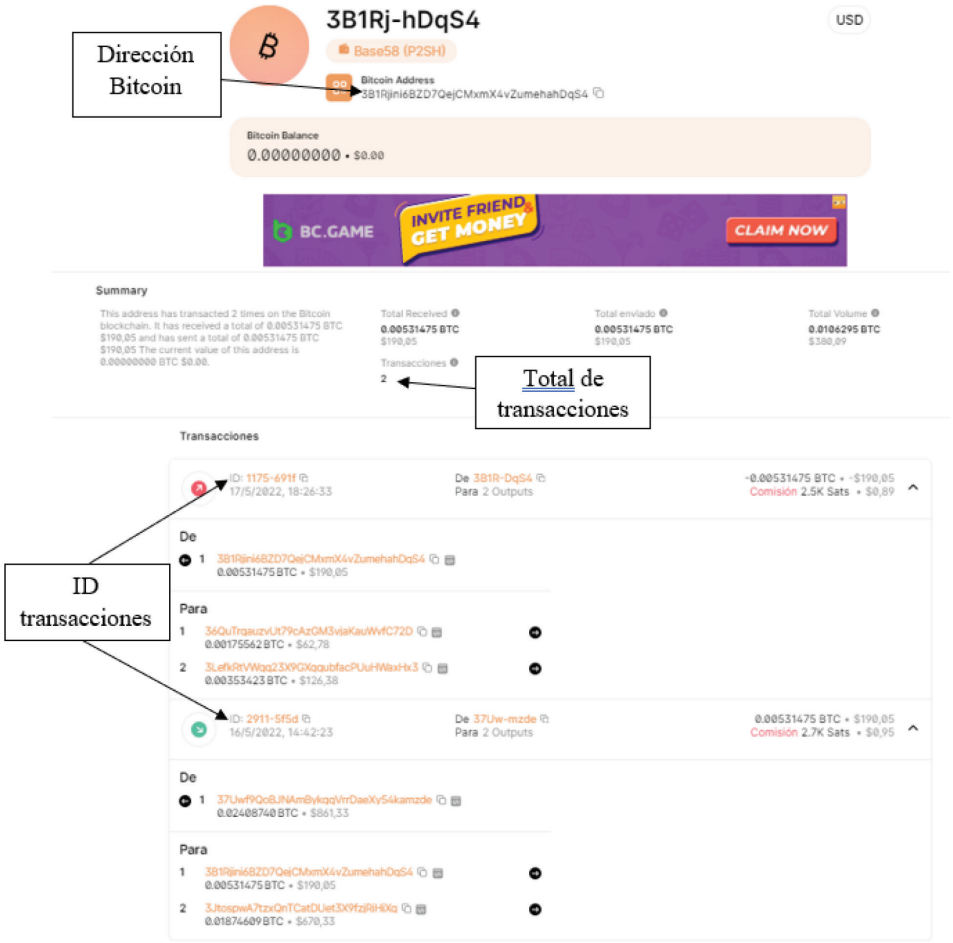
2) Si se introduce una dirección, aparecerá la imagen que se muestra más abajo como Figura 10.

   En el siguiente ejemplo se observan varios elementos que se han de tener en cuenta a la hora de trazar una dirección *Bitcoin*.

   La dirección que se ha introducido en el buscador figura completa en la parte superior de la imagen, el resto de direcciones, así como los *hash* (ID) de las transacciones, se muestran como enlaces y se pueden consultar clicando encima de ellas.

   Las transacciones de entrada van acompañadas de un símbolo de color verde. Por el contrario, las de salida van seguidas de un símbolo rojo. Estas últimas llevan aparejada una comisión, calculada, en el caso de *Bitcoin*, en una unidad llamada *satoshi*, que es la representación mínima en la que se puede operar en el sistema *Bitcoin*.

Figura 10: Información sobre una dirección de *Bitcoin*.



Nota. Recorte editado del buscador público *Blockchain Explorer*.

Por último, señalar que este buscador muestra la fecha y la hora en formato europeo y la zona horaria es la hora local, pero otras herramientas utilizan formatos distintos como UTC, que habrían de tenerse en cuenta.

3) La dirección de cambio:

Un supuesto que se puede dar en las transacciones con *bitcoin* es que una transacción de salida presente varias direcciones de destino, y que una de ellas pertenezca también al propio

remitente. Es la llamada dirección de cambio, donde se envía el saldo sobrante de la transacción.

Esto sucede porque no se envía la cantidad exacta de *bitcoin*, sino que existe un sobrante que retorna a la dirección de cambio que también pertenece al remitente.

En ocasiones es posible deducir qué dirección es la dirección de cambio, bien por los saldos o utilizando la herramienta *Wallet Explorer*, pero en otros casos resulta difícil saberlo. Existen algunos trucos para hacer esta averiguación:

- El primero es que exista una coincidencia entre las direcciones de remitente y destinatario, figurando la misma dirección en el apartado del remitente *(From)* y del destinatario *(To)*.

- Que la propia herramienta utilizada marque que se trata de la dirección de cambio como se recoge en la Figura 11. En este ejemplo se ha utilizado la herramienta *Blockchair*:

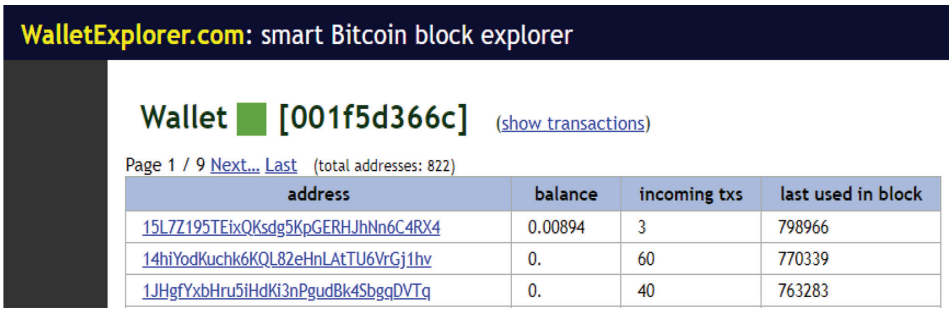
Figura 11: Dirección de cambio en el sistema *Bitcoin*.

Nota. Recorte aleatorio editado de una transacción del buscador público *Blockchair*.

- Que la dirección de remitente y la de cambio pertenezcan al mismo *cluster*.

Se utilizaría la herramienta *Wallet Explorer*, introduciendo la dirección del remitente en el buscador y clicar en «*show wallet addresses*». Todas las direcciones que figuren en el listado pertenecen al mismo remitente. Un ejemplo visual se observa en la Figura 12.

Figura 12: Direcciones incluidas en un *cluster* por la herramienta *Wallet Explorer*.



Nota. Recorte aleatorio de un *cluster* del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

Este es un buen momento para introducir el concepto de *cluster*.

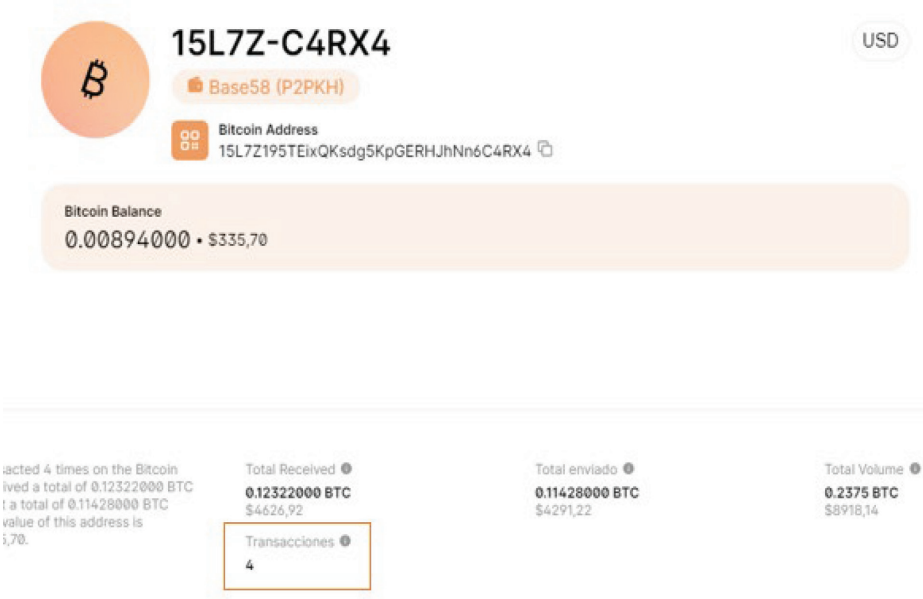
Un *cluster* es la agrupación de direcciones dentro de un monedero de criptoactivos, billetera o *wallet*. A efectos operativos, esto significa que gracias a un *cluster* se pueden saber las direcciones controladas por un mismo monedero, pero existe una diferencia entre *cluster* y monedero, ya que el *cluster* es la agrupación de direcciones, pero un monedero puede verse como un solo *cluster* o como varios.

Para saber cuántas direcciones tiene un *cluster* se puede acudir a la herramienta *Wallet Explorer*.

A continuación, se explica en un ejemplo práctico:

Se utiliza la dirección *Bitcoin* 15L7Z195TEixQKsdg5KpGERHJhNn6C4RX4, que según *Blockchain Explorer* presenta 4 transacciones como se observa en la Figura 13.

Figura 13: Información sobre la dirección 15L7Z195TEixQKsdg5KpGERHJhNn6C4RX4.



Nota. Recorte editado de una dirección del buscador público *Blockchain Explorer*.

Esta misma dirección se introduce en el buscador *Wallet Explorer*, que la relaciona con un monedero o *wallet*, en este caso es el número 001f5d366c (este nombre de monedero es un identificador que utiliza la propia herramienta).

La herramienta indica que desde este monedero se han realizado más de 2000 transacciones, por lo que existen más direcciones de *Bitcoin* asociadas a este monedero, ya que la que se ha consultado solo presentaba 4 transacciones. Para conocer el resto, basta con clicar en el enlace «*show wallet addresses*», que aparece resaltado en la Figura 14.

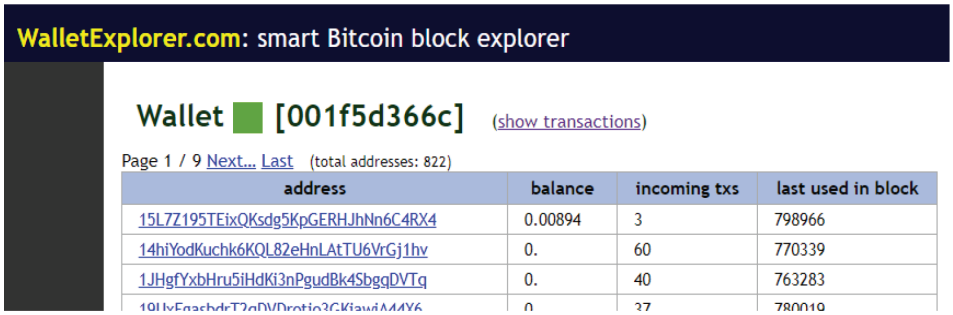
Hay que tener en cuenta que se están utilizando herramientas de rastreo que a menudo no logran identificar todas las direcciones de un monedero, por ello resulta interesante usar varias herramientas por si alguna aporta más información.

Figura 14: Información sobre un *cluster* a través de la herramienta *Wallet Explorer*.

Nota. Recorte editado de un *cluster* del buscador público *Wallet Explorer*.

En este caso, la herramienta indica que el monedero controla 822 direcciones, el balance de cada una de ellas y las transacciones que han operado, como se puede ver en la Figura 15.

Figura 15: Información sobre un *cluster* a través de la herramienta *Wallet Explorer*.



Nota. Recorte de un *cluster* del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

Esta herramienta no siempre identifica si el monedero pertenece a un servicio de criptoactivos como, por ejemplo, a una *exchange*, en estos casos existen indicadores que permiten pensar que la dirección que se está trazando pertenece a un monedero de un servicio de criptoactivos identificado. Uno de los indicadores de que la dirección trazada pertenece a un servicio de criptoactivos es que figuren cientos o miles de transacciones y cientos de direcciones asociadas al mismo.

Si la herramienta sí identifica el monedero de un servicio de criptoactivos identificado como, por ejemplo, una *exchange*

o proveedor de criptoactivos, lo que hace es titular junto al número de *wallet* el nombre del servicio; un ejemplo visual es el recogido en la Figura 16.

Figura 16: Identificación de un monedero.

Nota. Recorte del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

- Otro truco para identificar una dirección de cambio es que las cantidades sean redondas ya que es un indicador de que esa transacción se corresponde al envío efectivo y la otra al cambio. Un ejemplo es el recogido en la Figura 17.

Figura 17: Identificación de dirección de cambio por cantidades redondas.

Nota. Recorte aleatorio de una transacción del buscador público *Blockchair* (*Blockchair*, 2023).

Es más probable que el remitente envíe una cantidad exacta al destinatario, es decir, 2,5 *bitcoin* y no 0,419232 *bitcoin*, que seguramente se corresponderían con el excedente y, por lo tanto, la dirección bc1qjh-

0j25ng7525544uzjy8q8pxavekhefcaumj5 sería la dirección de cambio en esta operación.

- Por último, que la cantidad al cambio en dólares sea redonda es un indicador de que esa transacción es la correspondiente al envío y la restante al excedente. Para ello habría que consultar *CoinMarketCap* para conocer el valor de la criptomoneda enviada en el día de su envío y realizar el cálculo.

4) Varias direcciones de envío o remitente:

También se puede dar el caso de que una transacción salida presente varias direcciones de remitente, en este caso las direcciones que aparezcan en el apartado de *from* o de pertenecen a la misma persona. Es el caso de la transacción que aparece en la Figura 18.

Figura 18: Direcciones del remitente.

Nota. Recorte aleatorio de una transacción del buscador público *Blockchain Explorer* (*Blockchain Explorer*, 2023).

Esta transacción presenta 4 direcciones, que envían un total de 0,5 *bitcoin* a la dirección bc1qwq4qlw2h0920vyjwv9sca499tl2km9fkv8ylq7. Como se puede observar, la suma de las cantidades de las 4 direcciones permite alcanzar la cantidad enviada y el pago de la *fee*. Cabe señalar que la cantidad sobrante de la transacción (0,78 *bitcoin*) es enviada a la dirección bc1qgtsgwf905d2raq4ukt9fhj86daupzrtf7mcysh (dirección de cambio y también del remitente, que es posible

deducir al ser la misma que las dos últimas que figuran en el apartado del remitente [De]). Es decir, la cantidad de fondos no es suficiente para enviar el pago por lo que se envía desde varias direcciones con fondos, fusionándose para realizarlo. Las direcciones pertenecen al mismo remitente.

Asimismo, como sucede en este caso con la dirección bc1qgtsgwf905d2raq4ukt9fhj86daupzrtf7mcysh, se observa la misma en varias ocasiones en el apartado del remitente. Esto es posible ya que los fondos de *bitcoin* no se fusionan, es decir, son dos entradas diferentes a esa dirección o dos fragmentos de *bitcoin* generados por separado que se están gastando en la misma transacción.

A modo resumen, los pasos a seguir para realizar una trazabilidad de *Bitcoin* serían:

1) Introducir en el buscador *Blockchain Explorer* u otra herramienta la dirección *Bitcoin* que se quiere trazar.

2) Introducir la misma dirección en la herramienta *Wallet Explorer* para saber a qué monedero está asociada y el resto de direcciones, para ello habrá que clicar en «*show wallet addresses*». Se pueden dar dos situaciones:

   La primera que no liste la *wallet* como perteneciente a ningún proveedor de criptoactivos, figuraría un código alfanumérico como se puede observar en la Figura 19.

Figura 19: Información sobre un *cluster*.

Wallet [156b7c55c2] (show transactions)

Page 1 / 1 (total addresses: 3)

address	balance	incoming txs	last used in block
1JgnPM5WyhSktkskrGGE9D2AvzQvTpzydW	0.	2	447866
1K2WJRiLXU3bcWZ8Y4ifuxagdALPzsN1dM	0.	1	447866
1Mx8facDozfFzo9oLtY36PZf2qmfkZntkr	0.	1	447866

Page 1 / 1 (total addresses: 3)

Nota. Recorte del buscador público *Wallet Explorer* (*Wallet Explorer*, 2023).

En este ejemplo se observan tres direcciones en el mismo *cluster*, que pertenecen al mismo monedero. Al no identificar ningún proveedor de criptoactivos, interesará seguir trazando.

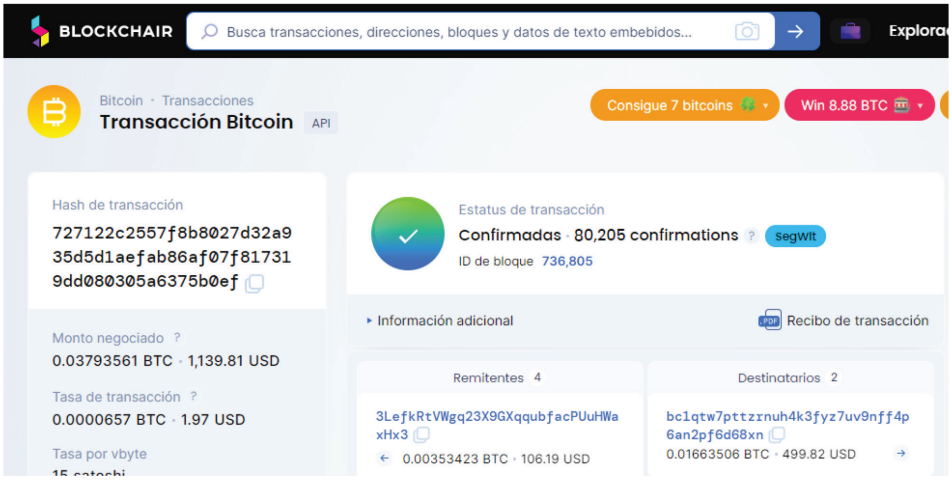
Y la segunda situación es que la herramienta *Wallet Explorer* indique que la dirección introducida sí pertenece a un proveedor de criptoactivos; en este caso en vez de un código alfanumérico aparecería la denominación del servicio, como se puede observar en la Figura 20.

Figura 20: Información sobre un *cluster* identificado.

Nota. Recorte del buscador público Wallet Explorer (Wallet Explorer, 2023).

3) Por otro lado, si en vez de una dirección se introduce un *hash*, aparecerá la imagen que se muestra en la Figura 21. En este ejemplo se ha utilizado el buscador *Blockchair*.

Figura 21: Información relativa a un *hash*.



Nota. Recorte aleatorio de una transacción del buscador público *Blockchair* (*Blockchair*, 2023).

Otra forma de trazar transacciones de *Bitcoin* es mediante el *hash* de la operación. Esta forma es útil cuando se trata de direcciones que presentan numerosas transacciones, al centrarse en la operación objeto de análisis.

Además, introduciendo el *hash*, a través de los buscadores *Blockchain Explorer* o *Blockchair*, clicando en el símbolo de flecha, es posible seguir los fondos hacia delante y hacia atrás entre direcciones *Bitcoin*.

3.3.2 Red *Ethereum*

La Red *Ethereum* fue creada en 2013 y su cadena de bloques o *Blockchain* comenzó a funcionar en 2015. Se trata de una plataforma descentralizada creada para almacenar códigos y programas informáticos que pueden ejecutarse en cualquier lugar.

Es de código abierto y en ella se pueden utilizar *ether* (ETH) y otros muchos *tokens* y NFT como medio de pago o como elemento integral de un contrato inteligente. Una herramienta de consulta es *Etherscan*.

La Red *Ethereum* usa un sistema llamado *Proof of Stake* (prueba de participación) para la validación y creación de los bloques que contienen las transacciones operadas en esta red. En este sistema, los usuarios con *ether* se eligen al azar para validar la red, ordenando transacciones y creando nuevos bloques. Se requiere menos energía y *hardware* para este tipo de consenso.

El *ether* es la criptomoneda nativa de *Ethereum*. En esta red también se puede operar con diversos *tokens* a través de la norma ERC-20, que es un estándar técnico utilizado para la creación e implementación de contratos inteligentes *(smart contract)* en la *blockchain* de *Ethereum*. Este estándar define las reglas que los *tokens* deben seguir dentro de la Red *Ethereum*. La lista completa de todos los *tokens* ERC-20 puede consultarse en *Etherscan*.

Para poder enviar esos *tokens*, es necesario tener un pequeño saldo de *ether* en el monedero.

Los más usados por los investigados son las llamadas *stablecoin* o monedas estables, que son aquellos *tokens* diseñados para minimizar la volatilidad del precio de los criptoactivos. *Tether* (USDT), *USD Coin* (USDC), *Binance* USD (BUSD) y DAI son los más utilizados y están colaterizados con el dólar (paridad 1:1 con el dólar). Es común ver como los investigados cambian sus criptoactivos *bitcoin* (BTC) o *ether* (ETH) por *stablecoin* para mantener el valor de los criptoactivos.

Mención especial para el *token tether* (USDT) por ser uno de los principales *tokens* que se encuentran en las investigaciones. Este *token* se ejecuta sobre la Red *Ethereum*, aunque también existe implementación sobre *Bitcoin* y *Tron*.

Los *tokens* deben ejecutarse a través de un contrato inteligente o *smart contract*, que son contratos inteligentes de ejecución automática que residen en una dirección de la Red *Ethereum*.

En la herramienta de *Etherscan*, junto a la dirección, figura un símbolo de documento que indica que es un contrato.

Tanto los *tokens* como los contratos inteligentes o *smart contract* no tienen requisitos para su creación y cualquiera puede crearlos, lo que ha llevado a que muchos resulten proyectos fraudulentos.

Otra forma de operar en la Red *Ethereum* es a través de plataformas descentralizadas o DeFi, que son servicios que facilitan la interacción directa entre usuarios sin intermediarios. Permite a los usuarios de la plataforma que conecten o vinculen directamente sus monederos para comprar, vender o intercambiar criptomonedas o *tokens*. Las más famosas son *SushiSwap* y *Uniswap*.

Además, este ecosistema DeFi permite a los usuarios suministrar liquidez de criptomonedas o *tokens* a través de contratos inteligentes o *smart contract*, por una pequeña recompensa.

Estas funcionalidades hacen más complejo el trabajo de rastreo ya que los servicios descentralizados no reportan información de las transacciones debido a que los intercambios se

realizan de forma anónima, sin registro, identificación o reglas KYC/AML.

Para empezar a trazar en la Red *Ethereum* se debe conocer el formato que presenta una dirección de esta red; las direcciones comienzan por 0x.

Algunos ejemplos obtenidos de manera aleatoria del buscador *Etherscan* serían los siguientes:

- 0x974CaA59e49682CdA0AD2bbe82983419A2ECC400

- 0x0829190D34F282c780A92f7b0ae739d859f6aecf

- 0x503828976D22510aad0201ac7EC88293211D23Da

Las direcciones de *Ethereum* se pueden compartir públicamente para recibir *ether*, *tokens* y NFT, y para ver un saldo en relación a la dirección. Se utilizan para almacenar *ether*, *tokens* y contratos, entre otros.

También hay que conocer los formatos de las claves privadas; en *Ethereum* la clave privada contiene 64 caracteres hexadecimales.

A continuación, se explica cómo trazar en la Red *Ethereum* ya que presenta algunas particularidades y diferencias con la Red *Bitcoin*.

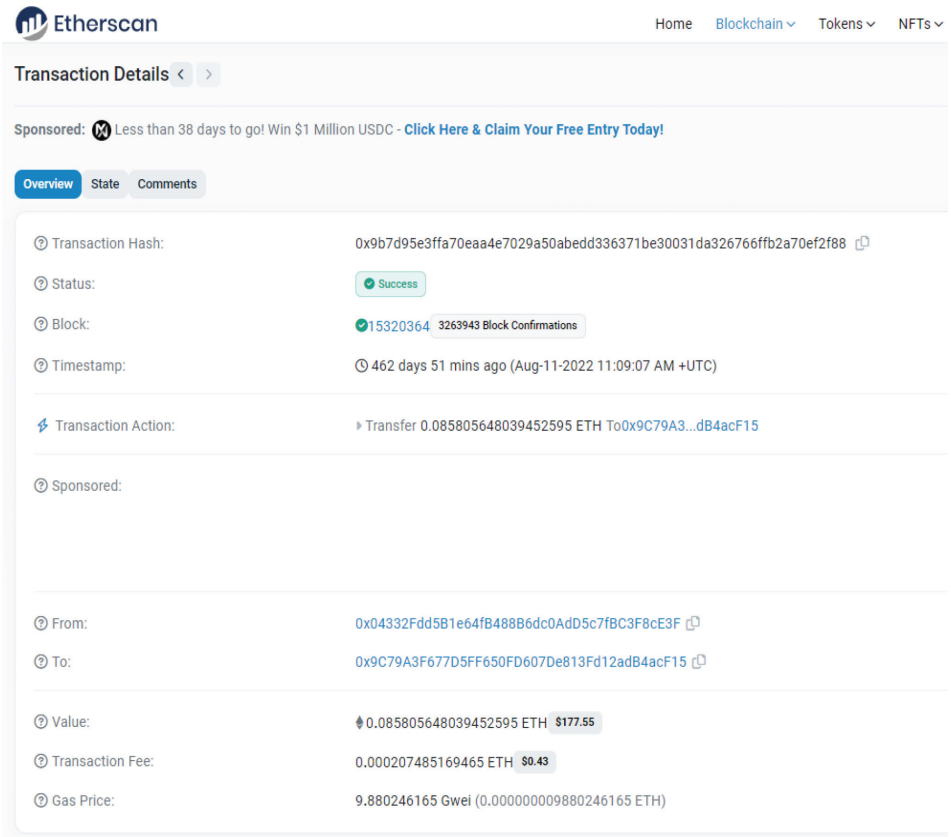
Si se utiliza la herramienta *Etherscan* los pasos a seguir serían los siguientes:

1) Introducir en el buscador el *hash*, la dirección o el bloque que se desee trazar.

   Este buscador permite explorar bloques, transacciones, contratos inteligentes o *smart contract*, transferencias de *tokens* y transacciones internas, entre otros.

2) Si se introduce un *hash* en el buscador aparecerá la siguiente imagen recogida en la Figura 22.

Figura 22: Información relativa a un hash a través de la herramienta *Etherscan*.



Nota. Recorte aleatorio de una transacción del buscador público *Etherscan* (*Etherscan*, 2023b).

Este tipo de búsqueda puede aportar diferente información, como cuándo tuvo lugar una transacción en concreto, cuándo fue verificada, las direcciones de origen o remitente y de destino, qué tarifa de transacción o *fee* se pagó. A diferencia de si se introduce en el buscador una dirección, que figurarán todas las transacciones operadas por esta.

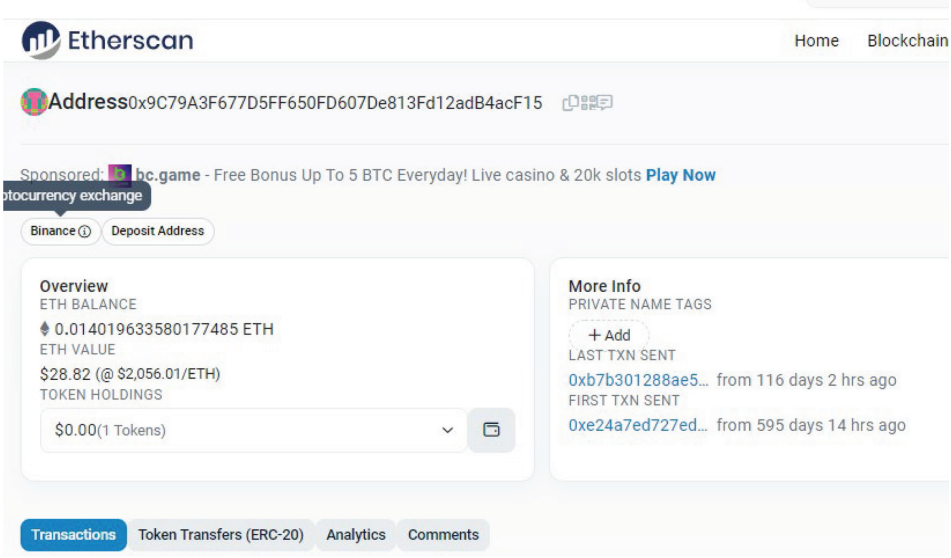
Etherscan, a diferencia de *Wallet Explorer*, no reconoce las direcciones como parte de un *cluster*, por lo que se debe trazar siempre en un contexto y si es posible listar las direcciones.

Si se quiere seguir los fondos, en este ejemplo se trazarán los 0,08 ETH en la dirección de destino *(to)* 0x9C79A3F677D-5FF650FD607De813Fd12adB4acF15.

3) Si se introduce una dirección de la Red *Ethereum* aparecerá la imagen que se recoge en la Figura 23.

   En el caso de que este buscador arroje un resultado negativo, se pueden consultar otras cadenas de bloques para verificar esta dirección en ellas.

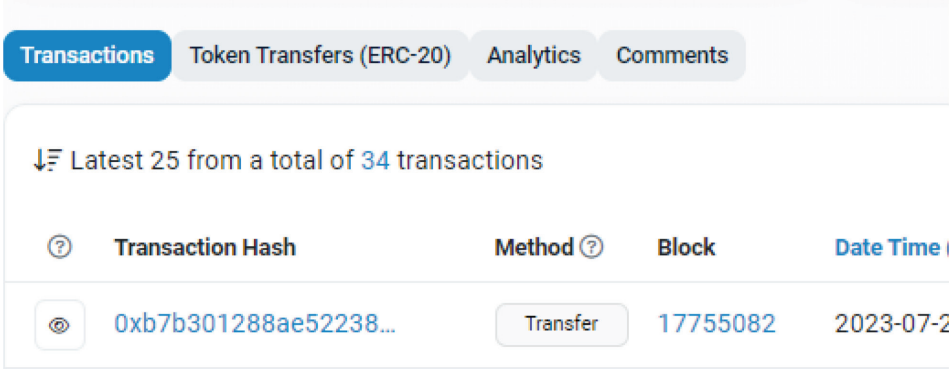
Figura 23: Información sobre una dirección en la Red *Ethereum*.



Nota. Recorte aleatorio de una dirección del buscador público *Etherscan* (*Etherscan*, 2023b).

El primer apartado que figura con respecto a una dirección, «*Transactions*», es el referente a todas las transacciones operadas en *ether* con esa dirección tanto de entrada como de salida; un ejemplo visual es el que se recoge en la Figura 24.

Figura 24: Información sobre las transacciones asociadas a una dirección de la Red *Ethereum*.



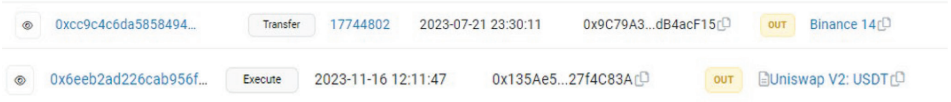
Nota. Recorte aleatorio del apartado *Transactions* del buscador público *Etherscan* (*Etherscan*, 2023a).

A diferencia de *Bitcoin*, la Red *Ethereum* no utiliza direcciones de cambio. Esto hace más fácil conocer dónde terminan los fondos, ya que las transacciones en la Red *Ethereum* van de una dirección a otra dirección. Esto puede resultar similar a transacciones entre cuentas bancarias.

En la imagen anterior se ven todas las transacciones que ha operado la dirección que se ha introducido en el buscador; en este caso figuran treinta y cuatro. Si fuese de interés filtrar por transacciones de entrada o de salida, en la parte superior derecha figuran tres puntos que al clicar sobre ellos se despliegan varias opciones de filtrado.

Otra ventaja de este buscador es que algunos servicios ya están etiquetados, por ejemplo, se pueden ver varias direcciones con etiquetas de *exchange*, como *Binance*, *Kraken*, *Bitfinex*, *Huobi*, *Gemini*, etc. También se pueden encontrar contratos de *tokens* y plataformas de NFT. A continuación, se muestran dos ejemplos en la Figura 25.

Figura 25: Identificación de direcciones asociadas a *exchanges*.



Nota. Recorte aleatorio editado del apartado *Transactions* del buscador público *Etherscan*.

En este apartado también se puede ver el tipo de transacción que tuvo lugar en la pestaña «*Method*». Son varias las operativas que pueden figurar como, por ejemplo, «*Approve*», «*Multicall*», «*Transfer*» o «*Swap*».

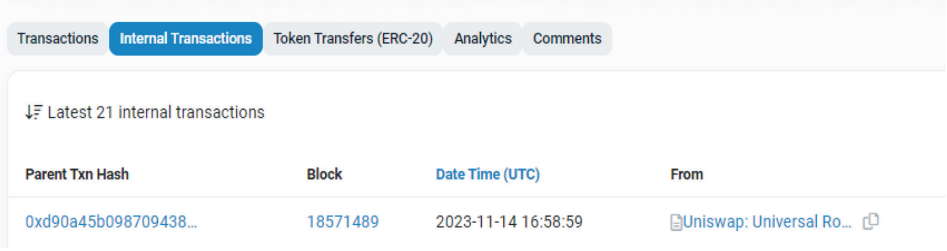
Esto puede dar al investigador que está trazando una idea del tipo de transacción que se está realizando, y si se clica en la transacción de interés y se observa el apartado «*logs*» se obtendrá toda la información sobre el método utilizado.

A continuación de «*Transactions*», figura el apartado «*Internal txns*», relativo a las transacciones internas que están relacionadas con las transacciones que interactúan con un contrato inteligente o *smart contract*.

Esta pestaña muestra, por ejemplo, el uso de servicios descentralizados como *SushiSwap* o *Uniswap*, y también entradas de mezcladores o *mixer*.

Esta pestaña no siempre estará visible, solo si la dirección ejecutó transacciones internas. Si fuese visible aparecería tal y como se observa en la Figura 26.

Figura 26: Información relativa a transacciones a través de *smart contract*.

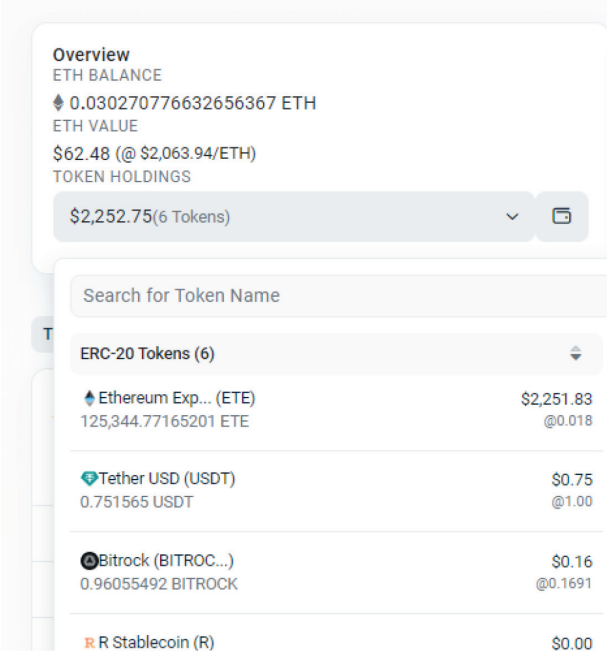


Nota. Recorte aleatorio del apartado *Internal Transactions* del buscador público *Etherscan* (*Etherscan*, 2023b).

La siguiente pestaña que figura es «*ERC20 Token Txns*», relativa a las transacciones operadas con *tokens* ERC20 de la Red *Ethereum*. El sistema *Ethereum* permite a los usuarios mantener o almacenar la moneda nativa de *Ethereum*, *ether* (ETH), y uno o más de estos *tokens* en una dirección de *Ethereum*. *Etherscan* indica los *tokens* depositados en esa dirección y su valor a día de la consulta.

Cuando se introduce la dirección a trazar en el buscador, uno de los apartados que figura es «*Token*»; si figura alguno como es el caso del siguiente ejemplo, en la pestaña «*ERC20 Token Txns*» se podrán consultar las transacciones operadas con los mismos de la misma manera que en el apartado de «*Transactions*» ya explicado. El apartado referido puede observarse en la Figura 27.

Figura 27: Información sobre los *tokens* de una dirección de la Red *Ethereum*.



Nota. Recorte aleatorio de una dirección del buscador público *Etherscan* (*Etherscan*, 2023b).

Esta dirección presenta un valor de *ether* 0,03 y otras cantidades de 6 tokens diferentes, que se corresponden al día de la consulta con un valor de más de 2.000 dólares. En la pestaña «*ERC20 Token Txns*» se puede obtener más información al respecto.

4 Conclusiones

A continuación, se realiza una síntesis de los puntos que se consideran más relevantes:

- El uso de los criptoactivos ha experimentado un notorio aumento en los últimos años, introduciendo consigo una serie de conceptos novedosos en la economía española. Este fenómeno ha permitido a los usuarios operar de nuevas formas, lo que entraña una serie de ventajas y riesgos inherentes que deberían conocer.

- Por ello, adquirir conocimientos sobre trazabilidad resulta de gran utilidad no solo desde la perspectiva policial, sino también como ciudadano inmerso en una sociedad donde la tecnología *Blockchain* y los criptoactivos ganan cada vez más terreno. De esta manera, las Fuerzas y Cuerpos de Seguridad pueden rastrear fondos fraudulentos y localizar a los criminales que abusan de estos elementos y, al mismo tiempo, los ciudadanos pueden verificar el estado de sus transacciones mediante esta tecnología, que ha llegado para quedarse.

- Debido al incremento en el uso de los criptoactivos, su presencia en las investigaciones policiales también ha crecido, presentándose de diferentes formas: utilizados como método de pago, en operativas de blanqueos de capitales procedentes de diferentes tipologías delictivas y también como productos de inversión que sirven de reclamo en estafas. Son varios los elementos que dificultan su seguimiento e incautación y que resultan de interés para los delincuentes, como son la rapidez que presentan las transacciones con estos activos, su carácter internacional y, en cierta medida, su anonimato.

- Este panorama social ha generado la necesidad de muchos países de ponerse al día en materia de criptoactivos, colocándolos en una posición preferente en su agenda normativa. Un ejemplo es el Reglamento de Mercados de Criptoactivos (MICA) [Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos], que se ha convertido en el primer instrumento regulador de estos activos, pero que no será de aplicación hasta el 30 de diciembre de 2024 como dice su artículo 149. Esta norma ha dado cobertura jurídica a los criptoactivos y establecido unas reglas comunes a todos los operadores en la Unión Europea.

- Existen multitud de criptoactivos en la actualidad, si bien son varios los que se encuentran con mayor frecuencia en las investigaciones policiales, como *bitcoin*, *ether*, *monero*, *tether* y otras *stablecoins*.

- Debido al diseño de algunos de los criptoactivos existentes es posible trazarlos a través de fuentes abiertas, si bien, en ocasiones, sería conveniente la utilización de herramientas comerciales específicas de trazabilidad que ayudarán en esta tarea al investigador. Hay que tener en cuenta que el análisis de las transacciones con herramientas de código abierto debe estar basado siempre en el contexto de la investigación. El análisis de las transacciones, junto con el análisis de la información obtenida de otras fuentes, resulta de gran importancia para detectar la actividad delictiva e identificar a los responsables.

- Los puntos de compromiso en investigaciones con criptoactivos, y donde se deben centrar los esfuerzos del investigador, es en el momento en que son intercambiados por otros criptoactivos o por dinero *fiat*, ya que permiten una mayor trazabilidad y es posible que se puedan identificar a las personas que podrían estar detrás de la operativa investigada.

Glosario

BILLETERA: monedero o *wallet* en inglés, cartera digital que contiene las claves necesarias para acceder a los criptoactivos del usuario.

BITCOIN: con mayúscula, presenta un significado más amplio que *bitcoin*, y corresponde a la red, la tecnología, el protocolo o la *blockchain*.

BITCOIN (BTC): en minúscula, es cada unidad de criptoactivo, divisible en unidades *satoshis* (1 BTC equivale a 100.000.000 *satoshis*).

BLOCKCHAIN O CADENA DE BLOQUES: es la tecnología que da soporte a los criptoactivos, es descentralizada y está distribuida en redes de usuarios, en ella se almacenan las transacciones y se graban los paquetes de datos.

CAPITALIZACIÓN DEL MERCADO: sirve para estimar el tamaño o magnitud de un criptoactivo o proyecto respecto de otro. Se calcula al multiplicar el precio de un criptoactivo por la cantidad de unidades que están en circulación.

CLUSTER: grupo de direcciones de criptoactivos que están vinculadas o asociadas de alguna manera. Las direcciones pueden pertenecer a un usuario o entidad. Estas agrupaciones pueden ser utilizadas para el análisis de transacciones y seguimiento de fondos en la *blockchain*, resultando útil para detectar patrones de gasto, comportamientos y relaciones entre diferentes partes en el ecosistema de los criptoactivos.

CNMV: abreviatura de Comisión Nacional del Mercado de Valores. Es el organismo encargado de la supervisión e inspección de los mercados de valores españoles y de la actividad de cuantos intervienen en los mismos.

CÓDIGO ABIERTO: forma de distribuir el contenido digital que permite a los usuarios disponer y en ocasiones modificar el contenido.

CONSENSO: acuerdo unánime de los miembros de una red de *blockchain* sobre las transacciones, lo que permite crear un bloque. Es una de las principales características de la tecnología *blockchain*.

CONTRATO INTELIGENTE: o *smart contract* en inglés.

CRIPTOACTIVO: activo digital que utiliza la criptografía para garantizar la seguridad de las transacciones. Las criptomonedas *bitcoin* y *ether* son ejemplos de criptoactivos.

DEFI: abreviatura de *Decentralized Finance* en inglés. Se trata de un conjunto de servicios financieros que operan en una red *blockchain*, basados en contratos inteligentes o *smart contract* en inglés, que buscan descentralizar el acceso a esos servicios sin depender de intermediarios.

DESCENTRALIZACIÓN: distribución de tareas entre más de una institución para evitar una única institución central que monopolice las funciones, procesos o poderes. Es una de las principales características de la tecnología *blockchain*.

DEX: abreviatura de *exchange* descentralizado. Su principal característica es que opera sin que medie intermediario centralizado, es decir, las transacciones se realizan directamente entre los usuarios a través de contratos inteligentes en *blockchain*. Un ejemplo es Uniswap, que opera en la Red *Ethereum* y permite el intercambio de *tokens* ERC-20 de manera descentralizada.

DINERO FIAT: o dinero fiduciario, es cualquier moneda emitida de forma convencional por un gobierno y declarada como medio legal de intercambio, por ejemplo, el euro o el dólar.

ERC-20: estándar de *tokens* que utilizan la Red *Ethereum*. Es el más utilizado.

ESA: abreviatura de autoridades europeas supervisoras en inglés.

ESMA: abreviatura de Autoridad Europea de Valores y Mercados en inglés. Forma parte del Sistema Europeo de Supervisión Financiera y su objetivo es garantizar una supervisión financiera adecuada en toda la Unión Europea.

ETHER (ETH): activo nativo de la Red *Ethereum*.

ETHEREUM: red distribuida de código abierto basada en *blockchain*. Esta red ofrece el desarrollo de aplicaciones descentralizadas.

EXCHANGE: plataforma o servicio de intercambios de criptoactivos, también permite el cambio de dinero fiat por criptoactivos y viceversa, además de otros servicios como la custodia de fondos. Existen varios tipos: centralizados (CEX), descentralizados (DEX) o híbridos. Algunos de estos proveedores de servicios con criptoactivos son *Kraken*, *Binance*, *Coinbase* o *Huobi*.

FEE: comisión por la prestación de un servicio.

HASH: término informático que se refiere a la huella digital, formado por una combinación de números y letras, que permite saber si el documento original ha sido modificado. El *hash* permite verificar el contenido de una transacción.

LIQUIDEZ: capacidad de un criptoactivo para ser comprado o vendido en el mercado sin afectar significativamente a su valor. Una alta liquidez significa que hay suficientes usuarios dispuestos a comprar o vender el criptoactivo, lo que facilita las transacciones con ese activo digital.

NODO: ordenador conectado a una red *blockchain* que guarde las copias de registro de las transacciones. Cuantos más nodos haya en una red, más descentralizada y segura será.

NTF: o *token* no fungible, es un tipo de activo que representa la propiedad o autenticidad de un elemento específico a través de la tecnología *blockchain*.

STABLECOIN: su traducción en español sería moneda estable, que hace referencia a que su valor está ligado al de otro activo o divisa, como por ejemplo el dólar.

TOKEN: representación digital de un activo o servicio. La mayoría utilizan la Red *Ethereum*.

TRADING: se refiere a la compraventa de criptoactivos con el fin de obtener un beneficio.

VOLATILIDAD: es la variación de un activo en un periodo de tiempo determinado. En el caso de los criptoactivos se dice que presentan una alta volatilidad debido a que su precio puede variar significativamente en un corto periodo de tiempo.

Referencias

Blockchair (2023). Buscador público de cadena de bloques o *blockchain*. https://blockchair.com/es

Blockchain Explorer (2023). Buscador público de cadena de bloques o *blockchain*. https://www.blockchain.com/es/explorer

Callejo, C. y Ronco, V. (2020). *Criptomonedas para dummies*. Grupo Planeta.

Comisión Nacional del Mercado de Valores (2018). *Comunicado conjunto de la CNMV y del Banco de España sobre «criptomonedas» y «ofertas iniciales de criptomonedas» (ICO)*.

Comisión Nacional del Mercado de Valores (2021). *Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión*.

Comisión Nacional del Mercado de Valores (2022). *Estudio sobre las criptomonedas y la efectividad de las medidas impulsadas por la CNMV. Informe de Resultados mayo-junio de 2022*.

Etherscan (2023a). Buscador público de cadena de bloques o *blockchain*. https://etherscan.io/

Etherscan (2023b). Listado completo de *tokens* ERC-20. https://etherscan.io/tokens

Parlamento Europeo y Consejo. *Reglamento de Mercados de Criptoactivos (MICA) (REGLAMENTO (UE) 2023/1114 DEL, de 31 de mayo de 2023, relativo a los mercados de criptoactivos).*

Tronscan (2023). Buscador público de cadena de bloques o *blockchain*. https://tronscan.org/#/

Wallet Explorer (2023). Buscador público de cadena de bloques o *blockchain*. https://www.walletexplorer.com/