universidad de león

Departamento de Matemáticas

MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD

Trabajo de Fin de Máster

Ataques a Criptomonedas y seguimiento de carteras digitales

Attacks to Cryptocurrencies and tracing of digital wallets

Autor: Javier Rodríguez Villalobos

Tutor: Ricardo J. Rodríguez Fernández

UNIVERSIDAD DE LEÓN
Departamento de Matemáticas
MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD
Trabajo de Fin de Máster

ALUMNO: Javier Rodríguez Villalobos

TUTOR: Ricardo J. Rodríguez Fernández

TÍTULO: Ataques a Criptomonedas y seguimiento de carteras digitales

TITLE: Attacks to Cryptocurrencies and tracing of digital wallets

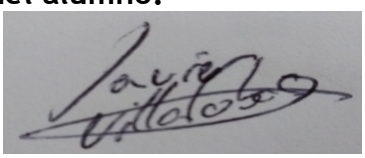
CONVOCATORIA: Septiembre, 2019

RESUMEN:

La tecnología blockchain o de cadena de bloques consiste en un registro público distribuido y descentralizado en el que sus participantes se conectan entre sí a través de una red punto a punto. Sus características principales son la descentralización de la base de datos del sistema entre los participantes de la red, la transparencia de las operaciones que se han realizado entre las partes, la inmutabilidad de los datos almacenados en el registro, la confiabilidad mutua entre las partes y la privacidad de los participantes. El presente trabajo fin de máster tiene como uno de sus objetivos principales describir en detalle el funcionamiento de la tecnología *blockchain,* indicando sus ventajas y desventajas, los tipos de redes existentes actualmente y el funcionamiento de la cadena de bloques. Otro de los objetivos de este trabajo es la exposición detallada de las diferentes formas de anonimizar las actividades asociadas a las carteras digitales y los mecanismos usados por terceros para desanonimizar a los usuarios de estas criptomonedas. Adicionalmente, en este trabajo se ha desarrollado un sistema que permite de manera automática la búsqueda de carteras digitales en foros y tablones de anuncios en Internet, a la vez que el posterior seguimiento y rastreo de sus movimientos producidos entre diferentes carteras, así como su posible vinculación a actividades ilícitas. A modo de ejemplo, la herramienta desarrollada se ha usado para detectar una cartera de bitcoin implicada en actividades ligadas a delitos informáticos.

Palabras clave: bitcoin, seguimiento, scrapping, neo4j, detección

Firma del alumno:



VºBº Tutor:

Digitally signed by RODRIGUEZ FERNANDEZ RICARDO JULIO - [redacted]
Date: 2019.09.06 12:24:02 +02'00'

(Septiembre, 2019)

ABSTRACT

The Blockchain technology consists of a distributed and decentralized public register in which the participants connect one each other thanks to a peer-to-peer network. Its main characteristics are the decentralization of the system database among the participants of the network, the transparency of the operations done among the peers, the immutability of the data stored in the register, the mutual reliability among the peers, and the peers' privacy. This master's degree dissertation aims to first describe in detail how the blockchain technology works, pointing out both advantages and disadvantages. Then, the different ways to anonymize all the activities associated to digital wallets, as well as the mechanisms used by third parties to deanonymize the users of cryptocurrencies are also described. In addition, an automatic tracing system was developed to search for digital wallets in online forums and in online notice boards, tracking and tracing all movements between digital wallets as well as the possible link to illicit activities. The system developed in this dissertation has been successfully applied to detect a digital wallet involved in illegal activities related to cybercrime.

Índice de contenidos

Índice de figuras

Índice de tablas

Glosario de términos

PoW - Prueba de trabajo. Tipo de consenso usado en redes *blockchain* que se encarga de verificar los bloques mediante el trabajo realizado en forma de cálculo computacional.

PoS - Prueba de participación. Tipo de consenso de redes *blockchain* en la que los nodos validadores son aquellos que tienen mayor cuota en la red.

PBFT - Sistema práctico de tolerancia a fallos bizantinos. Tipo de consenso de redes *blockchain* en la que las decisiones se toman de forma mayoritaria para evitar órdenes contradictorias.

PoET - Prueba de tiempo transcurrido. Tipo de consenso de redes *blockchain* en la que el nodo que se encarga de validar un bloque dispone de un tiempo determinado para realizar dicha operación.

DDoS - Ataque de denegación de servicio distribuida que se caracteriza por impedir el funcionamiento de un servicio en línea mediante la realización de múltiples peticiones al equipo atacado.

P2P - Red punto a punto. Se caracteriza porque los componentes de la red actúan de igual modo sin presentar diferencias entre ellos.

Nonce - Acrónimo en inglés del término número usado solo una vez. Se trata de un número arbitrario de un solo uso necesario para obtener un *hash*.

ECDSA - Algoritmo de firma digital de curva elíptica que se encarga de validar la identidad de una persona mediante un sistema de claves público-privadas.

RSA - Sistema criptográfico de clave pública nombrado en honor de sus creadores, Rivest–Shamir–Adleman.

BGP - Protocolo de puerta de enlace de frontera que sirve para intercambiar datos entre los proveedores de servicios de Internet.

DAO - Organización Autónoma Descentralizada u organismo similar a una empresa de capital riesgo, del que se diferencia en que carece de junta directiva.

AML - *Anti-money laundering*, término en inglés empleado para referir a las leyes que se aplican en un país contra el blanqueo de capitales.

CTR - *Counter-terrorism Regulatory*, término en inglés que refiere a la regulación antiterrorista y se utiliza para evitar la financiación de este tipo de actividades.

KYC - *Know-your-customer*, término en inglés que resume la política de control y verificación de la identidad de los clientes de una empresa.

Minero - Nodo encargado de validar las transacciones en la cadena de bloques.

Bitcoin - *Token* que se ofrece como recompensa por descifrar el *hash* criptográfico.

Bloque - Conjunto de datos en los que se almacena la información de las operaciones realizadas en la tecnología *blockchain*.

Darknet - Contenido alojado en servidores únicamente accesibles a través de la red TOR.

AMLD5 - Quinta Directiva Europea contra el blanqueo de dinero cuyo objetivo es acabar con la opacidad de los propietarios reales de los activos financieros.

Ransomware - Programa malicioso que encripta los archivos para exigir un rescate para acceder a ellos.

Sextorsión - Chantaje al que se ve sometido una persona para evitar la difusión de imágenes de carácter sexual, sean estas reales o no.

1 Introducción

El origen del desarrollo de la tecnología de cadena de bloques o *blockchain* remite a la publicación del texto en el que se realiza una disertación sobre el bitcoin de Satoshi Nakamoto el 31 de octubre de 2008 [1]. A partir de ese momento crucial y, sobre todo, del ascenso meteórico del mercado de las criptomonedas, la tecnología ha comenzado a despuntar y a usarse en otros campos fuera de las transacciones financieras.

Entre los pilares fundacionales de esta tecnología se puede observar la influencia de la ingeniería del software en materia de programación del código, la computación distribuida gracias al uso de las conexiones punto a punto o P2P, así como al *ledger* o libro central del registro. Asimismo, se hace uso de la criptografía para proteger la integridad de las cuentas y para la validación de las operaciones de formación de los bloques, garantizando así la incorruptibilidad de la información almacenada; y, por último, el empleo de características propias de la teoría de juegos en cuanto a la obtención del premio asociado a la resolución de las operaciones de validación en forma de *tokens* [2].

El germen de esta tecnología se remonta a la década de los 70 del siglo XX, cuando una serie de matemáticos y físicos empezaron a formular diferentes teorías acerca de la inmutabilidad de los registros, su protección, seguridad y su monetización junto con otros elementos de tipo filosófico y económico. No obstante, la tecnología de cadena de bloques empezó a definirse como tal a partir de 1991 tras la publicación del trabajo de Stuart Haber y W. Scott-Stornetta [3], donde hablan de una cadena de bloques protegida criptográficamente mediante marcas temporales para evitar su manipulación. Posteriormente, se añaden más elementos de protección contra cambios no deseados o manipulaciones, como son los árboles de Merkle [4] en los bloques de la cadena. Esto permite gestionar de manera eficiente la incorporación, procesamiento y validación de las operaciones registradas en un bloque.

Respecto al pago de *tokens* o criptomonedas por realizar determinadas funciones (como es, por ejemplo, la validación de los procesos), tiene su origen en una publicación de David Chaum [5] del año 1983. En dicho texto se habla de la posibilidad de realizar pagos electrónicos con monedas virtuales que sean anónimas y privadas y que no estén

supervisadas por las autoridades monetarias. Además, este mismo autor fue quien fundó y desarrolló la moneda digital *ecash*, considerada la primera moneda digital.

A pesar de que la tecnología comenzó a definirse a partir de la publicación de Haber y Scott-Stornetta en el 91, hay elementos que se promulgaron en los años 70, sobre todo los relacionados con la criptografía como son los algoritmos criptográficos Diffie-Hellman o RSA [6].

Por último, cabe destacar que en todos los ámbitos que se fusionan en el génesis de la tecnología de cadena de bloques se observa de manera clara la influencia del movimiento Cypherpunk [7]. Este movimiento activista aboga por el uso de la criptografía junto con la tecnología disponible para defender la privacidad y la libertad individual en la red. En el texto publicado por Timothy C. May [8] en 1992 se plantea la implantación de la criptoanarquía y sus efectos en las relaciones económicas, como la creación de una moneda electrónica, anónima y fuera del control de las instituciones políticas y financieras.

Como hito de la tecnología hay que destacar el bloque original o bloque génesis, que es como se conoce al primer bloque generado en la cadena de bloques Blockchain. Este bloque se añadió el 3 de enero de 2009 [9].

Entre las ventajas que se asocian a la utilización de criptomonedas como medio de pago digital destacan la transferencia inmediata de dinero a diferentes partes del mundo en apenas unos minutos, el pago de comisiones e impuestos más bajos que en el circuito bancario, así como la privacidad y seguridad de las transacciones, entre otras. Estas ventajas descritas también han sido aprovechadas por grupos delictivos de tipo terroristas o mafias para blanquear dinero y trasladarlo de forma fácil y sencilla, esquivando de esta manera las normativas de los controles de anti-blanqueo de capitales (AML), regulación antiterrorista (CTR) y de registro de usuario (KYC) [10].

Pesa a que la mayoría de los usuarios consideran la tecnología blockchain segura y libre de vulnerabilidades, los recientes ataques contra determinadas criptomonedas que han ocasionado pérdidas importantes a sus propietarios (como ha ocurrido con Bitcoin Cash, Ethereum o Verge) han demostrado que no es así [11]. Es preciso también tener en cuenta que la mayoría de los gobiernos y autoridades financieras no consideran las criptodivisas una divisa como tal, salvo casos aislados como el de Japón, por ejemplo. Además, su

volatilidad en los mercados financieros convierte a las criptomonedas en activos de alto riesgo para personas inexpertas.

Por último, se considera necesario hacer hincapié en los costes medioambientales que produce el uso de esta tecnología, sobre todo, a la hora de realizar la tarea de calcular los hashes de validación de los bloques a través de dispositivos electrónicos tales como ordenadores o servidores. Estos equipos tienen un consumo eléctrico muy alto y su uso intensivo genera una cantidad elevada de basura tecnológica. Todo esto provoca un impacto medioambiental muy alto [12].

Para la realización de este trabajo se han marcado una serie de objetivos a conseguir. En primer lugar, se hará una explicación detallada de los ataques que afectan a la seguridad y privacidad de los usuarios en el ámbito de las criptomonedas. En segundo lugar, se desarrollará un sistema que permita de manera automática la búsqueda de carteras digitales en foros y tablones de anuncios en Internet, junto con el posterior seguimiento y rastreo de los movimientos producidos entre las diferentes carteras digitales localizadas.

Por último, como objetivo secundario se ha incluido la detección de evidencias en el mismo momento en que se localiza una cartera digital, ya sea en forma de una dirección de correo electrónico, un nombre de usuario o *nickname* u otros datos relevantes. Estos datos servirán como indicios para una posible desanonimización. Además, se incluirá un mecanismo que facilite el marcado de posibles operaciones de mezclado y blanqueo de dinero en las transacciones que se han detectado entre diferentes cuentas.

La estructura de este trabajo es como sigue. En el Capítulo 2 se detalla el concepto de la cadena de bloques o blockchain, sus características principales, así como su funcionamiento y los mecanismos de consenso existentes. También se incluye en este capítulo el desarrollo que ha sufrido la tecnología en el ámbito de la privacidad, así como las acciones de anonimización utilizadas para evitar la identificación de los actores intervinientes en las operaciones. En el Capítulo 3 se detallan, de forma pormenorizada, todos los ataques documentados que han afectado a la tecnología blockchain, y dentro de ésta, particularmente los que afectaban al mercado de tokens o criptomonedas. El Capítulo 4 presenta el sistema desarrollado con el que se realizarán las tareas de detección, seguimiento y monitorización de las carteras digitales y de las transacciones realizadas. Posteriormente, se realizará una demostración práctica de detección y

seguimiento de las carteras digitales, así como el análisis de los movimientos con origen o destino a las mismas. Dentro de este apartado se tratará de localizar los nexos de unión con posibles actividades de blanqueo de capitales que tratan de legalizar o poner en circulación en el circuito monetario el fruto de estas actividades. En el Capítulo 5, se realizará un estudio de las aplicaciones de naturaleza similar a la desarrollada. Finalmente, el Capítulo 6 presenta las conclusiones y las posibles líneas futuras de trabajo.

De forma adicional, se incluye un anexo con el desglose temporal de las tareas realizadas en este trabajo haciendo uso de un diagrama de Gantt.

2 Tecnología Blockchain

En este capítulo se introducen de forma breve los conceptos asociados a la tecnología blockchain, así como su funcionamiento y las partes integrantes de la cadena. En primer lugar, se presenta la definición de la tecnología blockchain y sus características principales, junto con los tipos de redes que se han desarrollado actualmente. También se detalla el funcionamiento de la cadena de forma genérica. Por último, se incluyen los usos en los que ha derivado esta tecnología.

Una cadena de bloques es un sistema de registro distribuido o *ledger* que permite almacenar información de forma permanente en conjuntos de datos de mayor tamaño denominados *bloques*. Estos bloques son posteriormente validados por el resto de miembros mediante operaciones criptográficas. Una vez se ha añadido a la cadena, el bloque se encuentra enlazado con el bloque anterior, lo que evita posteriores modificaciones de la información; es decir, se garantiza que la información se pueda consultar en cualquier momento y que permanezca invariable [1, 13]. Estas operaciones en las que se almacena la información se distribuyen en forma de *transacciones* o *contratos inteligentes* que una vez aprobados y validados se añaden al registro.

Otra característica fundamental de la cadena blockchain es que forma una red punto a punto (*peer-to-peer*, P2P) en la que los miembros de la red o nodos están todos conectados entre sí. De esta manera, en caso de que uno de los nodos perdiera la conexión frente al resto, la cadena sigue funcionando.

Uno de los pilares en los que se apoya la tecnología blockchain es la *descentralización*, que permite que la información contenida en el registro no se almacene en un único punto, si no que cada miembro del sistema mantenga su propia copia actualizada. Cualquier modificación que sufra el registro se reflejará en el resto de los duplicados [13].

Junto a esta característica se encuentra la *transparencia*, dado que un registro almacenado en la cadena se puede consultar en cualquier momento y por parte de cualquier usuario que así lo desee; y la *confiabilidad*, gracias a que el consenso entre las partes permite que cada nodo pueda enviar o actualizar la información sin que intervenga en la operación un tercero, como puede ser un intermediario.

Otra de sus características idiosincrásicas es la *inmutabilidad*, puesto que la información registrada, una vez autenticada, se puede consultar en cualquier momento con la certeza de que no ha sido alterada intencionada o accidentalmente.

Por último, la *privacidad* que conllevan las operaciones que se realizan entre las partes son a priori desconocidas para el resto de componentes de la red, ya que solo es necesario conocer una parte de la información para realizar la operación.

Todas las características anteriores (descentralización, transparencia, confiabilidad entre las partes, inmutabilidad de los registros y privacidad) se consideran ventajas de la tecnología blockchain. Sin embargo, la adopción de esta tecnología también presenta algunas desventajas [13, 14]:

1. **Inmutabilidad de la información**. Se considera una desventaja cuando se ha validado una operación que incluye errores, ya que es muy difícil corregirlos y el coste de modificar la información es muy alto.
2. **Ausencia de un marco regulatorio y legal** que imponga una normativa común a todos los actores, sobre todo en resolución de conflictos entre las partes.
3. **Problemas asociados a la velocidad del procesamiento de la información debido a un problema en la red**. Esto provoca que no se pueda acceder correctamente a la versión actual del registro.
4. **Excesiva cantidad de recursos utilizados** tanto para realizar la operación de inserción como de validación ya sea en forma de energía usada como cálculo computacional realizado.
5. En el caso de los tokens, como por ejemplo Bitcoin o Monero, su relación con **actividades ilegales y de blanqueo de capitales**.
6. **Escalabilidad del sistema**, máxime cuando la red alcanza un tamaño considerable y los participantes no pueden atender todas las peticiones requeridas de procesamiento.
7. **La existencia de bugs y vulnerabilidades en el código** que afectan a la seguridad de los nodos o del software utilizado.
8. **Costes más altos respecto a otras tecnologías** como, por ejemplo, las transacciones financieras.

2.1 Tipos de redes blockchain

A. Tipo público o *permissionless*

En este tipo de *blockchains*, ilustrado en la Figura 1, cualquier usuario sea o no partícipe de la red puede comprobar las transacciones que se realizan dentro de la misma y participar en el mecanismo de consenso que se encarga de la verificación y validación de las transacciones y su registro posterior en el bloque [15]. Entre sus características, destacan la descentralización, la inexistencia de jerarquía entre los diferentes componentes de la red y la transparencia y visibilidad entre todas las partes. Se le conoce como *permissionless* ya que cualquier usuario puede acceder a la red sin necesidad previa de registro o permiso por parte del resto de usuarios de la red.

La red más conocida de este tipo es la que integra la criptomoneda de Bitcoin o Ethereum.

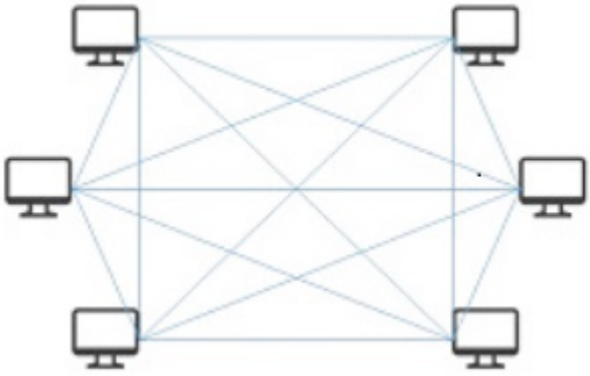


Figura 1: Blockchain de tipo público. Fuente: [14]

B. Tipo privado o permissioned

En este tipo de red, el acceso a la red está restringido solo a los participantes autorizados previamente por la entidad gestora de la red o por los integrantes de la comunidad [15]. Un ejemplo se muestra en la Figura 2. Los usuarios deben cumplir una serie de requisitos establecidos para incorporarse a la red. Este tipo de red se caracteriza por la existencia de una red centralizada y una jerarquía entre los nodos de la red. Solo los actores integrantes pueden visualizar el registro y las transacciones que se realizan entre las partes. Esto provoca que las transacciones y su verificación sean más rápidas con respecto a las de tipo público, de forma que el gasto energético es menor. Su denominación, *permissioned*, remite a la necesidad de recabar el permiso previo de la entidad gestora o

de los miembros de la comunidad para poder acceder a la red y participar en las transacciones que se generen dentro de ella.

Entre este tipo de redes, destaca Ripple o las que han lanzado las empresas del sector financiero o logístico.

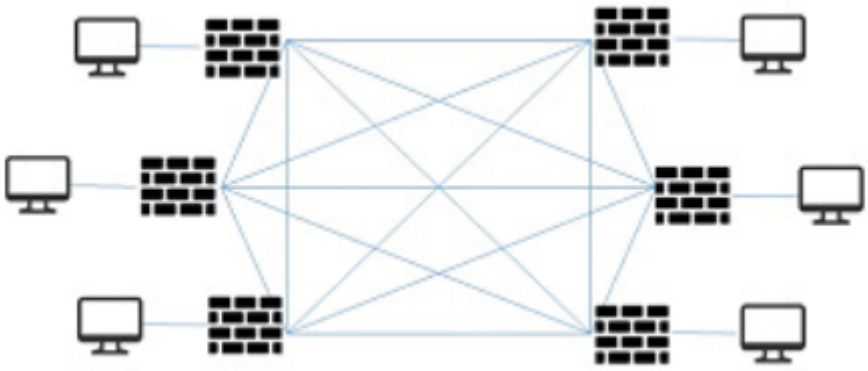


Figura 2: Blockchain de tipo privada. Fuente: [14]

C. Tipo híbrido

Este tipo es una combinación de los dos anteriores, ya que contiene en cierto grado características de ambas redes, como se observa en la Figura 3. Normalmente, en estas redes la parte de la cadena visible para los usuarios externos es el registro de las operaciones (*ledger*), realizado mediante el hash; mientras que otras partes de la red como, por ejemplo, la transacción y la información que contiene la misma, solo son visibles entre las partes intervinientes. Al estar en una posición intermedia entre ambos tipos, el grado de descentralización y jerarquización varía en diferentes grados.

Un ejemplo de este tipo de red son las asociadas a Hyperlegder.

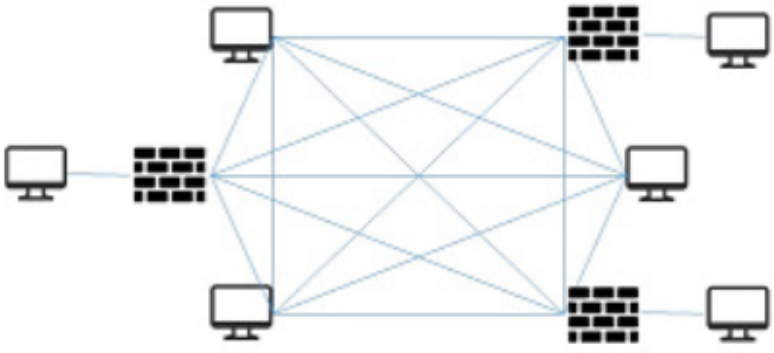


Figura 3: Blockchain de tipo mixta o híbrida. Fuente: [14]

2.2 Funcionamiento de la cadena de bloques

De forma general, una cadena de bloques funciona como se muestra en la Figura 4. Se explican en más detalle a continuación:

1. Un usuario o nodo de la red realiza una operación o transacción que envía a otro usuario. Si esta información cumple una serie de requisitos, el trozo del código o contrato inteligente generado se aprueba y se graba en un bloque, que es luego enviado a la red para que el resto de componentes sepa de su existencia.

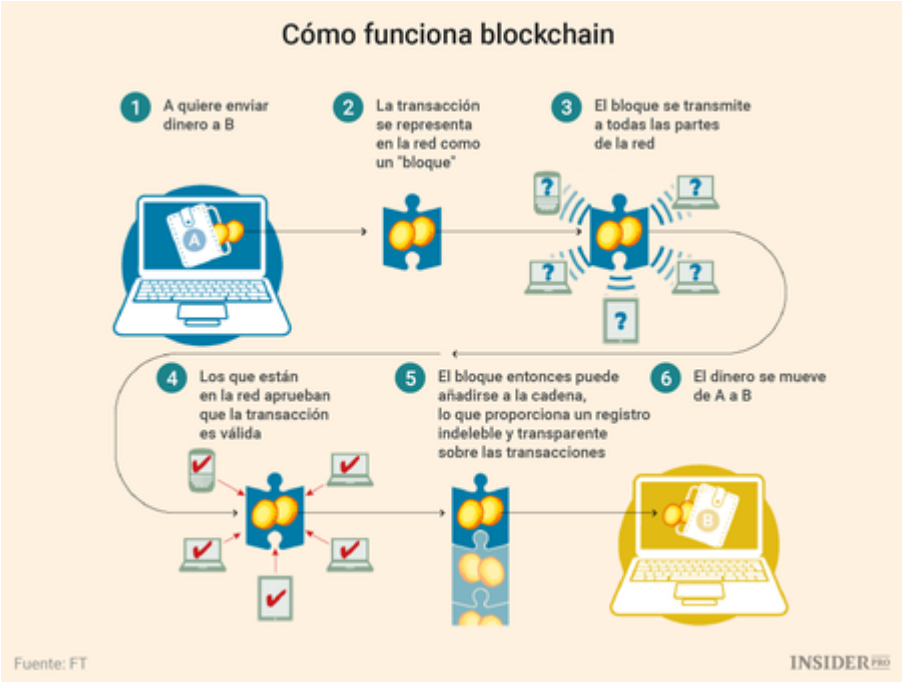


Figura 4: Cómo funciona una transacción en blockchain. Fuente: Financial Times (https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64)

2. En dicho bloque se siguen agrupando más operaciones hasta que se alcanza un tamaño determinado, y el bloque se trasmite al resto de componentes de la red para que lo validen.

3. Posteriormente, los nodos validadores (o mineros en las cadenas que se rigen por el algoritmo de consenso PoW, explicado más adelante) tratan de encontrar el algoritmo hash que permite validar el bloque. Para que se siga cumpliendo el principio de inmutabilidad de la cadena, este hash debe guardar relación con el anterior y además debe ser único para evitar que pueda romperse la seguridad del algoritmo. Para ello se necesita un número arbitrario y de un solo uso que permite obtener este hash a partir del anterior y que además debe estar relacionado con el anterior. Mientras se realiza el cálculo y una vez se obtiene un resultado, este se prueba que cumple la condición preestablecida. Es decir, que enlace el hash obtenido del bloque con el hash anterior a través del *nonce*.

4. Finalmente, una vez que se ha generado el hash del nuevo bloque y este ha sido validado por los nodos competentes (o por un determinado número de nodos), se añade el nuevo bloque a la cadena. Este bloque incluirá todas las operaciones realizadas, la referencia al bloque anterior (o hash) y cualquier otra información que haya sido definida. Un ejemplo de la estructura interna de un bloque se muestra en la Figura 5.

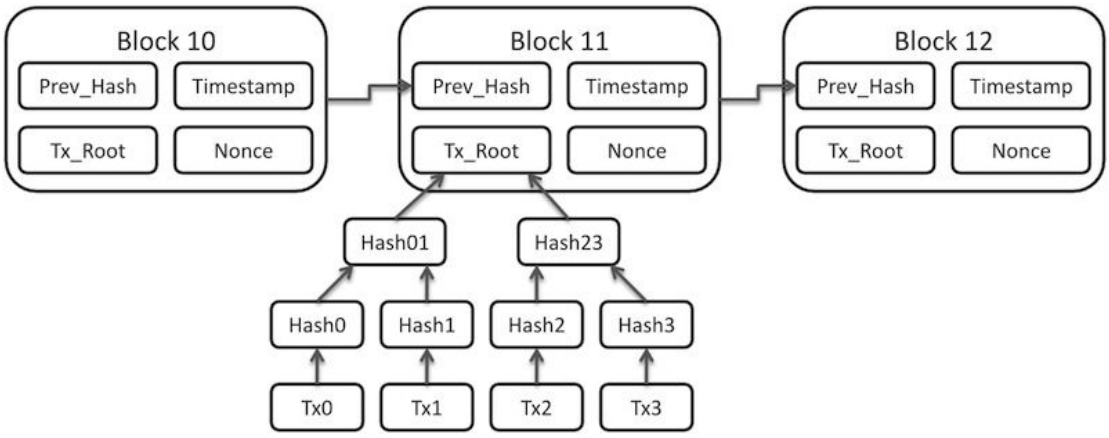


Figura 5: Estructura interna de un bloque. Fuente: theblockchain.es (https://www.theblockchain.es/cadena-bloques-blockchain/)

5. Durante el proceso de validación puede suceder que otro nodo obtenga un hash que también sea considerado válido. En este momento, y hasta que se valide uno de los bloques, se genera una bifurcación a la que se sigue añadiendo

información. Una vez se ha validado uno de los bloques, se descarta el bloque "perdedor" y toda la información que contenga (véase la Figura 6). De esta forma, se evita que se genere información por duplicado.

Dependiendo del mecanismo de consenso utilizado, a los nodos que han participado en el cálculo se les ofrece una recompensa en forma de *tokens*. En el caso de que se quisiera revertir la operación, el gasto sería demasiado alto, lo que disuade a los nodos maliciosos de modificar el bloque y la información que contiene.

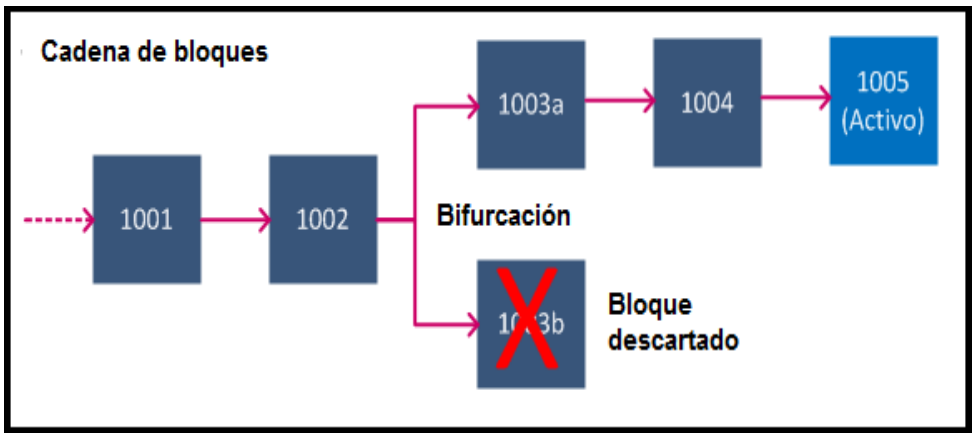


Figura 6: Bifurcación de la cadena de bloques. Fuente: elaboración propia

2.3 Partes de un bloque

Aunque en cada tipo de *blockchain* los bloques pueden presentar algunas diferencias, por normal general, cada bloque se encuentra integrado por los siguientes componentes [2,16]:

a) el hash criptográfico del bloque anterior;
b) el hash criptográfico del bloque siguiente, que junto con el anterior permite realizar la trazabilidad del bloque dentro del registro y guarda los principios de inmutabilidad de la información;
c) el *nonce*, acrónimo en inglés de número usado una vez. Se trata de un número empleado para calcular el hash criptográfico del bloque y que debe guardar relación con el bloque anterior;
d) el número del bloque, que sirve para indicar la posición en la que se sitúa dentro del registro;

e) un marcador temporal o *timestamp*, que sirve para señalar la fecha en la que se generó dentro de la cadena;

f) las transacciones realizadas. En este apartado se incluyen todas las operaciones realizadas entre las diferentes partes y que se han registrado en el bloque una vez que han sido comprobadas y verificadas por un número determinado de componentes de la red. Es un número variable teniendo en cuenta su tamaño en bits; y

g) otra información no relevante como puede ser el número de transacciones realizadas, la cantidad registrada total en dichas operaciones o cualquier otro dato.

2.4 Mecanismos de consenso

Se denomina consenso a la operación de aceptación o validación por parte de la mayoría de los miembros que forman parte de la red de los datos que se inscriben en un bloque dentro de la cadena, estando libres de errores, duplicidades o manipulaciones. Con ello, se pretende evitar que haya datos inconsistentes desde el primer elemento hasta el último registrado hasta el momento, así como evitar el añadido de información que no haya sido previamente validada de alguna forma por parte de los componentes de la red.

Toda información que se trate de añadir a la cadena debe ser previamente analizada y validada por parte de un número determinado de miembros del sistema que certifican la validez de la operación y su posterior inserción en la cadena. Para poder solucionar los problemas de discrepancia que puedan surgir entre los miembros de la red, se plantean diferentes mecanismos de consenso que permiten alcanzar un acuerdo común para todas las partes que intervienen en el proceso de validación del bloque. A continuación, se hará una breve explicación de cada uno de los mecanismos de consenso más conocidos y utilizados.

Estos mecanismos de consenso varían dependiendo de la criptomoneda, como se puede observar en la Tabla 1.

Nombre	Tipo de red	¿Es convertible a otras divisas?	Tiene plataforma de cambio	Mecanismo de consenso
Bitcoin	Pública	Sí	Sí	PoW
Ethereum	Pública	Sí	Sí	PoS
Ripple	Privada	Sí	Sí	PBFT
Bitcoin Cash	Pública	Sí	Sí	PoW
Litecoin	Pública	Sí	Sí	PoW
Stellar	Pública	Sí	Limitado	PBFT
Cardano	Híbrida	Sí	Limitado	PoS
IOTA	Pública	Limitado	No	PBFT
NEO	Privada	Limitado	No	PBFT
Monero	Pública	Sí	Sí	PoW
Dash	Pública	Sí	Sí	PoW-PoS

Tabla 1: Criptomonedas y características

A. Sistema tolerante a fallos bizantinos (PBFT)

Este mecanismo deriva del problema de los generales bizantinos en el que se trata de encontrar una solución lógica al problema de que se produzcan órdenes contradictorias entre las partes [17], como puede ser la adopción de una solución que conlleve la inserción en la cadena de uno u otro bloque.

Para evitar que se produzcan fallos de forma intencionada por parte de nodos maliciosos, se establece un mecanismo de votación para la toma de decisiones por parte de los nodos validadores, en el que si se alcanza el 66% de los votos de dichos nodos el bloque queda automáticamente validado. Estos nodos han sido verificados y acreditados previamente por una autoridad antes de participar en la toma de decisiones.

Destaca por su eficiencia energética. Entre sus debilidades destaca su centralización en uno o pocos nodos que ejercen la autoridad sobre el resto, lo que le hace vulnerable a los ataques de tipo Sybil, donde un nodo malicioso trata de hacerse con el control de la red mediante el uso de engaños e imponer sus decisiones al resto de nodos haciéndoles pensar que sus intenciones son legítimas. Además, su escalabilidad es menor respecto a otros mecanismos de consenso.

B. Proof of Work (PoW)

Es el algoritmo de consenso por antonomasia que se caracteriza porque su funcionamiento está presentado de forma detallada en el texto fundacional del bitcoin [1]. Consiste en premiar el esfuerzo de trabajo realizado por un minero (nodo validador) para obtener el hash correcto. Es decir, en este caso se premia a aquellos nodos que realizan un esfuerzo computacional para obtener el hash que permite enlazar un bloque con el anterior de forma segura. El premio otorgado se adjudica al primero que haya finalizado el cálculo del hash de forma correcta y que, además, haya sido validado por un número determinado de nodos [18]. En caso de que se hayan localizado varios hashes que resuelven el cálculo, el premio se concede al primero que obtiene la validación por el resto de mineros. El resto de subramas que pueden generarse se eliminan una vez se obtiene el consenso entre varios nodos. Este tipo de algoritmo es el que se utiliza en la red bitcoin y en la mayoría de redes blockchains de tipo público.

Entre sus inconvenientes, destaca que provoca un gasto de energía y poder computacional de forma constante y su elevado grado de vulnerabilidad a ataques del 51% (este ataque se explicará más en detalle en el apartado 3) [14].

C. Prueba de autoridad (PoA)

Este algoritmo se basa en la validación de las transacciones y los bloques efectuados entre las partes por parte de un pequeño grupo de agentes autorizados que son conocidos por el resto de los miembros de la red [19].

Entre sus ventajas, frente a otros mecanismos, destaca su escalabilidad, su eficiencia computacional y su rapidez a la hora de validar las operaciones, además de su reducido gasto energético. Por el contrario, presenta como desventaja la censura que puede sufrir un nodo por parte de otros miembros de la red. Asimismo, es vulnerable a la actuación de nodos maliciosos y frente a ataques de tipo DDOS (se explica más adelante) o Sybil.

D. Prueba de tiempo transcurrido (PoET)

Se caracteriza por conceder a cada componente de la red un tiempo de ejecución sin tener en cuenta su tamaño y sus características [14]. Una vez se ha consumido ese tiempo, el proceso de creación del bloque se concede a otro participante.

Su ventaja es que el coste de participación en la validación es muy bajo y su desventaja principal es que no es funcional en blockchains públicas.

E. Prueba de capacidad o de espacio (PoC)

Se caracteriza porque el nodo que realiza las operaciones de validación reserva un espacio en disco en cual almacena de los cálculos realizados en el equipo [20]. Una vez ha obtenido el resultado, el espacio se libera pudiendo usarse para otra tarea.

Su principal ventaja es su eficiencia computacional frente al PoW, porque utiliza para ello espacio que no se está utilizando en ese momento. Entre sus desventajas destaca que no es inmune a la actividad de malware, lo que puede provocar un descenso del rendimiento del algoritmo de consenso.

F. Prueba de quemado (PoB)

Este algoritmo de consenso, que deriva del PoW, se caracteriza porque el nodo que se encarga de validar los datos contenidos en los bloques es aquel nodo que malgasta en favor del sistema los tokens obtenidos por realizar los cálculos criptográficos necesarios [21].

Entre sus ventajas destaca que el gasto tanto energético como en equipamiento es menor respecto a otros consensos. Por el contrario, se produce un cálculo de operaciones innecesario lo que provoca que el proceso de validación sea más lento. Además, es vulnerable a los mismos ataques que afectan al PoW al descender de éste.

G. Proof of Stake (PoS)

Es el otro algoritmo de consenso más conocido. Se caracteriza por estar basado en la participación de los nodos que han sido elegidos previamente según unos criterios de cuota. El nodo validador se elige de entre aquellos que tienen en su poder más tokens almacenados, es decir, aquellos que han invertido en crear su propio stock de criptomomedas son lo que tienen más posibilidades de validar la operación y de paso, el mayor porcentaje de la recompensa generada [14].

Dentro de este consenso hay variantes, como el DPoS (Delegated PoS), donde se delega la participación ante los nodos validadores que resultan elegidos para verificar un bloque; y el LPoS (Leased PoS), donde se repercute la recompensa entre aquellos usuarios que alquilan su stock a otros nodos [15].

Entre sus ventajas con respecto al PoW, destaca que requiere un gasto energético menor y, además, prima a los nodos en base a su participación en el cálculo del hash. Como inconvenientes principales destacan su vulnerabilidad a los ataques DDOS y a los ataques de tipo eclipse, que permiten aislar un nodo del resto de la red, así como la concentración de la tarea de validación en unos pocos nodos.

En la Tabla 2 se puede observar un resumen general de las principales ventajas y desventajas que contiene cada uno de los mecanismos de consenso explicados anteriormente.

Mecanismo de consenso	Principales ventajas	Principales desventajas
PBFT	Eficiencia energética al no necesitarse a otro para la validación	Centralización en uno o pocos nodos. Vulnerable a ataques Sybil
PoW	Cálculo de hashes potentes y seguros	Gasto de energía y poder computacional elevado. Vulnerable a ataques del 51%
PoA	Escalabilidad, eficiencia computacional y rapidez de validación	Censura. Vulnerable frente a ataques DDOS o Sybil.
PoET	Coste de participación en la validación es muy bajo	Inoperable en blockchains públicas
PoC	Eficiencia computacional	Vulnerable al malware
PoB	Gasto energético y en equipamiento bastante menor.	Gasto operacional elevado y es vulnerable al ataque del 51%.
PoS	Gasto energético menor. Prima la participación de los nodos	Concentración de la validación en pocos nodos. Vulnerable a los ataques DDOS y Eclipse

Tabla 2: Principales ventajas y desventajas de los mecanismos de consenso.

2.5 Anonimización y privacidad

El término anonimización se ha popularizado en los últimos años gracias sobre todo a la tecnología blockchain y a la implantación del nuevo Reglamento General de Protección de Datos. Según recogen la Real Academia de la Lengua (RAE) y la Fundación del Español Urgente (Fundéu), ´anonimizar´ es la acción de «Expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad.» [22].

La anonimicidad se considera como uno de los elementos claves de la la tecnología blockchain. En el documento de Satoshi Nakamoto [1], se considera importante que cualquier transacción que se realice entre dos o más participantes sea anónima para el resto de componentes de la red. En la práctica, al guardarse un registro de las operaciones que se realizan en la cadena, la operación ya no es anónima. Son anónimas las titularidades de los intervinientes en las operaciones (únicamente se conoce las carteras digitales, pero no sus propietarios), pero no la operación en sí. Con las acciones de desanonimización se trata de localizar y poner nombre a los propietarios de las carteras digitales, es decir, se intenta potenciar el rastreo por parte de terceros, haciendo uso de determinados fallos o vulnerabilidades de los protocolos utilizados por la red permitiendo la identificación de una o ambas partes que han intervenido en la operación. Por todo esto se dice que las criptomonedas son pseudo-anónimas.

En los diferentes estudios realizados respecto a las principales criptomonedas utilizadas por los usuarios, las transacciones que pueden ser desanonimizadas al no tomar las medidas necesarias de protección frente a acciones de desanonimización a la hora de transferir o recibir criptomonedas varían desde el 63 % en el caso Monero hasta el 85% en el caso de Zcash, tal y como se puede comprobar en la Tabla 3 [23].

Criptomoneda	% Transacciones desanonimizables	% Transacciones parcialmente desanonimizables	% Transacciones difícilmente desanonimizables
Bitcoin	65	21	5
Zcash	85	8	7
Monero	63	15	22

Tabla 3: Porcentaje de transacciones desanonimizables y anonimizables por criptomoneda. Fuente: [23]

Una característica fundamental que facilita las labores de desanonimización es el tipo de la red. Si la red es *permissionless*, aun usando algoritmos criptográficos como ECDSA o RSA en la firma para proteger la identidad del partícipe de la operación, se puede vincular fácilmente. Esto es, se puede localizar al responsable de la transacción pudiendo comprobar alguno de los datos contenidos en el bloque como son la dirección de envío o de destino y datos de las operaciones como el intervalo temporal en el que se realizó el importe transferidor o el balance de la cartera de una de las partes [23].

Nombre	Lenguaje de programación	Algoritmo de encriptación	Tipo de Pseudo-anonimización
Bitcoin	C++	SHA-256d	Enlazable
Ethereum	C++, Go, Rust	Etash	Enlazable
Ripple	C++	ECDSA	Enlazable
Bitcoin Cash	C++	SHA-256d	Enlazable
Litecoin	C++	SHA-256d	Enlazable
Stellar	C++, Go, Java	FBA	Enlazable
Cardano	C++, Go, Rust	Etash	Enlazable
IOTA	Java	SHA-3	Enlazable
NEO	C#	SHA256 y RIPEMD160	Enlazable
Zcash	C++	EquiHash	Inenlazable
Monero	C++	CryptoNight	Inenlazable
Dash	C++	X11	Inenlazable

Tabla 4: Criptomonedas: Algoritmo de encriptación y tipo de anonimización.

Tal y como se puede comprobar en la Tabla 4, las criptomonedas Bitcoin y Ethereum, entre otras, son pseudo-anónimas enlazables ya que las transacciones realizadas se registran en

el ledger incluyendo las direcciones de las carteras que han intervenido, el importe y la fecha de realización. Es decir, al ser transparentes por naturaleza, es posible vincular una transacción con los actores que la han realizado. En el caso de Zcash y Monero, son consideradas pseudo-anónimas inenlazables [24,25] debido a que las operaciones que se realizan entre las partes van a un *pool* o fondo común que se encarga de completar la transacción y enviar el importe al destinatario final. De esta manera, se evita revelar las partes intervinientes en la operación eliminando el rastro de la misma.

Para proteger la identidad de los usuarios de la red blockchain, estas han incorporado una serie de mecanismos o protocolos que añaden una capa adicional de privacidad y seguridad a los participantes. Entre estos cabe destacar los servicios de mezclado que permiten realizar las operaciones de forma conjunta entre varias carteras mediante la asignación temporal de la propiedad a un intermediario (servicios como CoinJoin o CoinShuffle) [26], o el envío de los fondos a varios mezcladores de dinero entrelazados. También es posible hacer uso de los anillos de firmas, carteras silenciosas o usar diferentes algoritmos criptográficos para establecer otras capas de seguridad y privacidad a las carteras y transacciones.

2.5.1 Otras formas de desanonimización

La presencia de bugs y vulnerabilidades en el software empleado en las redes blockchain, en las *smart contracts*, o en las páginas web de las casas de cambios y en las apps de carteras digitales puede ayudar a desvelar la identidad online del propietario mediante la publicación del libro de registro [27].

Asimismo, se recomienda evitar casas de cambio o apps de carteras fraudulentas que permiten a los agentes malintencionados robar los fondos almacenados y señalar a los propietarios de una cartera. Esto último permite a los agentes maliciosos realizar ataques específicos contra dicho usuario para infectar su equipo mediante el envío de phishing y obtener las credenciales de otros servicios.

De forma adicional, se recomienda a los usuarios de criptomonedas que lleven a cabo una serie de acciones y buenas prácticas para proteger su seguridad y privacidad y, con ello, eviten ser desanonimizados. La principal recomendación es el uso de una red privada virtual (VPN) que permite ofuscar la IP real que se ha utilizado en el momento de realizar

la operación. Al estar basada la arquitectura de red en el protocolo P2P, se puede llegar a descubrir la IP real utilizada y con ello la identidad del usuario final [28].

Del mismo modo, los usuarios deben evitar publicar la dirección o el identificador de la cartera digital en foros y perfiles de redes sociales, ya que se puede realizar un seguimiento de las transacciones efectuadas provocando finalmente la revelación de la identidad, además de facilitar información para ser víctimas de ataques de malware o phishing. Uno de los objetivos de este proyecto es aprovecharse de este tipo de información para intentar desanonimizar a los propietarios de carteras digitales.

Otra recomendación es no reutilizar una misma cartera durante mucho tiempo y evitar el intercambio con carteras no fiables que puedan estar contaminadas y servir para desenmascarar al propietario de una cuenta con los riesgos para su privacidad.

Por último, hay que tener en cuenta las presiones regulatorias, normativas legales y financieras que pueden obligar a las casas de cambio a cumplir con leyes de anti-lavado de dinero (AML), conocimiento del cliente (KYC), antiterroristas (CTR) y protección de datos (GDPR).

2.5.2 Acciones posibles de desanonimización

Básicamente, es posible desanonimizar e identificar a los usuarios que realizan transacciones de criptomonedas en redes blockchain mediante las siguientes acciones:

- *Análisis web*, que incluye la investigación de datos en línea, registros de sesiones de Internet, determinación de la dirección IP y el destino físico.
- *Análisis de la estructura de la cadena de bloques*, que incluye el marcado y seguimiento de forma automática y manual del historial de transacciones y su asociación con datos web y otras pruebas relevantes.

En el rastreo de carteras digitales se realizan tareas de vigilancia en busca de éstas y otras evidencias en los comentarios y anuncios publicados en los foros, tiendas y páginas web, fundamentalmente alojadas en los servicios ocultos de la *Darkweb*.

Además, teniendo en cuenta la naturaleza de las redes blockchain, se pueden utilizar otras

herramientas, como las que permiten realizar tareas de monitorización de los nodos involucrados en la red. Al ser redes P2P, es posible detectar las IP utilizadas por dichos nodos salvo que utilicen una conexión VPN para ofuscar la dirección IP real con la que se conecta al blockchain o usen la red TOR.

En el seguimiento de carteras digitales y su vinculación a actividades ilícitas o de blanqueo se incluyen la presencia de las direcciones de carteras en páginas y foros de servicios de la *Darkweb* como los de mezclado de transacciones con el fin último de entorpecer la vinculación con las operaciones de blanqueo de capitales. Una vez localizadas, se realiza un estudio de los movimientos realizados por dichas carteras en forma de transacciones o contratos inteligentes con los que se mueven los fondos de tokens y criptomonedas. Para ello, se realizan peticiones a las cadenas de bloques para obtener la información registrada en el ledger. De forma seguida, se extrae la información y se clasifican las carteras teniendo en cuenta el uso real de la misma. Es decir, si la cuenta es de cuenta es de uso personal se indica como tal, pero si pertenece a una casa de cambio, se señala dicho uso y, además, el nombre de la casa de cambio.

Asimismo, se usan direcciones contaminadas para marcar las direcciones que utilizan los servicios de mezclado o criptomonedas con algoritmos de ofuscación como, por ejemplo, Monero.

2.6 Usos del blockchain

Además del mercado de intercambio de criptomonedas y de operaciones financieras, el uso del blockchain se ha diversificado hacia otros muchos campos, entre los que destacan la logística (aplicado por la empresa TradeLens) [29], la trazabilidad de los productos alimentarios (Carrefour) [30], el sector sanitario (MedRec) [31], la protección de los derechos de propiedad intelectual (Binded) [32] o la confianza y la protección del periodismo independiente (CIVIL) [33].

Entre los usos maliciosos principales destaca el pago por ataques de ransomware, un tipo de extorsión que usa un tipo de malware que infecta un equipo y encripta toda su información, solicitando un pago para el rescate de los datos. En la mayoría de los casos, las víctimas no consiguen la clave de desbloqueo a pesar de haber realizado el pago. Entre los ataques más famosos destacan los protagonizados por WannaCry, Locky o Cryptolocker

[34], entre otros. Informes recientes detallan la ocurrencia de más de 200 millones de ataques de ransomware en todo el mundo en el año 2018 [35].

Otro uso ilegal de las criptomonedas es el cryptojacking. Se trata del secuestro de un dispositivo electrónico sin el consentimiento o conocimiento de la víctima para el minado de criptomonedas. Esto se logra inyectando un código en el dispositivo (generalmente JavaScript), que se ejecuta en segundo plano después de que la víctima haya entrado en una web infectada. Los réditos obtenidos de esta operación se envían a la cuenta del propietario del software malicioso. El caso más famoso de este tipo fue protagonizado por el software minero Coinhive [36]. La víctima puede identificar este problema al detectar que su dispositivo trabaja con bastante lentitud sobre todo cuando navega por Internet.

También cabe destacar el uso combinado de los dos anteriores, que se conoce como minería de punto final o «endpoint miners», que consiste en infectar con ransomware un equipo exigiendo un pago para su liberación. Mientras se espera que la víctima haga el pago, el equipo realiza operaciones de minado, de forma que se produce un doble perjuicio para la víctima. Un ejemplo es ABD Miner, que venía preinstalado en móviles baratos Android de fabricación china y que no estaban sujetos a la vigilancia de la marca fabricante [37].

Entre las actividades maliciosas unidas a las criptomonedas, destacan el pago de productos y servicios en la Darknet, gracias a la capa de anonimato proporcionado por la red Tor con los que se trata de evitar el rastreo del pago. Entre estos destacan los mercados de productos ilegales de Silk Road y Hansa en 2017 [38].

Por último, se deben tener en cuenta otros delitos asociados a las actividades anteriores, como son el blanqueo de capitales y el lavado de dinero procedente de actividades ilícitas (narcotráfico, secuestros, yihadismo, etc.). Los actores de este tipo de actividades se aprovechan de la mayor privacidad de estas operaciones para lograr introducir en los circuitos financieros el dinero de procedencia dudosa, además de enviar a otras partes del mundo el dinero obtenido de estas actividades sin que entre en el radar de las autoridades. Un ejemplo del lavado de dinero a través de carteras digitales se muestra en la Figura 7.

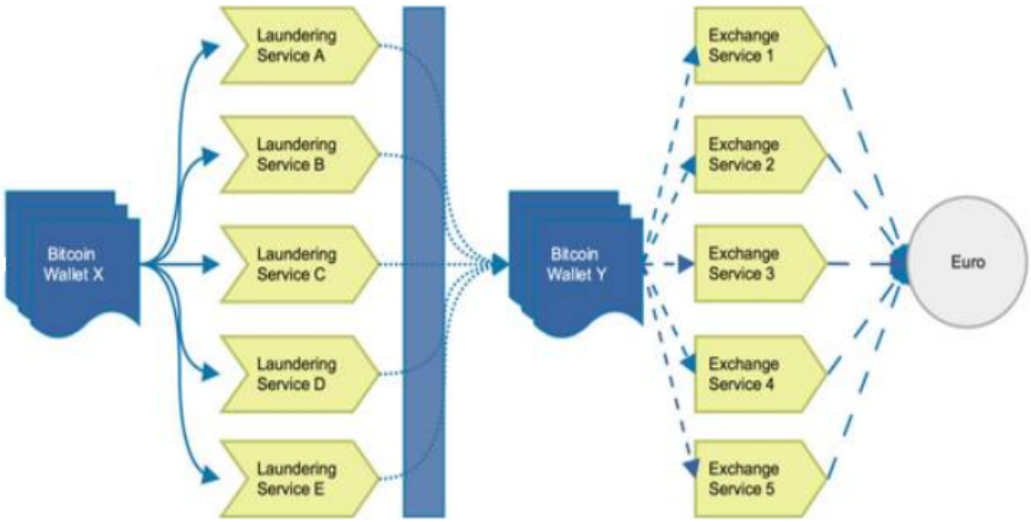


Figura 7: Método de lavado de dinero procedente de carteras digitales. Fuente: TuDelft.nl (https://pure.tudelft.nl/portal/files/46267036/JFC_11_2016_0067.pdf)

Las criptomonedas también han sido utilizadas como cebo para realizar estafas en forma de falsas operaciones de mercado financiero como ofertas iniciales de monedas en las que los fondos depositados son robados por el propio emisor o estafas piramidales. Otro factor de riesgo son los robos de carteras alojadas en casas de cambio víctimas de ataques, como lo que le ocurrió a Mt. Gox en el 2014 [39].

Como dato importante para destacar, el Banco Central Europeo considera las criptomonedas como monedas de cambio, y ha solicitado las autoridades competentes a actualizar las normas monetarias para tratar de combatir de forma eficaz estos delitos al no estar bajo la regulación financiera de ninguna institución. A este respecto, destaca en la Unión Europea la entrada en vigor de la 5ª Directiva Europea contra el blanqueo de capitales conocida como AMLD5 [40].

3 Amenazas y vectores de ataques

En este apartado se explican de forma detallada todos los ataques que han afectado a esta tecnología aprovechándose de sus vulnerabilidades, bugs o de los errores de factor humano. Se describen de forma pormenorizada todos aquellos ataques que han sido probados con éxito, así como algunos otros de carácter más teórico.

3.1 Ataque de denegación distribuida de servicio o DDoS

Los ataques DDoS se manifiestan de varias maneras dependiendo de la naturaleza de la aplicación, la arquitectura de la red y el comportamiento de los pares. Este ataque provoca que un nodo o grupo de nodos queden aislados del resto de la red al no poder retomar su conexión con la red, ya que han recibido demasiadas solicitudes impidiendo que el equipo o red atacada responda de forma ordenada a las mismas [41].

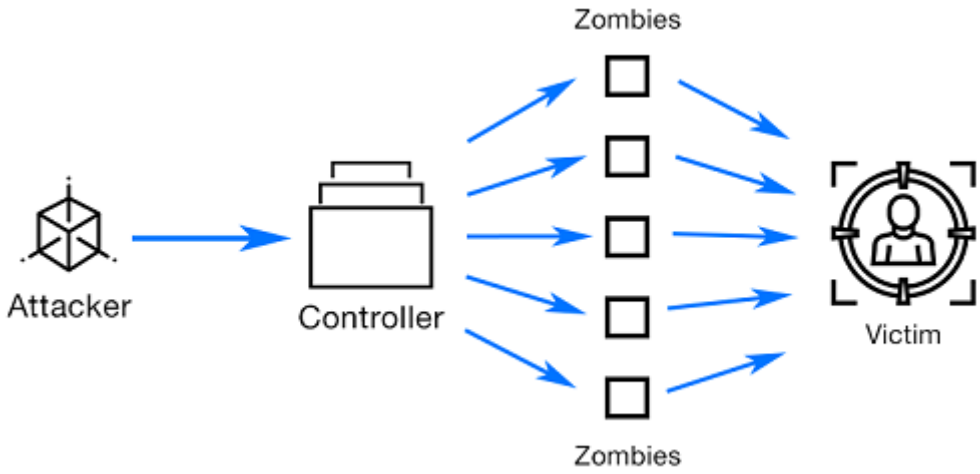


Figura 8: Ejemplo de un ataque de tipo DDoS. Fuente: medium.com

Entre sus efectos perniciosos se encuentran la imposibilidad por parte de la víctima de actualizar su versión de blockchain almacenada, realizar transacciones, agregar o validar los bloques, o separar a un grupo de mineros de la rama principal. Además, este ataque puede utilizarse de forma conjunta con otros (como, por ejemplo, el ataque del 51%), como se ha comprobado en casos recientes en los que un grupo (denominado pool) de mineros de carácter malicioso ha conseguido validar otros bloques completamente diferentes de los que se deberían haber validado y, además, cambiar las transacciones que habían sido previamente validadas por otras completamente diferentes (esto último provoca un ataque de doble gasto) [41]. Esta acción modifica la cadena y evita que otros

mineros con menor poder computacional puedan imponer sus bloques sobre lo que dicte el pool.

3.2 Ataque del 51%

Este ataque se caracteriza porque un participante (o conjunto de participantes) une sus activos o poder de minado en un pool para aumentar considerablemente sus opciones de validar las operaciones que se registren en la cadena [41]. Al encontrar más rápido que otros nodos el valor nonce, que permite obtener el hash de la firma del bloque, se puede alterar el orden natural y obligar al resto de la red a aceptar las operaciones validadas por el atacante. Esto puede provocar que se modifique la información contenida en el bloque y que se derive en una operación de doble gasto o crear una bifurcación que se impone al resto de la red al inscribir un bloque diferente al que se debería haber validado en el ledger de la cadena de bloques.

Aunque se define como un proceso costoso de realizar por parte del atacante, se ha demostrado que puede realizarse con extrema facilidad, sobre todo en redes blockchain de poco valor gracias a servicios que permiten alquilar poder computacional. Estos servicios, entre los que destaca NiceHash o Antminer D3 [42], permiten alquilar por horas sus equipos para realizar ataques con un coste ínfimo en el caso de criptomonedas con poca capitalización o en los que la participación de nodos dentro de la red es limitada. La Tabla 5 muestra el coste por hora para las diferentes criptomonedas existentes.

Entre la multitud de ejemplos de este ataque, destaca el que afectó a la criptomoneda Verge en la que varios nodos agrupados en un pool controlaron a su antojo la red, provocando pérdidas al resto de usuarios por un importe de 20 millones de euros [11].

Criptomoneda	Algoritmo	Ratio Hash	Coste 1 hora de ataque	Porcentaje de hash alquilado sobre el total de la red
Bitcoin	SHA-256	79,631 PH/s	$752,776	0%
Ethereum	Ethash	160 TH/s	$95,752	3%
BitcoinCash	SHA-256	2,212 PH/s	$20,908	2%
Litecoin	Scrypt	322 TH/s	$19,734	2%
BitcoinSV	SHA-256	938 PH/s	$8,870	4%
Monero	CryptoNightR	316 MH/s	$4,301	3%
Dash	X11	4 PH/s	$2,823	4%
EthereumClassic	Ethash	11 TH/s	$6,440	44%
Zcash	Equihash	4 GH/s	$9,644	4%
LitecoinCash	SHA-256	7 PH/s	$63	574%
BitcoinPrivate	Equihash	2 MH/s	$5	8,096%

Tabla 5: Coste de una hora de ataque y poder de cálculo que se puede alquilar respecto al total de la red a fecha de 1 de septiembre de 2019. Fuente: Crypto51.app

3.3 Ataque Sybil

Tal y como se aprecia en la Figura 9, se caracteriza por un atacante o grupo de atacantes que crean de forma intencionada multitud de nodos supuestamente independientes que, en realidad, trabajan de forma coordinada entre sí para engañar al nodo objetivo del ataque [16]. De esta forma, ciertos nodos legítimos pueden sufrir una usurpación de identidad al estar solo conectados a los del atacante. La vulnerabilidad del sistema depende de la facilidad para crear nuevas identidades y la importancia de la cadena de confianza, que puede hacer que todas las identidades sean tratadas por igual.

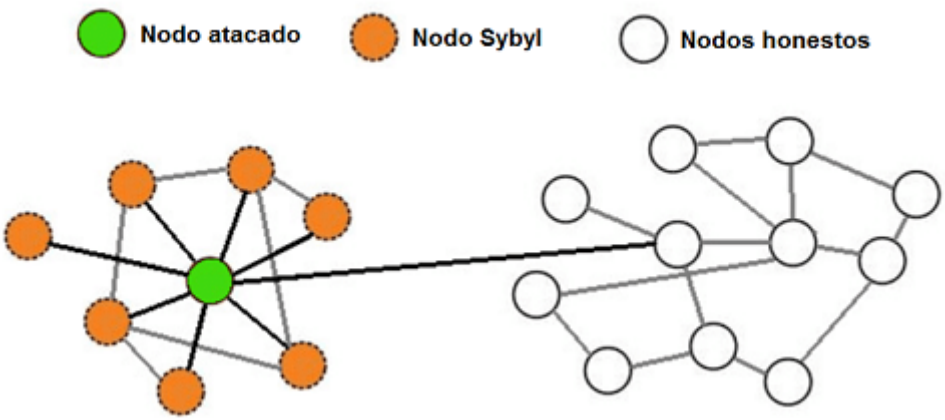


Figura 9: Representación gráfica ataque Sybil. Fuente: coindesk.com (https://www.coindesk.com/bitcoins-security-model-deep-dive)

3.4 Ataques relacionados con la red

Estos ataques se aprovechan de las debilidades de la infraestructura de red, destacando los que afectan a los paquetes IP como los secuestros BGP o el enrutamiento a través de proveedores de Internet maliciosos [43]. En el primer caso, se trata de secuestrar los paquetes de red, alterándolos y enviándolos modificados al equipo de la víctima que los considera válidos. En el segundo caso, se ralentiza la recepción o envío de paquetes provocando que el usuario quede desconectado de la red evitando que actualice su ledger, valide bloques o realice transacciones.

Otra variedad dentro de estos ataques de red es el secuestro de DNS. Este se produce cuando un nodo se conecta por primera vez a la red blockchain, dado que necesita averiguar qué nodos están activos y para ello, realiza una petición a los servidores de la red para obtener las direcciones IPs de los nodos que aceptan conexiones entrantes. Una vez que se ha conectado correctamente a la red, sigue enviando solicitudes y recibiendo direcciones IPs de los pares activos a los que conectarse. Este mecanismo de petición y resolución de DNS puede ser aprovechado por nodos maliciosos, mediante un ataque MITM (Man-In-The-Middle) [44], tal y como se observa en la figura 10, para inyectar una lista no válida de nodos o envenenar la caché DNS del cliente del software de resolución. Si el atacante inyecta una lista falsa de *nodos*, el usuario se verá comprometido. Como resultado, el usuario se conecta a nodos maliciosos en la red falsificada y los nodos maliciosos pueden agregar bloques falsos a la cadena almacenada en el equipo del usuario.

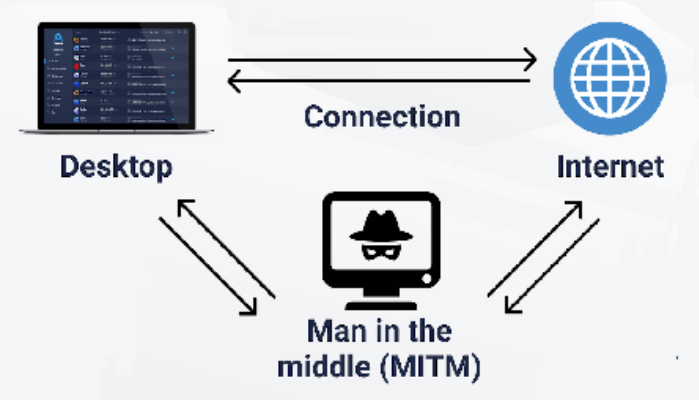


Figura 10: Ataque MITM contra red blockchain. Fuente: Atomicwallet.io (https://support.atomicwallet.io/article/18-why-is-it-important-to-use-a-vpn).

3.5 Ataque tipo eclipse

Este ataque se caracteriza por el control de forma efectiva de todas las conexiones entrantes y salientes de la víctima, aislándolo del resto de la red [17] como se observa en la figura 11. De este modo, trata de modificar su visión del bloque, obligar a la víctima a realizar operaciones computacionales innecesarias, imponerle un bloque distinto del validado o forzarle a realizar operaciones de doble gasto con el consecuente quebranto.

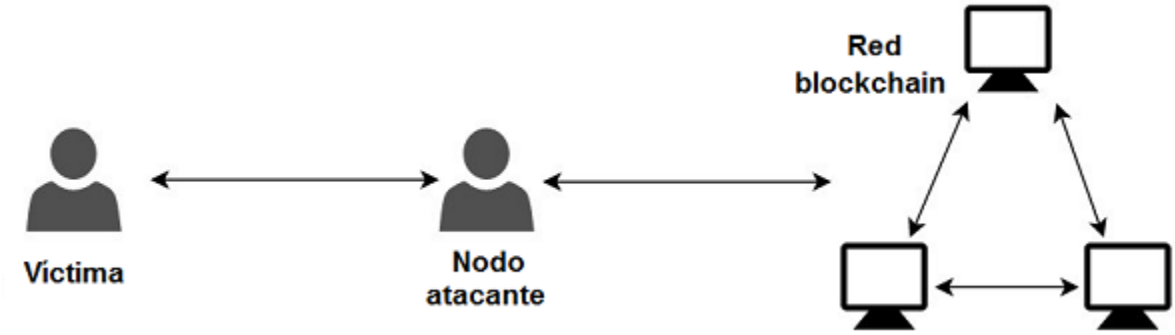


Figura 11: Representación gráfica del ataque eclipse. Fuente: Packt (https://hub.packtpub.com/what-can-blockchain-developers-learn-from-eclipse-attacks-in-a-bitcoin-network-koshik-raj/)

3.6 Ataque de repetición o doble gasto

El ataque de repetición o doble gasto consiste en realizar una misma transacción en dos diferentes blockchains [17]. Por ejemplo, cuando una criptomoneda se bifurca en dos monedas separadas, los usuarios tienen activos iguales en ambos ledgers lo que les

posibilita la oportunidad de realizar una transacción en cualquiera de las dos cadenas, como se puede comprobar en la Figura 12.

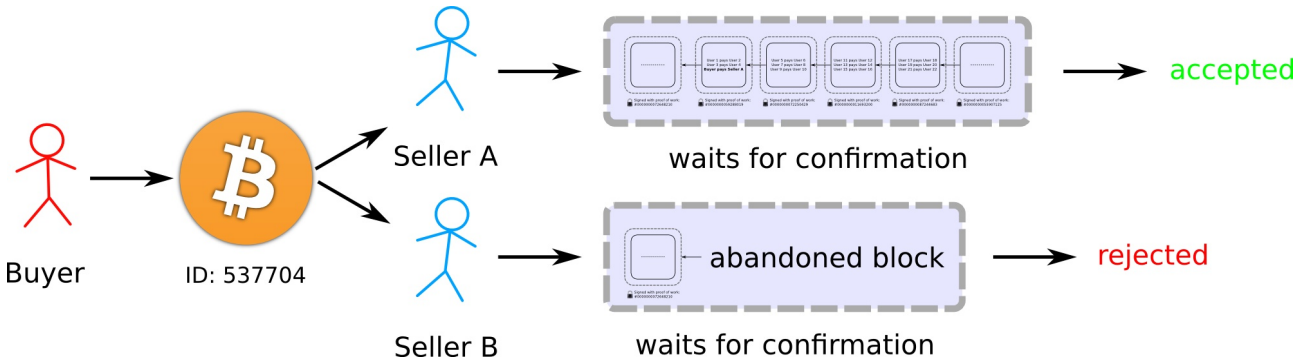


Figura 12: Ataque doble gasto. Fuente: Medium.com (https://medium.com/@sumanthneppalli/on-blocktimes-and-confirmations-4b6057dd49d7)

En este caso, el atacante rastrea los datos registrados de una transacción en uno de los ledger y los reproduce en el otro, con lo que la dirección de la cartera de origen de los fondos pierde activos por partida doble, uno de la transacción real y otro de la replicada en la otra red. Este ataque se probó con éxito en la bifurcación de la red Ethereum y permitió a los atacantes robar fondos por valor de 6 millones de dólares americanos [45].

La posibilidad de doble gasto introduce el concepto de inflación en el mercado de criptomonedas, aunque según el documento original de bitcoin [1] esto no sería posible. La inflación se produce al ser aceptadas por la red las operaciones en la que se ha producido el ataque, de forma que las criptomonedas falsas se han generado como si fueran reales.

3.7 Ataque de carrera

Un ataque tipo race se ejecuta cuando un atacante crea dos transacciones que entran en conflicto [16]. La primera transacción se envía a la víctima, quien acepta el pago y envía el producto sin esperar la confirmación de la transacción. Al mismo tiempo, una transacción en conflicto que devuelve la misma cantidad de criptomoneda al atacante se transmite a la red, lo que finalmente invalida la primera transacción. El atacante aprovecha el tiempo que tarda en validarse una transacción para su propio beneficio.

3.8 Ataques contra contratos inteligentes

Estos ataques se focalizan en las vulnerabilidades que se encuentran en el software, como pueden ser los lenguajes de programación utilizados, el entorno en el que se ejecuta o la forma en la que se codificó [26]. Dentro de los ataques contra contratos inteligentes, el más famoso fue el que afectó a DAO (Decentralized Autonomous Organization) en 2016. DAO era una organización con un funcionamiento de empresa de capital riesgo que se encargaba de financiar proyectos. Una de sus características destacadas era que las decisiones se tomaban entre los participantes, sin la necesidad de tener un consejo de dirección. El ataque sufrido consistió en aprovechar una vulnerabilidad presente en los contratos inteligentes por la que se permitía al atacante realizar operaciones de forma recursiva para la retirada de fondos, sin que estos fondos se descontaran previamente del balance de la cuenta hasta pasado un tiempo definido en la función. El atacante consiguió así 3.6 millones de la criptomoneda Ether [42].

Relativas a la codificación empleada, los ataques de reentrada pueden suponer un riesgo para los usuarios que realizan un contrato. Estos se producen cuando un usuario no actualiza el saldo contenido en el contrato antes de enviar las criptomonedas contenidas en el mismo. Si el envío es capturado por un atacante, este puede realizar varias peticiones y obtener fondos con el mismo contrato.

Relativas al lenguaje de programación utilizado en el software de las aplicaciones, como por ejemplo, las máquinas virtuales (Ethereum Virtual Machine). Estos errores pueden ser defectos propios del lenguaje que se encuentran presentes en un contrato inteligente, en la cadena de bloques o en los errores que se producen al acceder al contrato. Todo esto permite a un atacante acceder a las funciones sensibles presentes en el contrato y modificarlas a su antojo.

Relativos al entorno en el que se ejecutan, se encuentran los ataques de Denegación de servicio dirigidos o DOS que afectan al propietario de un contrato inteligente que intenta realizar una transacción. El agente malicioso realiza múltiples peticiones de reembolso desde direcciones diferentes con el objetivo de eliminar al resto de competidores de la subasta para adjudicarse el contrato.

3.9 Robo de carteras

Las carteras digitales se clasifican en carteras frías (*cold wallets*) o basadas en hardware y que no tienen conexión a internet; o carteras calientes (*hot wallets*) o basadas en software y que se encuentran conectadas a Internet (se muestran ejemplos de ambas carteras en la Figura 13). Este tipo de robos se caracteriza por aprovecharse de las vulnerabilidades y los bugs presentes en las carteras digitales como pueden ser vulnerabilidades en el software empleado para realizar una determinada operación o defectos de operación de algoritmos criptográficos que permiten el robo de las credenciales utilizadas por la víctima, como, por ejemplo, su clave privada.

Figura 13: Ejemplos de cartera fría y caliente. Fuentes: Ledger.com (https://shop.ledger.com/pages/ledger-nano-x) y blockchain.com

Estos robos también pueden producirse mediante una infección previa de la cartera. En el caso de las carteras frías, con malware preinstalado de fábrica o con errores en el software de los drivers [46], el software usado, o incluso por la infección posterior por parte de malware que infecte el dispositivo al cual se conecta.

3.10 Selfish mining

Este ataque, también conocido como de retención del bloque, permite a un actor malicioso o *selfish miner* no transmitir un bloque validado con éxito al resto de la red [46]. Es decir, aunque haya encontrado el hash correcto que le permite validar el bloque, no lo

comparte con el resto de miembros si no que sigue calculando el siguiente hash que le permita validar el siguiente bloque. Tras encontrar el resto de mineros el primer bloque, el minero deshonesto publica ese bloque y el siguiente posterior con lo que obtiene la recompensa de ambos bloques. Para que sea exitoso este ataque, el minero debe construir y mantener por su cuenta una cadena privada con un tamaño superior en un bloque respecto de la pública, además de tener suficiente poder computacional para realizar los cálculos de forma ágil.

Una variación del selfish mining, conocido como *Fork-after-Withhold* (mostrado en la Figura 14), consiste que el minero malicioso oculta un bloque ganador y lo descarta o lo libera más tarde para crear una bifurcación, según la situación que desee crear. Esto puede provocar que un grupo de mineros calcule varios bloques que finalmente no sean validados por la red, lo que les supone una pérdida de tiempo en el cálculo de bloque.

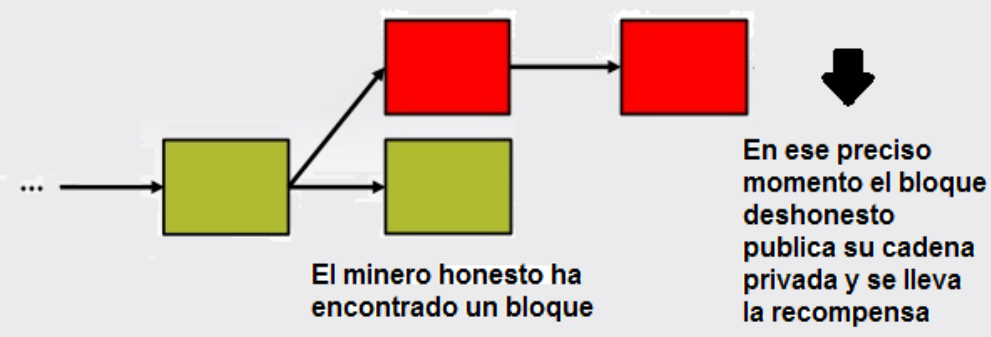


Figura 14: Ataque selfish mining. Fuente: Elaboración propia

3.10.1 Vulnerabilidad de los algoritmos hash

Los algoritmos hash se utilizan para crear firmas digitales seguras y robustas y en la generación de claves robustas con las que proteger las carteras. Los atacantes se aprovechan las vulnerabilidades presentes en los algoritmos criptográficos para descifrar la información contenida en la transacción o aprovecharse de la generación de una clave defectuosa que permite al atacante obtener dicha clave y acceder a la cuenta para transferir los fondos a la cuenta del atacante.

3.11 Ataques contra los usuarios

Por último, existen ataques que tratan de robar las carteras digitales de los usuarios

atacando directamente a los propietarios. Por ejemplo, el ataque de secuestro del portapapeles (*Clipboard hijacking*) [48], que se produce mediante la infección del equipo de la víctima con malware que monitoriza el portapapeles del equipo infectado en busca de direcciones de carteras digitales. Cuando detecta que la víctima ha copiado una en el portapapeles, la sustituye por la del atacante sin el conocimiento de la víctima. Si la víctima no revisa posteriormente la dirección, los fondos serán transferidos a la cuenta del atacante.

También son posibles los ataques de *phishing* contra los usuarios. Considerado por muchos expertos el ataque en el que con una inversión mínima de tiempo y dinero se puede obtener la mayor tasa de éxito, se trata de conseguir las credenciales de la víctima haciendo uso de ingeniería social, es decir, engañándola haciéndole creer que la aplicación o la página web es legítima y, con ello, ganarse la confianza para obtener las credenciales de acceso a los servicios que el atacante ha marcado como objetivo. Esto puede suceder en el caso de una falsa casa de cambio o de una mezcladora maliciosa. Los usuarios pueden ser también víctimas de otros malware, como los criptojacking comentados anteriormente.

4 Sistema de detección y de seguimiento de carteras digitales

En este capítulo, se explica de forma pormenorizada la parte práctica de este trabajo, que consiste en el desarrollo de un sistema para realizar la detección de carteras digitales publicadas en foros alojados en la Internet abierta y en la Darknet. Además, se incluye un caso de uso de detección y seguimiento de una cartera digital localizada en un foro de Internet. Por último, se detallan los problemas encontrados en la realización de la parte práctica de este trabajo.

4.1 Descripción del sistema

En la Figura 15 se muestra el diagrama de alto nivel del sistema. En primer lugar, se recolecta la información de los comentarios y *posts* de las páginas objetivo de estudio en busca de carteras digitales de tipo bitcoin. Aunque el análisis se ha centrado en este tipo de carteras, el sistema es extensible a otras carteras digitales. Los datos recopilados se almacenan en la base de datos creada a tal efecto. En segundo lugar, se envía una petición de información al ledger sobre la cartera descubierta para recabar la información relativa a la misma. La información recibida se guarda en la tabla correspondiente de la base de datos. Por último, la información obtenida de la cartera digital en la base de datos, se almacena en un archivo para su posterior lectura por la herramienta Neo4j, que proporciona una base de datos de grafos, en el que se representa gráficamente y se interpretan los resultados.

El sistema se compone de diferentes scripts:

- **Script de recolección y cribado de información:** este script se encarga de recorrer las páginas para analizar y recolectar la información que se encuentra dentro de los comentarios y *posts*. A continuación, una vez se han eliminado los datos que no son interesantes para el estudio, se procede a buscar la presencia de carteras digitales de tipo Bitcoin. En caso de que la búsqueda ofrezca resultados afirmativos, se busca la posible presencia de evidencias (nombres, correos electrónicos, etc.) y se almacenan en la base de datos. Este script está generado en Python y hace uso del framework de Scrapy junto con expresiones regulares. Scrapy es un framework desarrollado en Python que permite analizar páginas web aprovechándose de la estructura determinada por los estándares de páginas web.

- **Script de extracción de información de la cartera**: este script se encarga de realizar peticiones al ledger de la cadena de bloques objetivo (bitcoin) y de guardar toda la información relacionada con la cartera que se encuentra en la cadena de bloques. Está creado en Python y se conecta con la librería PyMySQL para la inserción de la información obtenida mediante la herramienta de consulta Bitcoin Explorer, disponible en la página web *www.blockchain.com*, en la base de datos.
- **Script de visualización**: este script sirve para poder visualizar, dentro de la herramienta correspondiente, las relaciones que pueden existir entre las diferentes carteras digitales. Este script se ejecuta en la herramienta Neo4j que usa el lenguaje CypherText, similar a SQL como puede verse en la Figura 16. Neo4j es una base de datos orientados a grafos, que permite almacenar las relaciones existentes entre los datos tratados sin necesidad de utilizar tablas como en un sistema tradicional de base de datos.

Todos los scripts generados para este trabajo se han publicado de manera libre y gratuitamente en la plataforma GitHub (*https://github.com/jrodrv01/bitcoin_searcher*) con licencia GNU/GLPv3.

En la figura 17 se puede observar la estructura de la base de datos del sistema. En la clase *AdditionalData* se almacenan como información adicional de interés las evidencias que se han encontrado junto a una cartera digital, como pueden ser direcciones de correo electrónico, direcciones de servicios ocultos de Tor o números de teléfono. La clase *eWallet* almacena la información relativa a la cartera digital. En concreto, se almacena su hash identificativo, si ha sido usada en algún momento o está inactiva, y el saldo actual que tiene la cartera detectada. En la clase *Transaction* quedan almacenados los datos relativos a las transacciones que se realizan entre las carteras digitales, como son el hash identificativo, el importe y la fecha en la que se realizó la transacción. La clase *Block* se usa para almacenar los datos relativos al bloque en el que están registradas las transacciones, junto con la fecha de validación del bloque y su identificador hash.

Como se puede observar en la figura 17, existe una relación n-aria dentro de la clase eWallet, ya que una misma cartera puede ser receptora y emisora en diferentes transacciones. Hay también una relación 1-n entre la clase *Block* y entre la clase *Transaction* dado que un bloque contiene varias transacciones. La clase *Transaction, de hecho,* es una clase de la relación existente entre carteras. Por último, hay una relación

1- 0* entre la clase *eWallet* y la clase *AdditionalData*, dado que una cartera puede o no presentar alguna evidencia en forma de información adicional.

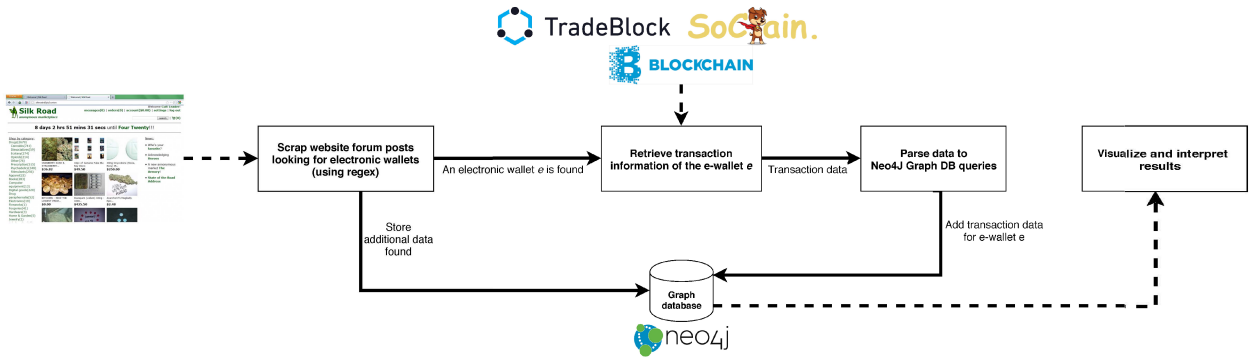


Figura 15: Diagrama de alto nivel del sistema. Elaboración propia

```
SELECT * FROM Ewallet AS sen
JOIN Transaction AS t ON (sen.hash_address = t.hash)     SQL
JOIN Ewallet AS rec ON (t.hash = rec.hash_address)

MATCH
(s:Ewallet)- [:SEND_MONEY_TO] -> (r:Ewallet)             CYPHERTEXT
```

Figura 17: Comparativa código Cypher y SQL. Fuente: Elaboración propia

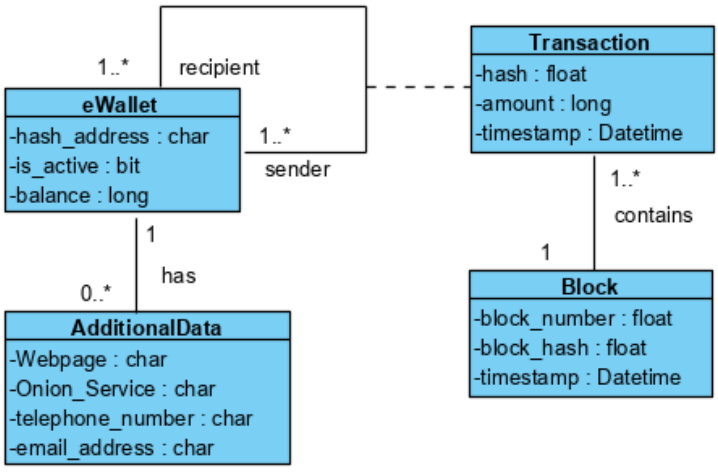


Figura 16: Diagrama de la base de datos. Elaboración propia

4.2 Ejemplo de uso

A modo de ejemplo, se ha aplicado el sistema desarrollado en las páginas web de Forocoches (*https://www.forocoches.com*) y el tablón de imágenes 4Chan (*http://www.4chan.org/*), localizadas en el internet abierto, y las páginas de foros

CebollaChan (*http://s6cco2jylmxqcdeh.onion*), el tablón de anuncios Torchan (*http://zw3crggtadila2sg.onion*) y la página de preguntas y respuestas por parte de la comunidad de Respuestas Ocultas en español (*http://efxg3mscme5hy7je.onion/*), localizadas en la red TOR. Para poder acceder a estos últimos ha sido necesario utilizar el navegador web proporcionado por TOR Project.

Una vez comprobado en qué elementos HTML se almacenan los comentarios que se desean extraer, se usan los scripts de recolección de información adaptados de forma individual para cada página para rastrear las webs señaladas, extrayendo los comentarios para guardarlos en un archivo con formato de valores separados por comas. Seguidamente, se evalúan los datos almacenados en el fichero, eliminándose todas las etiquetas HTML, CSS u otro tipo de datos extraídos como son los símbolos de retornos de carro, saltos de línea o tabulaciones. Después de conseguir los elementos de interés de cada una de estas páginas, la parte del sistema encargada del cribado de la información mediante el uso de expresiones regulares, tal y como se muestra en la figura 18.

```
bitcoin_address_finder=(r'[1 3][a-km-zA-HJ-NP-Z1-9]{25,34}')
ethereum__address_finder=(r'0x[a-z0-9]{40}')
onion_service_finder=(r'(?:https?\:\/\/)?[\w\-\.]+\.onion')
web_address_finder=(r'^((https?|ftp|smtp):\/\/)?(www.)?[a-z0-9]+\.[a-z]+(\/[a-zA-Z0-9#]+\/?)*$')
email_address_finder=(r'([\w\.,]+@[\w\.,]+\.\w+)')
bitcoin_hash_finder=(r'[a-fA-F0-9]{64}')
```

Figura 18: Expresiones regulares usadas para detectar carteras digitales y evidencias asociadas a las mismas. Elaboración propia

En la página web de Forocoches se localizó la cartera digital «169ScU5kenSR4oAvqhWjzDhMZ2iXLCrnVe», que fue utilizada por los ciberdelincuentes para recibir el pago de una campaña de sextorsión enfocada al público hispanohablante. En este caso concreto, un usuario había publicado el mensaje de sextorsión en un comentario lo que facilitó su detección. Se ha usado esta cartera digital como ejemplo para ilustrar el funcionamiento del sistema.

Una vez se ha obtenido la dirección de la cartera digital, el siguiente paso es lanzar la parte del sistema encargada de la extracción de los datos asociados a la cartera recopilada, como son las transacciones realizadas o el balance de la cuenta, entre otros datos. Una

vez conseguida esta información, se procede a generar el código en lenguaje Cyphertext en el que se establecen las instrucciones que se quieren usar en Neo4j para guardar la información conseguida en la base de datos. Posteriormente, y tras introducir las consultas en Neo4j, se visualiza de forma gráfica las relaciones entre las diferentes carteras. Con esto, se pretende comprobar el camino por el que se mueve el dinero obtenido en operaciones fraudulentas y observar si han utilizado servicios de blanqueo o mezclado de dinero.

De forma adicional, se señalarán las carteras que se consideren sospechosas de haber cobrado una comisión por estas tareas de blanqueo y mezclado. Para ello se establece un porcentaje mínimo de entre el 1% y el 3%, según los datos indicados en otros estudios de blanqueo de capitales [49] [50].

En la Figura 19, se visualiza en la herramienta Neo4j la cartera digital con el hash «169ScU5kenSR4oAvqhWjzDhMZ2iXLCrnVe», detectada previamente en un comentario en la web de Forococoches. Se observan 2 transacciones, una con destino a la cartera objetivo y otra de salida. Las cantidades trasferidas eran de poca entidad.

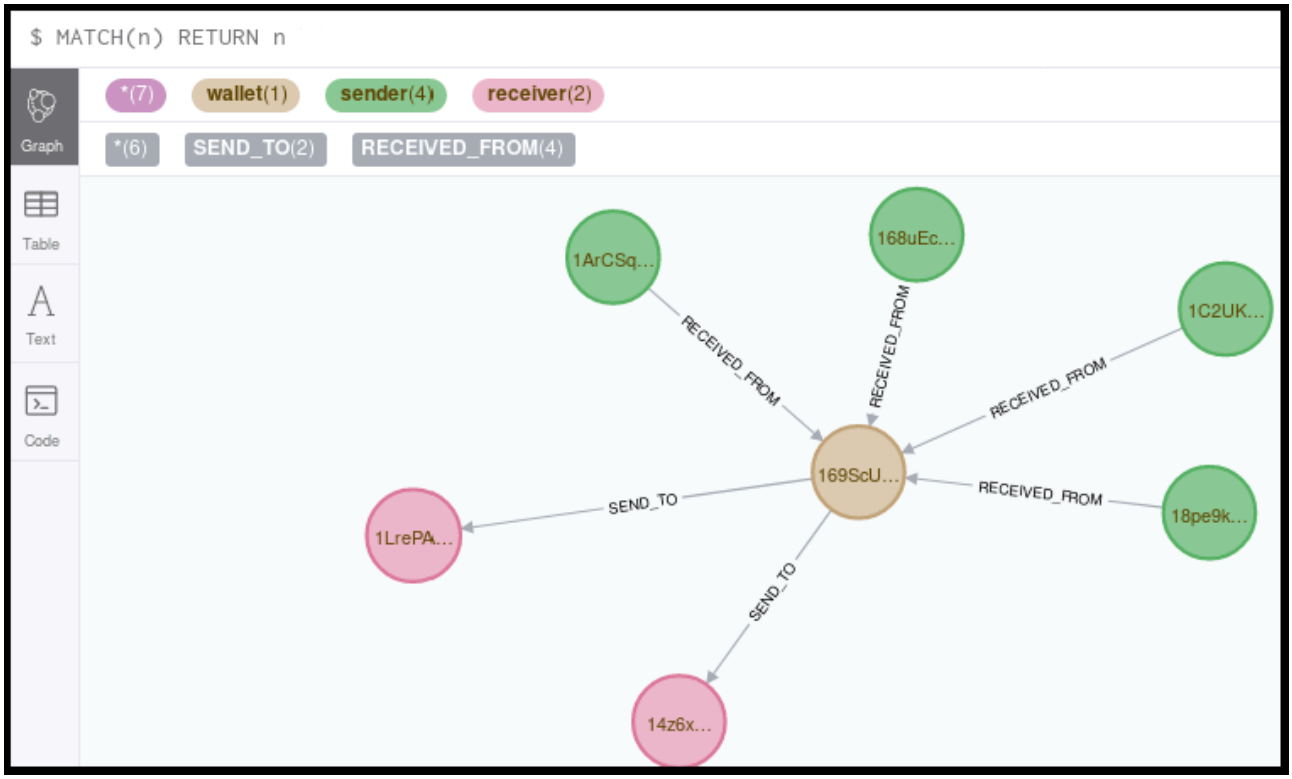


Figura 19: Pantalla de Neo4j. Elaboración propia

4.3 Problemas encontrados

Entre los inconvenientes que se han encontrado a la hora de realizar este trabajo, destacan la imposibilidad de automatizar las operaciones de recolección de datos con el *framework* utilizado (Scrapy), ya que la estructura interna de las páginas web varía de unas de otras. Para solventar este inconveniente se han desarrollado módulos específicos dentro del script para el tratamiento de cada página web objeto del estudio. En el caso de que un usuario quisiera analizar otra página diferente a las que se han usado de ejemplo en este estudio, debería implementar por su cuenta un módulo específico para la web que se desea analizar.

De manera similar, se ha observado que en los chats de tipo público no es tan sencillo conseguir la información de interés debido al uso de HTML, JavaScript o CSS, lo que obliga a estudiar la estructura de cada página por separado para observar en la localización exacta del dato para extraer.

5 Trabajo relacionado

En este apartado se detallan los productos actuales disponibles en el mercado junto con los análisis de tipo preventivo y activo que llevan a cabo las diferentes empresas en materia de AML, CTR y KYC para poder detectar actividades asociadas a delitos, ya sean informáticos o vinculados al tráfico de drogas o de armas u otro tipo, que buscan aprovecharse de las redes blockchain para pasar desapercibidos a los ojos de las fuerzas de orden y de las autoridades financieras de los diferentes países.

Actualmente en el mercado es posible encontrar disponibles varias herramientas que combinan ambos análisis junto con herramientas de Big data e Inteligencia artificial, con lo que se facilitan las tareas de investigación y recopilación de evidencias, así como de desanonimización. Hay que destacar que todas estas herramientas hacen uso de software de terceros *open source* como puede ser peticiones a blockchain.com u otras webs, en las que se realizar peticiones a los ledger de las redes blockchain, o la herramienta hyperlegder, entre otros.

Dark Web Monitor es una herramienta creado por TNO [51]. Se caracteriza por realizar tácticas de monitorización y de recolección de información sobre actividades en línea en áreas delictivas como drogas, armas, delitos cibernéticos y falsificación, entre otras. Además, guarda evidencias como son servicios ocultos, publicaciones en el foro, nombres de usuario y muchas otras como direcciones de criptomonedas, direcciones de correo electrónico, etc. Con ello, también, buscan errores cometidos por los ciberdelincuentes en el pasado [52].

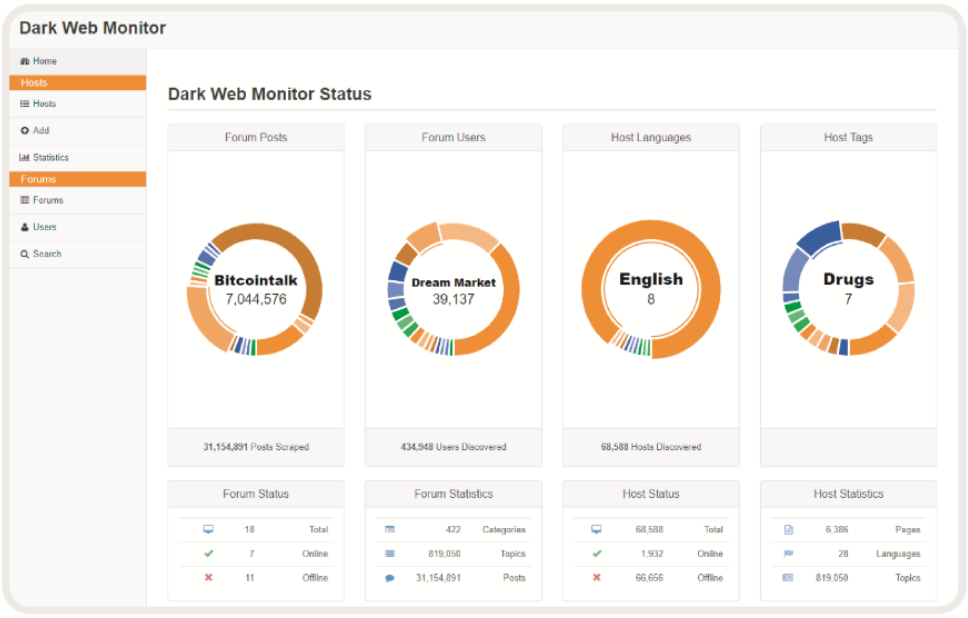


Figura 20: Pantalla principal de la herramienta *Dark Web Monitor* de TNO. Fuente: [51]

Crystal de BitFury Group [53] es un software que incorpora herramientas de detección de operaciones de lavado de dinero en redes blockchain. Permite analizar carteras sospechosas y realizar labores de investigación y prevención.

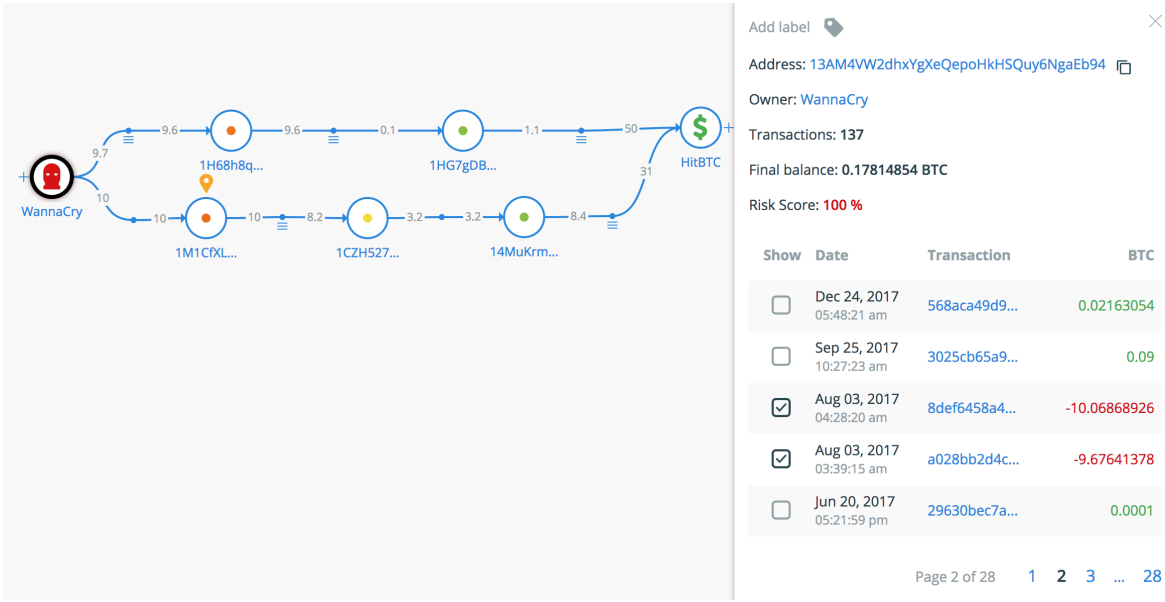


Figura 21: Herramienta Crystal de BitFury. Fuente: Coindesk.com (https://www.coindesk.com/bitfury-enters-bitcoin-crime-fighting-business-crystal-launch)

Chainalysis ofrece las herramientas KYT y Reactor, mostradas en la Figura 22, con las que es posible realizar tareas de monitorización, seguimiento y rastreo de operaciones ilegales en las transacciones [54, 55].

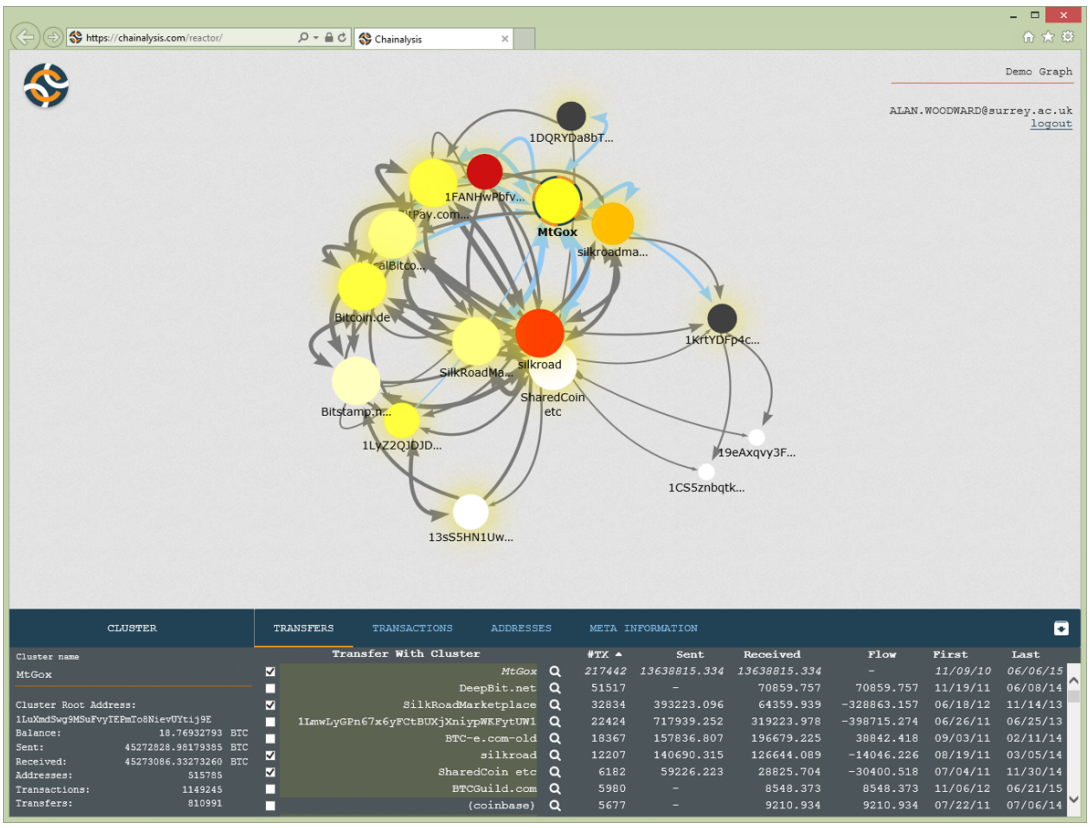


Figura 22: Pantalla de la aplicación Chainalysis Reactor. Fuente: Blog Cyber Matters (https://www.profwoodward.org/2016/01/blog-post_30.html)

Elliptic ofrece herramientas de rastreo en la *Darkweb* y en los *dark marketplaces* permitiendo el uso de análisis forense para evaluar las transacciones. Además, incluye una herramienta que permite la confiscación de bienes nominados en criptomonedas [56].

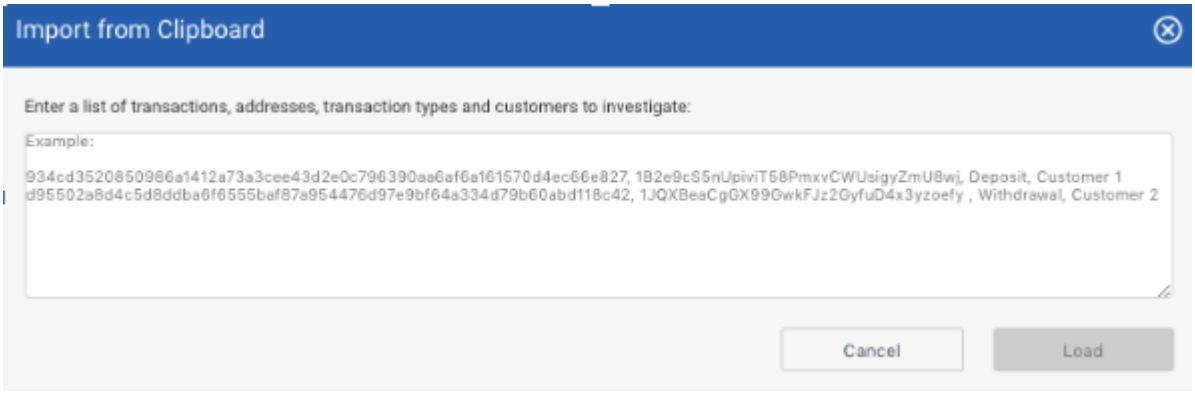


Figura 23: Detalle de la herramienta de Crypto Forensics de Elliptic.co Fuente:Elliptic.co (https://www.elliptic.co/)

Otras herramientas disponibles en el mercado son Coinfirm [57], Coinbase Neutrino [58] y Qlue de Blockchain Intelligence Group [59].

Con respecto a los sistemas anteriormente descritos en este apartado, aunque éstos hacen uso de herramientas *open source*, cuentan con el inconveniente de que son de pago o de acceso limitado. El sistema desarrollado en este trabajo aporta una herramienta de código abierto y de carácter gratuito que permite realizar tareas elementales de análisis forense, como, por ejemplo, la detección de carteras digitales alojadas en Internet —ya sea en abierto o en la *Darknet* y que han podido utilizarse para realizar actividades ilícitas. Además, permite al obtener del ledger la información relativa a dicha cuenta, establecer las relaciones entre las diferentes carteras digitales y detectar aquellas cuentas pertenecientes a servicios de blanqueo o mezclado de dinero en los casos en el que el importe de la transacción este dentro del porcentaje establecido por estos servicios para realizar la operación como se ha detallado anteriormente.

6 Conclusiones

En este capítulo se describen los resultados realmente obtenidos y se plantean las líneas de trabajo futuras.

Respecto a las aportaciones, se ha descrito de forma pormenorizada el funcionamiento de la tecnología blockchain y, dentro de ésta, de los mecanismos de consenso más importantes. Asimismo, se ha incluido información relativa a la anonimización y sus posibles formas teniendo en cuenta sus características. También se han indicado los diferentes ataques y vulnerabilidades que presenta la tecnología blockchain.

Dentro de la parte práctica, se ha desarrollado una herramienta que permite la recolección de carteras digitales que han participado en actividades ilícitas, como es el caso de la cartera «169ScU5kenSR4oAvqhWjzDhMZ2iXLCrnVe», usada para recibir el pago de una campaña de sextorsión enfocada al público hispanohablante. Cabe destacar, además, en los casos en los que se cree que han podido hacerse uso de servicios de mezclado, se han marcado las carteras sobre las que se sospecha son de titularidad de estos servicios. Esto se ha hecho mediante una función que revisa el importe de la transacción considerando el rango de las comisiones cobradas por parte de los servicios de mezclado (entre el 1% y el 3%, según se indica en la literatura).

Asimismo, es preciso mencionar como contrariedad que no se han incluido en la esfera de actuación de este trabajo aquellas páginas web en las que se requiera estar registrado para visualizar el contenido y que podían haber generado más información interesante, como puede ser el caso de foros privados como el onion service DNM Avengers, centrado principalmente en la compra y prueba de sustancias estupefacientes; u OnionLand, centrado en otros productos que se pueden encontrar en la *Darknet*.

Los inconvenientes observados en este proyecto es que la información recolectada, aun haciendo labores de limpieza y pulido previo, presenta ruido que puede provocar falsos positivos. Por último, la imposibilidad de contar con datos de organismos de ciberseguridad acerca de las actividades ilícitas con determinadas carteras digitales que hayan sido utilizadas como tal en delitos cibernéticos, como pueden ser campañas de ransomware.

Como líneas de trabajo futuro, se plantea la necesidad de abstraer en la medida de lo posible las acciones de recolección de información para evitar el estudio personalizado del código web de cada tipo de página estudiada. Igualmente, sería deseable incluir un detector de uso que identifique si la cartera que ha realizado el pago en un servicio de mezclado es para uso personal y no está ligada a actividades ilícitas, como puede ser el pago de un servicio o compra. Esto permitiría evitar la pérdida de tiempo y recursos en el seguimiento de este tipo de carteras.

Bibliografía

[1] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [en línea]. 2008. [Consulta: 24 mayo 2019]. Formato PDF, 180 KB. Disponible en https://bitcoin.org/bitcoin.pdf

[2] ZOHAR, Aviv. Bitcoin: Under the hood. *Communications of the ACM [en línea].* September 2015. Vol. 58 No. 9, Pages 104-113. [consulta: 13 marzo 2019]. DOI:10.1145/2701411 Disponible en: https://cacm.acm.org/magazines/2015/9/191170-bitcoin/abstract

[3] HABER, Stuart, SCOTT-STORNETTA, W. *How to Time-Stamp a Digital Document* [en línea]. 1991. [consulta:25 Julio 2019]. Formato PDF, 160KB. Disponible en: https://www.anf.es/pdf/Haber_Stornetta.pdf

[4] BECKER, Georg. *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis* [en línea]. Ruhr-Universität Bochum. 2008. [consulta: 18 julio 2019]. Formato PDF, 370 KB. Disponible en https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf

[5] CHAUM, David. *Blind Signatures for Untraceable Payments* [en línea]. University of Houston Clear Lake, 1983. [consulta: 03 agosto 2019]. Formato PDF 264 KB. Disponible en https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF

[6] RIVEST, R.L., SHAMIR, A. y ADLEMAN, L.. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* [en línea]. Laboratory for Computer Science, Massachusetts Institute of Technology, 1977. [consulta: 24 mayo 2019]. Formato PDF, 178 KB. Disponible en https://people.csail.mit.edu/rivest/Rsapaper.pdf

[7] *Cypherpunk*. Wikipedia: the free encyclopedia.30 August 2019, 05:26 (UTC). [consulta: 12 agosto 2019]. Disponible en: https://en.wikipedia.org/wiki/Cypherpunk

[8] MAY, Timothy C.. *The crypto Anarchist Manifesto* [en línea]. 1992 [consulta: 03 agosto 2019]. Formato HTML. Disponible en https://www.activism.net/cypherpunk/crypto-anarchy.html

[9] Bloque 0 de Bitcoin [en línea]. 2009. [consulta: 26 agosto 2019]. Disponible en https://www.blockchain.com/btc/block-height/0

[10] FANUSIE, Yaya J., ROBINSON, Tom. *Bitcoin Laundering: An Analysis of Illicit Flows into digital currency services* [en línea]. Elliptic - FDD's Center on Sanctions and Illicit Finance (CSIF)
January 12, 2018

[11] «*Privacy Coin Verge Succumbs to 51% Attack [Again]*». CCN Markets. 22/05/2018. [consulta: 11 mayo 2019]. Disponible en https://www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again/

[12] La huella de carbono de los Bitcoins. Revista Quo 12/06/2019. [consulta: 26 agosto 2019]. Disponible en https://www.quo.es/tecnologia/a27944608/huella-carbono-bitcoins/

[13] LIN, IUON-CHANG, LIAO, TZU-CHUN, *"A Survey of Blockchain Security Issues and Challenges"*, I. J. Network Security 19, 2017, pp. 653-659.

[14] JAWAHERI, Husam y otros. *When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis* [en línea]. *2017*. [consulta: 24 mayo 2019]. Formato PDF, 623 KB. Disponible en:https://arxiv.org/pdf/1801.07501.pdf

[15] SAAD, M., SPAULDING, y otros. *Exploring the Attack Surface of Blockchain: A Systematic Overview* [en línea]. *2019 [Consulta: 15 junio 2019]. Formato PDF, 1749 KB. Disponible en https://arxiv.org/pdf/1904.03487.pdf*

[16] MUKHOPADHAY, U. y otros. A brief survey of Cryptocurrency systems, *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, Nueva Zelanda, 2016, pp. 745-752 Consulta:[18 junio 2019]. DOI:10.1109/PST.2016.7906988 Disponible en: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7906988&isnumber=7906913

[17] FENG, Qi y otros. *A survey on privacy protection in blockchain system* [en línea]. 2018. [consulta 16 junio 19]. Formato PDF 356 KB. Disponible en https://www.sciencedirect.com/science/article/pii/S1084804518303485

[18] CAI, Yuanfeng y ZHU, Dan. *Fraud detections for online businesses: a perspective from blockchain* [en línea]. 2016. [consulta: 25 junio 2019]. Financial Innovation. Formato PDF,411 KB. 10.1186/s40854-016-0039-4. Disponible en https://jfin-swufe.springeropen.com/track/pdf/10.1186/s40854-016-0039-4

[19] RUFFING, Tim, MORENO-SÁNCHEZ, Pedro y KATE, Aniket. *CoinShuffle: Practical Decrentralized Coin Mixing forBitcoin* [en línea]. Springer. 2014. [consulta: 15 mayo 2019]. Formato PDF, 433 KB. Disponible en: https://petsymposium.org/2014/papers/Ruffing.pdf

[20] DZIEMBOWSKI, Stefan y otros. Proofs of Space. In Advances in Cryptology (CRYPTO) [en línea]. August 2013. [consulta: 15 junio 2019]. Formato PDF, 396 KB. Disponible en: https://eprint.iacr.org/2013/796.pdf

[21] HIGGINS, Graham. *Proof of Burn* [en línea]. 2017. [consulta: 22 julio 2019]. Formato PDF, 129 KB. Disponible en: https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf

[22] *Diccionario de la lengua española - Entrada: anonimizar*. Real Academia Española, © 2019. [consulta: 15 agosto 2019]. Disponible en: https://dle.rae.es/?id=2jjMiRi

[23] KAPPOS, George y otros. *An Empirical Analysis of Anonymity in Zcash* [en línea]. 2018. [consulta: 24 abril 2019]. Formato PDF, 1612 KB. ISBN 978-1-931971-46-1. Disponible en: https://arxiv.org/pdf/1805.03180.pdf

[24] SINGH, Kalpana, HEULOT, Nicolas y BEN HAMIDA, Elyes. *Towards Anonymous, Unlinkable, and Confidential Transactions in Blockchain*. IEEE Blockchain 2018, Jul 2018, Halifax, Canada. hal-01812004

[25] MILLER, A., MÖSER, LEE, K. y NARAYANAN, Lee. *An empirical analysis of linkability in the monero blockchain* [en línea]. 2017 [Consulta: 22 junio 2019]. Formato PDF, 1696 KB. Disponible en: https://arxiv.org/abs/1704.04299.

[26] GARMAN, Christina y otros. *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity* [en línea]. 2014. [consulta: 16 junio 2019]. Formato PDF, 323KB. DOI: 10.1007/978-3-662-44774-1_10. Disponible en: *https://www.ifca.ai/fc14/bitcoin/papers/bitcoin14_submission_12.pdf*

[27] JIANG, Bo, LIU, Ye y CHAN, W.K.. *ContractFuzzer: Fuzzing Smart Contracts for Vulnerability Detection* [en línea]. 2018 [consulta: 15 abril 2019]. DOI: 10.1145/3238147. Disponible en: https://arxiv.org/ftp/arxiv/papers/1807/1807.03932.pdf

[28] *Internet Organised Crime Threat Assessment 2018* [en línea]. Europol. 2018. [consulta: 11 junio 2019]. Disponible en: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

[29] *Tradelens: Trade made easy*. TradeLens. © 2019, [consulta: 27 julio2019]. Disponible en https://tour.tradelens.com/

[30] *Blockchain alimentario*.Carrefour. © 2019. [consulta: 13 agosto 2019]. Disponible en: https://actforfood.carrefour.es/Por-que-actuar/BLOCKCHAIN-ALIMENTARIO

[31] *Binded. Copyright made simple*. Binded Inc. © 2017. Consultado 16/05/2019 Disponible en: https://binded.com/

[32] *What is MedRec?*. Mit Media Lab. © 2016. Consultado 10/08/2019 Disponible en: https://medrec.media.mit.edu/

[33] «*Civil*».The Civil Media Company © 2019 [consulta: 10 agosto2019]. Disponible en: https://civil.co/

[34] *Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures* [en línea]. ECB Crypto-Assets Task Force. 2019 [consulta: 10 mayo 2019] Formato PDF, 1680KB. ISSN :1725-6534, Disponible en: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

[35] Panda MediaCenter. *'Locky'. Así funciona el último Ransomware*. 22/02/2016.[consulta: 17 julio 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/cryptolocker-locky-como-funciona/

[36] May's Most Wanted Malware: Cryptomining Malware Digs into Nearly 40% of Organizations Globally». CheckPoint 06/07/2018. [consulta: 21 marzo 2019]. Disponible en :https://blog.checkpoint.com/2018/06/07/mays-wanted-malware/

[37] *ADB.Miner worm is rapidly spreading across Android devices*. Zdnet Inc. 6/02/2019. [consulta: 24 marzo 2019]. Disponible en: https://www.zdnet.com/article/adb-miner-worm-is-rapidly-spreading-across-android-devices/

[38] *The Feds Just Collected $48 Million from Seized Bitcoins* Fortune. 2/10/2017. [consulta: 24 agosto 2019]. Disponible en: https://fortune.com/2017/10/02/bitcoin-sale-silk-road/

[39] *Apparent Theft at Mt. Gox Shakes Bitcoin World*. The New York Times. 25/02/2014. [consulta: 11 julio 2019]. Disponible en: https://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html

[40] *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance)* [en línea]. Publications Office of the EU. 19/6/2018. [consulta: 14 julio 2019]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

[41] LI, X. y otros., *A survey on the security of blockchain systems* [en línea].2017. [consulta: 20 abril 2019]. Disponible en: http://dx.doi.org/10.1016/j.future.2017.08.020.

[42] *PoW 51% Attack Cost*. Crypto 51, © 2019 [consulta: 24 agosto 2019]. Disponible en: https://www.crypto51.app/

[42] *PoW 51% Attack Cost*. Crypto 51, © 2019 [consulta: 24 agosto 2019]. Disponible en: https://www.crypto51.app/

[43] *Blockchain meets Internet routing*. ETH (Eidgenössische Technische Hochschule) Zürich. © 2015. [consulta: 24 julio 2019]. Disponible en: https://btc-hijack.ethz.ch/

[44] GARBA, A., GUAN, Z., LI, A. y CHEN, Z. *A*nalysis of Man-In-The-Middle of Attack on Bitcoin Address. En: *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT,* pp. 388-395. ISBN: 978-989-758-319-3. Disponible

[45] BUTERIN, Vitalik. *CRITICAL UPDATE Re: DAO Vulnerability* [En línea]. Ethereum Blog. 17/06/2016. [consulta: 24 junio 2019]. Disponible en https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

[46] MIHOV, Dimitar. *All Ledger wallets have a flaw that lets hackers steal your cryptocurrency* [en línea]. The Next Web. 6/02/2018. [Consulta: 30 julio 2019]. Disponible en: https://thenextweb.com/hardfork/2018/02/06/cryptocurrency-wallet-ledget-hardware/

[47] KWON, Yujin y otros. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin. *CCM'17 Oct. 30-Nov. 3, 2017*, Dallas, TX, USA. ACM. 2017 [Consulta: 25 julio 2019]. http://dx.doi.org/10.1145/3133956.3134019. Disponible en: https://arxiv.org/pdf/1708.09790.pdf

[48] *Blockchain Threat Report*[en línea]. Junio 2018. [consulta: 10 marzo 2019]. MacAfee. Formato PDF, 1197KB. Disponible en: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-blockchain-security-risks.pdf

[49] HOUBEN, Robby y SNYERS, Alexander. *Cryptocurrencies and blockchain* [en línea]. Policy Deparment for Economic, Scientific and Quality of Life Policies. European Parliament. 2018. [Consulta: 25 mayo 2019]. Formato PDF, 976 KB. Disponible en: https://www.europarl.europa.eu/supporting-analyses

[50] CHOHAN, Usman W., *The Cryptocurrency Tumblers: Risks, Legality and Oversight* [en línea]. November 30, 2017. [consulta: 30 junio 2019] . Formato PDF, 120 KB. Disponible en: https://ssrn.com/abstract=3080361

[51] *TNO Dark Web Monitor*. TNO Group, © 2019 [consulta: 10 agosto 2019]. Disponible en https://dws.pm

[52] WEBBERG, Rolf van, OERLEMANS, Jan-Jaap y DEVENTER, Oskar van. *Bitcoin money laundering mixed results?. An explorative study on money laundering of cybercrime proceeds using bitcoin* [en línea]. 2018. [consulta: 16 junio 2019]. Formato PDF, 595 KB. Disponible en: www.emeraldinsight.com/1359-0790.htm

[53] *Crystal Bitfury*.Bitfury Group Limited, © 2019 . Consultado 23/08/2019 Disponible en: https://crystalblockchain.com/

[54] *Chainalysis Reactor,*Chainalysis Inc. © 2019 Consultado 23/08/2019. Disponible en: https://www.chainalysis.com/

[55] *Crypto Crime Report* [en línea]. Chainalysis Inc, January 2019. [consulta: 14 mayo 2019]. Formato PDF 1026 KB Disponible en: https://blog.chainalysis.com/2019-cryptocrime-review

[56] *Elliptic Crypto Forensics*.Elliptic Enterprises Limited, © 2019 [consulta: 23 agosto 2019]. Disponible en: https://www.elliptic.co/what-we-do/cryptocurrency-forensics

[57] *Coinfirm AML Platform*. Coinfirm Limited, © 2019 . Consultado 23/08/2019. Disponible en: https://www.coinfirm.com/products/aml-platform

[58] *Coinbase Neutrino*. Coinbase, © 2019 [consulta: 23 agosto 2019. Disponible en: https://www.neutrino.nu/

[59] *Qlue*. Blockchain Intelligence Group, © 2015 . [consulta: 23 agosto 2019. Disponible en: https://blockchaingroup.io/qlue1/

ANEXO A: Diagrama de Gantt

El presente trabajo desarrollado ha tenido una duración de 760 horas. El mismo se ha dividido en las siguientes tareas:

1. Estudio de la tecnología blockchain: 250 horas
2. Análisis de las herramientas disponibles en el mercado: 30 horas
3. Preparación del entorno de trabajo: 30 horas
4. Análisis de los requisitos y diseño de la herramienta: 70 horas
5. Codificación de la herramienta: 160 horas
6. Pruebas en entorno real y correcciones: 40 horas
7. Planificación, edición y corrección de la memoria del trabajo: 180 horas

Todo el proceso temporal se puede comprobar en la Figura A.1

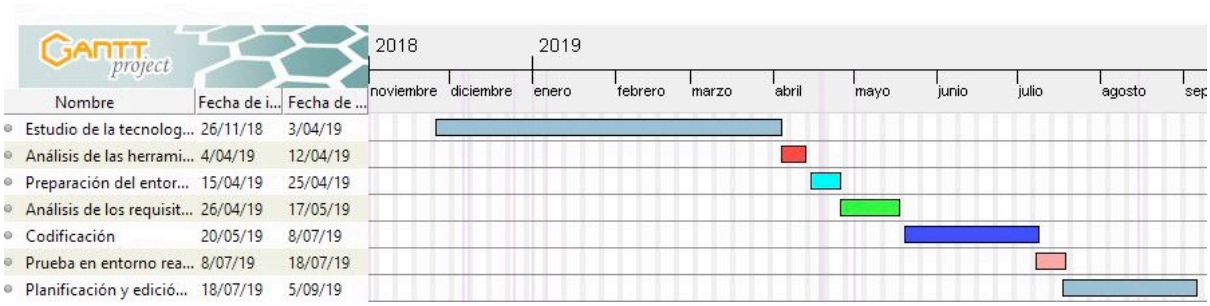


Figura A.1: Diagrama de Gantt del proyecto. Fuente: Elaboración propia

El seguimiento de las tareas realizadas ha sido de forma quincenal con reuniones con el tutor, en el que se han explicado las acciones realizadas, las dudas y problemas surgidos, así como la planificación de las tareas para la siguiente reunión.