Trabajo Final Integrador

Titulo: El rastro virtual de las criptomonedas

Autor: Alfredo Sixto Torrez

POSGRADO ESPECIALIZACIÓN EN INFORMÁTICA FORENSE

Facultad de Ingeniería

Director:

Mg. Ing. Guillermo Ramos - Unicen (Tandil)

UNIVERSIDAD FASTA | FACULTAD DE INGENIERÍA

Fecha de publicación: 19/08/2022

Contenido

Resumen 3
Objetivo general 4
Capítulo 1 4
Introducción 4
Fundamentos Técnicos de la Blockchain: ver ANEXO I 6
Direcciones 6
Monederos o billeteras 7
Transacciones 10
Esquema General de Bitcoin 12
Capítulo 2 14
EXCHANGES 14
Exchanges Centralizados 14
Exchange Descentralizados 15
RIPIO 16
BINANCE 19
Capítulo 3 23
PURI(Proceso Unificado de Recuperación de Información) 23
Capítulo 4 27
Anonimato y ofuscamiento 27
BLOCKCHAIN EXPLORERS 29
OXT 34
WALLET EXPLORER 38
MALTEGO 41
BITCOIN WHOS WHO 48
BITNODES 49
CHAINALYSIS 52
CIPHERTRACE 53
Capítulo 5 53
Delineando una propuesta para rastreo de criptomonedas en PURI 53
Capítulo 6 60
Conclusiones 60
ANEXO I 63
Fundamentos Técnicos de la Blockchain 63
Glosario 67
Bibliografía: 70

Resumen

Este trabajo final integrador consiste en proponer aportes para llevar a cabo una investigación de ciberdelitos por ataques de ransomware donde se utilizaron criptomonedas, dentro del marco de la metodología PURI.
Primeramente, se hace una introducción a los Fundamentos técnicos de la Blockchain y en particular el Bitcoin. Luego se estudian conceptos de direcciones, monederos, transacciones y esquema general del funcionamiento del Bitcoin.
Se describen características y diferencias de los exchanges centralizados y descentralizados. Se analiza las características de un Exchange nacional y otro extranjero. Para el primer caso se eligió a RIPIO y para el segundo a BINANCE.
Posteriormente se describe de manera resumida la metodología PURI (Proceso Unificado de Recuperación de Información) cuáles son sus fase, actividades y tareas. Se relevan y analizan diferentes herramientas para el rastreo de transacciones de criptomonedas siendo estas las siguientes: Blockchain Explorers, OXT, Wallet Explorer, Maltego, Bitcoinwhoswho, Bitnodes. También se mencionan a las empresas Chainalysis y CipherTrace que son lideres en el área de rastreo de criptomonedas y se comentan algunas de sus herramientas.
Para finalizar se aborda una propuesta de rastreo de criptomonedas enmarcada dentro de la metodología PURI.

Palabras clave: Bitcoin, Herramientas de rastreo, Criptomonedas, Blockchain, ransomware.

Objetivo general

El objetivo general del presente trabajo integrador consiste en estudiar y proponer aportes para un método de investigación y rastreo de un ciberdelito de ransomware donde se utilizaron criptomonedas, en el contexto de la metodología PURI[1].

Actividades Relevantes

Estudio de *Blockchain* y criptomoneda Bitcoin, sus funcionalidades y arquitectura.

Análisis y estudio de aplicabilidad de la Metodología PURI a ciberdelitos, de forma tal que permita la investigación y rastreo de este tipo de incidentes en donde se utilizaron criptomonedas, tomando como referencia la modalidad ransomware.

Evaluar los alcances y limitaciones de herramientas existentes para el rastreo de ciberdelitos usando criptomonedas.

Capítulo 1

Introducción. Fundamentos técnicos de la Blockchain. Direcciones. Monederos. Transacciones. Esquema general del Bitcoin.

Introducción

El protocolo informático Blockchain se desarrolló alrededor de 1991[2]. Su intención era vincular una huella inalterable a los registros digitales para prevenir la manipulación en fechas. Con el paso del tiempo se le ha visto gran potencial para ser aplicado en otros ámbitos debido a las propiedades que ofrece. En el año 2009, Satoshi Nakamoto[3] lo implementó para el desarrollo del Bitcoin, un tipo de moneda digital, hoy muy popular en el sector financiero, que es una comunidad que se esfuerza por alcanzar altos estándares de seguridad. La tecnología Blockchain que se utiliza con éxito como parte de monedas digitales en todo el mundo tiene muchos aspectos a considerar sobre incidentes que se puedan presentar en estas operaciones como las estafas electrónicas, ataques a los propietarios de Bitcoins, ataques de ransomware, hackeo a las plataformas de intercambio de criptomonedas, operaciones de criptomoneda relacionadas con fraude financiero y lavado de activos etc. Por eso muchas veces se tiende a asociar a las

[1] **PURI** ("Proceso Unificado de Recuperación de Información" es un Modelo desarrollado por la facultad de Ingeniería de la Universidad FASTA. Cuyo objetivo es establecer una guía de las tareas a desarrollar para la prestación de un servicio de informática forense en un ámbito judicial o particular).

[2] En 1991 aparece el primer trabajo de una cadena de bloques segura utilizando criptografía que fue evolucionando hasta que, en 1998, Wei Dai describe una solución descentralizada para pagos electrónicos basada en criptografía de clave pública. Este primer trabajo es evolucionado por otros autores hasta que en 2008 se publica, con el pseudónimo de Satoshi Nakamoto, el artículo que define el mecanismo para implementar una moneda digital: Bitcoin. Fuente: https://blog.addalia.com/historia-del-blockchain.

[3] **Satoshi Nakamoto** es el pseudónimo usado por la persona o grupo de personas que crearon el protocolo Bitcoin y su *software* de referencia.

criptomonedas con operaciones criminales, como si esta hubiera nacido exclusivamente para tales fines, sin embargo, es evidente que esto dista mucho de la realidad.

Los malwares como el ransomware siguen siendo un importante problema de ciberseguridad, que está en constante crecimiento generando mucha preocupación en los sectores públicos y privados, así como también a víctimas individuales. Durante el año 2021 se han producido ataques de ransomware de alto perfil es decir a empresas con demandas de rescate sin precedentes del rango de 6 a 8 cifras. Debido a esta situación muchas empresas han endurecido sus políticas de seguridad informática para hacer frente a estos ataques, incluido la realización regular de copias de seguridad de sus datos. Esto ha llevado a no tener la necesidad de pagar las demandas del ransomware para poder restaurar sus funciones críticas. Desafortunadamente esto ha provocado una nueva forma de ataque de los ransomware y es el uso cada vez mayor de ataques de doble extorsión. En un ataque de ransomware tradicional, los datos de la víctima se cifran hasta que se recibe el pago. Sin embargo, en un ataque de doble extorsión, los actores del ransomware no solo encriptan los datos de la víctima, sino que luego amenazan con liberar públicamente los archivos robados si no se paga el rescate. Otra tendencia del ransomware que se dio durante el año 2021[4] fue exigir el pago en monedas de privacidad como Monero (XMR) si bien algunos grupos de ransomware exigen XMR únicamente, también ha aparecido una nueva tendencia que es ofrecer pagos en XMR o Bitcoin (BTC) pero cobrando un rescate mayor si la víctima elige pagar en BTC. Por ejemplo, podemos mencionar el caso de DarkSide[5], el grupo detrás del ataque al oleoducto colonial de EE. UU., el cual aceptaba pagos en BTC como XMR, pero cobraba un precio un 10-20 % más alto por los pagos en BTC. Esto se puede ver en la siguiente imagen que se muestra a continuación, debajo de "$ 350,000" y "700,000", una nota dice "(+20%)" para BTC.

Figura 1: Opciones de pago ransomware DarkSide

Ejemplo de opciones de pago de DarkSide en BTC (con una tarifa adicional del 20 %) o XMR - Fuente: CipherTrace Intelligence

[4] CypherTrace: Currentes trends in Ransomware https://4345106.fs1.hubspotusercontent-na1.net/hubfs/4345106/Content/Current%20Trends%20in%20Monero%20Usage%20and%20Ransomware_FINAL.pdf?_hstc=56248308.fc10ee5a5a46f6ac5deb3603066bf9e3.1659911525689.1659911525689.1659911525689.1&_hssc=56248308.1.1659911525689&_hsfp=3830081572

[5] DarkSide es un grupo de hackers dedicados al Delito informático que realizan ataques usando ransomware por medio del cual cifran los datos de las victimas con fines extorsivos exigiendo un pago por el desbloqueo y la no divulgación de los datos. Dentro de sus hitos más significativos está el Ciberataque a Colonial Pipeline.

En la actualidad es más fácil y masiva la utilización de las criptomonedas para cobros anónimos de dineros, sobre todo en Bitcoin, lo que la hace una moneda muy corriente en ciberdelitos, pagos extorsivos y lavado de dinero. Ante este escenario surge la necesidad de contar con conocimientos y procedimientos científicos que tengan como base las técnicas de la informática forense para realizar una investigación de delitos con esta tecnología y llegar a los responsables de los mismos.

Fundamentos Técnicos de la Blockchain: ver ANEXO I

Se incorporo este ítem como un anexo a fin de que el lector conocedor de esta tecnología pueda obviar esta parte.

Direcciones

Una dirección de billetera, es una cadena de 26-35 caracteres alfanuméricos. Es todo lo que se necesita saber para poder enviar y recibir Bitcoins. Se puede usar cualquier dirección de Bitcoin para transferir criptomoneda a cualquier otra dirección en la red, siempre que el software de billetera del remitente sea compatible con ese tipo de dirección. Una dirección Bitcoin convencional (P2PKH) es simplemente una cadena de texto codificada en **Base58Check** que tiene hasta 20 bytes de longitud y que consiste en el hash de la clave pública asociada con la dirección.

Al igual que existen varias versiones del Protocolo de Internet, como IPv4 e IPv6, existen múltiples formatos de direcciones de Bitcoin. Hay tres formatos de direcciones de Bitcoin Core para elegir, P2PKH, P2SH y bech32

Dirección P2PKH o heredado

Una dirección de Bitcoin tradicional (P2PKH) es una cadena de texto codificada en Base58Check que tiene hasta 20 bytes de longitud y que consiste en el hash de la clave pública asociada con la dirección. Este formato de dirección de Bitcoin comienza con un 1, y se trata de una dirección P2PKH o heredada, por ejemplo,**1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2**. Este era el formato de dirección original de Bitcoin y todavía funciona hasta el día de hoy. P2PKH significa Hash de pago a Pubkey, es decir, pagar a un hash de la clave pública del destinatario. Las direcciones heredadas no son compatibles con segwit, pero aún se puede enviar BTC desde una dirección P2PKH a una dirección segwit sin ningún problema.

Dirección P2SH

Las direcciones P2SH están estructuradas de manera similar a P2PKH, pero comienzan con un 3 en lugar de un 1, por ejemplo, **3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy**. P2SH, que significa pago al hash de script, permite una funcionalidad más elaborada que las direcciones heredadas. La función de script P2SH se usa más comúnmente para efectuar transacciones a direcciones multifirmas, aunque este no sea su único uso. Las direcciones con formato P2SH están diseñadas para admitir un conjunto de firmas que sea igual o menor a la cantidad de claves privadas que están vinculadas o asociadas a ellas. Es decir, en una dirección multifirma que tenga 3 claves asociadas, las 3 claves pueden ser los firmantes, o en su defecto sólo 2 o 1 de ellas.

Dirección Bech32

Las direcciones Bech32 son claramente diferentes de las direcciones de estilo P2. Cada una comienza con «bc1» y son más extensas que una dirección P2SH heredada debido a este prefijo. Bech32 es el formato nativo de direcciones segwit, y es compatible con la mayoría de las carteras de software y hardware.

Monederos o billeteras

Las wallets son dispositivos que sirven para depositar, gestionar y transferir las criptomonedas que están bajo nuestro poder. Se tratan de aplicaciones softwares, o también hardware, que se diseñan exclusivamente para almacenar las claves públicas y privadas de Bitcoin u otros activos criptográficos.

En este sentido, mientras los monederos físicos se los tiene en el bolsillo del pantalón o en la cartera, las wallets pueden estar en un teléfono móvil, PC, página web o en un dispositivo físico del tamaño de un llavero o pendrive.

Antes de comenzar con la clasificación de los diferentes tipos de monederos o wallets se describirán algunos términos que se aplican a los monederos:

- **Llave publica:** ya hablamos de las direcciones por lo cual también debemos hablar de llaves públicas, puesto que cuando se genera una wallet desde cero se crea a la par una llave pública y una privada que gestionará su funcionamiento. La llave pública, al igual que la dirección, es un elemento identificador y en base a ella se generan todas las direcciones de una red. No obstante, la llave pública sirve como una forma de identificar quien es el propietario de una determinada dirección. Aunque algunos pueden creer que la dirección y llave pública son lo mismo, en realidad esta última es un elemento criptográfico que permite la creación de la primera y que funciona para verificar que efectivamente un usuario ha firmado una transacción como propietario de determinados activos. Es decir, es un elemento de validación financiera dentro de la red.
- **Llave privada:** La llave privada, por otro lado, es aquel código criptográfico que permite al usuario gastar, transferir, retirar, cambiar o enviar sus criptomonedas de un destino a otro. O sea, es el elemento que resguarda los activos criptográficos y que hace posible que se firmen las transacciones para que sean emitidas. Cuando se genera una wallet, se crea a la par una llave privada y una pública. Sin embargo, mientras la pública funciona como una forma de verificación comunitaria de que efectivamente has sido tú quien firmaste determinada transacción, la llave privada es un elemento que esta solo disponible para el propietario y que otorga total control sobre el dinero en dicha dirección.
- **PIN o contraseña:** Adicionalmente a los elementos técnicos que permiten el funcionamiento interno de una wallet, los propietarios del monedero podrán crear un PIN que resguardará la firma del monedero. En pocas palabras, es una contraseña que ha sido decidida por el dueño del monedero y que servirá para verificar que cada vez que se haga una transacción esta efectivamente está siendo hecha por el propietario.

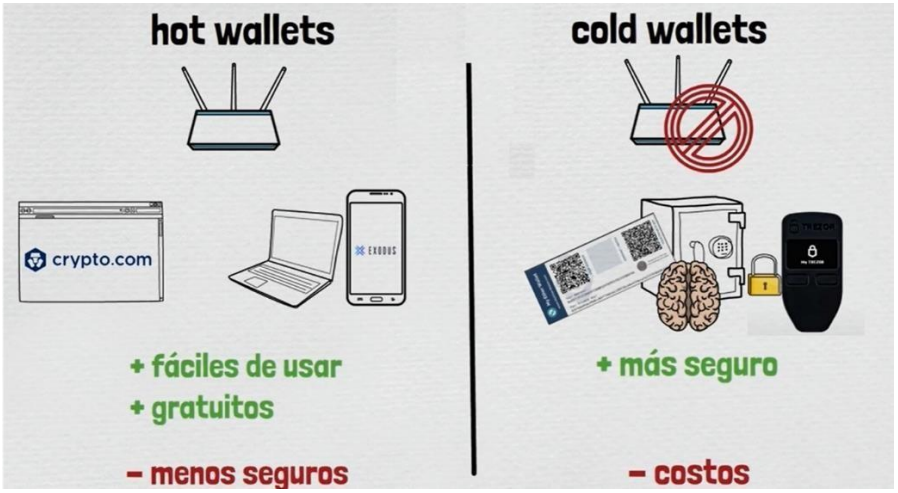
Debido a ello, el PIN no es un dato que debe ser compartido en redes o con personas, ya que gracias a este elemento se podrían realizar cuantas transacciones se deseen.

- **Semilla o frase de recuperación:** La frase semilla, conocida en inglés como seed phrase o también como frase de recuperación, es un conjunto de entre 12 y 24 palabras que tiene como finalidad respaldar nuestro monedero de criptomonedas. Gracias a ella, si perdemos acceso a la computadora o teléfono en donde teníamos nuestro monedero, podemos recuperar nuestro acceso utilizando esta frase en serie. Debido a que se trata de un elemento que regenera un monedero cerrado o cuyo acceso se perdió temporalmente, no se debe compartir con ningún tercero, ya que de hacerlo estaríamos dando el acceso total a nuestro dinero.

Existen una gran variedad de clasificación de monederos. Para simplificar comenzaremos clasificando a los monederos o wallets en dos tipos: Hot wallets y cold wallets

Los hot wallets hacen referencia a cualquier monedero que se encuentre conectado de cualquier forma a la internet como por ejemplo podemos mencionar a los wallets de plataformas en línea como los exchanges, monederos instalados en computadoras con acceso a internet y wallets instalados en nuestro teléfono móviles en forma de aplicaciones. En cambio, los cold wallets hace referencia a cualquier tipo de monedero que no esté conectado a la internet por lo tanto se tratan de dispositivos que no pueden ser hackeados remotamente. A continuación, se describen los tipos de wallets más comunes dentro de estas 2 clasificaciones

Figura 2: Clasificación de Wallets (Billeteras)



Fuente: https://www.youtube.com/watch?v=TO4eWY8lk5E

HOT WALLETS

CASAS DE CAMBIO O EXCHANGE

Las wallets de web o plataformas en línea, tal y como dice su nombre, son productos alojados y desarrollados en un portal de Internet. La plataforma permite que los usuarios puedan manejar sus criptomonedas sin tener que instalar ninguna aplicación, lo cual puede ser ventajoso para que accedan a sus monedas desde cualquier lugar del mundo o dispositivo que cuente con

conexión a la Web. Un claro ejemplo de este tipo de monederos son los utilizados en los exchanges en los cuales para poder operar con criptomonedas necesitamos crear una cuenta.

Debido a que poseen un formato que hace que la wallet siempre este en línea y conectada a Internet, se trata de una opción que tiene un nivel de seguridad bajo y son vulnerables a sufrir ciberataques. Aunque suelen ser más sencillas de utilizar.

BILLETERAS PARA TELÉFONOS MÓVILES

A diferencia de las wallets de web, estos se tienen que descargar en el sistema operativo del celular y están —en su mayoría— diseñados para agilizar el proceso de uso y trading de criptomonedas, ya que por lo general se tratan de interfaces intuitivas con múltiples opciones para transferir dinero. Asimismo, la información de la wallet suele estar protegida por un PIN o contraseña, con la que se aprueba la firma de las transacciones. Pueden existir, además, dos subtipos de esta wallet. Aquellas que son custodiadas por una empresa, en donde la frase de recuperación y los datos de la cuenta son compartidos por el usuario y la empresa. O, por el contrario, aquellas de auto custodia, en donde es el usuario quien recibe la frase de recuperación de su wallet y se encarga de resguardar su propio dinero.

SOFTWARE DE ESCRITORIO

Las wallets de escritorio son aquellas aplicaciones que se pueden descargar en el disco duro de una computadora. Una de sus características más significativas es que estas solo se encuentran conectadas a la Internet cuando se abren, así que suelen ser una opción de almacenamiento más segura que la media.

Al igual que en el caso de las wallets para teléfonos móviles, existen aquellos cuya custodia está compartida y otros en donde recae totalmente en el usuario, quien es el único que tiene acceso a la frase de recuperación y, por ende, posee el control total de su dinero.

COLD WALLETS

BILLETERAS FISICAS – COLD (HARDWARE)

Cuando hablamos de wallets hardware nos estamos refiriendo a dispositivos físicos. Bajo la forma de un pendrive, llave u objeto de tamaño pequeño, los usuarios pueden administrar sus criptomonedas en un lugar donde el acceso a Internet esté controlado.

Para entender cómo funcionan hay que tomar en cuenta que estos dispositivos son alimentados por un USB, el cual se puede conectar a una computadora para acceder a sus funciones de transacción. Es decir, la única manera de tener acceso a los activos allí almacenados es conectando de forma voluntaria el dispositivo, porque de lo contrario resulta casi imposible que de forma remota se puedan gastar las criptomonedas.

Debido a esta característica, los monederos de hardware (o también conocidos como wallets frías) son considerados una de las formas de almacenamiento de activos criptográficos más

segura. Adicional a su diseño físico, las criptomonedas que se encuentran dentro del dispositivo están protegidas por un número de PIN cuando se conectan a Internet, y por lo general es el usuario quien tiene control total de la frase de recuperación de sus criptomonedas.

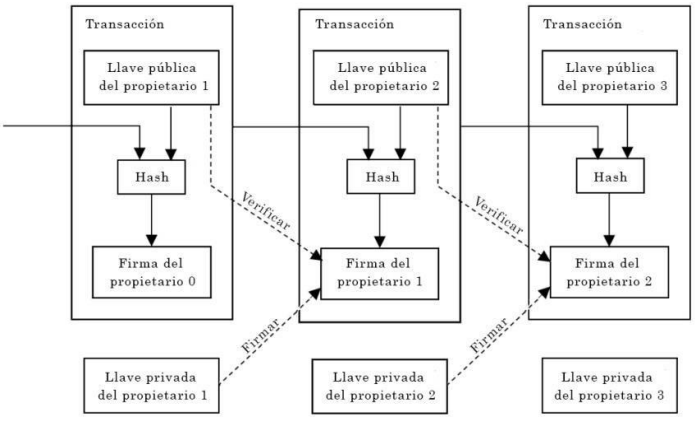
BILLETERAS DE PAPEL

Como si se tratase de imprimir una factura, las wallets de Bitcoin y criptomonedas también se pueden generar de cero en un papel. El usuario solo necesita acceder a portales web que se dedican a crear las llaves de una dirección, tales como bitaddreess.org (Generador de billetera Bitcoin del lado del cliente utilizando lenguaje JavaScript), donde se imprime un billete con la dirección donde están almacenadas las criptomonedas y un código QR para escanear. Asimismo, estas billeteras se pueden proteger con contraseñas. Los usuarios pueden acceder a sus Bitcoins escaneando el código QR desde su teléfono celular, desde donde podrán consultar el saldo de su wallet y enviar las monedas a otras direcciones. Debido a que se trata de wallets impresos en papel (por consiguiente, no se encuentran conectados a Internet las 24 horas del día) es una opción que aporta seguridad respecto a los ataques cibernéticos.

Transacciones

Las transacciones representan el flujo de las criptomonedas en la red. Las transacciones en Bitcoin son estructuras de datos firmadas digitalmente que cambian el propietario de unidades de Bitcoins asignándolas a otra dirección o propietario. En términos simples, una transacción dice a la red que el propietario de un número de Bitcoins ha autorizado la transferencia de algunos de esos Bitcoins a otro propietario. El nuevo propietario puede ahora gastar esos Bitcoins creando otra transacción que autorice la transferencia a otro propietario, y así sucesivamente, en una cadena de propiedad.

Figura 3: Firmas de Transacciones en Bitcoin

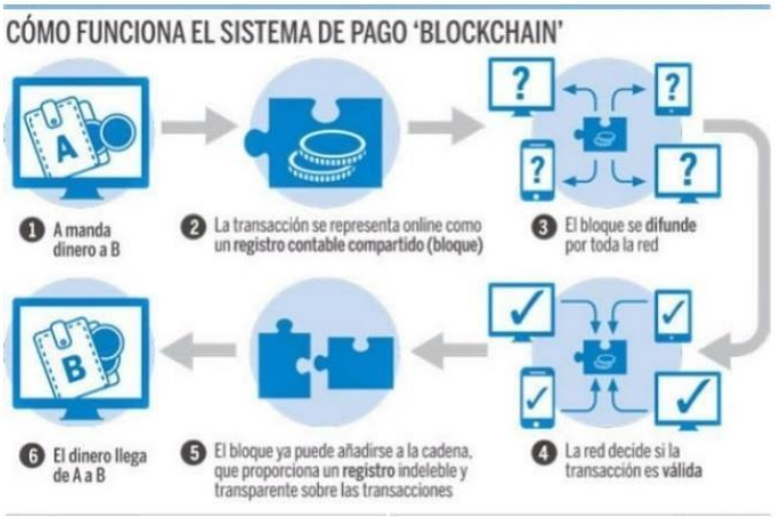


Fuente: Bitcoin: A Peer-toPeer Electronic Cash System. Satoshi Nakamoto(2009)

Las transacciones son como líneas en un libro contable de doble entrada. Simplificando, cada transacción contiene una o más "entradas", que son débitos contra una cuenta Bitcoin. En el otro lado de la transacción, hay una o más "salidas", que son créditos añadidos a una cuenta Bitcoin.

Las entradas y salidas (débitos y créditos) no suman necesariamente la misma cantidad. En su lugar, las salidas suman un poco menos que las entradas y la diferencia representa una comisión de transacción implícita, que es un pequeño pago recogido por el minero que incluye la transacción en el libro contable. Aproximadamente cada 10 minutos, se añade un nuevo bloque a la red Bitcoin con la lista de las últimas transacciones. La transacción también contiene la prueba de propiedad para cada cantidad de Bitcoin (entradas)desde las que se transfiere valor, en forma de una firma digital del propietario, que cualquiera puede validar independientemente. En términos de Bitcoin, "gastar" es firmar una transacción que transfiera valor desde una transacción previa hacia un nuevo propietario identificado por una dirección Bitcoin.

Figura 4: envió de criptomonedas de un usuario "A" a otro "B"



Fuente: https://telosworld.com/las-empresas-se--inician-Blockchain/ (2018)

Al mirar una transacción en la cadena de bloques, mostrará su(s) entrada(s) (input) (el origen de los Bitcoins enviados), su valor, un sello con el tiempo (certificando una vez y para siempre cuándo ocurrió dicha transacción) y su(s) salida(s) (output) (el destino de los Bitcoins enviados). Puede haber más de un input y output, por la forma en que se envían y se reciben los Bitcoins. A continuación, se describen 4 situaciones que se pueden presentar al realizarse transacciones con Bitcoin de una manera simplificada y que reflejan su funcionamiento

Caso 1: este el caso más sencillo en una transacción donde se tiene una sola entrada y una sola salida. El usuario A dueño de la dirección A envió 0,05 BTC a la dirección B eso significa que en la Dirección A había exactamente la suma que se quería transferir al receptor de la transacción, está de más decir que el receptor puede ser el mismo usuario A o un Usuario B diferente.

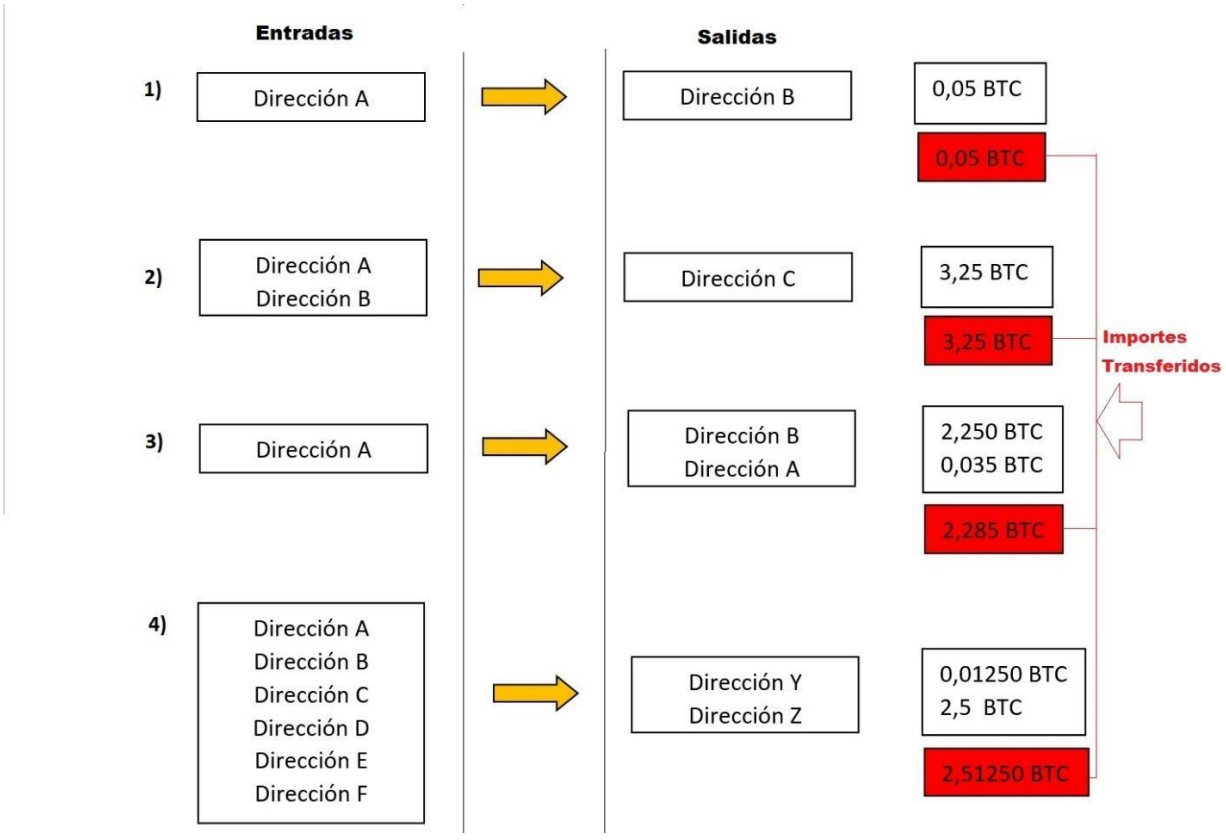
Caso 2: Supongamos ahora que el usuario A no tiene ninguna dirección con la suma exacta que intenta transferir para este caso el usuario A puede usar diferentes direcciones que posee y combinarlas en una sola transacción con más de una entrada. A los fines de una investigación esta propiedad del protocolo Bitcoin es importante puesto que el remitente de los 3,25 BTC firmo una transacción que involucra 2 entradas de direcciones diferente (Dirección A y Dirección B) por lo cual se puede asumir que él tiene las claves privadas asociadas con ambas direcciones, y por lo tanto era el propietario del monto reflejado en aquellas direcciones. Eso significa que si se

revela la identidad de una de las direcciones involucradas en una transacción multi-entrada, todas las demás direcciones estarán también identificadas.

Caso 3: en esta situación tenemos un usuario A que quiere enviar 2,250 BTC desde su Dirección A a la Dirección B, pero en este caso el usuario A no tiene una dirección con el monto exacto sino con un poco más de Bitcoins 2,285 BTC. El protocolo tiene una propiedad que permite que el cliente del remitente cree automáticamente un 'cambio de dirección'. Cuando la entrada es mayor que el monto que se quiere transferir, se crea una nueva dirección para recibir el 'cambio' o 'vuelto'. Esta nueva dirección es propiedad de la misma persona que originó la transacción es decir ese cambio tiene como salida la Dirección A que pertenece al usuario A y cuando este monto se gaste o se consolide con otras direcciones en una nueva transacción, todas las transacciones resultantes se vincularán al mismo propietario que es el usuario A dueño de la Dirección A.

Caso 4: Si se tiene una transacción con muchas entradas y un 'cambio de dirección' o vuelto distinto a las entradas, todas estas direcciones se pueden atribuir a la misma entidad o usuario.

Figura 5: Propiedades de las transacciones



Fuente: Elaboración propia

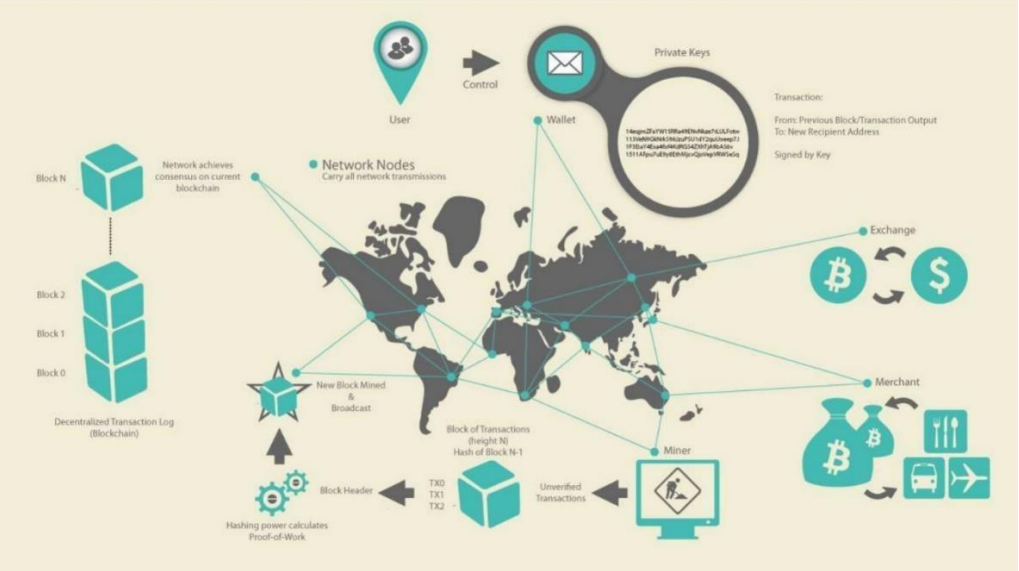
Esquema General de Bitcoin

En el siguiente diagrama (Figura 6) se muestra una Visión general de Bitcoin, vemos que el sistema Bitcoin es un conjunto de conceptos y tecnologías que conforman un ecosistema de dinero digital. El almacenamiento y transmisión de valor entre los participantes de la red Bitcoin

se consigue mediante la utilización de las unidades monetarias llamadas Bitcoins. Los usuarios de Bitcoin se comunican entre ellos usando el protocolo Bitcoin, principalmente a través de Internet, aunque también se pueden utilizar otras redes de transporte. La pila de protocolos Bitcoin, disponible como software open source, puede ejecutarse sobre una amplia variedad de dispositivos, incluyendo laptops y smartphones, lo que hace que la tecnología sea fácilmente accesible.

Los usuarios pueden transferir Bitcoins a través de la red para hacer prácticamente cualquier cosa realizable con monedas convencionales, incluyendo comprar y vender bienes, enviar dinero a personas y organizaciones, o extender créditos. Los Bitcoins pueden comprarse, venderse e intercambiarse por otras monedas en casas de cambio especializadas. En cierta forma Bitcoin es la forma de dinero perfecta para Internet, ya que es rápido, seguro y carente de fronteras. A diferencia de las monedas tradicionales, los Bitcoins son completamente virtuales. No existen monedas físicas y en sentido estricto, ni siquiera existen monedas digitales. Las monedas están implícitas en transacciones que mueven valor de un remitente a un destinatario. Los usuarios de Bitcoin poseen claves que les permiten demostrar la propiedad de las transacciones en la red Bitcoin, otorgando acceso a gastar su valor transfiriéndolo a un nuevo destinatario. Esas claves están normalmente almacenadas en una cartera digital (en inglés, "wallet") en el computador de cada usuario. La posesión de la clave que libera una transacción es el único prerrequisito para gastar Bitcoins, poniendo completo control en las manos de cada usuario.

Figura 6: Visión General de Bitcoin



Fuente: Elogios a Mastering Bitcoin

Capítulo 2

Exchanges. Exchanges Centralizados y Descentralizados. RIPIO. BINANCE.

EXCHANGES

Los Exchanges de Criptomonedas son plataformas digitales en las cuales se permite el intercambio de monedas digitales por dinero fiduciario (fiat) u otras criptomonedas o activos. A los Exchange se los puede comparar con las casas de cambio que trabajan con dinero fiduciario en el mundo real.

En Argentina los exchanges más conocidos son: ArgenBTC, Ripio, SatoshiTango, Qubit, Buenbit, y Bitex, entre otros. Y a nivel internacional se destacan: Binance, Coinbase, Bitstamp, Kraken, Huobi, itbit, entre otros. Los Exchanges presentan una constante expansión que se ha diversificado en función del uso y necesidad del cliente.

Actualmente existen dos tipos de exchanges, los centralizados (CEX) y los descentralizados (DEX). Los centralizados requieren de un intermediario para realizar las transacciones, mientras que los descentralizados se genera una comunicación directa entre ambas partes (P2P), a continuación, se describe con más profundidad los CEX y DEX.

Exchanges Centralizados

Desde sus inicios las criptomonedas tuvieron como característica fundamental la descentralización. No obstante, la mayoría de las negociaciones se realizan a través de medios centralizados como es el caso de la mayoría de los exchanges. Estos, son empresas o entes mediadores, quienes fijan las tasas de cambio, comisiones, políticas, reglas y términos de las mediaciones y transacciones entre los usuarios. En muchos exchanges existe una tercera persona de confianza, que intermedia entre las negociaciones realizadas por los clientes, o traders a través de la plataforma. En este sentido, los defensores de este tipo de negociación alegan que mediante la centralización se aporta liquidez, dinamismo y expansión al mercado online de criptomonedas. Entonces, el carácter descentralizador de las negociaciones se desvanece, al existir un tercero que medía entre éstas. En este caso, la persona o empresa centralizadora es quien controla las entradas y salidas en la plataforma. Además, es la que recibe una comisión por cada negociación que realicen sus clientes en sus plataformas. Entre los Exchange centralizados más populares se pueden mencionar algunos como: Binance, Bitfinex, Bittrex, Coinbase, Kraken, entre muchos otros que se pueden clasificar en esta categoría. Estas plataformas cumplen con las normas de “Conoce a tu Cliente” y “Anti lavado de Dinero” conocidas como normas KYC y AML[6] respectivamente. Esto implica que los usuarios deben identificarse

[6] AML es un acrónimo del término en inglés Anti-Money Laundering. Se utiliza principalmente en el sector financiero, legal y del compliance para referirse a los controles estándares que deben realizar las empresas y organizaciones para poder evitar, identificar e informar sobre conductas sospechosas de lavado de dinero o blanqueo de capitales que pueden darse al realizar su actividad.
KYC (Know Your Customer) es cuando una empresa o institución está obligada a verificar la identidad de un cliente antes de proveerle de servicios y/o productos.
AML y KYC son dos conceptos estrechamente relacionados y que deben entenderse como parte del proceso de identificación de usuarios. Siendo así, la relación entre los procesos KYC y AML es fundamental para prevenir el blanqueo de capitales en las relaciones contractuales y transacciones.

debidamente antes de poder usar los servicios que la plataforma ofrece. Por lo tanto, no son plataformas que le dan privacidad y anonimato a las negociaciones. También, cabe destacar que existen varios niveles de identificación del usuario. Cuanto mayor sea el nivel de identificación, más datos serán solicitados y por ende, su margen de operatoria será aún mayor.

Ventajas de los exchanges centralizados

1. Gran nivel de funcionalidad, son fáciles de usar mediante transacciones rápidas.
2. Su manera de operar se actualiza constantemente, para brindar un mejor servicio y fidelidad del cliente.
3. Tienen una mayor liquidez, es decir, mayor ganancia por sus comisiones.

Desventajas en los exchanges centralizados

1. El control centralizado que se ejerce sobre los fondos.
2. No existe privacidad del usuario.
3. El riesgo de hackeo es mayor, debido a la centralización de los datos.
4. Los montos que se cobran por concepto de comisiones son mayores, en comparación con los DEX.

Exchange Descentralizados

En los DEX no existe el ente mediador entre los clientes. El control de las negociaciones se realiza a través de un software especializado. Este permite, que los clientes puedan realizar sus transacciones en modo P2P. Al no existir una tercera persona que intermedie entre las partes, las tasas de cambio son fijadas por los propios clientes al momento de realizar la negociación. Al tratarse de negociaciones directas entre los clientes, el sistema aporta el carácter de privacidad y anonimato entre las partes que negocian. En este sentido, muchas personas y gobiernos argumentan que este tipo de negociación, al no estar reguladas por un tercero de confianza, se presta para actividades ilícitas, como el lavado de dinero y el financiamiento de actividades que atenten contra el bien común de la sociedad. Algunos ejemplos de DEX son: Bitsquare, Changelly, Localbitcoin, EtherDelta, OpenLedger, Shapeshift y Waves. Actualmente, varios exchanges centralizados, ofrecen un servicio llamado operaciones Over the Counter (OTC) donde los usuarios pueden comerciar criptomonedas directamente entre ellos, haciendo que el exchange no regule totalmente la operación. Ejemplos de estos, son Binance, Huobi, OkCoin, entre otros.

Ventajas de los exchanges descentralizados

1. La posibilidad de un control absoluto del dinero de los usuarios.
2. Al igual que el anonimato que brinda la red Blockchain estos tipos de exchange brindan ese anonimato a sus usuarios.
3. Las comisiones que se pagan en estos exchanges suelen ser menores que en los centralizados.
4. Existe mayor confianza y seguridad en estas debido a que la operación se realiza con otra persona y no a través de un intermediario.

Desventajas en los exchanges descentralizados

1. No es de fácil uso para usuarios principiantes, puesto que requiere un conocimiento más profundo del sistema.

2. Sus funciones son de momento menos avanzadas que en los exchanges centralizados.
3. La libre oferta y demanda en estos exchanges pueden generar efectos colaterales como demoras en los tiempos de ejecución de las transacciones.
4. No existe tanta liquidez como en las exchanges centralizadas.

Pasos para adquirir criptomonedas en un exchange

Paso 1: el usuario se registra en la plataforma. Una vez que el sistema validó el usuario está listo para operar. Generalmente estas plataformas sobre todos los exchanges centralizados solicitan una serie de datos y una identificación (pasaporte, dni, etc.) también puede requerirse una foto selfie y hasta la constancia de un servicio a su nombre.

Paso 2: hay que "fondear" el wallet del exchange. Es decir, transferir fondos de moneda fiduciaria a la billetera. Las plataformas que operan en Argentina en general utilizan transferencias bancarias en moneda local, que se puede realizar desde el home banking por medio de una transferencia de fondos en pesos argentinos vía cbu/cvu al cbu/cvu que pertenece al exchange. Hay que tener en cuenta que la cuenta de origen de fondos de la moneda fiduciaria debe estar a nombre del usuario del exchange esto es así en casi todas las plataformas. Por lo cual es muy importante elegir bien el exchange y corroborar que esa plataforma permita recibir fondos de una cuenta bancaria en pesos argentinos, para no efectuar el registro de usuario en vano ya que, si el exchange no admite pesos argentinos, el usuario no va a poder fondear la cuenta. Algunos exchange que admiten transferencias en pesos son: ripio – satoshitango – bitso – argenbtc – decrypto – buenbit. Otra cuestión importante al momento de elegir un exchange es verificar que trabaje con las criptomonedas que se desea operar, ya que como se indicó anteriormente, no todos los exchanges permiten operar con el universo de criptos.

Paso 3: una vez que se tengan fondos en la cuenta ya se puede operar. Se ingresa a la billetera y desde ahí empezar a comprar por ejemplo Bitcoin, la operación es muy fácil de ejecutar, y depende de la configuración de cada plataforma. Pero en general todas son muy sencillas de operar se selecciona la criptomoneda que se pretende adquirir, se selecciona el método de pago, y se valida la operación.

RIPIO

Ripio es tanto un exchange como una billetera virtual. Surgido en Argentina en el año 2013, este sitio ha tenido un extraordinario crecimiento, al punto que hoy cuenta con oficinas en tres continentes y más de 300 empleados. La plataforma Ripio tiene todo lo necesario para comprar, vender, almacenar y transferir criptomonedas de una manera rápida y simple. Para el caso de Bitcoin que es un sistema contable que admite hasta 8 decimales, o sea que la red es capaz de procesar operaciones a partir de los 0.00000001 BTC y que pasado a dólares sería poco menos de medio centavo de dólar sin embargo cuando se va a operar con alguna plataforma de las denominadas exchanges, éstas tienen sus propios mínimos. En el caso de Ripio tiene establecido el mínimo para compra de BTC en 1500 pesos argentinos.

En Argentina, Ripio establece un precio de compra y venta en pesos para cada una de las criptomonedas que ofrece, teniendo en cuenta su valor promedio en pesos en el mercado local. En general, la cotización de las criptomonedas en pesos es cercana al resultado de multiplicar su cotización internacional en dólares por el tipo de cambio informal peso-dólar. A esta cotización se le aplican costos operativos y comerciales incluidos en el precio final, como sucede con cualquier otro broker o exchange en el mercado.

Para comenzar a operar con ripio, lo primero que se debe realizar es registrarnos en RIPIO para esto debemos informar una cuenta de correo (usuario) e ingresar una contraseña. Una vez que estamos registrados por la plataforma hay que activar nuestra cuenta, lo que consiste en completar una verificación **KYC** (*Know Your Customer*) y al tratarse de Exchange centralizado como dijimos antes nos va pedir información personal la cual después va a pasar por un proceso de validación. Los datos que debemos informar al Exchange son:

- Apellido Y Nombre
- Fecha de Nacimiento
- Nacionalidad
- Numero de documento
- Responsable inscripto
- Genero
- Domicilio
- Celular
- Foto del frente del DNI
- Foto reverso del DNI
- Selfie de nuestro rostro para validar identidad

Ripio trabaja con 2FA ("**Two Factor Authentication**") o autenticación de dos factores.

Al momento de escribir el presente trabajo, Ripio dispone de diecisiete (17) criptomonedas, las cuales son: **Bitcoin, ether, USD Coin, litecoin, DAI, Tether, UNI, UBI, Smooth love potion, Ripio coin, MANA, chainlink, dogecoin, chiliz, basic attention token, Axiel infinity y AAVE.**

Los productos o servicios que ofrece esta plataforma

Wallet

La *wallet* de Ripio se puede comprar, vender, enviar y recibir criptomonedas rápidamente, accediendo a las cotizaciones de todas las criptomonedas en tiempo real.

Exchange

Si además de invertir en criptomonedas, también queremos hacer trading con ellas, Ripio pone a nuestra disposición su exchange. En esta plataforma de trading no tendra las mismas ofertas

de pares de criptomonedas que en otros exchanges como el de Binance, pero puede ser buen punto de partida para empezar a hacer trading con este tipo de activos. El exchange de Ripio está basado en la tecnología de TradingView.

OTC

OTC es un servicio Premium de Ripio para clientes que quieren comprar grandes cantidades de criptomonedas con liquidez inmediata para todo tipo de órdenes a precios competitivos. Este servicio está orientado al servicio corporativo y para poder acceder al mismo es necesario invertir un mínimo de 5.000 USD (o su equivalente en pesos argentinos). Además, es necesario estar registrado como una persona física o jurídica para poder hacer uso de Ripio OTC.

Earn

Ripio Earn sirve para realizar inversiones y recibir un interés como ganancia, como por ejemplo a través del staking.

El retorno obtenido de estas inversiones no es muy grande y depende de la criptomoneda en cuestión. Por ejemplo, se puede recibir un 2.5 % anual por Bitcoins, un 4 % por Ethereum y hasta un 6 % por los USDC que se tenga en Ripio.

Métodos de pago y comisiones en Ripio

Para poder realizar operaciones de compras de criptomonedas se debe tener fondos en pesos en nuestra cuenta de Ripio. Por medio de la opción depositar es posible enviar fondos a una cuenta de RIPIO por tres mecanismos:

- Transferencia Bancaria la cual tiene una comisión del 0 %
- Mercado Pago, tiene una comisión de 3 %.
- Efectivo que se puede hacer por Rapipago o Pago fácil, tiene una comisión de 2,5 %.

Una vez que el usuario tenga los fondos suficientes en su cuenta de RIPIO estará en condiciones de comprar criptomonedas, lo cual lo puede realizar desde la web como también desde la APP mobile de RIPIO.

Ripio COIN

Ripio en septiembre de 2021 lanzo su propia criptomoneda **Ripio Coin (RPC)** que es un token basado en Ethereum (ERC-20) y fue creado para impulsar a la comunidad de usuarios de Ripio. Además de poder comprar RPC como cualquier otra criptomoneda, los usuarios de Ripio pueden reclamar o ganar tokens RPC realizando diversas acciones tanto en la web de Ripio como en la aplicación móvil, como por ejemplo validar sus cuentas, depositar y/o retirar fondos, comprar y vender criptoactivos, recomendar los productos a otros usuarios y participar en "airdrops" programados.

Seguridad

El exchange tiene medias de seguridad estándar como ser autenticación de **doble factor, prevención de fraude e integridad de datos.** Según la empresa afirma que el 95 % de sus fondos son almacenados fuera de línea bajo métodos de cold storage (Los servidores están desconectados de internet para evitar hackeos). Posee cifrado SSL para la navegación en Ripio, protección contra ataques DDoS (suministrada por Cloudflare) del sitio web y sus usuarios ante

cualquier tipo de amenaza online. Como medida para prevenir delitos y fraudes financieros, la verificación *Know Your Customer* (KYC) es obligatoria.

BINANCE

Binance es el principal exchange de criptomonedas a nivel mundial y desde su creación en 2017 ha sido liderado por su fundador Changpeng Zhao. Las características que lo han hecho muy popular en la comunidad de criptomonedas son sus bajas comisiones de negociación y su constante innovación.

Binance se ha involucrado en todos los aspectos del ecosistema de las criptomonedas, su constante innovación la ha convertido en una de las plataformas de criptomonedas más utilizadas, y el trabajo de los desarrolladores y miembros de la comunidad de Binance asegura que la plataforma está mejorando continuamente. Se ha convertido en un lugar excelente para aquellos que negocian con criptomonedas por primera vez y para los entusiastas de las criptomonedas con experiencia.

Aunque Binance se fundó en China, después de un par de meses de su fundación trasladó su sede de China a Japón para evitar los inminentes cambios regulatorios que prohibían las criptomonedas en China. Un año más tarde, en 2018, Binance abrió oficinas en Taiwán y anunció que se trasladaba a la isla de Malta, donde los exchanges de criptomonedas reciben mejor acogida. Además, tiene oficinas repartidas por todo el mundo, como las de California (Estados Unidos), Londres (Reino Unido), París (Francia), Berlín (Alemania), Moscú (Rusia), Estambul (Turquía), Singapur, Nueva Delhi (India), Kampala (Uganda), Manila (Filipinas), Ho Chi Minh (Vietnam), Jersey y otros lugares de Asia.

REGISTRO Y VERIFICACION

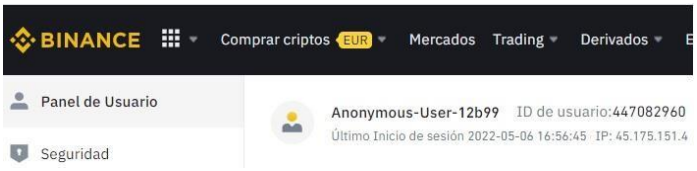
Al igual que en el Exchange de RIPIO el primer paso es el registro en el sitio web de binance para este proceso solo debemos ingresar un correo electrónico y definir una contraseña. Una vez validado nuestra cuenta de correo el siguiente paso es la activación de la cuenta la cual consiste en validar nuestra identidad, donde este proceso de verificación es el típico KYC “Conozca a su cliente”. La información requerida al usuario para validar su identidad es:

- Apellido Y Nombre
- Fecha de Nacimiento
- Nacionalidad
- Documento de identidad oficial (pasaporte, DNI)
- Genero
- Domicilio
- Celular
- Foto del frente del DNI
- Foto reverso del DNI
- Selfie de nuestro rostro para validar identidad

El proceso de verificación es bastante sencillo y normalmente se completa rápidamente. Una vez que hayamos informado nuestro número de celular se activa la seguridad de autenticación de doble factor para el ingreso. Binance para cada usuario crea un ID de usuario dentro de la

plataforma para identificarnos y va llevando registro de todas nuestras actividades dentro de la plataforma.

Figura 7: Información de usuario recolectada por binance



Fuente: Elaboración propia

Si se elige no verificar nuestro perfil, como usuario podemos seguir operando haciendo retiro de dinero, pero estarán limitadas a 2 BTC por día. Los que verifican su perfil pueden retirar hasta 50 BTC al día.

PRODUCTOS O SERVICIOS

- **Binance Academy** – Un centro de formación de libre acceso con recursos educativos sobre cadena de bloques y criptomonedas.
- **Binance Card** – Una tarjeta de pago de criptomonedas que se puede utilizar como una opción de pago para las compras diarias al igual que una tarjeta bancaria normal.
- **Binance Chain y Binance Coin (BNB)** – Un ecosistema de cadena de bloques impulsado por la comunidad con su propio token nativo (BNB) y un exchange descentralizado (DEX).
- **Binance Charity** – Una fundación sin ánimo de lucro dedicada a promover la filantropía en torno a las cadenas de bloques y el desarrollo global sostenible.
- **Binance Cloud** – Una solución de intercambio de criptomonedas para negocios de criptomonedas.
- **Binance Crypto Loans** – Una función que permite a sus usuarios obtener criptopréstamos garantizados por sus activos en criptomonedas.
- **Binance DEX** – El exchange descentralizado de Binance construido sobre la cadena Binance.
- **Binance Fiat Gateway** – Un portal que te permite comprar criptomonedas usando varias monedas fiduciarias (actualmente soporta casi 40 monedas diferentes.)
- **Binance Futures** – Una plataforma de criptoderivados que permite operar con futuros con un apalancamiento de hasta 125 veces.
- **Binance Info** – Una criptoenciclopedia de código abierto.
- **Binance Jersey** – Un exchange europeo de criptomonedas que facilita las operaciones con Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Binance Coin (BNB) y Bitcoin Cash (BCH) en euros (EUR) y libras esterlinas (GBP).
- **Binance JEX** – Plataforma de operaciones de criptoactivos que ofrece servicios de operaciones al contado y de derivados.

- **Binance Labs** – Un fondo de impacto de la infraestructura de Binance y la iniciativa para potenciar los proyectos de Blockchain.
- **Binance Launchpad** – Una plataforma de crowdfunding de criptomonedas para lanzar ofertas iniciales de intercambio (OIE). La innovación de Binance convirtió a Launchpad en la primera plataforma de crowdfunding para OIEs del sector.
- **Binance OTC** – Mesa de negociación extrabursátil para inversores y otros operadores de gran volumen. Incluye Ark, EOS, ARPA, TROY, Lisk, LOOM, Tezos, KAVA, THETA entre otros.
- **Binance P2P trading** – Una plataforma de negociación de criptomonedas P2P como LocalBitcoins o LocalCryptos que admite pagos a través de WeChat, AliPay, transferencias bancarias y QIWI.
- **Binance Research** – Una plataforma de investigación de grado institucional que realiza análisis para los inversores en el ámbito de las criptomonedas.
- **Binance Savings** – Una plataforma que habilita la opción de prestar los criptoactivos con la finalidad de ganar intereses y la posibilidad de retirar los fondos en cualquier momento.
- **Binance Staking** – Una opción que permite el staking en Binance con diversas criptomonedas y obtener hasta un 16% de rendimiento anual.
- **Binance US y otras versiones localizadas del exchange de Binance** – Versiones reguladas del exchange de Binance dedicadas a determinados mercados en función de sus requisitos legales y normativos específicos.
- **Binance USD (BUSD) y Binance GBP** – Las monedas estables reguladas de Binance, lanzadas en asociación con Paxos Trust Company.
- **Trust Wallet** – Un monedero oficial, seguro y descentralizado de Binance. Cuenta con más de 5 millones de usuarios.

Seguridad

A partir de marzo de 2021 Binance cuenta con soluciones de control de riesgo de última generación basado en inteligencia artificial. Estas soluciones utilizan tanto la identidad como el reconocimiento facial. Además, también utilizan análisis de big data e investigaciones ciberforenses para supervisar cada transacción que tiene lugar en el exchange. Todo ello ayuda a identificar cualquier actividad sospechosa o irregular que se produzca en la plataforma. Gracias a toda esta seguridad, hace buen tiempo que no hay ningún intento de hackeo exitoso a su plataforma. De hecho, el último hackeo exitoso en Binance fue en mayo de 2019, cuando los hackers fueron capaces de utilizar un ataque que se basó en el phishing, rompiendo el 2-FA, y accediendo a una cartera caliente de Binance. Se llevaron aproximadamente 7.000 BTC por valor de 40 millones de dólares en ese momento, esta experiencia permitió a Binance mejorar su seguridad para futuros intentos de hackeos. Y también se aseguraron de reembolsar los fondos perdidos a sus clientes.

Conclusiones: Binance al ser un Exchange centralizado recolecta información personal del usuario (KYC), además va guardando información de las actividades del usuario registrando información por ejemplo de la ip de los dispositivos físicos con los que accede el usuario (PC, notebook, celular).

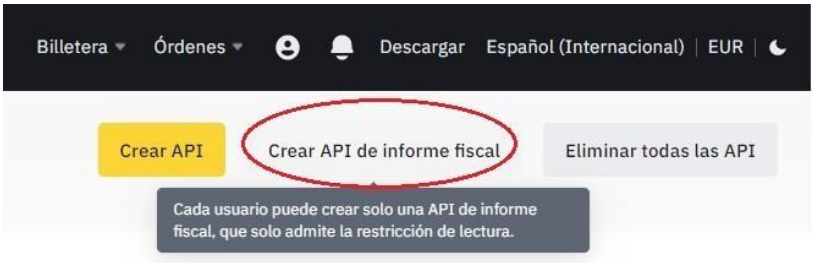
Figura 8: Información de usuario recolectada por binance

Fuente: Elaboración propia

Algo interesante que tiene Binance en el área de soporte es la opción “Solicitudes de autoridades policiales” por medio de la cual Gobiernos y autoridades policiales pueden realizar pedidos de información a Binance.

Por último, queda por comentar que Binance recientemente incorporo la posibilidad de sacar informes por la misma plataforma para el cumplimiento fiscal, esto permite hacer un seguimiento de toda la actividad con las criptomonedas de un usuario. Cada usuario de Binance tiene una opción para que todas las transacciones se rastreen y contabilicen automáticamente con la funcionalidad de herramientas fiscales para declarar impuestos y generar extractos y registros de transacciones pertenecientes a más de un año fiscal, usando la API de funcionalidad de herramientas fiscales puede declarar impuestos automáticamente a través de proveedores externos de la herramienta de impuestos. En la siguiente imagen se observa la opción para crear los informes fiscales.

Figura 9: Información de usuario recolectada por binance



Fuente: Elaboración propia

Capítulo 3

PURI(Proceso Unificado de Recuperación de Información)

A continuación, se describe de manera resumida lo que es el modelo PURI y sus componentes para su contextualización global como modelo y ver que se trata de un modelo adaptativo al cual se le puede incorporar nuevas funcionalidades como las orientadas a las criptomonedas que es el motivo del presente trabajo.

PURI: Fases, actividades y tareas.

El PURI nació como un proyecto de investigación de la Facultad de Ingeniería de la Universidad FASTA y tenía como objetivo establecer una guía de las tareas a desarrollar para la prestación de un servicio de informática forense en un ámbito judicial o particular. Este proyecto tuvo su inicio en el 2011 el cual fue evolucionando con el tiempo, en su primera versión estuvo orientada a la recuperación de información en un equipo de escritorio. Luego surgió una versión de PURI para Smartphones en conjunto con la Universidad UNIANDES de Ecuador, y posteriormente una versión del PURI orientada a redes y entorno distribuidos. Con el tiempo el PURI se transformó en un modelo teórico de las tareas involucradas en la aplicación forense de las ciencias de la información. El Modelo PURI establece una guía de labores a desempeñar desde el área técnico-informático forense, organizándolas en fases, actividades y tareas.

En la siguiente figura se puede observar las fases que intervienen en el modelo

Figura 10: Modelo PURI

Fases del modelo PURI - Fuente: El Rastro Digital del Delito (2017)

Las fases de relevamiento y recolección, son del tipo exploratorio y es deseable que sean ejecutadas por un profesional con perfil investigador, donde el técnico tenga un rol de asistencia y asesoramiento. En las siguientes fases adquisición, preparación, extracción y análisis, y presentación son claramente de la informática forense por ello es de esperar que las tareas involucradas sean llevadas a cabo por profesionales especializados en esta temática con la asistencia que se requiera de los investigadores del caso.

A continuación, se describen cada una de las fases

Fase de Relevamiento: abarca la investigación para conocer el caso e identificar los posibles objetos de interés. Esta fase puede identificarse con labores investigativas de una investigación judicial, o con labores de reconocimiento o exploración cuando se trata de un caso extra judicial.

Las actividades de esta fase son:

1. Identificación de documentación legal y técnica: consiste en identificar toda la documentación legal, de infraestructura, diseño, hardware, software o cualquier otra documentación relevante que permita conocer el caso con mayor profundidad.
2. Identificación de infraestructura IT: Consiste en identificar la infraestructura de red y/o hardware sobre el cual se va a trabajar. Es muy importante identificar correctamente los objetos intervinientes para preparar adecuadamente las fases de recolección y adquisición.

Fase de Recolección: abarca las acciones y medidas necesarias para obtener los equipos físicos, y/o las posibles fuentes de datos, sobre los cuales se debera trabajar posteriormente.

Las actividades que componen esta fase son:

1. Detección de Infraestructura IT: esta actividad se compone de tareas concernientes con inspeccionar el lugar para determinar todos los objetos de interés para la investigación. Estas inspecciones pueden ser oculares como también por medio del uso de técnicas y herramientas específicas, por ejemplo, se puede mencionar la técnica de enumeración utilizando la herramienta nmap.
2. Recolección de objetos: esta actividad se centra en la correcta realización de las tareas de secuestro, embalaje y transporte.

Fase de Adquisición: abarca todas las actividades en las que se obtiene la imagen forense de la información que luego se extraerá y analizará. Esta fase puede realizarse en el lugar del hecho durante un allanamiento, o bien en un laboratorio forense luego de haber recolectado los objetos.

1. Adquisición de datos persistentes: consiste en realizar la imagen del medio de almacenamiento persistente como ser un disco rígido, cd/dvd, tarjeta de memoria y pen drive entre otros.
2. Adquisición de datos volátiles: consiste en realizar un volcado de la memoria principal a un archivo para su análisis posterior.
3. Adquisición de paquetes de red: consiste en adquirir un volcado del contenido del tráfico de red mediante la técnica de sniffing.
4. Adquisición de smartcards: consiste en adquirir una copia de la información contenida en algún tipo de tarjeta inteligente SIM (suscribe identity module) comúnmente utilizada en la telefonía móvil.
5. Validación y resguardo: esta actividad consiste en asignar y calcular el hash a las imágenes forense y volcados de memoria capturados durante las tareas de adquisición.

6. Transporte no supervisado: es el acto de transportar la imagen forense sin la supervisión del especialista en adquisición o el responsable asignado.

Fase de Preparación: involucra las tareas técnicas de preparación del ambiente de trabajo del informático forense, restauración de la imagen y selección del conjunto de herramientas a utilizar en función de lo requerido en los puntos periciales.

Esta fase incluye las siguientes actividades

1. Preparación de extracción: consiste en preparar el espacio de almacenamiento en disco necesario requerido, y el entorno de trabajo para descomprimir, recomponer y validar las imágenes forenses, mapear la imagen a un dispositivo del sistema operativo y generar las máquinas virtuales.
2. Identificación de tecnologías de la información en el objeto: consiste en identificar la cantidad de particiones, sistemas operativos, sistemas de archivos, máquinas virtuales y medios de cifrados presente.
3. Preparación del ambiente: consiste en preparar en el entorno de trabajo el conjunto de técnicas y herramientas necesarias para efectuar el servicio forense encomendado.

Fase de Extracción y Análisis: abarca la extracción de datos, análisis, búsqueda y descubrimiento de la evidencia digital. Comprende las tareas de extracción de la información de las copias forense, selección de la potencial evidencia digital, y su análisis en relación al caso y a los puntos periciales o requerimientos de un particular.

Esta fase se compone de las siguientes actividades:

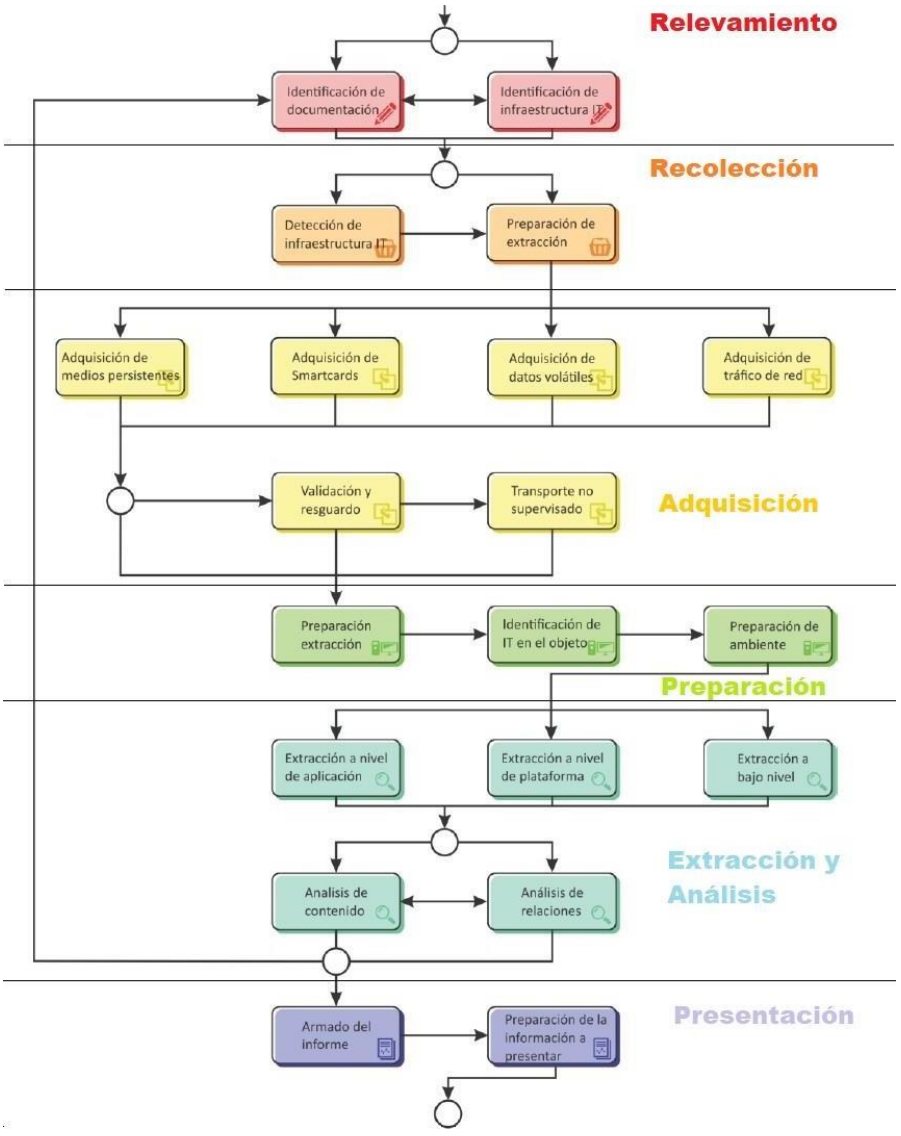
1. Extracción a nivel de aplicación: consiste en la búsqueda y extracción de datos a nivel de aplicación.
2. Extracción a nivel de plataforma: consiste en la búsqueda y extracción de datos a nivel de la plataforma lo que incluye los sistemas operativos, sistemas de archivos y su configuración.
3. Extracción a bajo nivel: esta actividad contiene las tareas de recuperación de información lógica al nivel más bajo de abstracción que es a nivel de bloques de datos puros excluyendo al sistema operativo.
4. Análisis de contenido: incluye tareas para el análisis de la información propiamente dicha que se almacena en los datos extraídos en las tareas anteriormente mencionadas.
5. Análisis de relaciones: incluye un conjunto de tareas de alto nivel que implican el análisis de las relaciones entre los distintos elementos extraídos, el contenido recuperado y los elementos previos aportados.

Fase de Presentación: comprende la preparación de los informes necesarios, el material a entregar y la presentación del caso en un juicio o a los solicitantes. Las actividades involucradas son:

1. Armado del informe: implica la documentación de todas las actividades y tareas realizadas en un informe pericial que sea claro, preciso, concreto y redactado en un lenguaje técnico-científico comprensible para una autoridad judicial.
2. Preparación de la información a presentar: consiste en la preparación de la información y la evidencia digital hallada en el caso para una eventual presentación, ya sea en juicio o a los solicitantes del servicio forense.

A continuación, se presenta un diagrama donde se observan las actividades de cada fase del modelo PURI. Las actividades que corresponden a una misma fase están identificadas del mismo color.

Figura 11: Detalle de actividades por fase del Modelo PURI



Fuente: El Rastro Digital del Delito (2017)

Capítulo 4

Anonimato y ofuscamiento. Herramientas de ayuda: Blockchain Explorers, OXT, Wallet Explorer, Maltego, Bitcoinwhoswho, Bitnodes, Chainalysis y CipherTrace.

Anonimato y ofuscamiento

Cuando se realizan transacciones en Bitcoin generalmente se utiliza una billetera y una o más direcciones de Bitcoin. La billetera y la dirección no están vinculadas a un nombre o a una identidad de persona física por lo cual brindan cierto grado de anonimato, pero vale decir que la tecnología Bitcoin no es completamente anónima, sino que es pseudo-anónima en el sentido de que una dirección no está directamente vinculada a una cuenta o identidad pero todas las transacciones generadas en la red Bitcoin quedan almacenadas en una gran base de datos descentralizadas de registros contables de la Blockchain y en una investigación podemos pasar de una transacción a otra ya que todas las transacciones son visibles. Por cada transacción podemos ver importes transferidos, direcciones intervinientes etc. pero todo esto carece de sentido a menos que podamos asociar estas direcciones con un recurso confiable del mundo real y que nos permita obtener información KYC (Know Your Customer). Poder identificar estos recursos es clave en la mayoría de las investigaciones donde existen pagos ilícitos cuyo cobro se realiza en Bitcoins con el fin de anonimizar el rastro de dicho beneficio.

Sin embargo, un usuario suele descargar una billetera, comprar sus Bitcoins, realizar transacciones a través de Internet y en algún momento va a necesitar vender sus Bitcoins. En este proceso, pueden dejar rastros que eventualmente conduzcan a la identidad de la persona detrás de la billetera, las direcciones, las transacciones y los flujos de dinero. Otro problema añadido para este tipo de investigaciones es la navegación anónima que agrega una dificultad adicional.

Una forma muy común utilizada por los ciberdelincuentes para aumentar el anonimato y ocultar su dirección IP es la utilización de la red Tor para su navegación en los sitios web de Internet. Al hacer uso de la red Tor, la dirección IP del usuario se vuelve anónima, lo que hace muy dificultoso rastrear la identidad y la ubicación del usuario. De esta manera, sus transacciones de Bitcoin no pueden vincularse a su dirección IP y, por lo tanto, no pueden vincularse a una persona. A esto debemos agregarle el uso de medidas de seguridad que dificulten o imposibiliten aún más su identificación, como pueden ser el uso de un proxy al conectarnos a Internet o a través de una VPN todos estos recursos crean una capa más de anonimato en Internet.

Los mixers, también conocido cripto mixers o mezcladores de criptomonedas, surgen con la idea de mejorar el anonimato de los usuarios de criptomonedas. El término surge de la combinación de “cripto” y el término en inglés “mixer”, que en español significa “mezclador”, a través de estos servicios se busca mezclar las criptomonedas con el fin de realizar múltiples combinaciones con incontables transacciones que hacen imposible detectar el origen y el destino de esos activos. Estos servicios no solo están disponibles en foros clandestinos, sino que en cualquier sitio legal de la Internet y al alcance de cualquiera, quienes lo ofrecen generalmente lo anuncian como una opción para mejorar la privacidad.

Figura 12: Flujo de "lavado de dinero" a través de cripto mixers

Fuente: https://www.welivesecurity.com/la-es/2022/04/29/que-son-cripto-mixer-servicio-anonimato-transacciones/

En la siguiente tabla se muestran algunas aplicaciones existentes que se pueden utilizar para hacer un rastreo o seguimiento de transacciones y direcciones en Bitcoin. Existiendo en algunos casos versiones totalmente gratuitas, otras con versiones gratuitas como pagas donde la versión gratuita tiene menos funcionalidades que la versión paga y otras con versiones únicamente pagas, pero más restrictivas en cuanto a quienes la pueden adquirir estando destinada a entidades gubernamentales o instituciones financieras, por ejemplo.

Estas son herramientas potenciales para su uso en una investigación que involucre rastreo de criptomonedas.

Figura 13: Herramientas de rastreo

Herramienta	Descripción	Versión	WEB
Blockchain explorers	Explorador de bloques	Gratuita	https://www.blockchain.com/es/explorer
OXT	Explorador de bloques	Gratuita	https://oxt.me/
Wallet Explorer	Explorador de bloques con identificación de monederos	Gratuita	https://www.walletexplorer.com/
Maltego	Recopilación de información en la web	Gratuita /Pago	https://www.maltego.com/
Bitcoinwhoswho	Explorador de direcciones de Bitcoin	Gratuita	https://www.bitcoinwhoswho.com/
Bitnodes	Permite dimensionar la red Bitcoin en base a la detección de nodos accesibles	Gratuita	https://bitnodes.io/
Chainalysis	Brindan servicios de software e investigación a agencias	Pago	https://www.chainalysis.com/

	gubernamentales, bolsas, instituciones financieras y compañías de seguros y ciberseguridad.		
ChiperTrace	Brinda soluciones de inteligencia en criptomonedas para bancos bolsas de valores, instituciones financieras y gobierno.	Pago	https://ciphertrace.com/

Fuente: Elaboración propia

A continuación, se describen las funcionalidades de cada una de las herramientas mencionadas

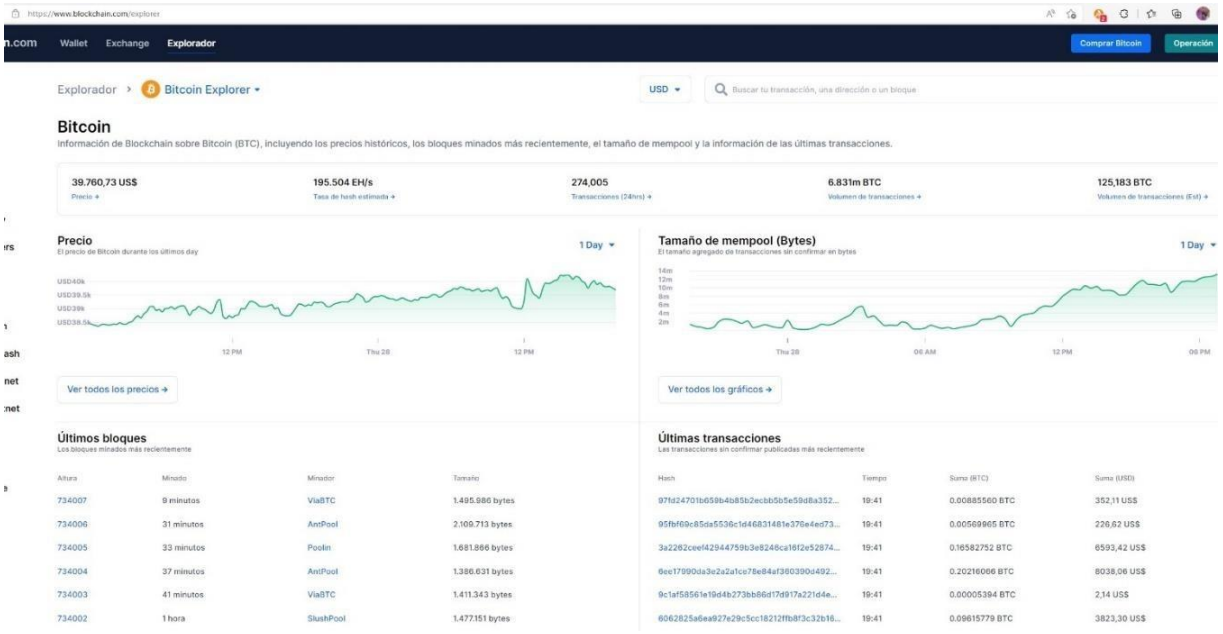
BLOCKCHAIN EXPLORERS

Con la excepción de algunas criptomonedas cerradas o muy seguras, las Blockchains son de fuente abierta y por lo tanto son un recurso útil para ser usadas en una investigación. Si durante una investigación se localiza una dirección que pertenece a un sospechoso (transacciones sospechosas), como puede ser su publicación en un foro, por ejemplo, es sencillo determinar el valor que ha tenido la dirección o tal vez que todavía tiene y que se almacena en dicha dirección. Para hacer esto necesitamos usar un explorador de bloques. Un explorador de blockchain es un motor de búsqueda que se utiliza para encontrar información sobre transacciones de Blockchain. Un explorador de bloques permite buscar por transacción, dirección o por número de bloque. Para el caso de Bitcoin, podemos mencionar a continuación algunos ejemplos de buscadores:

- www.blockchain.com
- www.blockcypher.com
- www.btc.com
- blockstream.info

Otros, como www.blockchair.com y www.bitinfocharts.com, proporcionan exploradores multidivisas es decir para muchas monedas como Bitcoin, Dogecoin, Ethereum, Litecoin y más. Básicamente, todos muestran la misma información, pero con diferentes interfaces gráficas, por lo que es importante comprender los elementos primarios. A continuación, veremos el funcionamiento de blockchain.com/explorer por medio del cual podemos buscar una dirección Bitcoin, Bitcoin Cash o dirección Ethereum. Para comenzar a ver qué tipo de información nos muestra un explorador de bloques podemos ingresar a la página del mismo www.blockchain.com y observar las siguientes Información desplegada de la Blockchain sobre Bitcoin (BTC), como ser los precios históricos, los bloques minados más recientemente, el tamaño de mempool y la información de las últimas transacciones.

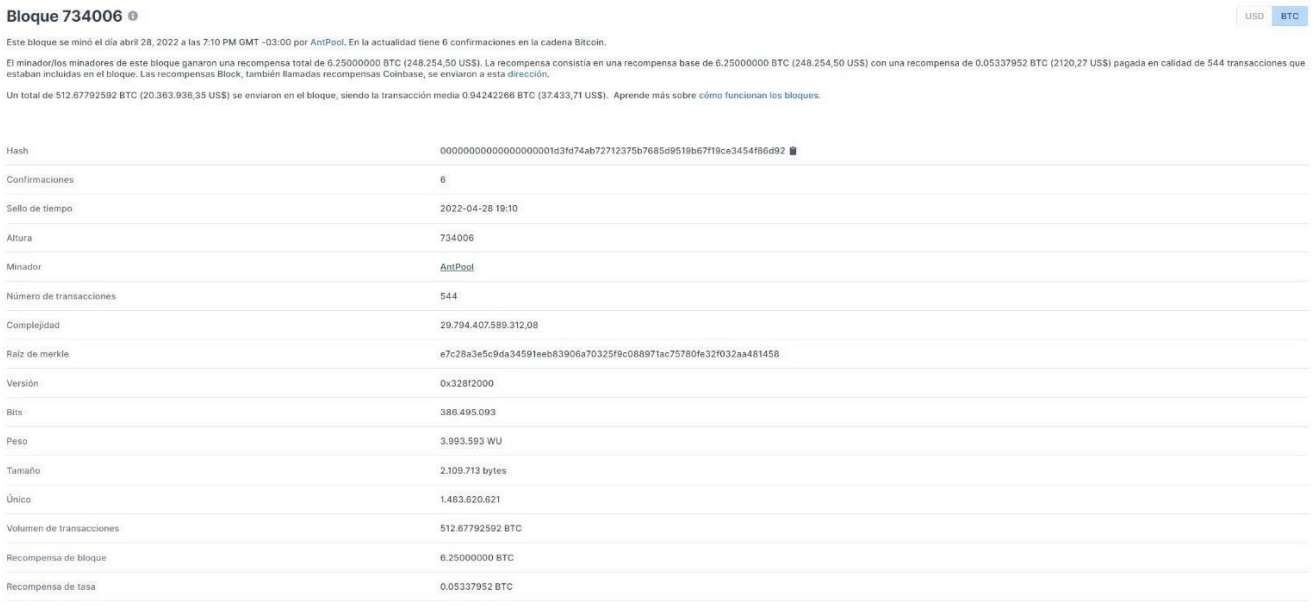
Figura 14: Bitcoin explorer



Fuente: Elaboración propia

Si analizamos la información de uno de los bloques que fueron creados recientemente al escribir este trabajo por ejemplo el bloque 734006 podemos ver los siguientes datos: hash o identificador del bloque, cantidad de confirmaciones, cantidad de transacciones del bloque, el que confirmo las transacciones del bloque o minero que sería el que va a recibir la recompensa, recompensa del bloque que es lo que se paga al minero por generar este bloque etc. Y por último se muestran cada una de las transacciones dentro del bloque.

Figura 15: Información de Bloque



Fuente: Elaboración propia

Generalmente en una investigación por ejemplo nos interesa saber los movimientos de entrada/salida de una dirección y todas las transacciones asociadas a la misma. De la misma manera también nos puede interesar saber sobre una transacción en particular para averiguar las direcciones que intervinieron en la misma y sus importes. Blockchain explorer permite realizar búsquedas por número de transacción, dirección o número de bloque. Si por ejemplo ingresáramos una consulta por número de dirección de Bitcoin el resultado de esa búsqueda devolverá una lista de todas las transacciones donde la dirección ha sido una «entrada», donde pagó dinero a otra dirección, o una «salida», donde recibió dinero de otra dirección. En la consulta de una dirección de Bitcoin con Blockchain explorer, podemos observar un bloque de metadatos en la parte del panel superior seguido de una serie de transacciones que figuran más abajo, para este ejemplo utilizaremos la siguiente dirección: “1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa”

Figura 16: Información de Dirección

Fuente: Elaboración propia

Los metadatos de una dirección pueden ser muy interesantes ya que pueden ayudarnos a construir una imagen del uso de esta dirección. Por ejemplo, en este caso podemos observar la cantidad total de transacciones en la que ha participado esta dirección que son 3303, Cantidad total de Bitcoin que ha recibido esta dirección a lo largo del tiempo 68.53481349 BTC, la cantidad total enviada desde esta dirección a lo largo del tiempo 0.00000000 BTC y el saldo actual de la dirección 68.53481349 BTC.

A continuación, se muestran parte de las transacciones de la dirección antes mencionada

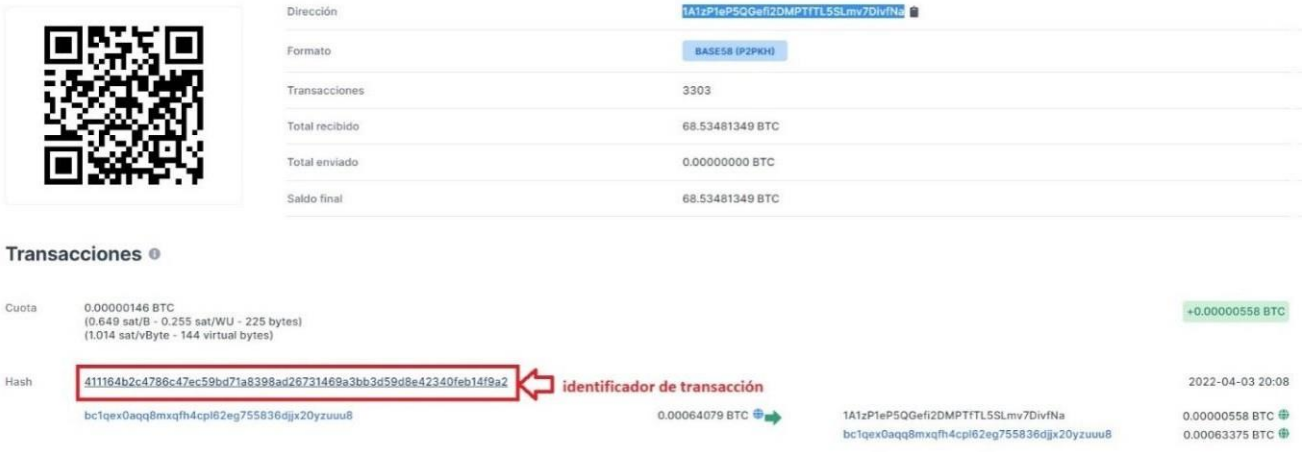
Figura 17: Transacciones

Fuente: Elaboración propia

Aspectos básicos a tener en cuenta en una transacción: En la siguiente figura vamos a analizar una transacción en la que intervino la siguiente dirección de Blockchain "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa".

Una transacción se identifica por su ID (hash) o identificador de la transacción. Cada transacción contiene entradas y salidas. La información principal que muestra una transacción son las direcciones a las que se enviaron los Bitcoins y las cantidades enviadas ("las salidas de la transacción") y la fuente de los fondos para la transacción ("las entradas de la transacción").

Figura 18: ID de Transacción



Fuente: Elaboración propia

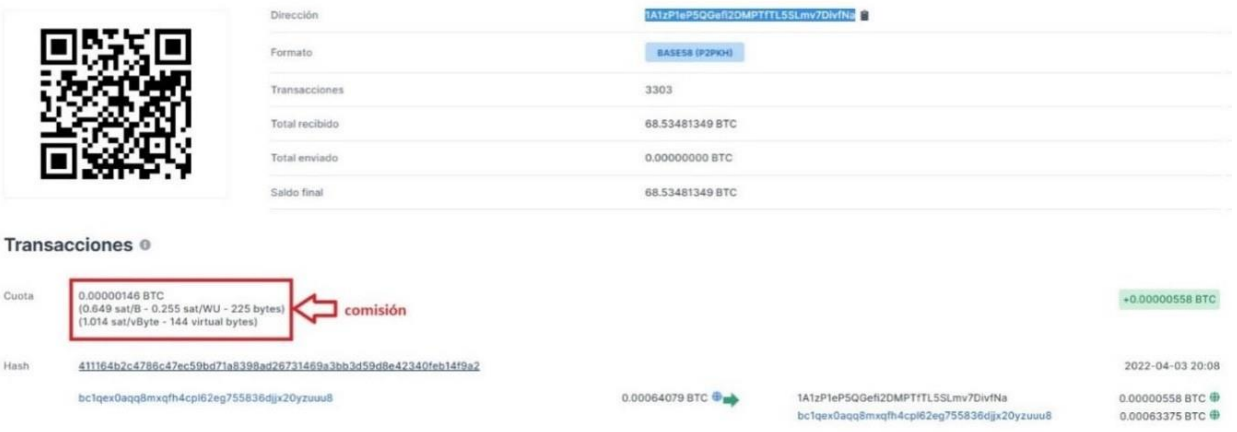
En la siguiente imagen a continuación se puede observar la dirección de envió o la que envía los fondos y el importe enviado.

Figura 19: Entradas de una transacción

Fuente: Elaboración propia

La gran mayoría de las redes Blockchain cobran tasas (comisiones) asociadas a sus transacciones y está la paga quien envía las criptomonedas en los bloques de validación de la red al completarse la operación.

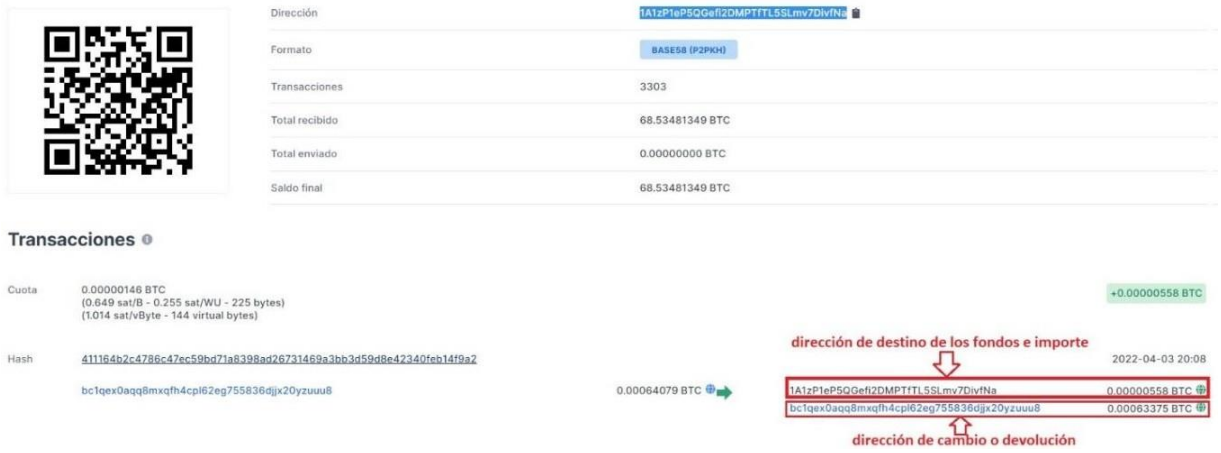
Figura 20: Comisión de una transacción



Fuente: Elaboración propia

La dirección de destino muestra la dirección de recepción de los fondos y para cada dirección podemos ver el importe exacto que están recibiendo.

Figura 21: Salidas de una transacción



Fuente: Elaboración propia

En este ejemplo se está enviando desde la dirección "bc1qex0aqq8mxqfh4cpl62eg755836djjx20yzuuu8" un valor de 0.00064079 BTC, donde parte de ese importe es enviado a la dirección de destino 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa por un valor de 0.00000558 BTC el resto de 0.00063375 BTC se envía a una dirección de cambio o dirección de devolución (bc1qex0aqq8mxqfh4cpl62eg755836djjx20yzuuu8), esta se trata de una dirección que se crea automáticamente para guardar el saldo restante de una transacción que queda bajo el control de la dirección que envía los fondos y esta es una función exclusiva de la Blockchain de Bitcoin.

Por último, queda señalar el estado de una transacción que puede ser confirmado o sin confirmar. Una transacción se considera valida cuando su estado es confirmado, en cambio las transacciones sin confirmar pueden ser declaradas invalida o cancelada, pero es mejor considerar a las transacciones sin confirmar como no recibidas aun y esperar hasta que se confirmen.

Los exploradores de bloques también aportan otra información como ser fecha y hora exacta de la operación, la lista de transacciones pendientes, los ganadores de recompensa por bloques, los volúmenes de comercio diario y muchos otros registros inmutables en la cadena de bloques. Poder interpretar correctamente la información presentada por los exploradores de bloques es clave para rastrear el origen y destino de un criptoactivo. Un explorador de bloques se puede usar para consultar una dirección que intervino en el pago de un rescate y ver que podemos encontrar detrás de las transacciones en las que intervino dicha dirección.

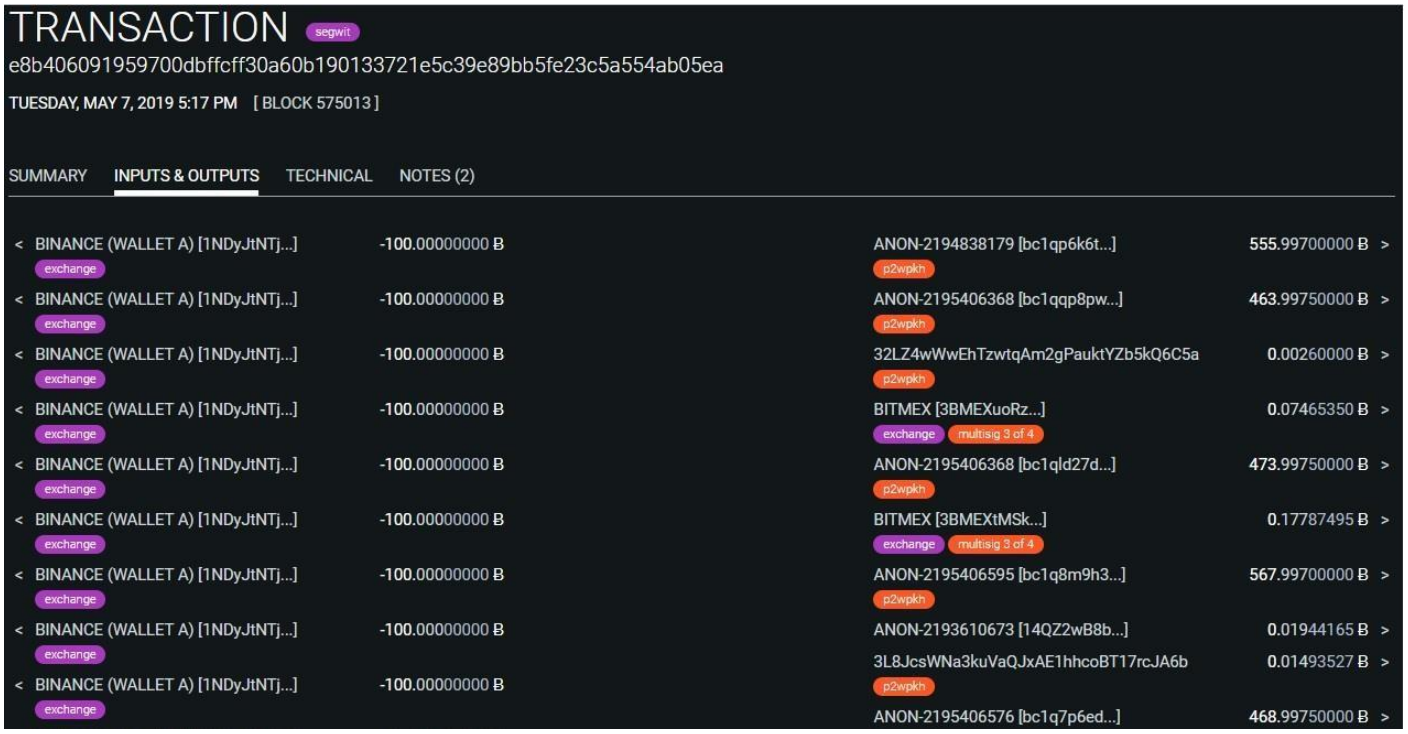
OXT

OXT es una plataforma de análisis de Blockchain de Bitcoin que forma parte del servicio de Samourai Wallet. Samourai Wallet es una cartera de criptomonedas para dispositivos móviles especializada en el almacenamiento de Bitcoin (BTC) donde los usuarios tienen el control de sus propias claves privadas. En diciembre de 2017 OXT fue adquirida por Samourai Wallet. Cuando

se accede a la página de inicio de OXT podemos observar que la misma es muy sencilla y tiene un explorador que permite realizar búsquedas por direcciones, bloques y transacciones.

Si bien este explorador en cuanto a sus funcionalidades es similar a Blockchain explorer tiene un formato de visualización de la información que nos hace un poco más sencillo la interpretación en un resultado de búsqueda. Por ejemplo, si se ingresa una búsqueda por un ID de transacción en OXT, podemos obtener un resultado como la imagen de la Figura 22 donde podemos observar en las entradas y salidas (INPUTS & OUTPUTS) de la transacción como OXT trata de identificar a que tipo de monedero pertenece las direcciones si pertenece a un Exchange y a cuál, si es una dirección multifirma etc.

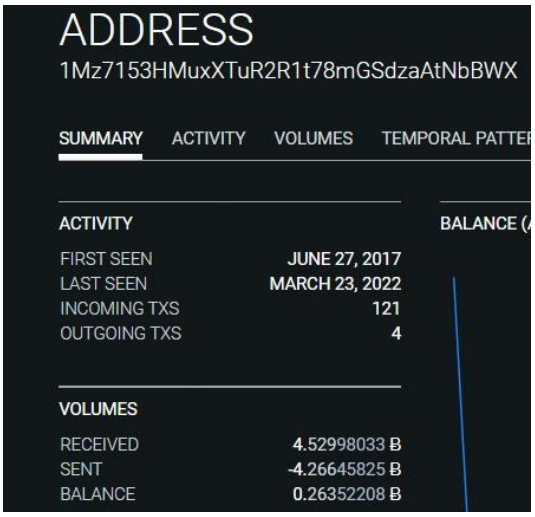
Figura 22: Transacción en OXT



Fuente: Elaboración propia

Otra parte interesante para visualizar cuando hacemos una búsqueda por una dirección asociada a pagos producto de ransomware, es el número de pagos que nos puede ayudar a discernir el número probable de víctimas y **https://oxt.me** nos presenta esta información de manera muy práctica. Por ejemplo, si buscamos la dirección: "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" podemos obtener la siguiente imagen

Figura 23: Resumen de dirección en OXT

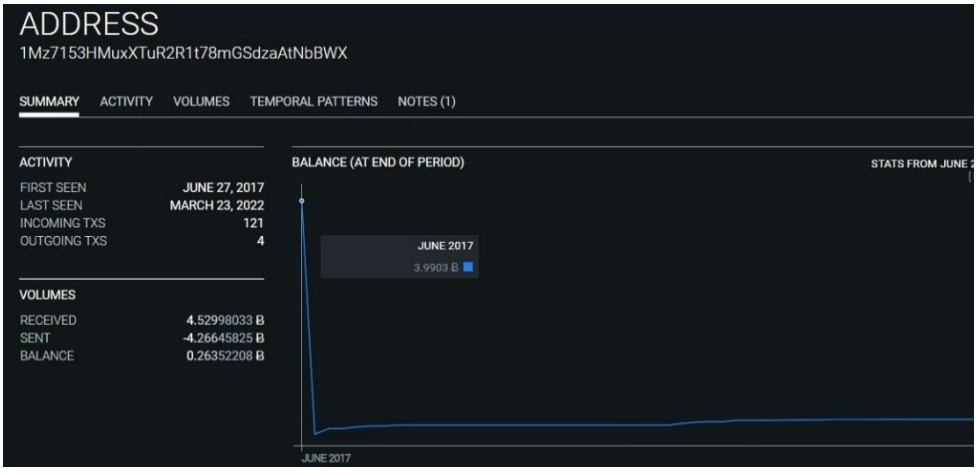


Fuente: Elaboración propia

En la Figura 23 se puede observar rápidamente cuando una dirección comenzó a usarse, cuando se utilizó por última vez, los valores recibidos y retirados. También nos muestra un desglose de las transacciones entrantes y salientes que, en este ejemplo, por tratarse de la dirección de pago del ransomware petya[7] se podría inferir que la cantidad de pagos entrantes cuyo valor es 121 sería el número de víctimas probables y cuántas direcciones se utilizaron para finalmente mover las monedas lejos de la dirección de la estafa.

OXT también puede rastrear el balance de la cartera a lo largo del tiempo y mostrara con una precisión aproximada las horas del día en las que más actividad tuvo, si miramos en el gráfico del balance de esta dirección podemos observar que el pico de actividad de pagos fue en junio de 2017.

Figura 24: Balance de dirección en OXT



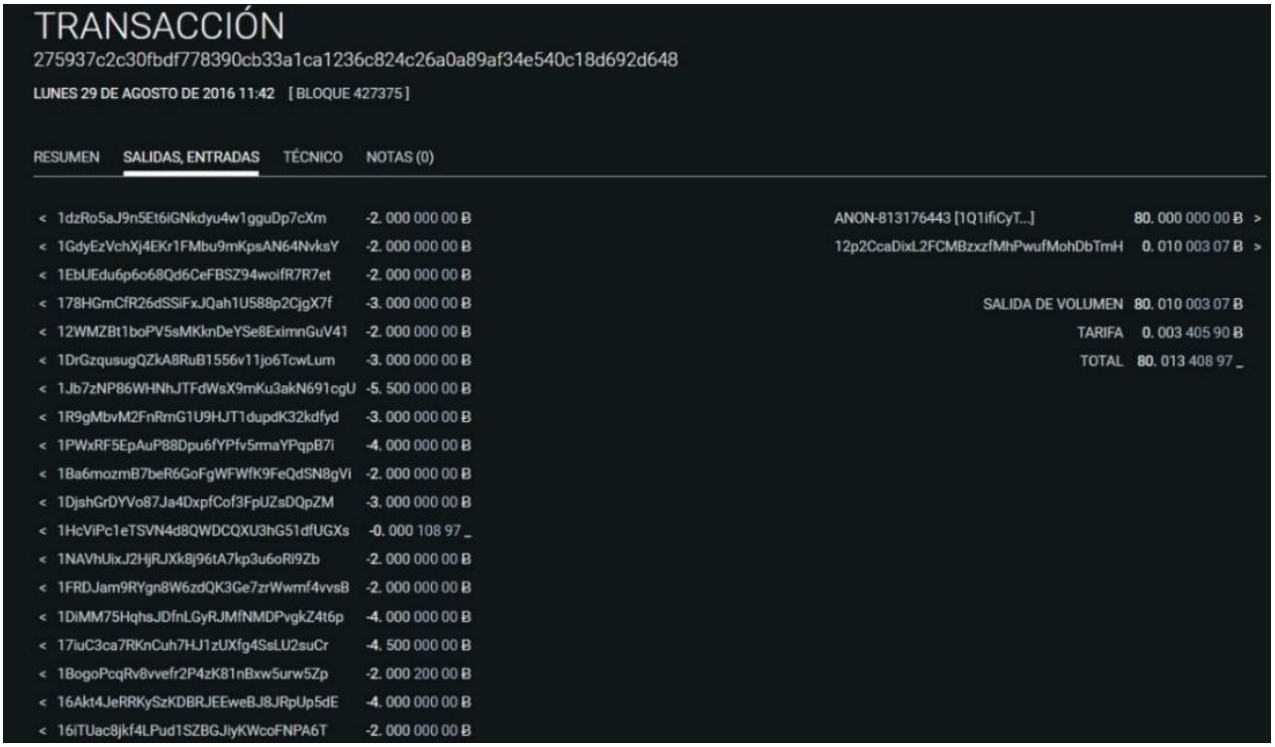
Fuente: Elaboración propia

[7] Petya es una familia de malware que encripta y que infecta ordenadores con sistemas operativos Microsoft Windows.

Otra de las funcionalidades muy interesante que posee OXT es su herramienta grafica que nos permite ver una transacción de una manera más visual por ejemplo sigamos a la siguiente transacción en OXT: "275937c2c30fbdf778390cb33a1ca1236c824c26a0a89af34e540c18d692d648"

En la parte de entradas y salidas de esta transacción podemos observar (30) entradas y (2) salidas

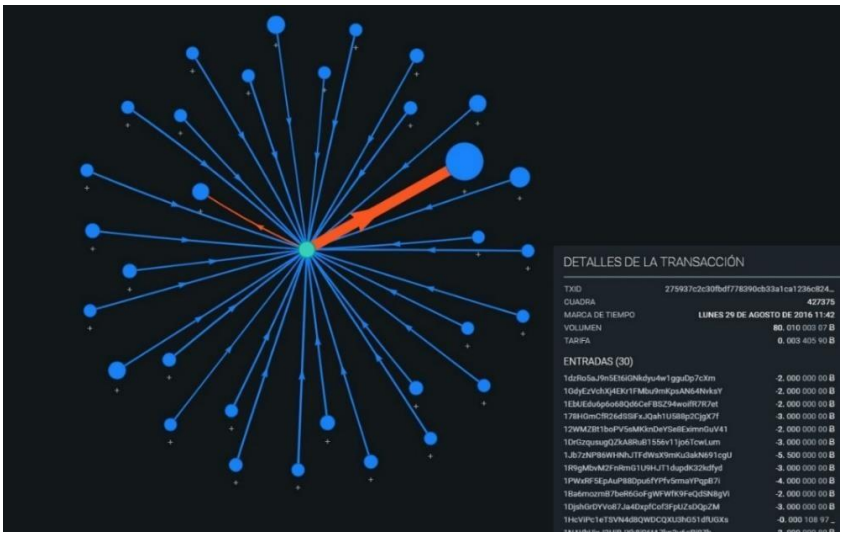
Figura 25: Balance de dirección en OXT



Fuente: Elaboración propia

Cuando realizamos un seguimiento muchas veces debemos ir moviéndonos de una transacción a otra y OXT tiene una manera grafica que puede facilitarnos esta tarea, podemos utilizar su herramienta grafica haciendo clic en el icono correspondiente y nos aparece la siguiente imagen que se corresponde a la transacción "275937c2c30fbdf778390cb33a1ca1236c824c26a0a89af34e540c18d692d648" donde el centro representa la transacción, las flechas con dirección entrante hacia el centro son las entradas y las flechas con dirección saliente son las salidas. En la Figura 26 se observa las flechas de color azul corresponden a las entradas y las flechas de color naranja son las salidas (las mismas fueron coloreadas apropósito). También se puede observar en las salidas que una de la flecha tiene un grosor mucho mayor que la otra, esto se debe a que cuanto mayor sea el grosor de la flecha mayor será el importe involucrado.

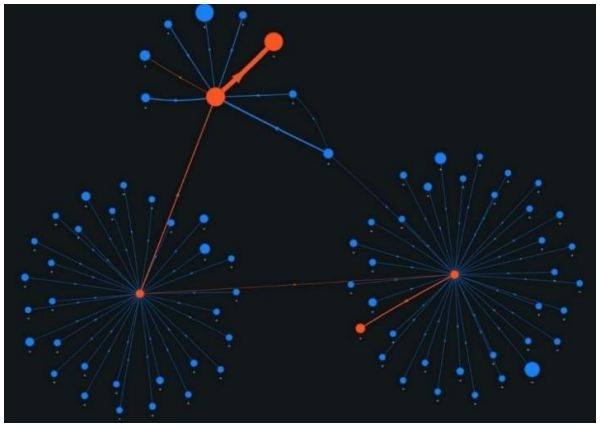
Figura 26: Herramienta detalles de transacción en OXT



Fuente: Elaboración propia

También en la gráfica podemos ir marcando para tener una trazabilidad del camino a medida que nos vamos moviendo entre transacciones (expandiendo el gráfico) como se observa en la siguiente imagen

Figura 27: Herramienta detalles de transacción en OXT



Fuente: Elaboración propia

WALLET EXPLORER

Trabaja de manera similar a los exploradores de bloques, pero su trabajo es correlacionar las direcciones con billeteras, en realidad lo que muestra wallet explorer es la cartera o monedero a la que pertenece esa dirección. Wallet explorer para poder asociar direcciones a monederos o carteras utiliza técnicas de agrupamiento para identificar una dirección y luego inferir la propiedad de otras direcciones de la misma entidad. Si ingresamos a la web de wallet explorer (https://www.walletexplorer.com/) e ingresamos una dirección de Bitcoin como ser "1Q1ifiCyTtoYsrq2MQjZqpHSFREDTteE8E" obtenemos el siguiente resultado:

Figura 28: Monedero en WalletExplorer

Fuente: Elaboración propia

Podemos observar que la dirección 1Q1ifiCyTtoYsrq2MQjZqpHSFREDTteE8E que es una billetera pertenece al monedero o cartera **0c6c74ea2b** la cual posee varias billeteras. Si queremos ver todas las billeteras de esta cartera podemos hacerlo haciendo clic en “mostrar direcciones de billetera”.

Figura 29: Billeteras de un Monedero en WalletExplorer

Fuente: Elaboración propia

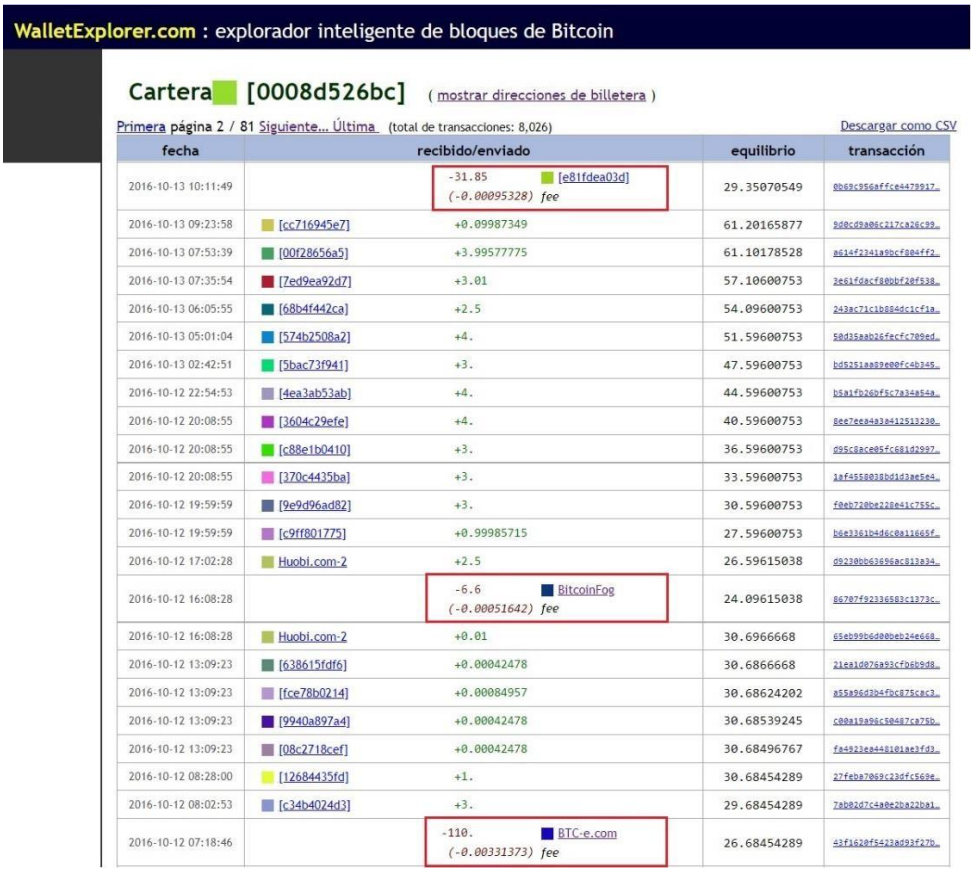
Otro punto importante es que en la imagen de la Figura 28 nos muestra las transacciones asociadas a todas las billeteras de la cartera, pero si solo quisiéramos ver las transacciones de la dirección investigada solo tenemos que hacer clic en mostrar solo la dirección 1Q1ifiCyTtoYsrq2MQjZqpHSFREDTteE8E y obtenemos la siguiente imagen

Figura 30: Billetera y sus transacciones en WalletExplorer

Fuente: Elaboración propia

En la siguiente figura se muestra una imagen recortada de los resultados obtenidos en wallet explorer de la dirección 12p2CcaDixL2FCMBzxzfMhPwufMohDbTmH, donde podemos observar por ejemplo que uno de los envió de criptomonedas se realizó a un mezclador o mixer de criptomonedas BitcoinFog con la finalidad de eliminar la posibilidad de rastreo y también se puede ver en la misma imagen otro envió a BTC-e.com. BTC-e fue una plataforma de intercambio de criptomonedas, pero fue clausurado en julio de 2017 por presunto lavado de dinero.

Figura 31: Monedero, billeteras y transacciones en WalletExplorer



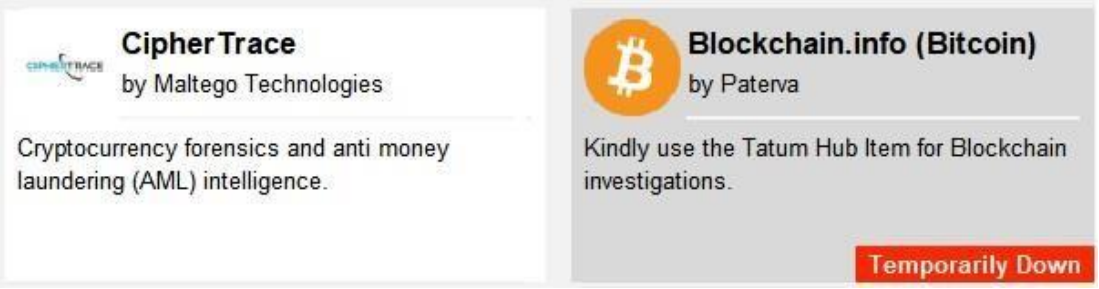
Fuente: Elaboración propia

MALTEGO

Maltego es una herramienta de análisis gráfico de enlaces que ofrece la extracción de datos y la recopilación de información en tiempo real, así como la representación de esta información en un gráfico basado en nodos, lo que permite identificar patrones y conexiones de orden múltiple entre dicha información. Con Maltego, se pueden extraer datos de fuentes dispersas, fusionar automáticamente la información coincidente en un gráfico y mapearla visualmente para explorar su panorama de datos. Maltego ofrece la posibilidad de conectar fácilmente datos y funcionalidades de diversas fuentes mediante el uso de transformadas. Para el caso de las criptomonedas Maltego posee dos API o transformadas que se pueden utilizar una es la de Cipher Trace que no está disponible para esta versión gratuita, solo en la versión de pago y la otra es la de blockchain.info (Bitcoin) que si está disponible para la versión gratuita.

CipherTrace desarrolla herramientas que son utilizado por agencias financieras o investigadores para consultar y monitorear los movimientos de criptomonedas, el riesgo de fraude y la atribución de identidad a billeteras sospechosas o de alto perfil de riesgo.

Figura 32: Transformadas de Criptomonedas para Maltego



Fuente: Elaboración propia

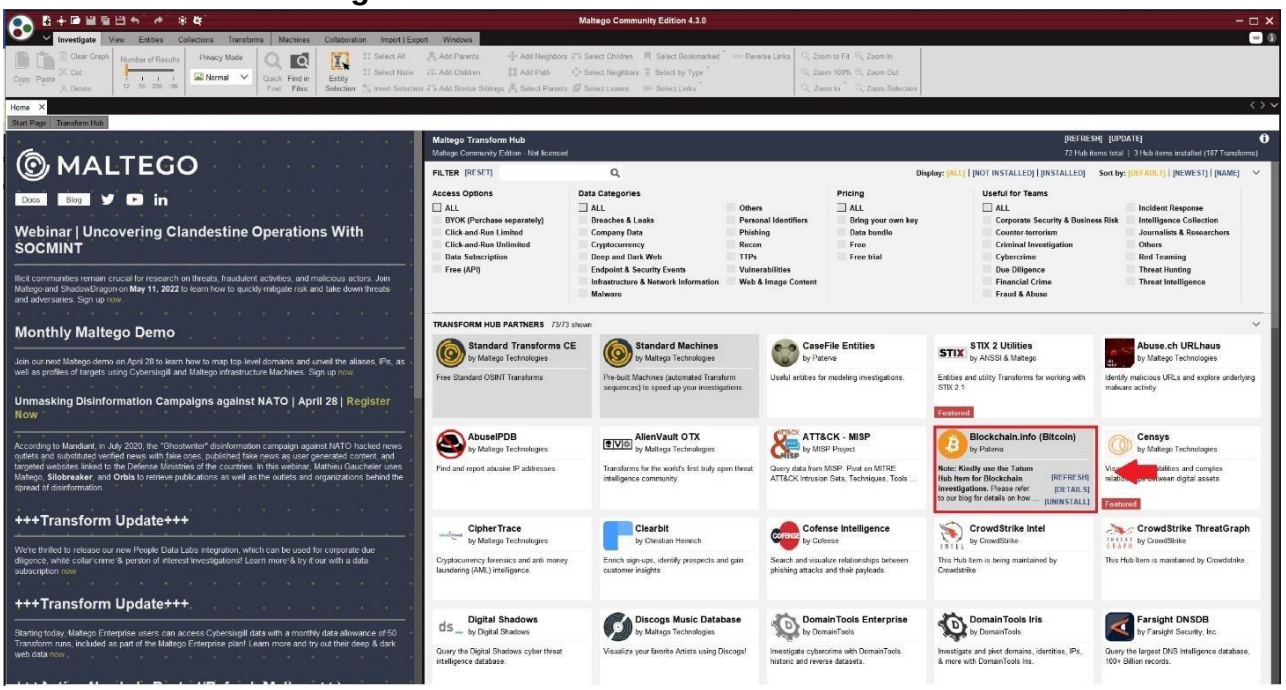
Maltego en investigaciones de la Blockchain puede rastrear múltiples transacciones que entran y salen en múltiples direcciones visualizando todo esto en un gráfico.

Para esta evaluación se utilizará la versión CE 4.3.0 (Community edition) que es una versión gratuita y el único requisito para su uso es estar registrado en el sitio web de paterva los creadores de maltego. Esta versión tiene ciertas limitaciones como ser el número de resultados que permite visualizar que es hasta un máximo de 12 resultados, no así la versión de pago.

Además de Maltego CE, existen otras versiones que son pagas como la Classic y XL que requieren de una licencia para poder ser utilizadas y además, tienen otras funcionalidades que no posee la versión comunitaria.

Maltego trabaja con el concepto de transformadas que son las que realizan el trabajo y existen muchos tipos de transformadas donde cada tipo sirve para trabajar sobre una entidad en particular como por ejemplo las transformadas para blockchain.info que permite analizar operaciones en Bitcoin. En la siguiente figura se observa la API que debe ser instalada desde el hub de transformadas de Maltego para poder buscar entidades de Bitcoin como ser una dirección BTC.

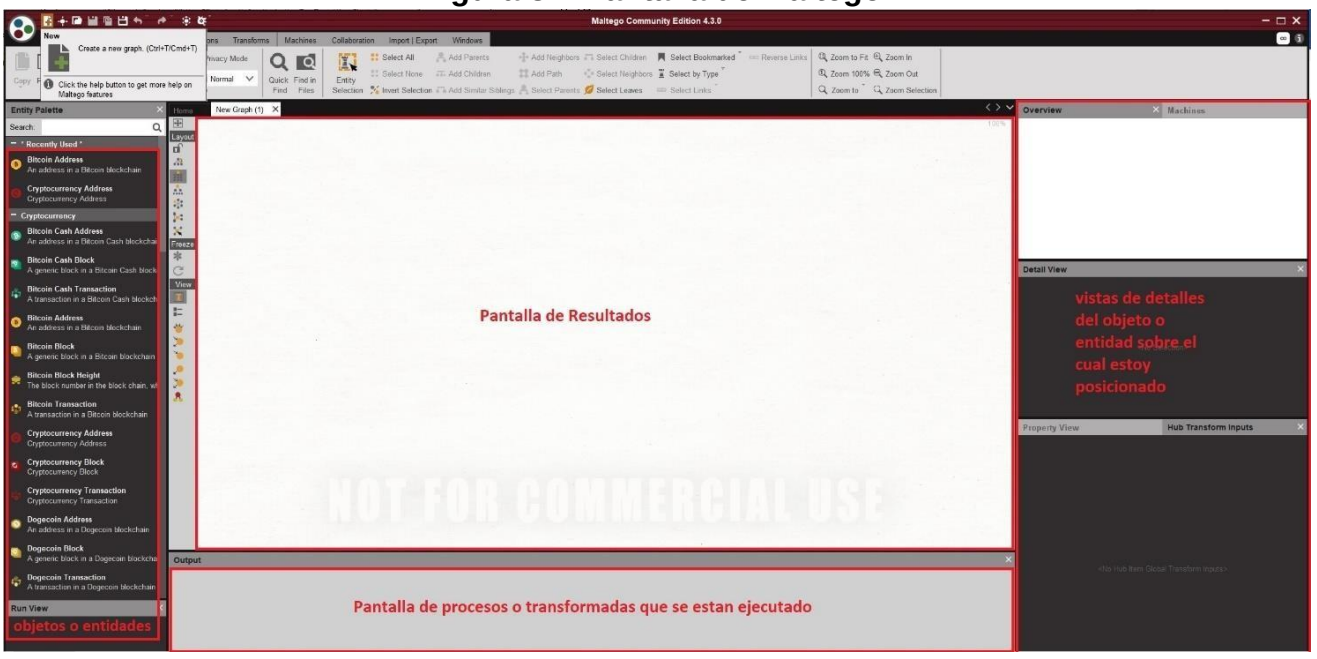
Figura 33: Instalando API Blockchain.info



Fuente: Elaboración propia

A continuación, se muestra una imagen con una descripción de las partes que componen una pantalla de trabajo en maltego a la cual se accede al crear un nuevo grafico

Figura 34: Pantalla de Maltego



Fuente: Elaboración propia

En la parte izquierda de la pantalla es donde se encuentran las entidades u objetos que podemos seleccionar con relación a las criptomonedas Maltego puede trabajar con Bitcoin, Bitcoin cash,

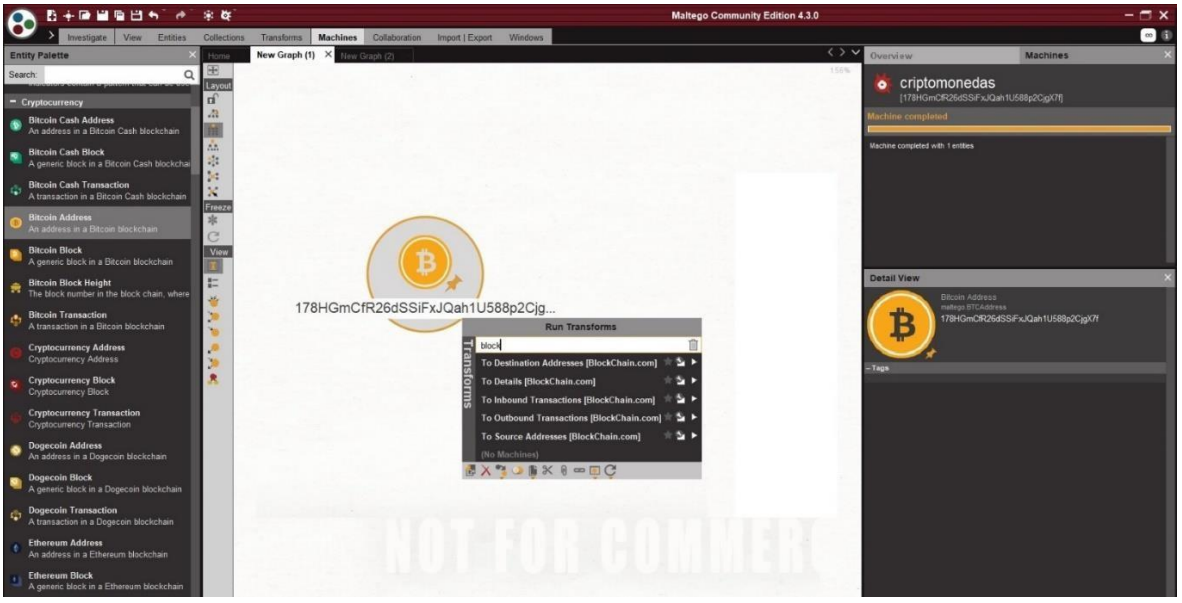
Ethereum, Dogecoin pudiendo obtener información por número de dirección, identificador de transacción y número de bloque.

Figura 35: Criptomonedas disponibles en Maltego

Fuente: Elaboración propia

Para nuestro estudio vamos a elegir la entidad “Bitcoin address”, lo arrastramos y soltamos en la pantalla de resultados a continuación ingresamos una dirección de Bitcoin en la parte de propiedades de la entidad Bitcoin address recién creada, en este caso utilizaremos la dirección de pago que daba el ransomware locky (178HGmCfR26dSSiFxJQah1U588p2CjgX7f), si hacemos click con el botón derecho sobre el objeto podemos observar las transformadas que podemos ejecutar sobre una dirección de Bitcoin.

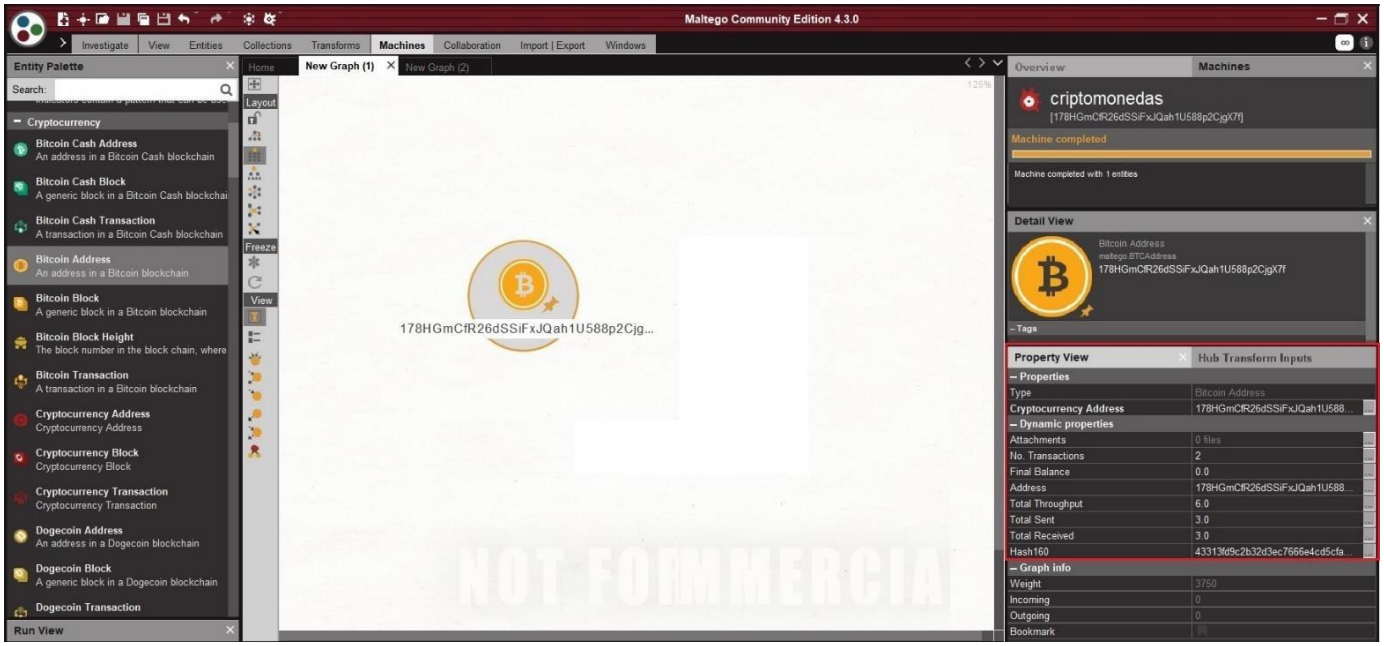
Figura 36: Transformadas para una dirección de Bitcoin



Fuente: Elaboración propia

Inicialmente le pedimos a maltego que corra las transformadas de detalles (“To Details”) para esta entidad y obtenemos el siguiente resultado (Figura 37) pudiéndose observar en la vista de propiedades del objeto información de cantidad de transacciones, monto recibido, monto enviado, balance etc.

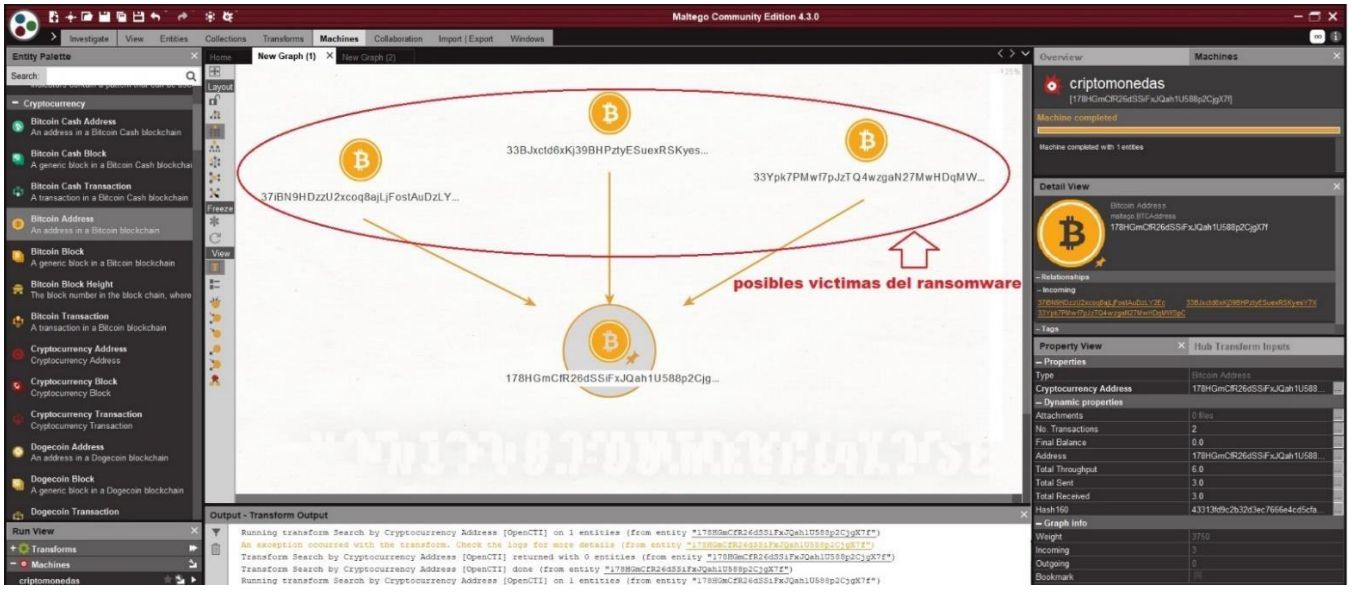
Figura 37: Objeto Bitcoin Address



Fuente: Elaboración propia

Ahora sobre la misma entidad podemos ejecutar las transformadas de “to source addresses” que son las direcciones de entrada o dicho de otra manera serían las direcciones de las victimas que hicieron algún tipo de pago a la cuenta del ransomware y obtenemos la siguiente figura.

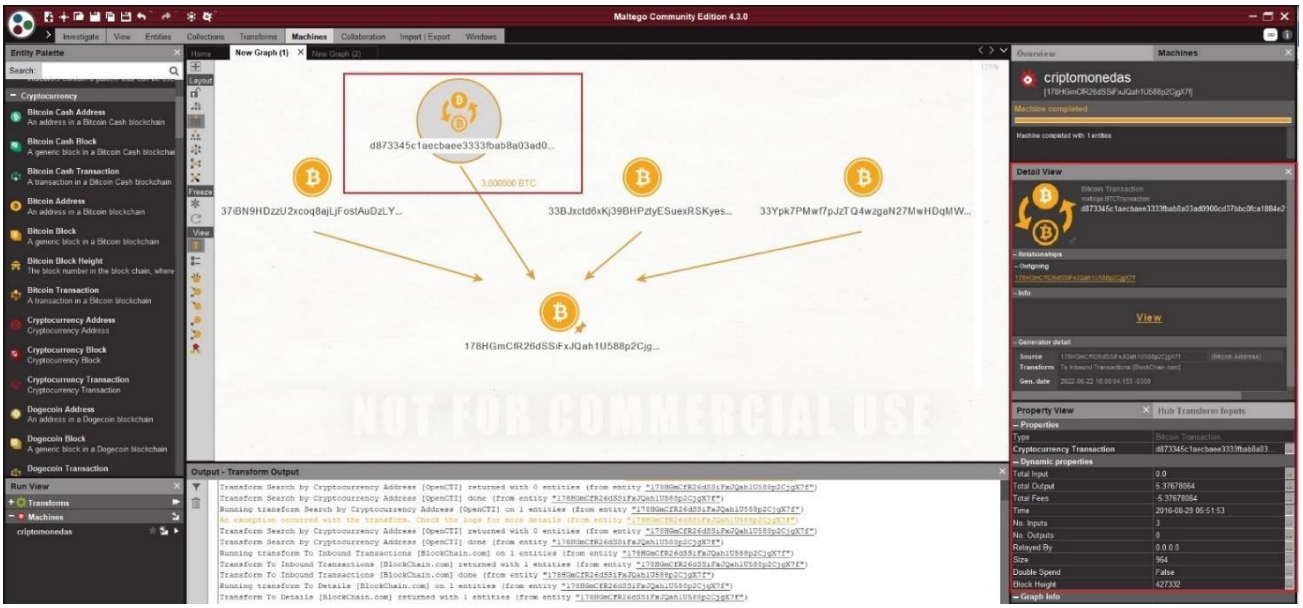
Figura 38: Direcciones de entradas sobre un Objeto Bitcoin Address



Fuente: Elaboración propia

Luego siempre posicionados sobre la entidad Bitcoin address vamos a ejecutar las transformadas que nos muestran las transacciones entrantes (“To Inbound Transactions”), esto se puede observar en la siguiente figura donde se agregó al grafico anterior un objeto más que corresponde a una transacción pudiéndose observar el importe transferido a la dirección de destino. En el mismo grafico podemos observar datos de la entidad transacción en la parte de vista de detalles y propiedades (Detail view y Property view).

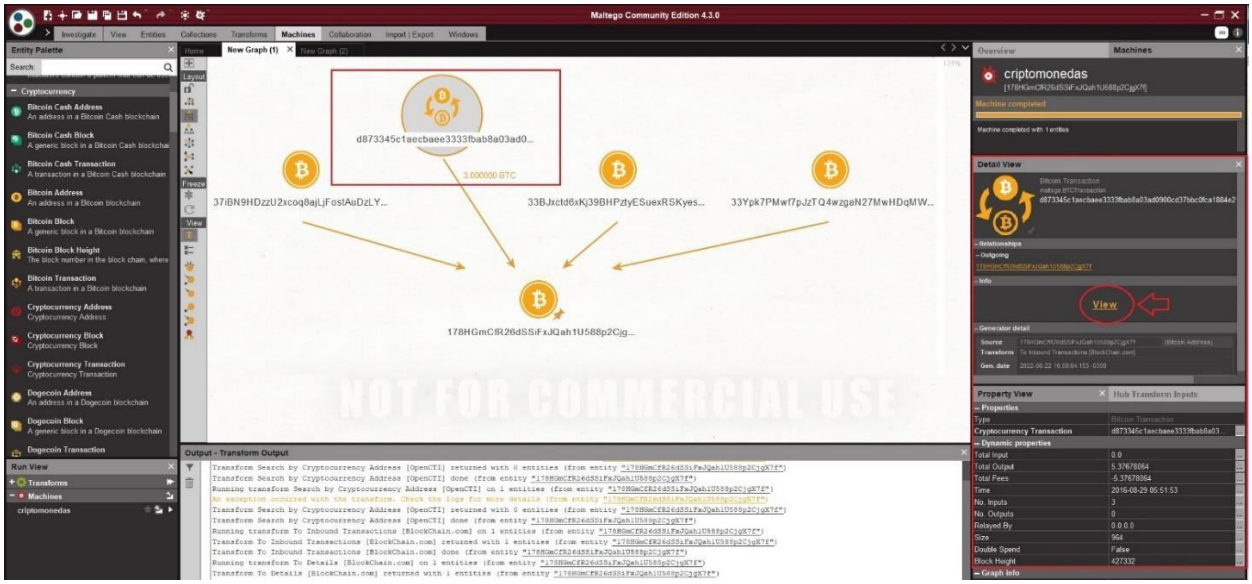
Figura 39: Transacciones y direcciones de entrada de un Objeto Bitcoin Address



Fuente: Elaboración propia

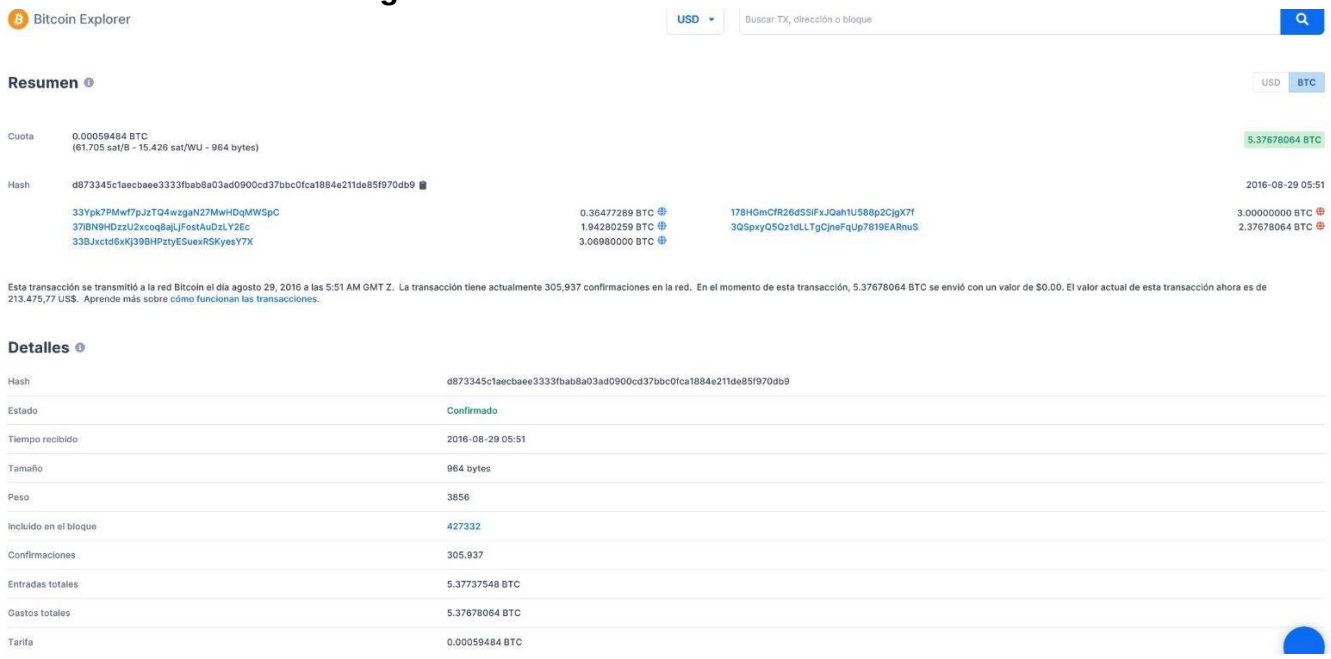
y si hacemos click en el enlace View en la vista de detalle de la transacción se nos abrirá una ventana de blockchain.info con los datos de dicha transacción.

Figura 40: Vista de detalle y propiedades de un objeto Transacción



Fuente: Elaboración propia

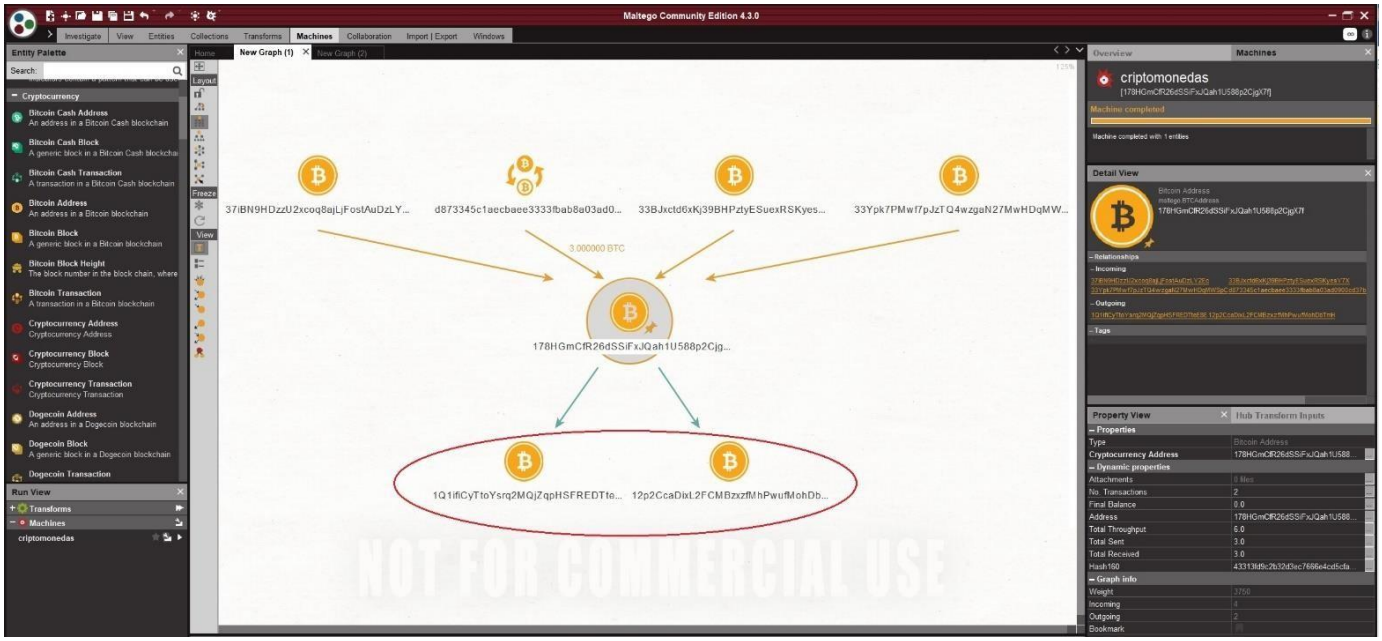
Figura 41: Visualización en blockchain.info



Fuente: Elaboración propia

A continuación, seguimos agregando más elementos a nuestra grafica con la opción “to Destination Addresses” podemos ver hacia que direcciones se movieron los fondos obteniéndose 2 direcciones más para su análisis.

Figura 42: Direcciones de Salidas

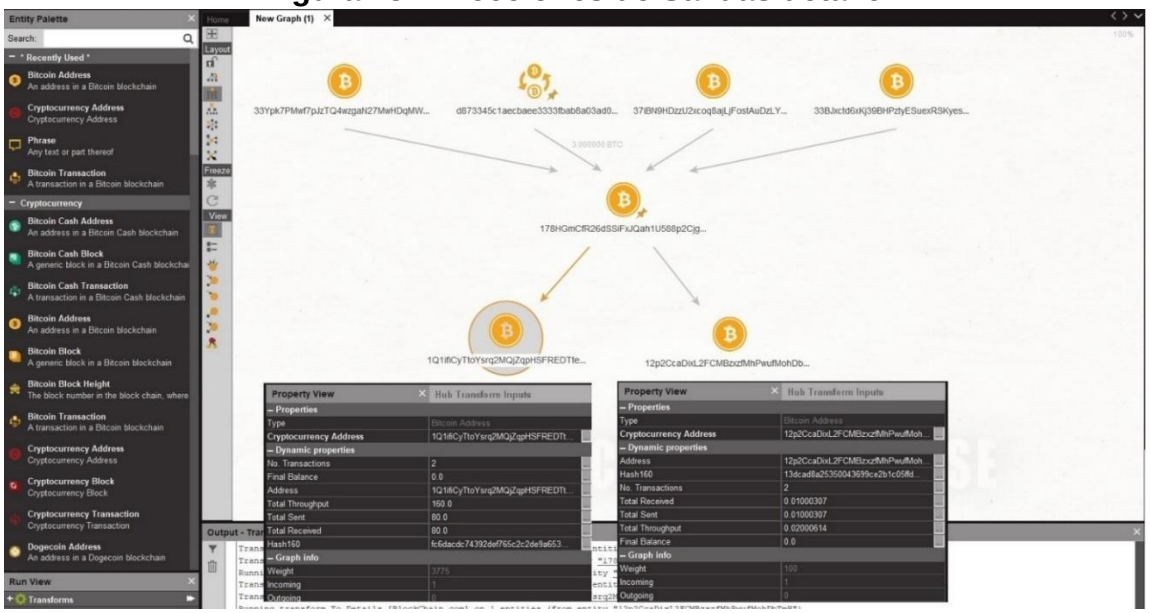


Fuente: Elaboración propia

Si visualizamos los detalles de estas 2 direcciones podemos observar que el total recibido y enviado en la dirección 1Q1ifiCyTtoYsrq2MQjZqpHSFREDTteE8E es de 80 BTC una suma muy

importante y en la dirección 12p2CcaDixL2FCMBzxzfMhPwufMohDbTmH el total enviado y recibido fue de 0.01000307 BTC por lo cual el paso siguiente seria continuar nuestro análisis por estas direcciones.

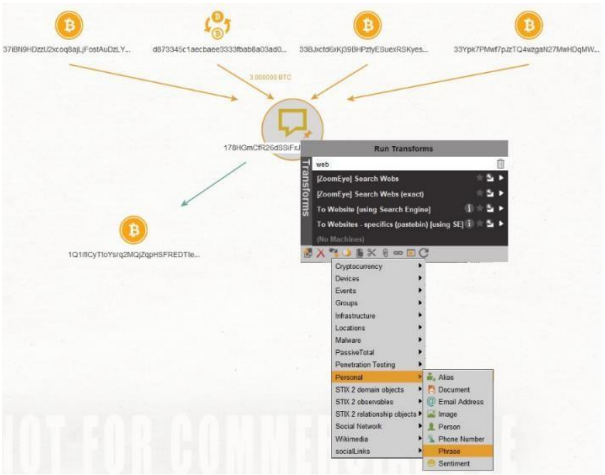
Figura 43: Direcciones de Salidas detalle



Fuente: Elaboración propia

Para elegir qué direcciones de Bitcoin seguir explorando en cada paso, elegiremos las que tengan mayor rendimiento (es decir, en base a cuántos Bitcoins ha recibido y enviado a lo largo del tiempo) que básicamente seria ejecutar las transformadas “To Details” y luego mirar la vista de detalle de esa dirección. Siguiendo esta mecánica descripta anteriormente podemos ir encontrando direcciones de Bitcoin para luego tratar de identificar los posibles propietarios de la dirección bajo investigación. Con maltego podemos realizar búsquedas por ejemplos en sitios web donde fueron publicadas una dirección bajo investigación una forma de hacerlo sería convertir la Entidad de dirección de Bitcoin en una frase como se muestra a continuación

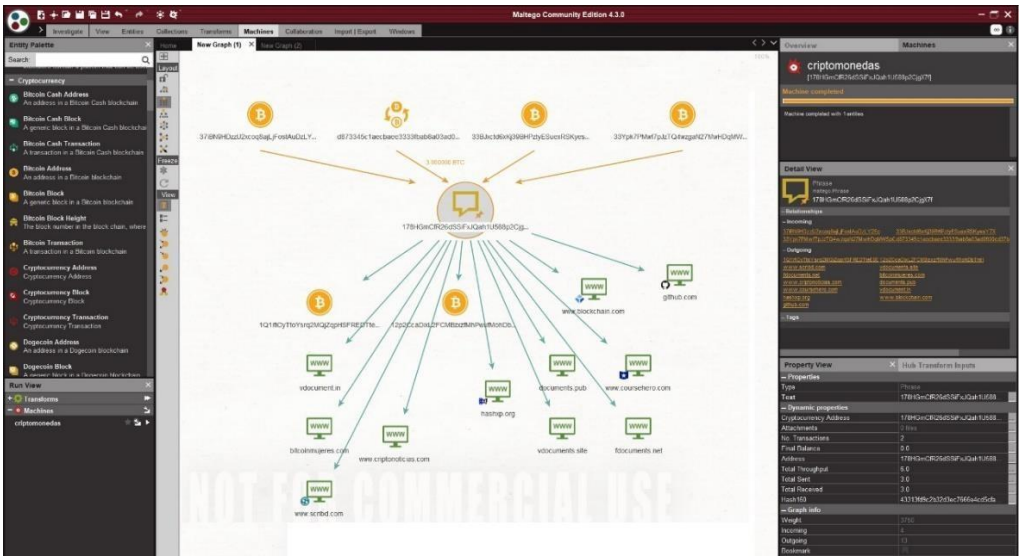
Figura 44: Convertir a frase direcciones de Bitcoin



Fuente: Elaboración propia

y luego usar la Transformación To website [user search engine] para encontrar todos los sitios web donde se la menciona como se muestra en la siguiente imagen

Figura 45: Búsqueda de dirección en sitios web donde se la menciona

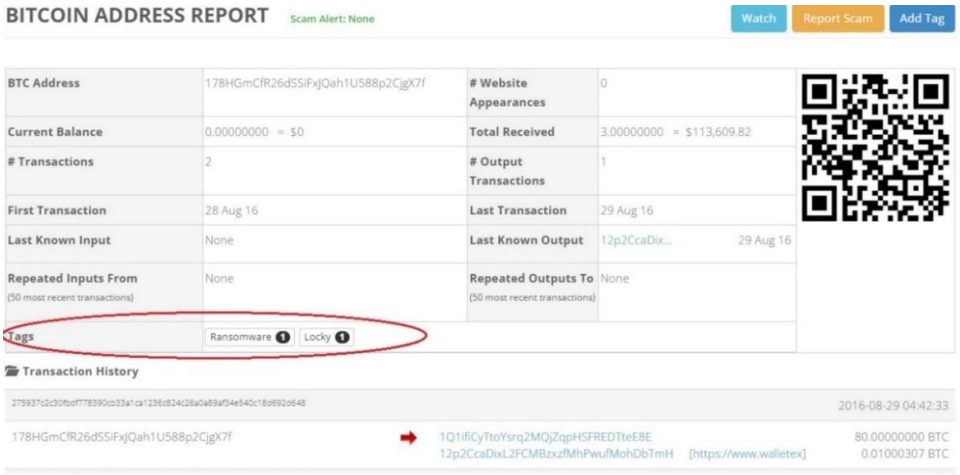


Fuente: Elaboración propia

BITCOIN WHOS WHO

Bitcoinwhoswho.com es otro sitio que brinda información muy valiosa para llevar a cabo investigaciones y en especial cuando se tratan de estafas. Este sitio no solo proporciona el saldo actual y el número de transacciones, sino también si la dirección de Bitcoin ha aparecido publicada en algún sitio web y también puede mostrar la dirección IP de la última transacción**.** Una cosa interesante es que permite denunciar direcciones que han participado de una estafa, chantaje o extorsión para que las transacciones con estas direcciones puedan detectarse y evitarse. También permite agregar etiquetas a las direcciones a fin de poder identificar direcciones fraudulentas.

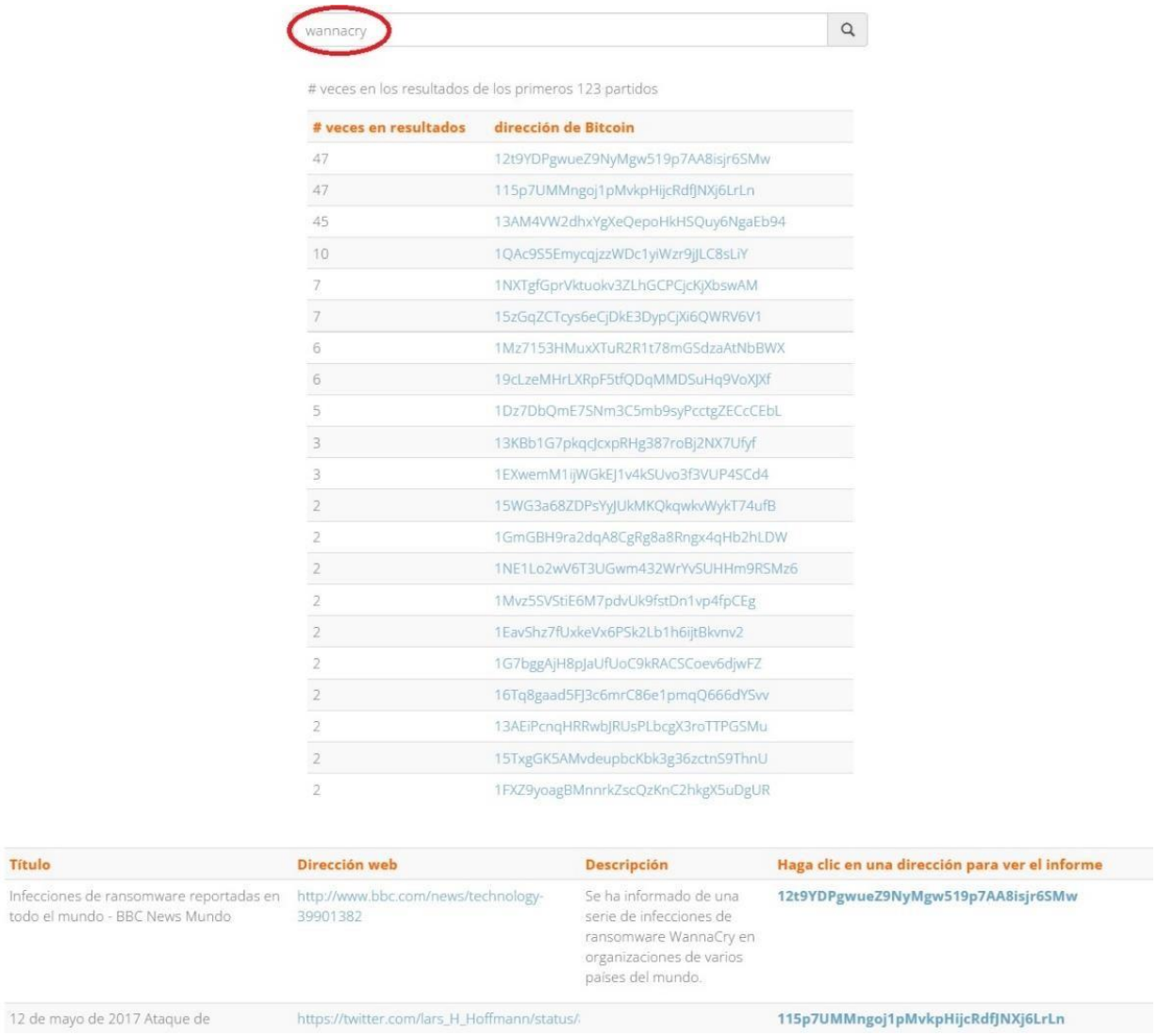
Figura 46: Información de Dirección en Bitcoinwhoswho.com



Fuente: Elaboración propia

Y además permite realizar búsquedas por tag o etiqueta. Por ejemplo, si buscamos por la etiqueta wannacry obtenemos el siguiente resultado que se muestra en la siguiente figura:

Figura 47: Búsqueda de Dirección por etiqueta en Bitcoinwhoswho.com



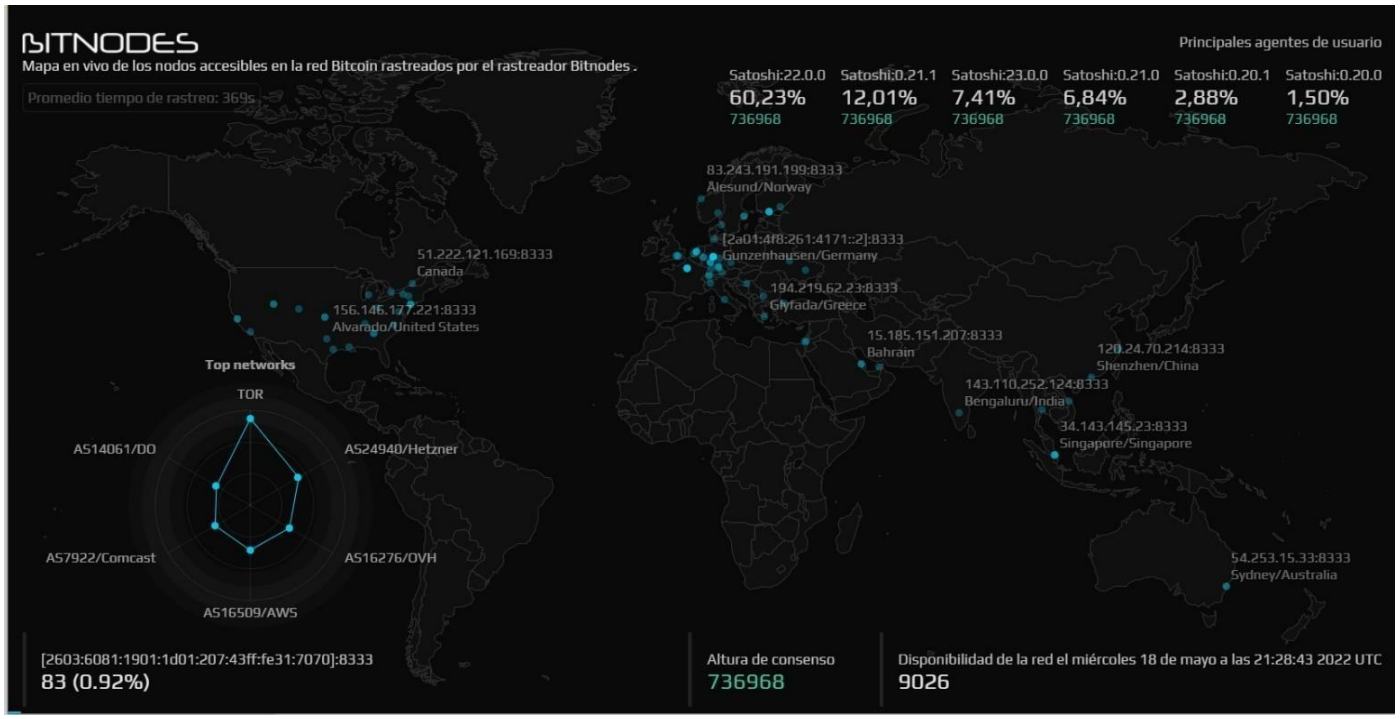
Fuente: Elaboración propia

BITNODES

Bitnodes es una herramienta que permite dimensionar el tamaño relativo de la red peer-to-peer de Bitcoin por medio de la utilización de un protocolo de descubrimiento. La metodología actual consiste en enviar mensajes getaddr de forma recursiva para encontrar todos los nodos accesibles en la red, a partir de un conjunto de nodos semilla y con esto hacer una representación visual en un mapa mundial de todos los nodos Bitcoins descubiertos. En Bitcoin core, los nodos más cercanos se identifican en el archivo peers.dat, entonces para que un cliente conozca más nodos, el protocolo de descubrimiento envía a estos nodos una petición para descubrir más

nodos y cuando estos nodos reciban la petición estos informaran los nodos más cercanos a ellos y así sucesivamente.

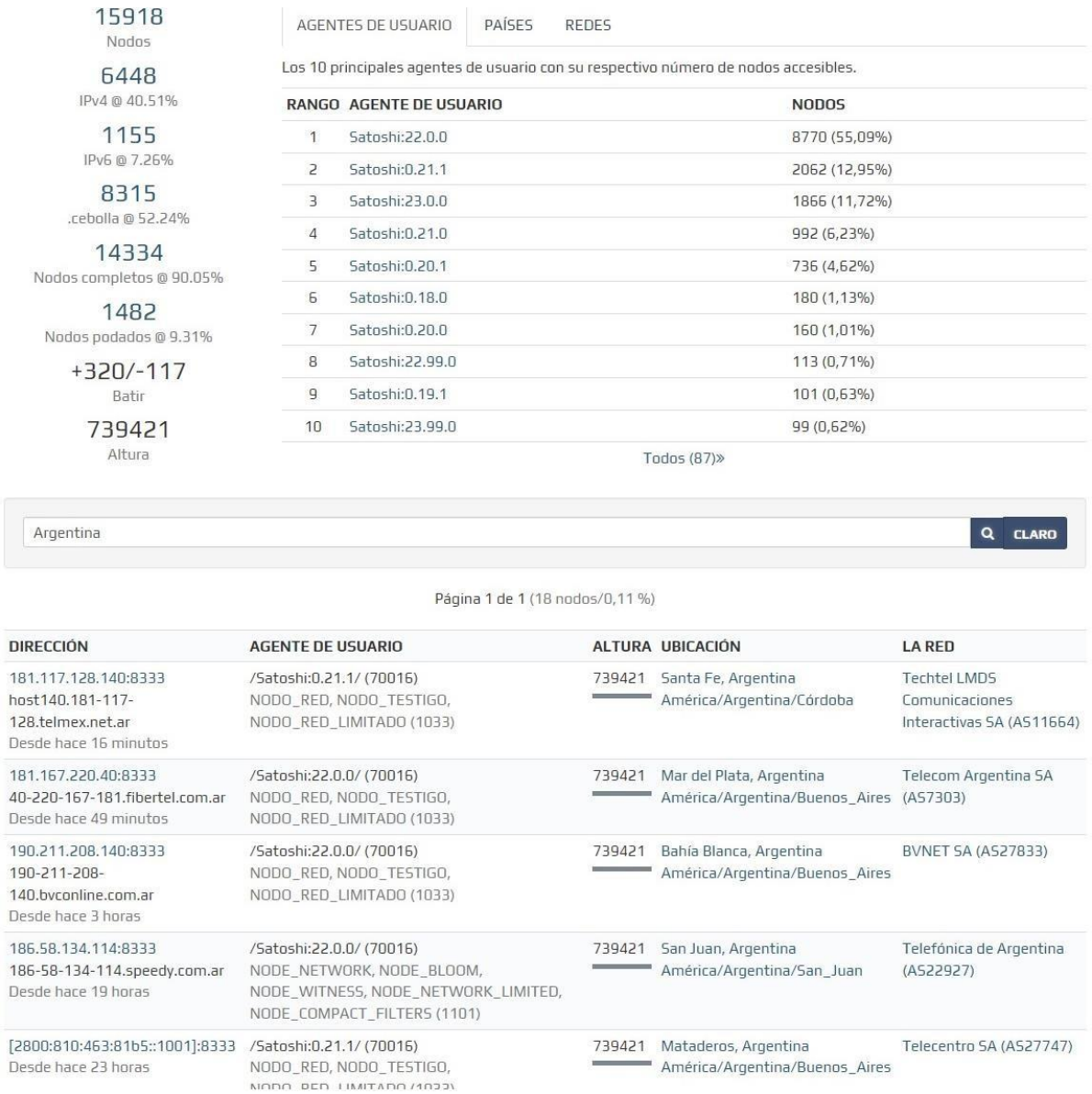
Figura 48: Mapa en vivo de nodos accesibles de la red bitcoin



Fuente: Elaboración propia

Bitnodes está mostrando en tiempo real los nodos accesibles de la red Bitcoin. Con esta información bitnodes puede establecer un ranking de países en base a la cantidad de nodos accesibles en el momento de realizar la consulta. También permite ver por país información detallada de los nodos accesibles en un tiempo determinado, por ejemplo, si queremos ver los nodos de Bitcoin activos de nuestro país podemos hacerlo seleccionando de la lista de países a la Argentina a continuación obtenemos una pantalla con información de la IP, el protocolo que está ejecutando y su versión, ubicación, red a la que está conectada, etc., de cada uno de los nodos. El resultado de esta consulta se muestra en la siguiente imagen aclarando que la misma varía de acuerdo al momento en que se realiza la misma

Figura 49: Instantánea de los nodos de Bitcoin accesibles de Argentina



15918
Nodos
6448
IPv4 @ 40.51%
1155
IPv6 @ 7.26%
8315
.cebolla @ 52.24%
14334
Nodos completos @ 90.05%
1482
Nodos podados @ 9.31%
+320/-117
Batir
739421
Altura

AGENTES DE USUARIO | PAÍSES | REDES

Los 10 principales agentes de usuario con su respectivo número de nodos accesibles.

RANGO	AGENTE DE USUARIO	NODOS
1	Satoshi:22.0.0	8770 (55,09%)
2	Satoshi:0.21.1	2062 (12,95%)
3	Satoshi:23.0.0	1866 (11,72%)
4	Satoshi:0.21.0	992 (6,23%)
5	Satoshi:0.20.1	736 (4,62%)
6	Satoshi:0.18.0	180 (1,13%)
7	Satoshi:0.20.0	160 (1,01%)
8	Satoshi:22.99.0	113 (0,71%)
9	Satoshi:0.19.1	101 (0,63%)
10	Satoshi:23.99.0	99 (0,62%)

Todos (87)»

Argentina — CLARO

Página 1 de 1 (18 nodos/0,11 %)

DIRECCIÓN	AGENTE DE USUARIO	ALTURA	UBICACIÓN	LA RED
181.117.128.140:8333 host140.181-117-128.telmex.net.ar Desde hace 16 minutos	/Satoshi:0.21.1/ (70016) NODO_RED, NODO_TESTIGO, NODO_RED_LIMITADO (1033)	739421	Santa Fe, Argentina América/Argentina/Córdoba	Techtel LMDS Comunicaciones Interactivas SA (AS11664)
181.167.220.40:8333 40-220-167-181.fibertel.com.ar Desde hace 49 minutos	/Satoshi:22.0.0/ (70016) NODO_RED, NODO_TESTIGO, NODO_RED_LIMITADO (1033)	739421	Mar del Plata, Argentina América/Argentina/Buenos_Aires	Telecom Argentina SA (AS7303)
190.211.208.140:8333 190-211-208-140.bvconline.com.ar Desde hace 3 horas	/Satoshi:22.0.0/ (70016) NODO_RED, NODO_TESTIGO, NODO_RED_LIMITADO (1033)	739421	Bahía Blanca, Argentina América/Argentina/Buenos_Aires	BVNET SA (AS27833)
186.58.134.114:8333 186-58-134-114.speedy.com.ar Desde hace 19 horas	/Satoshi:22.0.0/ (70016) NODE_NETWORK, NODE_BLOOM, NODE_WITNESS, NODE_NETWORK_LIMITED, NODE_COMPACT_FILTERS (1101)	739421	San Juan, Argentina América/Argentina/San_Juan	Telefónica de Argentina (AS22927)
[2800:810:463:81b5::1001]:8333 Desde hace 23 horas	/Satoshi:0.21.1/ (70016) NODO_RED, NODO_TESTIGO,	739421	Mataderos, Argentina América/Argentina/Buenos_Aires	Telecentro SA (AS27747)

Fuente: Elaboración propia

Para terminar el tema de herramientas a continuación, se mencionan 2 empresas que se especializan en inteligencia analítica de Blockchain CipherTrace y Chainalysis.

Generalmente, estas empresas proporcionan sus productos a agencias gubernamentales, instituciones financieras y exchanges de todo el mundo para ayudarlos a analizar lo que está sucediendo en Blockchain en un intento por desenmascarar a los actores de amenazas del mundo real detrás de las transacciones de criptomonedas.

CHAINALYSIS

Chainalysis es una de las firmas más importantes del mundo en análisis de Blockchain y desarrolla informes del sector, colabora con autoridades gubernamentales e instituciones financieras, y provee herramientas educativas y de análisis a empresas y exchanges en más de 40 países.

Con más de 5 años de antigüedad, y una dotación de aproximadamente 174 empleados distribuidos entre las ciudades de New York, Washington d.c., Londres y Copenhague, la empresa analiza los movimientos de compra, venta o transferencia de más de 100 criptomonedas existentes en la Blockchain pública.

Técnicamente Chainalysis diseña y desarrolla software contra el lavado de dinero para negocios de Bitcoin. Chainalysis Reactor utiliza inteligencia de código abierto (OSINT) junto con gráficos enriquecidos para ayudar a contextualizar el flujo de transacciones criptográficas sospechosas. Chainalysis también ofrece informes de seguimiento de actividades y herramientas de investigación basadas en identificar ciberdelincuentes, identificación de pagos de extorsión de Bitcoin realizados por víctimas a delincuentes y atribución para industrias de inteligencia de amenazas cibernéticas.

Si bien puede no conocerse en primera instancia las identidades de los titulares/usuarios de esas billeteras, muchas veces algunos descuidos de los usuarios inexpertos hacen posible dar con el paradero de éste o bien, de las operaciones relacionadas.

Para ello, se utilizan los metadatos de las operaciones analizadas, que le permiten a los analistas, identificar operaciones de calidad “sospechosa” y los posibles usuarios vinculados a ellas.

la información analizada está relacionada con:

- husos horarios en los que se hacen las operaciones,
- los rastros de las **direcciones ip** que puedan quedar entre la operación y el cruce con cualquier wallet o plataforma,
- información pública en las redes sociales,
- información existente en las bases de datos gubernamentales utilizadas en el marco de acuerdos firmados entre la empresa chainalysis.com y los gobiernos interesados en este tipo de herramientas.

Por último, para cerrar chainalysis, ha anunciado el lanzamiento de dos herramientas para la detección de sanciones que se proporcionarán a la industria de las criptomonedas de forma gratuita. Según información proporcionada por Chainalysis, las herramientas de detección incluyen dos componentes principales de un nuevo software de seguimiento que ayudará a los intercambios en la detección de billeteras y transacciones en busca de actividades que podrían estar eludiendo las sanciones económicas. La primera herramienta, que está disponible de inmediato, es on-chain oracle .

On-chain oracle es un contrato inteligente dirigido más específicamente a proyectos de finanzas descentralizadas (DeFi). Lo que hace es validar si una dirección de billetera de criptomonedas

se ha incluido o no en una lista de sanciones. Esto significa que esta información estará disponible automáticamente para un gran número de personas, en particular para las entidades que deseen verificar que una dirección pertenece a una lista de billeteras sancionadas por los Estados Unidos, la Unión Europea o las Naciones Unidas.

La segunda herramienta, cuyo lanzamiento está programado próximamente, es una interfaz de programación de aplicaciones (API). Una API utiliza exactamente los mismos datos que on-chain oracle para validar si una billetera está incluida en alguna lista de sanciones. Sin embargo, está diseñado para usarse en una variedad mucho más amplia de aplicaciones, incluidos intercambios de cifrado centralizados e interfaces de usuario móviles.

CIPHERTRACE

Esta empresa se creó en 2015 para desarrollar capacidades de seguridad y rastreo de criptomonedas y Blockchain, fue financiada por el Departamento Nacional de Estados Unidos. Cipher Trace posee diferentes tipos de productos y tiene uno en particular que permite llevar a cabo Investigaciones financieras y análisis forense de Blockchain, ese producto se llama Cipher Trace inspector el cual puede rastrear transacciones de Blockchain y examinar actividad sospechosa, identificar el uso de criptomonedas para lavar dinero y rastrear ransomware y otros pagos ilícitos.

Para realizar su trabajo CipherTrace inspector posee un buscador de cadenas de bloque que permite al usuario simplemente ingresar una dirección de criptomoneda o ID de transacción en una barra de búsqueda intuitiva que puede autocompletarse para direcciones largas.

Ciphertrace utiliza una poderosa base de datos para rastrear el flujo de fondos a lo largo del tiempo y a través de las entidades de la cadena de bloques. La interfaz de usuario es muy intuitiva mostrando visualmente los datos relacionados con una transacción, como una dirección criptográfica o una billetera específicas. La búsqueda intuitiva de Blockchain y el autocompletado agilizan y facilitan la investigación de ID y direcciones de transacciones de criptomonedas

CipherTrace aplica análisis avanzados de big data, utiliza algoritmos de agrupamiento propios, para agrupar puntos de datos dentro del amplio repositorio de atribución. El resultado es una vista amplia, catalogada y de alta resolución del panorama de transacciones de criptomonedas.

Esta plataforma de información de atribución de alta calidad de CipherTrace puede agregar y correlacionar rápidamente una variedad de indicadores y luego proporcionar a los usuarios evaluaciones de riesgo e inteligencia procesable. Además, estas amplias capacidades de atribución ayudan a los investigadores a recopilar evidencias con mayor rapidez.

Capítulo 5

Delineando una propuesta para rastreo de criptomonedas en base a PURI:

Las direcciones de Bitcoin están pensadas para funcionar como seudónimos con el fin de evitar que el carácter público del historial de transacciones permita identificar a algún usuario. En ciertas ocasiones cuando un usuario quiera realizar algunas transacciones como la compra de

criptomonedas utilizando dinero *fiat* tendrá que proporcionar algún dato identificativo a quien le proporcione el servicio en cuestión, por lo que su identidad quedara enlazada con la dirección que utilice para la adquisición de esa criptomoneda. Luego podría seguirse la cadena de transacciones a partir de esa dirección.

Los ataques de ransomware son casos muy frecuentes de comisión de delitos que involucran a las criptomonedas, en este tipo de ataques el malware hace su aparición de manera sorpresiva con un mensaje en el computador de la víctima, amenazando al usuario con perder todos sus archivos (ahora encriptados) en caso de no pagar un monto de rescate y en criptomonedas. En estos delitos queda claro que se considera a la criptomoneda como instrumento o medio comisivo de un delito.

Los ataques de ransomware donde solicitan el pago de un rescate en criptomonedas para poder recuperar sus datos, podrían resolverse rastreando los fondos entregados por la víctima o victimas al victimario con el fin de lograr dar con este último. Otra característica en estos ataques es que no hay una única víctima por lo general son muchos los damnificados por este tipo de ataques y es importante que se lleve a sede judicial estos delitos para que los ciberdelincuentes puedan ser denunciados. A continuación, se hace una primera aproximación para el uso del Modelo PURI en este tipo de delitos.

Aplicación del modelo PURI para un caso de un ciberdelito producido por ataque de ransomware donde el pago del rescate se realice en criptomonedas

Fase de relevamiento:

Todos los afectados por una infección de ransomware son víctimas de un delito y como tal pueden hacer la denuncia correspondiente. Esta fase abarca la investigación para conocer el caso y los posibles objetos de interés. Por ello esta etapa se inicia con el conocimiento del caso y las tareas investigativas de la denuncia realizada ante la justicia por parte del afectado que en estos casos puede ser una persona física, empresa u organización.

La Fiscalía actuante es la que determina en esta fase las actividades a realizar. Para este caso puede solicitar asistencia o asesoramiento de un perito informático con conocimientos en criptomonedas. El modelo PURI en esta fase posee dos actividades importantes: por un lado, tenemos identificación de la documentación legal y técnica, y por otro es identificar la infraestructura IT.

Para nuestro análisis se considera solo las situaciones donde las criptomonedas son un medio de comisión de delitos provocado por un ataque de ransomware. Estas situaciones de ataques por ransomware donde se encriptan todos o parte de los archivos de un computador o sistema informático de la entidad atacada, ya sea esta una persona física o una empresa, y donde el atacante solo desencriptara los archivos a cambio de un pago o rescate en criptomonedas (para nuestro estudio en Bitcoin) pueden encuadrarse en las siguientes figuras legales:

a. Daño informático definida por el art. 183, segundo párrafo del Código Penal[8]
b. Delito de extorsión previsto en el art. 168 del Código Penal.[9]

La resolución de estos casos radica en el rastreo de las criptomonedas pagadas o entregadas por la victima al victimario con el fin lograr saber quiénes se encuentran detrás de las direcciones de estos delitos y generalmente este rastreo se hace online analizando la Blockchain de Bitcoin. Con relación a los objetos de interés se debe prestar atención a las direcciones de Bitcoin del origen de los fondos transferidos por la víctima y la dirección de Bitcoin de destino de esos fondos, la cantidad de Bitcoins transferidos y la fecha de la transacción.

Fase de Recolección:

En esta etapa se da intervención al especialista de recolección (ER) quien se constituirá en el lugar del hecho con el acta de allanamiento y con pleno conocimiento de las medidas que el juez de garantías autorizó a realizar en dicha diligencia. La finalidad de este proceso es el secuestro del soporte de la evidencia digital.

En esta etapa se realiza una inspección visual para identificar la infraestructura y es fundamental que el o los equipos informáticos afectados no sean manipulados con el fin de preservar -de la mejor manera posible- la evidencia digital del delito. Cabe aclarar que, si bien se puede hacer una recolección de los equipos o sus medios de almacenamiento para su posterior análisis, en esta investigación la fuente de datos sobre la cual se va a trabajar y es objeto de interés es una dirección criptográfica de Bitcoin. Generalmente la dirección criptográfica de pago la victima la obtuvo cuando recibió un mensaje del ransomware en su pantalla en donde se le informa que han bloqueado el acceso a sus archivos o sistemas, que los mismos han sido encriptados y para recuperar sus datos o sistema se debe realizar el pago de un rescate en Bitcoin. Generalmente en este tipo de mensajes se incluye una dirección de *email*, donde la víctima deberá contactarse para recibir las indicaciones del pago del rescate. Después de establecer el contacto vía mail la victima recibirá una respuesta que contendrá una dirección de BTC a la cual se deberá transferir el monto solicitado. Esta dirección de pago será el primer paso para comenzar el rastreo. Se asume que la víctima ha realizado el contacto con los delincuentes y ha hecho el pago del rescate en Bitcoin conforme a las instrucciones recibidas. Con relación a los pagos de rescate por ransomware se recomienda hacer siempre la denuncia del incidente y no pagar el rescate, porque pagar no garantiza que se puedan recuperar los datos.

[8] ARTICULO 183. - Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.
En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. (Párrafo incorporado por art. 10 de la Ley N° 26.388, B.O. 25/6/2008)

[9] ARTICULO 168. - Será reprimido con reclusión o prisión de cinco a diez años, el que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos.
Incurrirá en la misma pena el que por los mismos medios o con violencia, obligue a otro a suscribir o destruir documentos de obligación o de crédito.

En esta fase cada elemento secuestrado debe estar correctamente embalado, clasificado y debe constar en el acta de secuestro con el cual se da inicio a la cadena de custodia, para su posterior transporte.

Fase de Adquisición:

Una vez finalizada la fase de Recolección, la Fiscalía actuante solicitara al encargado y/o al especialista en adquisición que determine una fecha y hora de la pericia con notificación a las partes a las partes intervinientes. Antes de comenzar con la tarea de adquisición se deberá identificar todos los equipos o dispositivos electrónicos/informáticos que fueron recibidos por la oficina para lo cual se deberán realizar las siguientes acciones:

1. Tomar foto de cómo se reciben los elementos a peritar y enuméralos de alguna manera. Luego identificar marca, modelo y número de serie de cada uno de estos equipos si lo poseen.
2. Buscar dentro de cada uno de los equipos identificados en el paso anterior los medios de almacenamientos persistentes que posean como ser discos rígidos, discos SSD u otros.

Una vez identificado debidamente los dispositivos se realizará una imagen forense del o los medios de almacenamientos persistente de los equipos afectados por el ransomware que puede ser in situ en la fase de recolección o en un laboratorio forense luego de haber recolectado los equipos dañados o sus medios de almacenamientos afectados. Luego de finalizar la imagen forense se realizará la comprobación de hashes del dispositivo original y su copia forense. Se aclara que esta imagen forense en principio se usara como evidencia de prueba para la investigación judicial pero el presente trabajo se centra en el rastreo de direcciones de Bitcoin partiendo de la dirección de pago del rescate y por medio de ella lograr determinar quien o quienes están detrás de estos ciberdelitos.

Fase de preparación:

Esta fase involucra las actividades técnicas en las que se prepara el ambiente de trabajo del informático forense donde la selección de las herramientas y técnicas apropiadas es fundamental para la correcta realización de las tareas encomendadas.

Las actividades principales en esta fase son la determinación de las herramientas a utilizar para el rastreo y análisis de las direcciones de Bitcoin en donde toda la información a obtener será en principio en línea. Dentro de las herramientas se pueden seleccionar para estos casos las siguientes herramientas gratuitas descriptas en la Figura 13: Blockchain explorers, OXT, Wallet Explorer, Maltego, Bitcoinwhoswho, Bitnodes o también en caso de tener licencias para la versión Classic o XL de Maltego que son pagos o alguna de las herramientas también de pago de ChainAlysis o Ciphertrace. Como complementos se pueden utilizar herramientas adicionales como OSINT para búsquedas fuera de la Blockchain como puede ser en foros, Facebook, Twitter etc.

Por otro lado, también se realizará una preparación del Ambiente para el análisis y examen de las imágenes forense obtenidas en la fase anterior a los fines de buscar rastros de billeteras en los equipos de la víctima, rastros de transacciones y/o direcciones de Bitcoin que sirvan en la

investigación. Este proceso consiste en la preparación del equipo con el cual se va a realizar dicha tarea como así también la las siguientes actividades:

- Preparación de Extracción Lógica: que consiste en la selección del conjunto de técnicas y herramientas a ser utilizadas. Cuando hablamos de extracción lógica nos estamos refiriendo al empleo del sistema operativo del equipo como intermediario para el acceso a los datos (las herramientas de extracción se comunican con el sistema operativo del equipo y es éste quien aporta los datos existentes en el sistema).
- Preparación de Extracción Física: que consiste también en la selección del conjunto de técnicas y herramientas a ser utilizadas. La extracción física implica la búsqueda a bajo nivel, directamente sobre los datos presentes crudos en el disco, sin contar con el sistema operativo como intermediario

Fase de extracción y análisis:

Abarca la extracción de datos, análisis, búsqueda y descubrimiento de la evidencia digital. Comprende la extracción de la información de las copias forenses, selección de la potencial evidencia digital, y su análisis en relación al caso ya los puntos periciales o requerimientos de un particular.

Para comenzar esta fase tenemos como punto de partida una dirección de rescate que generalmente es una dirección de Bitcoin. Esta etapa que se realiza básicamente en línea hay que rastrear partiendo de la dirección de pago y siguiendo las transacciones y las direcciones hacia donde se van moviendo los Bitcoins para poder determinar quienes se encuentran detrás de las direcciones que pueden ser muchas, tratando de agruparlas por cartera o billetera. Como primer paso de nuestra investigación tendremos que trabajar consultando las fuentes de datos disponible, es decir la Blockchain. Para ello debemos utilizar un explorador de bloques como ser blockchain.info o blockexplorer.com. con el cual podemos realizar un seguimiento de todas las transacciones de Bitcoin, ver las marcas de tiempo de cada transacción, las direcciones que envían dinero, las direcciones que reciben dinero etc. Por lo tanto, cuando tengamos una dirección de pago de un rescate podemos ingresarla a la blockchain.info y ver qué información encontramos, al tratarse de una dirección de pago de rescate probablemente existirán muchas víctimas que transfieren dinero a esa dirección con importes más significativos que las transacciones normales este sería el caso cuando se utiliza una misma dirección de pago de rescate para diferentes víctimas, otras veces se generan direcciones únicas para cada víctima. También se pueden hacer búsquedas para identificar flujos de entradas en base a patrones de pago conocidos.

En estas investigaciones, un tipo de análisis que se destaca se basa en la utilización de heurísticas para vincular direcciones controladas por el mismo usuario[10], en donde diferentes direcciones utilizadas como entradas para una transacción se las considera como si estuvieran controladas por el mismo usuario, esta heurística explota una propiedad inherente del protocolo Bitcoin. Otra heurística se basa en el llamado cambio de direcciones o vuelto el cual en contraste con el primero, explota un modismo actual de uso en la red Bitcoin en lugar de una propiedad inherente. Estas heurísticas nos permiten agrupar potencialmente las direcciones de entrada

10 Se basa en técnicas introducidas en 2013 por la investigadora Sarah Meiklejohn. “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names” (Ver Bibliografía)

para una transacción como así también la dirección de cambio y el usuario de entrada. Cuando se poseen distintas direcciones de un mismo usuario, es más fácil identificar quién está detrás de las direcciones, muchas veces por descuidos del propio usuario o bien por identificaciones de organismos fiscales.

Los fondos transferidos a direcciones de pago de rescate tienden a permanecer corto tiempo en dichas direcciones, ya que los delincuentes van a mover esos fondos a otras direcciones tratando de blanquearlos y es muy posible que en esos movimientos (transacciones) pasen por un Exchange. Para estos casos donde el movimiento de fondos ilícitos pasa por un Exchange se puede solicitar mediante orden judicial información de las direcciones sospechosas y como medida preventiva el bloqueo de los fondos si todavía se encuentran en el exchange. Muchos Exchange como por ejemplo Binance ya tienen incorporado un formulario en su web para realizar este tipo de peticiones. Por otro lado, sin perjuicio de lo dicho anteriormente podemos utilizar wallet explorer para correlacionar las direcciones con billeteras de intercambios u otras entidades importantes de Bitcoin.

Una técnica de ofuscamiento que suelen utilizar los delincuentes para dificultar más el rastreo es el uso de mezcladores o mixers para lavar las criptomonedas producto del ilícito.

Luego de terminado el rastreo de todas las direcciones involucradas es importante realizar un mapeo grafico con las transacciones y direcciones investigadas lo que nos va a permite tener una visión más global y ver hacia donde ir con la investigación. En este mapeo se debe prestar especial interés en las direcciones de salidas o direcciones hacia donde se enviaron los fondos. Para esto se puede utilizar herramientas de ayuda que permitan tener una visualización grafica de las direcciones involucradas y sus transacciones como pueden ser maltego y oxt.me, también se puede realizar manualmente lo que conlleva mucho más trabajo que la utilización de las herramientas antes mencionadas.

En caso de que se haya obtenido alguna dirección IP relevante en una investigación forense de criptomonedas, podría ser de utilidad el uso de la aplicación web Bitnodes para determinar a partir de una dirección ip si es que está conectada a la red Bitcoin o bien consultar el registro histórico de la misma cruzando los datos con información proveniente de la blockchain.info. Para complementar con Bitnodes se pueden utilizar servicios como Shodan[11] debido a que en general estos nodos responden como agentes de usuarios que incluye la palabra Satoshi además de la versión del protocolo que están ejecutando y por lo tanto es posible realizar búsquedas por puertos por defecto de los clientes Bitcoin que como en el caso de Bitcoin Core son el 8332 y 8333.

Una de las formas de obtener información personal sobre el propietario de una dirección de Bitcoin es cuando el propietario de una dirección sospechosa interactúa con un Exchange, entonces por medio de una orden judicial se puede solicitar al Exchange los datos personales del usuario que envió Bitcoins a tal dirección, en tal fecha y desde tal dirección. Otra manera es buscar información de los propietarios de direcciones Bitcoin fuera de la Blockchain y esto consistiría en recabar información personal publicada online por ejemplo podemos usar Google dorks o maltego por ejemplo para buscar sitios web donde se publiquen las direcciones de Bitcoin

[11] https://www.shodan.io/

sospechosas tratando de encontrar información que relacione esa dirección con una entidad persona u organización, ya que muchos publican sus direcciones Bitcoin en sitios web utilizando sus nombres reales como nombres de dominio registrados, otros publican direcciones de Bitcoin en foros en línea, a través de sus cuentas de redes sociales.

Adicionalmente, pueden existir billeteras electrónicas o *wallets* instaladas localmente, desde las cuales se hayan realizado transacciones relacionadas con el delito investigado. En ese caso es importante poder acceder al registro de direcciones de la billetera y el historial de transacciones, en las cuales podría llegar a detectarse una dirección solicitada como destino para un pago extorsivo.

Fase de Presentación:

En esta etapa el perito prepara un informe con todas las actividades realizadas. Se debe tener en cuenta que dicho informe será leído por personas que no tienen conocimientos técnicos de las actividades desarrolladas en cada fase por lo cual se recomienda aclarar todos los conceptos técnicos que se utilizaron y así como también las fuentes de información con las que se contaron para la realización de la pericia informática. Se recomienda incluir los siguientes conceptos en el informe:

- Breve introducción del caso, partes intervinientes, número de causa y delito.
- Explicar que es una función hash y para qué sirve.
- Explicar que es la Blockchain.
- Explicar que es Bitcoin y su relación con la Blockchain.
- Explicar que son las direcciones de Bitcoin.
- Explicar que son los monederos o wallets de Bitcoin.
- Explicar el concepto de clave privada.
- Explicar el concepto de los exploradores de bloques
- Documentar por cada punto pericial cual fue la evidencia digital encontrada.
- Es aconsejable presentar una versión digital del informe además de su presentación escrita.
- Esquema o diagrama de la trazabilidad de los fondos de las direcciones asociadas al ransomware.
- Incluir un glosario de términos.

Cadena de Custodia:

La cadena de custodia es una secuencia o serie de recaudos destinados a asegurar el origen, identidad e integridad de la evidencia, evitando que ésta se pierda, destruya o altere. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria. La cadena de custodia comienza desde el momento de hallazgo o recepción de la evidencia y finaliza cuando la autoridad judicial competente decide sobre su destino. En la cadena de custodia participan todos los funcionarios y/o empleados que intervengan durante las diferentes etapas del proceso judicial sobre las evidencias. La Blockchain almacena y contiene una historia clara y transparente de todas las transacciones realizadas de Bitcoin las cuales no pueden ser modificadas. Estos

registros pueden ser analizados para descubrir actividades sospechosas y poder asociarlas con las transacciones sospechosas bajo investigación.

a) Herramientas – Fase de extracción y análisis:

Listado de herramientas para el rastreo de criptomonedas fase de extracción y análisis

Nº	Herramienta	Tarea	Licencia	Sistema Operativo	Link
1	Blockchain explorers	Rastreo de direcciones y transacciones	Gratuita	WEB	https://www.blockchain.com/es/explorer
2	OXT	Rastreo de direcciones y transacciones	Gratuita	WEB	https://oxt.me/
3	Wallet Explorer	Rastreo de direcciones y transacciones con identificación de monederos	Gratuita	WEB	https://www.walletexplorer.com/
4	Maltego	Recopilación de información en la web	Gratuita Comercial	windows-linux-mac	https://www.maltego.com/
5	Bitcoinwhoswho	Rastreo de direcciones y transacciones con informacion adicional	Gratuita	WEB	https://www.bitcoinwhoswho.com/
6	Bitnodes	Busqueda y localizacion de un nodo de la red bitcoin	Gratuita	WEB	https://bitnodes.io/

Fuente: Elaboración propia

Capítulo 6

Conclusiones:

Si bien se carece de experiencia en investigaciones de este tipo se concluye que es potencialmente factible la utilización del modelo teórico denominado PURI para este tipo de investigaciones conforme como se lo describió en el Capítulo 5 con el agregado de las herramientas gratuitas que sirven para el rastreo de Bitcoin las cuales fueron descriptas en el capítulo 4. Es de destacar la capacidad de adaptabilidad del modelo PURI y por ello es potencialmente viable su aplicación no solo a un tipo de ciberdelito donde las criptomonedas son utilizadas como un medio comisivo de un delito como es el caso del ransomware, si no que puede ampliarse a otros ciberdelitos de la misma índole donde las criptomonedas funcionan como un mecanismo de pago entre los cuales pueden ser venta de drogas, extorsión con contenido sexual, venta de armas y lavado de dinero.

Si bien queda trabajo por hacer con relación a la aplicación del modelo PURI a las criptomonedas y en cierta medida esto va a depender de la experiencia que se vaya adquiriendo con su aplicación sería interesante avanzar a futuro en dos líneas de investigación la primera de ellas seria poder realizar una investigación forense en todas las formas de utilización de cualquier criptomoneda considerando las particularidades de cada una de ellas y sus diferentes implementaciones. La segunda aplicar el modelo PURI a investigaciones con criptomonedas donde estás sean consideradas como objeto del delito, que son básicamente delitos contra la propiedad como por ejemplo ataque a un Exchange, robo de criptomonedas a un particular etc.

A continuación, a modo de resumen y aporte se destacan los aspectos más importantes que se deben considerar en una investigación forense aplicado PURI a un ciberdelito de ransomware con pedido de rescate en Bitcoin.

1) Utilizando la cadena de bloques como herramienta de investigación y propiedades de las transacciones para establecer vínculos

Como se expresó antes las direcciones de Bitcoin son pseudo-anonimas y cada dirección que interviene en una transacción es almacenada en la Blockchain simultáneamente en miles de computadoras y servidores de donde pueden ser accedidas y analizadas por todos. Este tipo de análisis y seguimiento de las direcciones o transacciones se puede hacer tranquilamente con las herramientas antes descriptas a fin de reconstruir las actividades de transacciones de Bitcoin que están sometidas a un proceso de investigación. A diferencia del efectivo, una transacción digital siempre deja un rastro, y una vez que se perfora el velo del secreto, los activos pueden buscarse, encontrarse y decomisarse. Como lo han reconocido sus desarrolladores centrales, la consecución de un anonimato razonable con Bitcoin puede ser bastante complicada y el anonimato perfecto puede ser imposible. En su artículo original, Satoshi recomendó el uso de una dirección totalmente nueva para cada transacción realizada para evitar que las mismas sean vinculadas a un propietario común. Aunque ello seguiría siendo la mejor práctica sugerida, no es suficiente para garantizar el total anonimato debido a otras características incorporadas en el código Bitcoin

2) Obtener información a través de los Exchanges

Hoy en día todos los exchanges están obligados a implementar los controles de 'Conoce a tu Cliente' (KYC). Con base en esta información los exchanges pueden convertirse en socios útiles en una investigación. La información que puede ser proporcionada por los exchanges es la siguiente:

- Información Personal: nombre, fecha de nacimiento, dirección, teléfono, dirección de correo electrónico, imagen del documento de identidad o pasaporte.
- Información del Usuario: historial del balance, ingreso (ubicación, tiempo y dirección IP)
- Información financiera: número de cuenta bancaria o de tarjetas de crédito usadas para financiar la cuenta para retirar fondos.

3) Buscar a los propietarios de las direcciones de Bitcoin fuera de la Blockchain

En una investigación forenses se deben aplicar soluciones creativas para vincular las direcciones de Bitcoin con sus propietarios del mundo real, ya que no existe un registro de direcciones. Sin embargo, a continuación, se describen algunas tácticas complementarias para rastrear las direcciones de Bitcoin hasta sus propietarios. Entre ellas se encuentran:

- Buscar información personal publicada online

La estrategia puede parecer sencilla, pero requiere mucho tiempo y esfuerzo para llevarla a cabo. Búsqueda de direcciones Bitcoin en sitios web, redes sociales, foros en línea de tal manera de poder correlacionar las direcciones con nombres o identidades reales.

- Herramientas de análisis de transacciones

Algunas empresas utilizan un sofisticado software para vincular las direcciones de Bitcoin a personas o sitios web. Sin embargo, suelen reservar esos servicios solo para sus clientes y no

son accesibles al público. La política que promulga el modelo PURI es el uso de herramienta de software libre.

- Rastreo basado en análisis de trafico

Debido al diseño del Bitcoin es posible mediante el análisis de tráfico TCP/IP descubrir la identidad de quien realiza un pago en Bitcoin. Dado que la primera persona en anunciar una transferencia será con alta probabilidad el pagador de la misma. Por lo tanto, si logramos descubrir quién fue el primero en publicar una transacción se podrá deducir con gran probabilidad quien es el pagador de la misma y por ende el propietario de las direcciones de entrada utilizadas. Obviamente que para evitar esto bastaría con utilizar algún sistema de anonimización de las comunicaciones, como la darknet.

- Rastreo de compras

Cuando se realizan compras por ejemplo por internet las tiendas o casas de ventas suelen solicitar cierta información personal como nombres y dirección de envió, obviamente esto es relevante siempre que se utilicen Bitcoin para comprar productos físicos. Es probable que esta información se almacene en una base de datos, facilitando así la vinculación de las diferentes direcciones de Bitcoin con sus propietarios.

4) Cooperación entre entidades

Es fundamental el trabajo de manera conjunta con otras fuerzas de seguridad dentro del ámbito nacional y cuando se desarrollan en otras jurisdicciones fuera de nuestro país es importante desarrollar relaciones de trabajo efectivas con organismos internacionales o de otros países para facilitar el intercambio oportuno de inteligencia.

A nivel nacional existen agencias gubernamentales que nos pueden ayudar a investigar operaciones con criptomonedas como ser

- Procuraduría de criminalidad económica y lavado de activos (procelac)
- Equipos especializados en el ámbito de las fuerzas de seguridad argentinas (Gendarmería Nacional – Policía Federal Argentina, etc.)
- Equipos especializados en embajadas o agencias de investigación extranjeras con sede en argentina

ANEXO I

Fundamentos Técnicos de la Blockchain:

1) Descripción básica

La cadena de bloques es una gran base de datos que puede ser compartida por una gran cantidad de usuarios en forma peer-to-peer y permite almacenar información de manera ordenada e inmutable. Para el caso del Bitcoin esa información añadida a la Blockchain es pública y puede ser consultada en cualquier momento por cualquier usuario de la red. Para poder añadir información a la cadena de bloques es necesario que exista un acuerdo entre la mayoría de las partes. Pasado un cierto tiempo se puede asumir que la información agregada a un bloque ya no puede ser modificada. La creación de nuevos bloques es realizada por nodos denominados mineros. Los nodos denominados mineros son aquellos que participan en el proceso de escritura de datos en la Blockchain a cambio de una recompensa económica. El proceso que permite alcanzar un consenso entre los mineros de la Blockchain para el orden de escritura de bloques es lo que se llama prueba de trabajo o Proof-of-work (PoW). Es decir, para que un bloque sea aceptado el minero tiene que ser el primero en completar una PoW para el siguiente bloque de la Blockchain. Las pruebas de trabajo, consiste básicamente en validar/calcular nuevos bloques de transacciones esta tarea requiere de un costo computacional muy elevado, de forma que, para poder hacerse con el control de la red (y por tanto de qué se valida y qué no), un atacante necesitaría una potencia de cómputo extremadamente difícil de conseguir. La PoW es un rompecabezas matemático de dificultad ajustable. En concreto la PoW consisten en encontrar un parámetro (nonce) que consiga que al hacer el hash sobre todo el bloque incluido el nonce se obtenga un valor inferior a la dificultad actual establecida por la red. Se trata de encontrar un nonce que consiga un valor hash del bloque con un determinado número de ceros al inicio. Para lo cual el minero debe recurrir a la fuerza, probando valores del parámetro nonce hasta obtener un bloque valido. Este proceso de probar valores o fuerza bruta es un proceso computacionalmente costoso de ahí su nombre de “prueba de trabajo”. La dificultad de este rompecabezas criptográfico es fácilmente ajustable: se puede incrementar la dificultad aumentando el número de ceros necesarios para completar la PoW o decrementarla reduciendo dicho número de ceros.

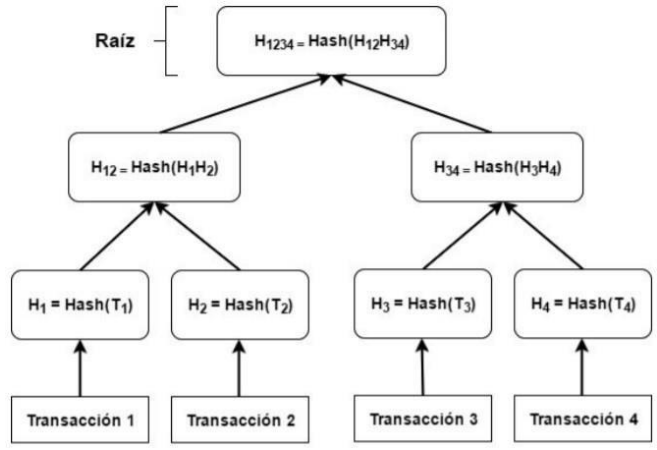
2) Estructura de los Bloques

La Blockchain almacena gran cantidad de datos y si consideramos que su tamaño es siempre creciente en el tiempo, ya que solo se van agregando datos. Debido a esto es deseable disponer de un mecanismo de consulta eficiente a la blockhain en otras palabras poder realizar consultas sin tener que descargar toda la información almacenada. Con este propósito, en la Blockchain de Bitcoin, se propone utilizar un árbol hash de Merkle[12] este tipo de estructura permite verificar de forma eficiente, y segura, el contenido de una gran cantidad de datos. En el árbol hash de Merkle (Figura 50) se puede almacenar diversas piezas de

[12] Un árbol hash de Merkle (Merkle Hash Tree) o árbol de Merkle o árbol hash es una estructura de datos en árbol, binario o no, que permite que gran número de datos separados puedan ser ligados a un único valor de hash, el hash del nodo raíz del árbol. De esta forma proporciona un método de verificación segura y eficiente de los contenidos de grandes estructuras de datos.

información independiente (en el caso del Bitcoin se trata de transacciones económicas) en las hojas de una estructura de árbol. Para armar el árbol se hace un hash de la información contenida en cada nodo hoja. A continuación, para generar los nodos de cada nivel superior del árbol se concatenan diversos valores hash de nivel inferior (seria 2 valores si el árbol es binario) y se le aplica la función hash a esta concatenación. Repitiendo este proceso hasta llegar a un nivel donde hay un solo nodo, denominado raíz del árbol. La ventaja de esta estructura es que permite consultar de forma autenticada y sin la necesidad de disponer de toda la información almacenada en el árbol. En particular, se puede consultar de forma autenticada cualquier contenido del árbol con una cantidad de valores hash proporcional al logaritmo del número de nodos del árbol. Por lo tanto, para validar un contenido únicamente hay que proporcionar los nodos adyacentes en cada nivel y el nodo raíz autenticado. Entonces para validar un contenido se calcula el valor raíz a partir de los nodos adyacentes proporcionados y se comprueba que coincida con el valor raíz autenticado. Este tipo de estructura es segura porque no se puede generar un conjunto de nodos adyacentes a voluntad que dé como resultado el valor del nodo raíz autenticado.

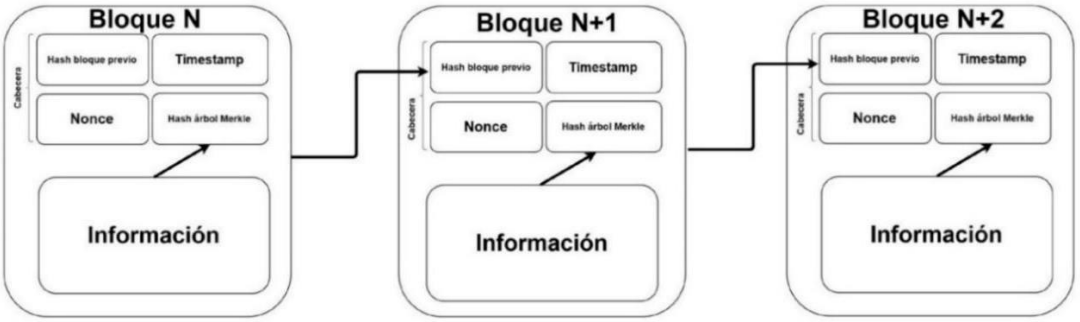
Figura 50: Árbol de Merkle



Fuente: Dolader, Bel y Muñoz (2017)

En la siguiente figura (Figura 51) se puede observar la estructura de los bloques de la Blockchain de Bitcoin y a continuación se describe la información que contiene cada bloque:

Figura 51: Cadena de bloques



Fuente: Dolader, Bel y Muñoz (2017)

- Hash del bloque anterior: este valor permite que los bloques queden entrelazados secuencialmente formando una cadena.
- Timestamp o marcade tiempo: la cual permite identificar el instante o tiempo en que se creó un bloque. Funciona como un elemento adicional de seguridad y transparencia
- Nonce: Este es el valor encontrado por fuerza bruta en el proceso de minado.
- El valor de la raíz del árbol de merkle de las transacciones (root hash): este valor hash permite referenciar toda la información del bloque, con el valor de la raíz del árbol y ciertos valores adicionales es posible realizar consultas a cerca de la información contenida en un bloque de manera eficiente y segura.
- Información del bloque: es la información contenida en los bloques para el caso del Bitcoin son las transacciones realizadas con la criptomoneda.

3) Propiedades fundamentales de la Blockchain

La creación de una Blockchain robusta debe garantizar 2 propiedades fundamentales[13]:

- Disponibilidad: asegura que una transacción honesta que ha sido emitida termine siendo añadida a la cadena de bloques, evitando que se produzca una denegación de servicio (Denial of Service, DoS) por parte de nodos corruptos.
- Persistencia: cuando un nodo da una transacción como estable, el resto de los nodos, si son honestos, validaran esta como estable haciéndola inmutable.

Para cumplir con la propiedad de disponibilidad, la Blockchain del Bitcoin implementa una red de nodos interconectados donde dichos nodos interactúan como iguales (red peer to peer). Esta red peer-to-peer de Bitcoin es descentralizada, lo que significa que cualquier usuario que desee puede contribuir. A diferencia de la Blockchain del Bitcoin otras utilizan un sistema de lista blanca (White list) donde solo pueden participar los nodos de la lista. En cualquier caso, los nodos que forman parte de la red peer-to-peer poseen cada uno de ellos una copia de la cadena de bloques. Esta gran cantidad de copias de la Blockchain proporciona gran disponibilidad y robustez. En la inserción de bloque en la red peer-to-peer de la Blockchain se distinguen diferentes estados para la información de bloque que está siendo procesada:

- Información candidata a ser añadida: es información que los nodos han enviado al resto de los nodos de la red peer-to-peer, pero que todavía no ha sido validada en ningún bloque.
- Información confirmada: es información validada por la red y se procede a añadirla al próximo bloque.
- Información estable: es información que forma parte de la Blockchain de manera inmutable.

4) Generación de bloques en la Blockchain

La generación de bloques en la Blockchain se realiza de manera descentralizada. La clave de esta descentralización es llegar a un acuerdo sobre qué información guardar en la Blockchain. Para poder lograr esto es necesario conseguir un consenso distribuido que

[13] The Bitcoin Backbone Protocol: Analysis and Applications – Juan A Garay, Aggelos Kiayias, Nikos Leonardos.

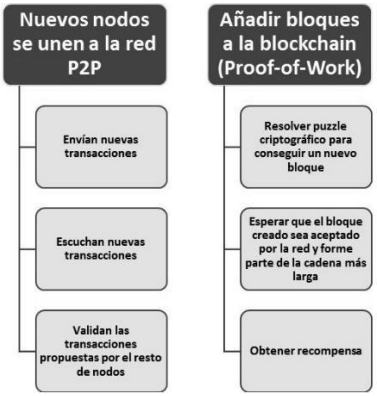
permita que los nodos honestos tengan la capacidad de generar la información valida conjuntamente y así evitar que nodos maliciosos puedan guardar información no deseada. Este mecanismo usado en Bitcoin permite resolver el problema del doble gasto (un usuario gastando dos veces el mismo dinero). En la siguiente figura (Figura 52) se muestra el proceso utilizado por Bitcoin para añadir bloques a la Blockchain.

En primer lugar, un usuario debe convertirse en un nodo dentro del sistema para poder escuchar y emitir nuevas transacciones. En segundo lugar, si el usuario desea convertirse en minero y crear nuevos bloques debe competir contra el resto de mineros de la red para resolver el rompecabezas criptográfico y así ser el que escriba el nuevo bloque en la Blockchain oficial.

El proceso de autenticación de las transacciones se basa en la criptografía asimétrica. Cada cuenta de usuario de Bitcoin posee dos llaves relacionadas matemáticamente una pública (identificador del usuario en la red que es conocida por todos) y una privada (es secreta y solo conocida por el usuario). La llave privada sirve para firmar las transacciones emitidas por el usuario, este especifica las cantidades de monedas a transferir y las llaves públicas de destino. La red y el resto de los usuarios usando la llave pública del emisor pueden obtener una prueba matemática de que la transacción fue efectivamente firmada por ese usuario y por nadie más, ya que nadie más tiene su llave privada.

Las nuevas transacciones generadas son validadas por los nodos más cercanos al emisor, descartando todas las transacciones invalidas y propagando al resto de los nodos las transacciones validas que son aquellas que cumplen con las especificaciones de la red. A continuación, se procede a añadir las nuevas transacciones a la cadena de bloques. Este proceso de confirmación de datos se lleva a cabo en Bitcoin mediante el proceso de minado PoW. Por ultimo los nodos comprueban que en el nuevo bloque creado todas las transacciones son válidas y que el bloque esta correctamente vinculado con su predecesor, es decir que contiene el hash del bloque anterior en su cabecera. En caso afirmativo el bloque es añadido a la Blockchain incrementando así la cadena. Este proceso se repite generando una nueva ronda de minado con las nuevas transacciones emitidas que aún no hayan sido agregadas en ningún bloque anterior de la Blockchain. Si el bloque es invalido es descartado y el resto de los nodos sigue el proceso de minado hasta encontrar un bloque valido.

Figura 52: Esquema del proceso de Bitcoin para añadir nuevos bloques



Fuente: Dolader, Bel y Muñoz (2017)

Glosario:

Base58Check: Las direcciones Bitcoin se codifican mediante una forma modificada de la codificación Base 58 a la que se conoce como Base58Check. La codificación Base58Check se utiliza para codificar secuencias de bytes utilizadas en Bitcoin (direcciones) convirtiéndolas en un formato de texto legible para el ser humano.

Binance: Binance es una plataforma de intercambio de criptomonedas (Exchange) y es considerada la plataforma de intercambio con el mayor volumen comercial del mundo.

Bitcoin: Es una moneda virtual o un medio de intercambio electrónico que sirve para adquirir productos y servicios como cualquier otra moneda. También hace referencia a la red y al software.

BTC: El acrónimo que representa la moneda Bitcoin.

Blockchain: Una cadena de bloques o Blockchain es un registro digital de transacciones. En el campo de las criptomonedas, es el historial de transacciones de cada unidad de criptodivisa que muestra cómo sus propietarios han ido cambiando a lo largo del tiempo. El Blockchain funciona registrando transacciones en bloques, añadiendo los nuevos en la parte delantera de la cadena.

Criptografía asimétrica: (en inglés asymmetric key cryptography), también llamada criptografía de clave pública (en inglés public key cryptography) o criptografía de dos claves (en inglés two-key cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Criptomonedas: Las criptomonedas son monedas virtuales. Pueden ser intercambiadas y operadas como cualquier otra divisa tradicional, pero están fuera del control de los gobiernos e instituciones financieras.

Darknet: La darknet, también conocida como red oscura, forma parte de la Deep web, que son páginas web y servicios a los que no se puede acceder a través de los motores de búsqueda tradicionales (Google, Bing, Yahoo). La darknet está formada por un conjunto de sitio ocultos a los que se accede a través de navegadores específicos, como puede ser Tor Browser.

DoS: un ataque de denegación de servicio, llamado también ataque DoS, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Exchange: Los exchanges de criptomonedas, también conocidos como plataformas o mercados de intercambio, son plataformas digitales que permiten intercambiar monedas digitales por dinero fiat y/u otras criptomonedas o mercancías.

Fiat: son las monedas emitidas por las autoridades monetarias de los países. Tienen valor como moneda porque es el propio estado el que impone y regula su uso tanto como medio de intercambio, como reserva de valor y como unidad de cuenta.

Hash: Es una función criptográfica que utiliza un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Dirección IP: La dirección IP es una etiqueta numérica, que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el Protocolo de Internet (Internet Protocol) que corresponde al nivel de red del modelo TCP/IP.

Monero: Monero es una criptomoneda de código abierto creada en abril de 2014. Esta criptomoneda cuenta con un alto nivel de privacidad y descentralización.

Nonce: es un número arbitrario que se puede usar una única vez en una comunicación criptográfica. En una red Blockchain basada en Proof of Work (Prueba de Trabajo) el nonce funciona en combinación con el hash como un elemento de control para evitar la manipulación de la información de los bloques.

OSINT: son las siglas de Open Source INTelligence, traducido al español es algo como inteligencia de código abierto o inteligencia de fuentes abiertas, básicamente se llama OSINT a una serie de procesos que tienen como misión hacer uso de fuentes de carácter público para poder buscar y recopilar toda la información pública posible sobre un objetivo en concreto (sea este una persona o no) con el fin de poder interpretar esa información y darle una utilidad.

Pishing: La palabra phishing quiere decir suplantación de identidad. Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esa persona.

Peer-to-peer: red entre pares o red entre iguales es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Una red peer-to-peer es la que propaga las transacciones y bloques a cada nodo Bitcoin de la red.

PURI: El Proceso Unificado de Recuperación de Información es el resultado de un proyecto de investigación de la facultad de ingeniería de la Universidad FASTA cuyo objeto consistió en establecer una guía de las tareas a desarrollar para la prestación de un servicio de informática forense en un ámbito judicial o particular.

Ransomware: Es un tipo de software malicioso que infecta los sistemas informáticos y restringe el acceso de un usuario a ese sistema o a los archivos contenidos en él a través del cifrado, exigiendo el pago de un rescate para poder acceder de nuevo a ellos.

Ripio: Ripio es una plataforma de intercambio y además una billetera virtual o wallet con la que se puede comprar y vender criptomonedas con moneda local, o también enviarlas y recibirlas hacia/desde otras wallets sin importar su procedencia.

Shodan: es un motor de búsquedas que tiene propósitos específicos. Shodan tiene como objetivo el ubicar a todo tipo de dispositivos que estén conectados a Internet, es decir, desde routers, APs, dispositivos IoT hasta cámaras de seguridad.

Staking: el proceso de staking consiste en adquirir criptomonedas y mantenerlas bloqueadas en una wallet con la finalidad de recibir ganancias o recompensas.

Trader: es todo aquel inversor o especulador que opera en los mercados financieros con la finalidad de obtener beneficios en el corto, medio o largo plazo.

VPN: significa "Virtual Private Network" (Red privada virtual) y son herramientas que permiten establecer una conexión protegida al utilizar las redes públicas. Las VPN cifran su tráfico en internet y disfrazan su identidad en línea.

Wallet: Las wallets o monederos de criptomonedas son el puente que nos permiten administrar nuestras criptomonedas. Puede ser una pieza de software o de hardware con los que realizar las operaciones de recepción y envío a través de la red Blockchain de cada criptomoneda.

White list: o lista blanca hace referencia a una lista de direcciones de criptomonedas que los usuarios definen como confiables.

XMR: Monero (o XMR por su identificador de mercado) es una criptomoneda de código abierto creada en abril de 2014. Esta criptomoneda cuenta con un alto nivel de privacidad y descentralización.

Bibliografía:

https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf Satoshi Nakamoto, (2008) Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer

https://drive.google.com/file/d/0Bx3RPktpv0NaNkpocWhwc29HSXM/view?resourcekey=0-WfAB5CA4eK7m1WZUhywgBg El rastro digital del delito – Aspectos técnicos, legales y estratégicos de la informática forense. Ana Haydée Di Iorio - Martín Alfredo Castellote - Bruno Constanzo - Hugo Curti - Julián Waimann - Sabrina Bibiana Lamperti - María Fernanda Giaccaglia - Pablo Adrián Cistoldi - Ariel Podestá - Juan Ignacio Iturriaga - Fernando Greco - Juan Ignacio Alberdi - Gonzalo M. Ruiz De Angeli - Santiago Trigo - Luciano Nuñez

https://info-lab.org.ar/images/pdf/PAIF.pdf Guía integral del uso de la informática forense en el proceso penal. Ana Haydée Di Iorio... [et al.]. - 1a ed. - Mar del Plata. Universidad FASTA, 2015.

https://discovery.ucl.ac.uk/id/eprint/1490261/1/Meiklejohn%20et%20al%20A%20fistful%20of%20bitcoins.pdf A fistful of bitcoins: characterizing payments among men with no names - S Meiklejohn, M Pomarole, G Jordan, K Levchenko, D McCoy, ...
Proceedings of the 2013 conference on Internet measurement conference

https://www.researchgate.net/publication/312829899_The_Bitcoin_Backbone_Protocol_Analysis_and_Applications The Bitcoin Backbone Protocol: Analysis and Applications

https://www.academia.edu/31139040/UNA_GU%C3%8DA_PARA_OPERADORES_Rastreo_de_Activos_Ilegales?email_work_card=thumbnail Una guía para operadores. Rastreo de activos ilegales.

https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf La Blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas Carlos Dolader Retamal, Joan Bel Roig y José Luís Muñoz Tapia Universidad Politécnica de Catalunya.

https://cseweb.ucsd.edu//~snoeren/papers/ransom-oakland18.pdf Tracking Ransomware End-to-end.

http://revistas.bibdigital.uccor.edu.ar/index.php/rbia/article/view/5164/3662
Constitución y marco legal de un Exchange en Argentina.

https://www.amlc.eu/wp-content/uploads/2019/04/The-Bitcoin-Trader-AMLC-September-2017.pdf The bitcoin trader

https://www.udesa.edu.ar/sites/default/files/cetys_criptomonedas.pdf LA LEY Publicación de noticias jurídicas Fecha de Publicación: 10/04/2019 AÑO LXXXIII Nº 68 - Edición especial: comentarios a la primera condena por apropiación de criptomonedas en argentina.

https://latamt.ieeer9.org/index.php/transactions/article/view/153/240 A Method for Blockchain Transactions Analysis

www.blockchain.com Pagina web de Blockchain que es un servicio de exploración de bloques de Bitcoin, así como un monedero de criptodivisas y un intercambio de criptodivisas que soporta Bitcoin, Bitcoin Cash y Ethereum.

www.blockcypher.com Brinda servicios web de Blockchain

www.btc.com sitio web de Blockchain y pool de minería.

www.blockchair.com Explorador de bloques, análisis y servicios web

www.bitinfocharts.com Estadísticas de criptomonedas

https://www.chainalysis.com web de la empresa chainalysis la cual proporciona datos, software, servicios e investigación a agencias gubernamentales, intercambios, instituciones financieras y compañías de seguros y ciberseguridad en más de 70 países.

https://ciphertrace.com web de la empresa CipherTrace que ofrece soluciones de cumplimiento de AML (Anti-Money Laundering) de criptomonedas para bancos, intercambios y otras instituciones financieras.

https://www.elliptic.co web de la empresa elliptic que realiza análisis, capacitación y certificación de Blockchain para empresas criptográficas, instituciones financieras y entes reguladores.

https://bfa.ar página web de Blockchain Federal Argentina

https://www.blockchain.com/es/ Sitio web de Blockchain en español

https://bitcoin.org/es/ Sitio Oficial de Bitcoin en español

https://bitcoinargentina.org/ Sitio de Bitcoin Argentina

https://www.youtube.com/watch?v=V9Kr2SujqHw¿Qué es el BLOCKCHAIN? Explicado por un INGENIERO INFORMÁTICO - (Bitcoin, NFTs y más)

https://www.youtube.com/watch?v=NspXln1Tg54 Análisis forense en Blockchain

https://www.welivesecurity.com/la-es/2022/04/29/que-son-cripto-mixer-servicio-anonimato-transacciones/ Mixers o Mescladores

https://www.criptonoticias.com/criptopedia/que-es-wallet-bitcoin-criptomonedas/#:~:text=Un%20monedero%20es%20una%20aplicaci%C3%B3n,se%20acople%20a%20sus%20necesidades. Página web sobre billeteras

https://medium.com/human-rights-foundation-espa%C3%B1ol/privacidad-y-criptomoneda-parte-i-qu%C3%A9-tan-privada-es-bitcoin-8bfe61c224d1 Privacidad y Criptomoneda, Parte I: ¿Qué tan privada es Bitcoin?

https://cointelegraph.com/news/chainalysis-launches-free-sanctions-screening-tools Chainalysis lanza herramientas gratuitas de detección de sanciones

https://www.criptonoticias.com/criptopedia/que-es-wallet-bitcoin-criptomonedas/Página web sobre billeteras

https://www.criptonoticias.com/tutoriales-guias/tutorial-aprende-a-usar-los-exploradores-de-blockchain/ Tutorial: aprende a usar los exploradores de blockchain

https://blockchain-media.org/es/bitcoin-explorer-all-what-u-need-to-know/ Bitcoin Explorer: Everything You Need to Know

https://es.cointelegraph.com/news/how-do-you-use-a-block-explorer ¿Cómo se usa un explorador de bloques?

https://www.crunchbase.com/organization/chainalysis/signals_and_news Recent News & Activity

https://graphsense.info/ plataforma de análisis de criptoactivos de código abierto

https://www.tecnicasdetrading.com/2020/08/almacenamiento-frio-criptomonedas.html Almacenamiento en Frío de Criptomonedas – Definición y Opciones

https://www.criptomonedas24.net/ripio/ Ripio: ¿Es Un Exchange Seguro? Análisis Y Opiniones 2022

https://www.iproup.com/economia-digital/30656-criptomonedas-ripio-lista-sus-tokens-en-kucoin

https://launchpad.ripio.com/blog/como-comprar-bitcoins-argentina pasos para crear cuenta en ripio

https://coinbureau.es/binance-analisis/ Reseña de Binance: Análisis en profundidad del Exchange

https://www.youtube.com/watch?v=chLm_rz8OMY BINANCE desde CERO: GUÍA COMPLETA: SPOT, LAUNCHPAD, EARN, STAKING - TUTORIAL en ESPAÑOL 2022

https://www.youtube.com/watch?v=TO4eWY8lk5E WALLETS para criptomonedas | Cómo usar MONEDEROS cripto desde cero | TUTORIAL en ESPAÑOL (1/4)

https://academy.binance.com/en/articles/what-is-kyc-know-your-customer ¿Qué es KYC (Conozca a su cliente)?

https://es.wikipedia.org/wiki/Conozca_a_su_cliente Conozca a su cliente.

https://www.maltego.com/blog/tracing-transactions-through-the-bitcoin-blockchain-with-maltego/ Tracing Transactions through the Bitcoin Blockchain with Maltego

https://www.maltego.com/transform-hub/blockchain-info/ Visualize the bitcoin blockchain Transforms in Maltego

https://www.youtube.com/watch?v=1iwsouV8ouQ&t=1066s Tracking Bitcoin Transactions on the Blockchain - SANS DFIR Summit 2017

https://www.bankinfosecurity.com/ransomware-where-does-bitcoin-money-go-a-10747 Ransomware Payments: Where Have All the Bitcoins Gone?