Universidad Cenfotec

Maestría en Ciberseguridad

Tema:

Diseño de un marco de referencia para el rastreo de clientes específicos de Bitcoin y otras criptomonedas en casos de delito

Elaborado por:

Charles Hill Gómez

Raúl Morales Víquez

Fecha: Agosto, 2018

Declaración de derechos de autor

Por este medio se declara que los contenidos desarrollados en esta tesis son de absoluta propiedad y responsabilidad de los señores Raul Morales Viquez y Charles Hill Gomez cuyo tema es el siguiente:

“Diseño de un marco de referencia para el rastreo de clientes específicos de Bitcoin y otras criptomonedas en casos de delito”

Derechos a los que renuncian a favor de la Universidad Cenfotec para que haga uso como a bien tenga, preferiblemente para fines académicos.

Dedicatoria y agradecimientos

Agradecemos a Dios por darnos la voluntad, la inspiración y la fuerza para llevar a cabo esta tesis.

A nuestros padres, nuestros hermanos, esposas y amigos que han sido gran parte de este caminar y que nos dieron su apoyo incondicional en todo momento.

A los profesores por su valiosa dedicación a la enseñanza, por sus consejos y por el apoyo mostrado en estos 3 años de maestría, donde siempre tuvieron la mejor disposición de ayudar y asesorar las preguntas pertinentes a este trabajo. Muy especialmente agradecemos al profesor Luis Naranjo por su dedicación, amabilidad y por sobre todo su gran conocimiento y aporte a la realización de este trabajo.

Finalmente agradecer a la Universidad para proveer las herramientas y las facilidades para realizar con éxito esta maestría.

Tabla de Contenido

Tabla de Figuras

Abstract

Esta investigación tiene como fin primordial establecer la creación de una metodología de mejores prácticas para que agencias policiacas, investigativas y gubernamentales puedan comprender el uso del Bitcoin (criptomoneda) y la forma correcta de rastrear estas transacciones, para así poder auditar e incluso reaccionar ante estas transacciones anómalas que algunas personas utilizan para cometer delitos. Actualmente existen conocimientos y técnicas para detectar el uso indebido de las criptomonedas, pero no existen manuales (hasta donde se pueda corroborar) que las agencias puedan utilizar paso a paso para verificar en caso de que se sospeche de un delito de esta naturaleza. La creación de un manual explicativo viene a llenar este vacío, de tal manera que estas agencias tengan una ventaja ante los cibercriminales, cada vez más especializados en temas de tecnología.

Capítulo 1. Introducción

1.1 Generalidades

Esta investigación tiene el propósito de proveer una herramienta adicional para los investigadores que requieran conocer la identidad del dueño o la persona que está accediendo a una billetera Bitcoin específica.

El producto de esta investigación es dependiente por completo de los investigadores, su nivel de compromiso con el mismo y su aplicación según sea requerido.

Sin embargo, es importante recalcar que esta no pretende ser una solución final para las investigaciones relacionadas, sino un marco de referencia ante una situación fraudulenta.

La información obtenida para cada caso requiere de un ataque individual y difiere en cada instancia.

1.2 Antecedentes del Problema

No existe, actualmente, un marco de referencia para la correcta detección de transacciones hechas en Bitcoin, el cual pueda ser utilizado por agencias de investigación ante posibles fraudes y extorsiones.

1.3 Definición y Descripción del Problema

En el mundo actual existen un gran número de nuevas formas de robo que van de la mano con los nuevos avances tecnológicos. Los criminales de hoy utilizan herramientas tecnológicas para recibir una remuneración por medio de actividades delictivas, en este caso, por medio del Bitcoin.

El Bitcoin tiene la característica de que, al ser anónimo, puede ser utilizado inescrupulosamente para cometer fraude, extorsión, secuestro o cualquier tipo de actividad ilegal.

Los organismos de investigación a nivel mundial se han dado la tarea de estar a la vanguardia cuando respecta a temas de investigación sobre los métodos utilizados por los delincuentes cibernéticos para llevar a cabo sus fechorías. Sin embargo, no existe una guía realmente para indicar cuáles son los pasos por seguir o los puntos a considerar cuando se presume existió un delito patrocinado por medio del Bitcoin. Todos los esfuerzos anteriores han llegado a generar diversas reacciones que estas agencias han tomado, algunas positivas y otras negativas, pero aun así es importante el llevar una guía que pueda ser de ayuda para esos grupos a la hora de reaccionar ante un delito cometido por medio del Bitcoin o sus extensiones.

1.4 Justificación

La razón principal para llevar a cabo esta investigación es encontrar cómo, por medio de una solución paso a paso, es posible documentar un marco de referencia que sea capaz de indicar a agencias de investigación las mejores prácticas para hacer el rastreo de transacciones fraudulentas hechas por medio del Bitcoin y, de paso, “des anonimizar las”, para dar con los responsables de los crímenes cometidos.

1.5 Viabilidad

La viabilidad de este proyecto se puede enfocar en tres facetas que permiten determinar si el proyecto es factible o no.

1.5.1 Punto de Vista Técnico. El manual que se tiene pensado crear es un marco de referencia según diversas fuentes académicas e investigativas, con el fin de proveer un instrumento de ayuda a agencias de investigación en momentos en que se ha cometido o se presume un delito por medio del Bitcoin. Por consiguiente, desde el punto de vista técnico, se profundiza sobre el Bitcoin, blockchain (base de datos que genera el Bitcoin) y el uso de este para generar transacciones

monetarias. Dentro del manual se incluirán unos algoritmos que son capaces de rastrear las direcciones IP de donde se generan las transacciones hechas por Bitcoin. Por ende, es necesario, dentro del marco de investigadores, tener recursos con conocimiento de desarrollo de software, así como licencias de los compiladores de código más utilizados en el mercado. Este manual incluirá código en lenguaje de programación Python, el cual es código abierto, por lo tanto, facilitará el aspecto de inversión en licencias.

1.5.2 Punto de Vista Operativo. La parte operacional de este manual recae en los investigadores, quienes lo desarrollarán dentro del marco práctico que se desea lograr. Una vez que sea distribuido dentro de los ámbitos de grupos o agencias de investigación, la ejecución y uso del manual deberá recaer en el personal de los departamentos de investigación cibernética, para ser capaces de aplicarlo y, además, delegarle las funciones a otros informáticos encargados de generar el código o aplicación según la fase de investigación que sea necesaria.

1.5.3 Punto de Vista Económico. Al ser un proyecto de investigación y creación de un manual, realmente no se requiere una inversión mayor a las horas-hombre destinadas para la investigación y creación del manual. En promedio de $100 la hora por esfuerzo de recurso, este proyecto se estima preliminarmente a tardar unas 12 horas semanales (esfuerzo parcial de trabajo), en 4 meses sumaría un total de 180 horas. Dos cabezas participantes resultarían en un costo preliminar de $36,000 (sin estimar otros gastos e imprevistos).

1.6 Objetivos

Se ha usado la taxonomía original de Bloom de 1956, para mostrar niveles jerárquicos en la producción del conocimiento y usar como punto de partida un estándar de amplia aceptación en la academia.

1.6.1 Objetivo General

Diseñar un marco de referencia para el rastreo de clientes específicos de Bitcoin y otras criptomonedas, por medio de agrupación de escenarios, para que las autoridades puedan determinar casos de delito.

1.6.2 Objetivos Específicos.

- Enumerar las diferentes definiciones y las implicaciones de la criptomoneda dentro de los ámbitos criminales actuales.
- Comprender los métodos de rastreo que se pueden aplicar para detectar actos delictivos con el uso de la criptomoneda.
- Organizar las mejores prácticas de detección de manera que puedan ser aplicadas siguiendo un orden, en la forma de una metodología que pueda ser estandarizada.
- Analizar las inquietudes manifestadas por un grupo de interés de referencia, a saber, el Organismo de Investigación Judicial de Costa Rica.

1.7 Alcances y Limitaciones

1.7.1 Alcances

Se realizará un manual de procedimientos bajo los estándares de investigación criminal, que documente el “modus operandi” conocido y los métodos existentes para contrarrestarlo, asimismo, permita determinar necesidades de las herramientas a desarrollar para su rastreo.

El fin primordial del manual es poder ser utilizado por las agencias policiales, investigativas o cualquier otro cuerpo de investigación criminal, que requiera una mejor forma para llevar a cabo una investigación relacionada al uso del Bitcoin.

1.7.2 Limitaciones

- Al no haber desarrolladores dedicados en el grupo, se procederá a hacer el manual de guía para el rastreo apropiado de transacciones por criptomoneda (y por ende el usuario originario).
- El manual será en metodología general para que pueda ser aplicado tanto para otras criptomonedas como para otros cambios de la metodología en el futuro.
- Al ser un manual general , existen limitaciones cuando se trata de legislaciones a nivel local, donde quizás algunas acciones tengan legalidad y, en otras, exista hasta inconstitucionalidad para llevarlas a cabo.

1.8 Marco de Referencia Organizacional y Socioeconómico

1.8.1 Historia

La organización, como tal, viene a ser la asociación entre los dos co-creadores de esta investigación (Raúl Morales y Charles Hill) y subsecuente manual procedimental que, en conjunto, propone una solución de corte consultivo y que tiene como fin ser promovido hacia entidades de tipo investigativo criminal (específicamente en el área de ciber crimen o delitos informáticos).

1.8.2 Tipo de Negocio y Mercado Meta

El negocio propiamente es la investigación criminal (con respecto a las criptomonedas). El mercado meta “per se” son las agencias de lucha contra el crimen (más concreto, las divisiones de delitos informáticos).

1.8.3 Misión, Visión y Valores

1.8.3.1 Misión

Desarrollar un manual de procedimientos para el rastreo e identificación de los posibles dueños de billeteras de criptomonedas envueltos o involucrados en actividades criminales.

1.8.3.2 Visión

Contrarrestar una herramienta que ha sido utilizada por delincuentes aprovechándose de su ofuscación ante personal no técnico.

1.8.3.3 Valores

Promover el sentido de colaboración, haciendo de esta investigación una oportunidad para el involucramiento de diversas organizaciones y agentes externos, al aportar en conjunto para crear una solución que satisfaga la necesidad creciente de respuesta inmediata y eficaz ante delitos cometidos contra otras personas u organizaciones por medio del uso inadecuado de la criptomoneda.

Evitar que las criptomonedas sean una excusa para la impunidad de personas u organizaciones que pretendan utilizarlas con fines criminales.

1.8.4 Políticas Institucionales

Realmente no hay un compendio, dado que este trabajo es una investigación académica, por ende, no hay políticas ni una estructura como tal. En la medida que este proyecto trascienda y genere algún tipo de esfuerzo, se podrían considerar como parte de la estructura de una futura organización.

1.9 Estado de la Cuestión

Las investigaciones analizadas se basan desde una perspectiva, en la cual se profundiza la definición y aplicación del Bitcoin. Originado desde un código fuente de prueba de concepto y un libro blanco que lo acompaña, el protocolo Bitcoin nunca se documenta completamente.

Según ” Birkuyov , Khovratovich y Pustogarov (2014) se definen los siguientes conceptos en conjunto con un ataque propagado por una red TOR:

1.9.1 Blockchain

Bitcoin opera en una lista de bloques, el Blockchain. Cada bloque contiene un encabezado y datos de transacción. El header de 80-byte contiene el hash de 256 bits del bloque anterior Hi-1, la marca de tiempo (en segundos) Ti, el nonce de

32 bits Ni (usado para generar bloques), el hash T Xi de la transacción de datos, y el parámetro de dificultad di. Para ser válido, el double-hash del encabezado del bloque debe ser más pequeño (como un entero) que un cierto valor, que es una función lineal del parámetro de dificultad:

Hi = SHA-256(SHA-256(Hi−1||Ti||T Xi||di||Ni||))) < f(di)

Actualmente debe ser más pequeño que 2192, es decir, tiene sus 64 bits más significativos igual a cero. Los mineros de Bitcoin primero recolectan todas las transacciones aún no incluidas en un bloque. Luego generan los campos de encabezado y prueban exhaustivamente nonces diferentes, marcas de tiempo y otros parámetros para obtener un bloque válido. Ellos son recompensados por 25 BTC siendo esta es la primera transacción en la listada. Cada vez que se crea un bloque, un minero lo transmite a la red, de modo que cada nodo lo conecte a lo interno del Blockchain.

Los compradores y beneficiarios del sistema se identifican en blockchain por sus direcciones de Bitcoin, o seudónimos. Un seudónimo es la codificación base58 del hash de la correspondiente llave pública. Cuando un comprador quiere transferir sus monedas a otro usuario, genera una transacción y la firma con su llave privada. Las transacciones firmadas se agregan al Blockchain por los mineros. Al verificar la firma, otros participantes de Bitcoin pueden verificar el nuevo propietario de las monedas. Birkuyov , Khovratovich y Pustogarov (2014) pp.p32-p38

1.9.2 Red Bitcoin P2P

Los pares de la red Bitcoin se conectan entre sí a través de un canal TCP no encriptado. No hay funcionalidad de autenticación en la red, por lo que cada nodo solo mantiene una lista de direcciones IP asociadas con sus conexiones.

Todas estas condiciones se aplican estrictamente y un bloque no concerniente se descarta.

Para evitar ataques de denegación de servicio, el protocolo Bitcoin minimiza la cantidad de información enviada por los compañeros. Los bloques válidos y las transacciones se transmiten, mientras que los que no son válidos, se terminan descartando los bloques. Por otra parte, Bitcoin implementa una reputación basada en su protocolo con cada nodo manteniendo un puntaje de penalización para cada conexión. Cuando se envía un mensaje mal formado al nodo, este último aumenta el puntaje de penalización de la conexión y prohíbe que la dirección IP falle durante 24 horas cuando la pena alcanza el valor de 100.

Por defecto, los compañeros de Bitcoin (tanto clientes como servidores) intentan mantener 8 conexiones salientes. Además, los servidores Bitcoin pueden aceptar hasta 117 conexiones entrantes (tener hasta 125 conexiones en total). Si alguno de las 8 salientes termina cayéndose, un par Bitcoin intenta reemplazarlos con nuevas conexiones. Si ninguna de las 8 conexiones salientes se desliga, el par permanecerá conectado a ellos hasta que sea reiniciado. En el caso de un cliente, llamamos a los 8 nodos a los que se establece nodos de entrada de conexiones. En Bitcoin el servidor acepta cualquier cantidad de conexiones desde una única Dirección IP siempre que el umbral para el número total de conexiones no se alcance. Birkuyov , Khovratovich y Pustogarov (2014) pp.p32-p38

1.9.3 Propagación del ataque

El protocolo de Bitcoin implementa una propagación de direcciones, mecanismo para ayudar a los compañeros a descubrir otros compañeros en la red P2P. Cada par de Bitcoin mantiene una lista de direcciones de otros pares en la red y cada dirección recibe una marca de tiempo que determina su frescura (tiempo de

creación). Los compañeros pueden solicitar direcciones de esta lista, una de la otra, usando mensajes GETADDR y publicitar de forma no solicitada direcciones conocidas por ellos utilizando mensajes ADDR. Cuando un nodo de Bitcoin recibe un mensaje ADDR, decide individualmente para cada dirección en el mensaje si reenviarlo a sus vecinos. Primero verifica si el número total de direcciones en el ADDR correspondiente en el mensaje no excede 10, y si la marca de tiempo adjunta no es mayor a 10 minutos. Si cualquiera de estos dos controles falla, la dirección no se reenvía; de lo contrario, la dirección es programada para reenviarse a dos de los vecinos del nodo en caso de que la dirección sea alcanzable y solo a un vecino, si no es alcanzable. Una dirección se considera alcanzable por un nodo si el nodo tiene una interfaz de red asociada con la misma familia de direcciones. De lo contrario, la dirección está marcada como inalcanzable. De acuerdo con la implementación de referencia actual, los nodos de Bitcoin reconocen tres tipos de direcciones: Direcciones IPv4, IPv6 y OnionCat. Limitando el número de los vecinos a los que se les envía una dirección, se reduce la cantidad total de tráfico en la red Bitcoin P2P.

Para elegir vecinos a los que reenviar una dirección, un nodo de Bitcoin hace los siguientes artículos: dirección a ser enviada, una semilla secreta, día actual, y la dirección de la memoria de la estructura de datos que describe el vecino. La expresión exacta para el valor hash es de poca importancia para el ataque. El hash mientras tanto permanece activo por 2 horas. El par luego ordena la lista de sus vecinos basado en los hashes calculados y elige la primera entrada o dos primeras entradas (que dependen de la accesibilidad de la dirección).

La transmisión real de los mensajes ADDR programados no ocurre de inmediato. Cada 100 milisegundos, un vecino se selecciona al azar de la lista de

todos los pares vecinos y la cola para los mensajes salientes de ADDR es enrojecida solo para este nodo. Se llama al nodo elegido a partir de un nodo de goteo redondo de 100 milisegundos y al procedimiento en su conjunto se le conoce como goteo.

Finalmente, para cada conexión, un par de Bitcoin recuerda las direcciones que fueron enviados a través de esta conexión. Antes de que un par reenvíe una dirección, primero verifica si la misma dirección ya fue enviada a través de la conexión. Este historial es limpiado cada 24 horas. Una nota importante es que el historial de las direcciones enviadas se mantiene por conexión y no por IP, es decir, si un par Bitcoin se vuelve a conectar, su historial se borrará. El número total de direcciones que un par de Bitcoin puede almacenar es limitado por 20480. Siempre que nuevas direcciones lleguen a un par, reemplazan a los viejos. Además, cuando un par recibe un mensaje GETADDR devuelve el 23% del número de direcciones que se almacena, pero no más de 2500 direcciones. Birkuyov , Khovratovich y Pustogarov (2014) pp.p32-p38

1.9.3 Descubrimiento del nodo vecino

Después de la puesta en marcha, un par Bitcoin descubre sus propias direcciones IP, que incluyen no solo sus direcciones de interfaces de red, sino también la dirección IP tal como se ve desde Internet (en la mayoría de los casos para usuarios de NAT se resuelve en una IPdirección del ISP del par). Para descubrir esto último, el par emite una solicitud GET a dos sitios web codificados los cuales responden con la dirección. Por cada dirección obtenida según el procedimiento de descubrimiento, el compañero asigna un puntaje. Las interfaces locales obtienen inicialmente la puntuación 1, la dirección IP externa un puntaje de 4 (en caso de que la dirección IP externa coincida con una local, aborda los puntajes

sumados). Cuando un cliente establece una conexión de salida a un par remoto, primero intercambia mensajes de VERSIÓN y el cliente anuncia su dirección con el puntaje más alto. El par remoto utiliza el algoritmo de propagación de direcciones descrito anteriormente. Los clientes repiten el mismo procedimiento para las restantes 7 salientes conexiones. Birkuyov , Khovratovich y Pustogarov (2014) pp.p32-p38

1.9.4 Propagación de la transacción

Reenviar una transacción de un compañero a otro involucra varios pasos. Primero, el emisor transmite un mensaje INVENTARIO con el hash de las transacciones. Segundo, el receptor ejecuta varios controles en la transacción y si él pasa chequeos, solicita la transacción real enviando un Mensaje GETDATA. El remitente luego transmite la transacción en un mensaje de TRANSACCIÓN. Cuando el receptor recibe la transacción, lo anuncia a sus compañeros en un mensaje de INVENTARIO.

Cuando un cliente genera una transacción, la programa para reenvío a todos sus vecinos. Luego calcula un hash de un valor compuesto por el hash de transacción y una semilla secreta. Si el hash calculado tiene dos últimos bits configurados en cero, la transacción se reenvía inmediatamente a los 8 nodos de entrada. De lo contrario, una cola de un vecino para las transacciones salientes se enjuaga cuando el vecino se convierte en el nodo de goteo (lo mismo que con los mensajes ADDR). Obviamente 1 de todas las transacciones se envían inmediatamente en promedio.

Al recibir una transacción, está programada para la entrega a todos los vecinos de los compañeros como se describió anteriormente. Al igual que con mensajes ADDR, un par de Bitcoin mantiene el historial de transacciones

reenviadas para cada conexión. Si una transacción ya estaba enviada a través de una conexión, no se volverá a enviar. El par de Bitcoin mantiene todas las transacciones recibidas en un grupo de memoria. Si el par recibió una transacción con el mismo hash que uno en el pool o en un bloque en la cadena de bloque principal, el recibido de la transacción es rechazado.

Las investigaciones, como la de Sameeh T.(2017), indican que los avances tecnológicos han hecho la vida mucho más fácil de lo que era hace 30 años. Ya no es necesario ir a un banco para depositar, retirar o transferir dinero de una cuenta a la otra. El advenimiento de la moneda virtual ha transformado por completo la industria bancaria. Hoy, se puede usar un teléfono celular o una computadora para realizar todas las formas de transacciones financieras. Aún mejor, la aparición de Bitcoin ha proporcionado un método de pago cifrado y altamente seguro que elude el modelo de banca centralizada. El problema se agrava aún más por el pseudo anonimato de las criptomonedas. Estos problemas hacen que sea bastante difícil hacer cumplir las leyes bancarias en casos de uso de criptomonedas. Todas estas características del Bitcoin y de la criptomoneda, en general, representan una atmósfera perfecta para el lavado de dinero, simplemente porque hace que sea muy difícil, o incluso imposible, que las agencias de la ley demuestren quién realizó una transacción concreta y de dónde provienen originalmente los fondos.

El uso de Bitcoin literalmente ha superado el volumen de transacciones diarias de Western Union y PayPal en términos de valores monetarios en los últimos años. El diseño innato de Bitcoin respalda fuertemente el anonimato, lo que atrae el lavado de dinero criminal. Los métodos tradicionales para comprar Bitcoins, a través de intercambios autorizados o negocios de servicios monetarios (MSB), no eliminan el anonimato de Bitcoin, aunque los MSB deben obtener e informar KYC, o

"conocer a su cliente" por sus siglas en inglés, que es la información de las transacciones de Bitcoins. Sin embargo, los métodos más nuevos para comprar Bitcoins pueden respaldar totalmente el anonimato y facilitar el lavado de dinero; por lo tanto, presenta todo un desafío para las agencias de aplicación de la ley. Dichos métodos incluyen transacciones de punto a punto (P2P), servicios de intercambio de propiedades para Bitcoin y cajeros automáticos de Bitcoin no registrados.

Sin embargo, este diseño (Bitcoin) trae consigo diversos riesgos, como indica Shaw T. (2015), la EBA (Autoridad Bancaria Europea, por sus siglas en inglés) resumió los riesgos de privacidad y protección de datos de los capitalistas de riesgo en su opinión de julio de 2014. Los 70 riesgos identificados en esta opinión fueron categorizados como riesgos para los usuarios, otros participantes del mercado, integridad financiera, sistemas de pago y reguladores. Los riesgos de privacidad y protección de datos identificados fueron la pérdida para los usuarios de las unidades de capital de riesgo cuando se les roba su "billetera electrónica" (que contiene su Bitcoin u otra moneda); está pirateado; si el hardware o software de la billetera electrónica funciona mal; si el intercambio de Bitcoin mismo es pirateado; si las identidades de los usuarios son robadas de las credenciales de ID proporcionadas durante el proceso de autenticación; los usuarios pierden la contraseña o las claves de su billetera electrónica, o el proveedor de billetera electrónica pierde la billetera de un individuo.

En una alerta de inversionistas de mayo de 2014, la SEC había advertido que existían problemas de seguridad con los intercambios de capital de riesgo, como cuando los intercambios interrumpen sus operaciones, de forma temporal o permanente, debido a "fraude, fallas técnicas, piratas informáticos o malware". Los Bitcoins también pueden ser robados por piratas informáticos".

En marzo de 2015, el informe Monedas digitales del Tesoro del Reino Unido arrojó: la respuesta a la convocatoria de información incluyó problemas de seguridad del usuario que surgen al transferir, obtener o mantener unidades de capital de riesgo. Más allá de la piratería, el fraude y la insolvencia, "los usuarios olvidaron o extraviaron sus credenciales de pago o los hackers pusieron en peligro su dispositivo y obtuvieron acceso a sus fondos de moneda digital" (Shaw T., 2015, párr. 3). El informe sugirió que se requerían estándares técnicos para el almacenamiento de Bitcoin y la ciberseguridad.

A pesar de que estos problemas son latentes y preocupan a muchos usuarios, Weinstein J. (2015) ayuda a explicar que, para los empresarios, ingenieros, capitalistas de riesgo y, ahora, los banqueros que están invirtiendo su tiempo, energía y dinero en negocios relacionados con Bitcoin, es la tecnología subyacente a la divisa la verdadera atracción: el blockchain.

Al mirar de cerca la tecnología de blockchain, se muestra más confiable para los policías que para los ladrones. Con empresas como Goldman Sachs, la Bolsa de Valores de Nueva York e IBM que ahora exploran el potencial de la blockchain para mejorar todo desde liquidación internacional de valores hasta el emergente Internet de las Cosas, es hora de que las fuerzas del orden reconozcan cómo también puede ayudarlos a atrapar a los malhechores.

La tecnología de blockchain utiliza la criptografía para verificar y confirmar todas las transacciones de Bitcoins y luego registra esas transacciones en un libro público de búsqueda. Esa tecnología tiene muchas otras aplicaciones más allá de la moneda y, entre otras cosas, podría revolucionar la forma en que las personas, las empresas y las instituciones financieras mueven dinero u otros activos. De hecho, hay un reconocimiento creciente, desde Silicon Valley a Wall Street, de que

Bitcoin es solo la primera "aplicación" que utiliza la tecnología subyacente de la Blockchain y que hay infinitas posibilidades para ella, lo que podría transformar la forma en que se hacen negocios, tal como fue la Internet hace más de 20 años.

Para que se materialice el potencial económico de esta tecnología, Bitcoin no puede convertirse, ni puede ser percibida como, la "moneda de los delincuentes". Por esa razón, es de importancia crítica que las fuerzas de seguridad puedan perseguir a los que usarían Bitcoin para facilitar crímenes.

Para ser claros, Bitcoin ciertamente plantea desafíos para la aplicación de la ley, el principal de ellos es la dificultad de identificar a un criminal que intenta permanecer en el anonimato. Este problema de atribución de "poner los dedos en el teclado" no es exclusivo de Bitcoin. Por el contrario, es endémico para las investigaciones de todos los delitos facilitados a través de Internet. Todos los días, los agentes y los fiscales tienen que encontrar formas de vincular una determinada dirección IP, nombre de chat o dirección de correo electrónico a un ser humano en particular. Ese proceso se hace más difícil cuando el sospechoso usa múltiples direcciones IP o proxies u otras tecnologías anónimas. Sin embargo, los agentes y fiscales trabajan incansablemente para superar esos desafíos con gran éxito. Bitcoin presenta simplemente otra variación de ese problema.

Contrario a la creencia popular, la tecnología que hace que Bitcoin funcione también tiene beneficios significativos para la aplicación de la ley.

En primer lugar, tener un registro público y rastreable de cada transacción de Bitcoin jamás realizada permite a las fuerzas del orden "seguir el dinero" de una manera que nunca sería posible con dinero en efectivo. Eso es cierto a pesar del anonimato percibido de Bitcoin; informes de anonimato de Bitcoin son muy exagerados. La dirección Bitcoin de un usuario es solo un número de cuenta que

permanece con el usuario. Si es posible conectar esa dirección a un usuario en particular, puede identificar y rastrear todas las transacciones en las que esa persona participó utilizando esa dirección. Además, las herramientas y técnicas para hacer esas conexiones están mejorando todo el tiempo.

Además, debido a que este libro mayor de las transacciones de Bitcoin es permanente, las fuerzas del orden público no tienen que preocuparse de que los datos no estarán disponibles meses o incluso años más adelante. Dado que el libro de contabilidad es de acceso público, las autoridades no tienen que preocuparse por qué tipo de proceso legal se requiere para acceder a los datos. Debido a que el libro de contabilidad no tiene fronteras, la policía puede obtener los datos sin tener que pasar por un gobierno extranjero.

Viéndose bien la situación actual, existen muchas áreas de oportunidad que este trabajo pretende atacar y realzar para beneficiar los distintos organismos de investigación que son parte del alcance del manual propuesto.

Capítulo 2. Marco Teórico o Conceptual

2.1 Bitcoin

Según la fuente oficial de Bitcoin, https://bitcoin.org/en/faq (2010), la definición oficial es la siguiente: “Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios.” (Bitcoin.org, 2010, párr. 1).

Bitcoin es la primera implementación de un concepto conocido como "moneda criptográfica", la cual fue descrita por primera vez en 1998 por Wei Dai en la lista de correo electrónico "cypherpunks", donde propuso la idea de un nuevo tipo

de dinero que utilizara la criptografía para controlar su creación y las transacciones, en lugar de que lo hiciera una autoridad centralizada. La primera especificación del protocolo Bitcoin y la prueba del concepto la publicó Satoshi Nakamoto en el 2009 en una lista de correo electrónico. Satoshi abandonó el proyecto a finales de 2010 sin revelar mucho sobre su persona. Desde entonces, la comunidad ha crecido de forma exponencial y cuenta con numerosos desarrolladores que trabajan en el protocolo Bitcoin (Bitcoin.org, 2010, párr. 3).

Bitcoin es controlado por todos los usuarios de Bitcoin del mundo. Aunque los programadores mejoran el software, no pueden forzar un cambio en el protocolo de Bitcoin, porque todos los demás usuarios son libres de elegir el software y la versión que quieran. Para que sigan siendo compatibles entre sí, todos los usuarios necesitan utilizar software que cumpla con las mismas reglas. Bitcoin solo puede funcionar correctamente si hay consenso entre todos los usuarios. Por lo tanto, todos los usuarios y programadores tienen un gran aliciente en proteger dicho consenso. (Bitcoin.org, 2010, párr. 5)

La red Bitcoin comparte una contabilidad pública llamada "blockchain". Esta contabilidad contiene cada transacción procesada, la cual permite verificar la validez de cada transacción. La autenticidad de cada transacción está protegida por firmas digitales correspondientes a las direcciones de envío, que a todos los usuarios tener control total al enviar Bitcoins desde sus direcciones Bitcoin. Además, cualquiera puede procesar una transacción usando el poder computacional de hardware especializado y conseguir una recompensa en Bitcoins por este servicio. Esto es comúnmente llamado "mining" o minería. (Bitcoing.org, 2010, párr. 8)

Algunas de las razones más comunes para adquirir Bitcoins son las siguientes:

- Pagar por bienes o servicios
- Comprar Bitcoins en una casa de cambio de Bitcoin
- Intercambio de Bitcoins con alguien en la zona
- Conseguir Bitcoins a través de la competitiva minería.

Si bien es posible encontrar individuos que desean vender Bitcoins a cambio de un pago por PayPal o tarjeta de crédito, la mayoría de las casas de cambio no permiten utilizar estos métodos de pago. Esto se debe a casos en los que alguien compra Bitcoins con PayPal y luego revierte la mitad de la transacción. Esto es comúnmente referido como reembolso.

2.1.1 Ventajas

- Libertad de pagos: con Bitcoin, es posible enviar y recibir cualquier cantidad de dinero instantáneamente desde y hacia cualquier lugar del mundo, en cualquier momento. Sin bancos con horarios. Sin fronteras. Sin límites impuestos. Los usuarios de Bitcoin siempre tienen un completo control sobre su dinero.
- Tasas muy bajas: los pagos con Bitcoin son actualmente procesados con tasas bajas o sin tasa alguna. Los usuarios pueden incluir una tasa en sus transacciones para recibir prioridad en el procesamiento de estas, lo que resulta en una confirmación más rápida de las transacciones por parte de la red. Además, los procesadores mercantiles están para asesorar en los procesos de transacción a los comerciantes, convirtiendo Bitcoins a la moneda fiduciaria y depositando fondos directamente en la cuenta bancaria del comerciante diariamente. Como estos servicios están basados en Bitcoin, son ofrecidos con cargos mucho más bajos que los que ofrecen PayPal o las redes de tarjetas de crédito.

- Menores riesgos para los comerciantes: las transacciones con Bitcoin son seguras, irreversibles, y no contienen datos personales y privados de los clientes. Esto protege a comerciantes contra pérdidas ocasionadas por el fraude o devolución fraudulenta, y no es necesario el cumplimiento de las normas PCI (Estándar de Seguridad de Pago para la Industria de Tarjeta de Pago, por sus siglas en inglés). Asimismo, los comerciantes pueden operar en nuevos mercados en los que las tarjetas de crédito no están disponibles o los niveles de fraude sean demasiado elevados. Esto conlleva a mejores comisiones, mercados más extensos y menos costes administrativos.
- Seguridad y control: los usuarios de Bitcoin tienen completo control sobre sus transacciones; es imposible que los comerciantes fuercen cargos no deseados o detectados, como puede suceder con otros métodos de pago. Los pagos de Bitcoin pueden realizarse sin que estén asociados a información de carácter personal. Esto ofrece un alto nivel de protección contra el robo de identidad. Los usuarios de Bitcoin también pueden proteger su dinero con copias de seguridad y encriptación.
- Neutral y transparente: toda la información sobre el suministro de Bitcoin está disponible en el Blockchain para cualquiera que quiera verificarlo y usarlo. Ningún individuo u organización puede controlar o manipular el protocolo Bitcoin porque es criptográficamente seguro. Se puede confiar en Bitcoin por ser completamente neutral, transparente y fiable.

2.1.2 Desventajas

- Grado de aceptación: mucha gente no conoce aún Bitcoin. Cada día, más negocios aceptan Bitcoin para aprovechar sus ventajas, pero la lista aún es pequeña y necesita crecer para que puedan beneficiarse de su efecto de red.

- Volatilidad: el valor total de Bitcoins en circulación y el número de negocios usando Bitcoin son muy pequeños comparado con lo que puede llegar a ser. Por lo tanto, eventos relativamente pequeños, intercambios o actividades empresariales afectan significativamente en el precio. En teoría, esta volatilidad decrecerá conforme el mercado y la tecnología Bitcoin madure. Nunca se ha visto una moneda naciente, por lo que es muy difícil (y excitante) imaginar que pasará. (Bitcoin.org, 2010, párr.11)
- Desarrollo en curso: el software de Bitcoin aún está en fase beta con muchas características incompletas en desarrollo. Se están desarrollando nuevas herramientas, características y servicios para hacer Bitcoin más seguro y accesible a las masas. Muchas aún no están listos para el público. La mayoría de los negocios con Bitcoin son nuevos y no ofrecen seguridad. En general, Bitcoin aún está en proceso de maduración.

Bitcoin está diseñado para permitir a sus usuarios enviar y recibir pagos con un aceptable nivel de privacidad como cualquier otra moneda. También es cierto que Bitcoin no es anónimo y no puede ofrecer el mismo nivel de privacidad que el dinero. El uso de Bitcoin deja registros públicos. Existen varios mecanismos para proteger la privacidad de los usuarios, más los que se encuentran en desarrollo. Aun así, queda mucho trabajo antes de que estas características sean correctamente usadas por la mayoría de los usuarios Bitcoin.

Han surgido algunas preocupaciones acerca de transacciones privadas con Bitcoin que podrían usarse para propósitos ilegales. Sin embargo, Bitcoin será sin duda sujeto a regulaciones similares a las que existen dentro de los sistemas financieros. Bitcoin no puede ser más anónimo que el efectivo y seguramente no

evitará que se realicen investigaciones criminales. Además, Bitcoin está creado para prevenir un gran número de crímenes financieros.

Bitcoin es dinero y el dinero siempre ha sido usado para propósitos legales e ilegales. Efectivo, tarjetas de crédito y los sistemas bancarios superan ampliamente a Bitcoin a la hora de financiar el crimen. Bitcoin puede traer innovación a los sistemas de pago y los beneficios de tal innovación son considerados mucho más valiosos que los potenciales inconvenientes. (Bitcoin.org 2010, párr.14)

Bitcoin está diseñado para dar un gran paso adelante en la seguridad monetaria y también podría jugar un gran papel contra muchas formas de crimen financiero. Por ejemplo, los Bitcoins son imposibles de falsificar. Los usuarios tienen control total sobre sus pagos y no pueden recibir cobros no aprobados como los que pueden verse con tarjetas de crédito. Las transacciones Bitcoin son irreversibles e inmunes a devoluciones fraudulentas. Bitcoin le permite asegurar el dinero contra robo utilizando fuertes y útiles mecanismos como por ejemplo las copias de seguridad, el cifrado criptográfico y las firmas múltiples. (Bitcoin.org, 2010, párr. 15)

Algunas preocupaciones han surgido acerca de que Bitcoin puede ser más atractivo para los criminales debido a que puede utilizarse para hacer pagos privados e irreversibles. Sin embargo, estas características existen actualmente en el dinero efectivo y en las transferencias bancarias, las cuales son ampliamente usadas. El uso de Bitcoin sin duda es sujeto a regulaciones similares a las que existen en los sistemas financieros y no es diferente a la hora de realizar investigaciones criminales. Comúnmente, los avances importantes siempre han sido percibidos con polémica antes de comprender correctamente sus beneficios. Un buen ejemplo de ello es Internet. (Bitcoin.org 2010, párr. 16)

El protocolo Bitcoin no puede ser modificado sin la cooperación de casi todos sus usuarios, que eligen el software que utilizan. Intentar asignar derechos especiales a una autoridad local dentro de las reglas de una red Bitcoin global no es una posibilidad. Cualquier organización poderosa podría elegir invertir en hardware de minado para controlar la mitad del poder computacional de la red y tener el poder de bloquear o revertir transacciones recientes. Aun así, no hay garantías de que pudieran mantener este poder, ya que requiere invertir tanto como todos los otros mineros del mundo juntos. (Bitcoin.org 2010, párr.17)

Sin embargo, es posible regular el uso de Bitcoin de manera similar a cualquier otro instrumento. Al igual que el dólar, Bitcoin se puede utilizar para una amplia variedad de propósitos, algunos de los cuales se pueden considerar legítimos o no, dependiendo de las leyes de cada territorio. En este sentido, Bitcoin no es diferente a cualquier otra herramienta o recurso y se puede someter a regulaciones diferentes en cada país. El uso de Bitcoin podría ser difícil bajo regulaciones muy restrictivas, en cuyo caso sería difícil determinar qué porcentaje de usuarios continuaría usando esta tecnología. Un gobierno que decida prohibir Bitcoin podría estar evitando el desarrollo de empresas y mercados nacionales, desplazando la innovación a otros países. El desafío para los reguladores es, como siempre, el desarrollo de soluciones eficientes que a la vez no obstaculicen el crecimiento de nuevos mercados y empresas. (Bitcoin.org, 2010, párr.18)

2.1.3 Valor del Bitcoin

Los nuevos Bitcoins son generados por un proceso competitivo y descentralizado llamado "minería". Este proceso se basa en que los individuos son premiados por la red por sus servicios. Los mineros de Bitcoin procesan las

transacciones y aseguran la red usando un hardware especializado y recogen Bitcoins a cambio de este servicio. (Bitcoin.org 2010, párr.19)

El protocolo Bitcoin está diseñado de manera que los nuevos Bitcoins se crean con un ritmo fijado. Esto hace que la minería de Bitcoin sea un negocio muy competitivo. Cuanto más mineros acceden a la red, incrementa la dificultad para obtener beneficios y los mineros deben buscar la mayor eficiencia para reducir sus costes operativos. Ninguna autoridad central o desarrollador tiene el poder de controlar o manipular el sistema para incrementar sus beneficios. Cada nodo Bitcoin que hay en el mundo rechazará automáticamente todo lo que no se ajuste a las normas que se esperan del sistema a seguir. (Bitcoin.org, 2010, párr.20)

Los Bitcoins se crean a velocidad predecible y decreciente. El número de Bitcoins creados cada año se reduce a la mitad de forma automática a lo largo del tiempo hasta que la emisión de Bitcoin se detenga por completo al llegar a los 21 millones de Bitcoins. Llegados a este punto, probablemente los mineros de Bitcoin serán mantenidos exclusivamente por las numerosas y pequeñas tasas de transacciones. (Bitcoin.org, 2010, párr. 21)

Los Bitcoins tienen valor porque son útiles como moneda. Tienen las características del dinero (durabilidad, portabilidad, fungibilidad, escasez, divisibilidad y reconocibilidad) basado en propiedades matemáticas en vez de confiar en propiedades físicas (como el oro y la plata) o confiar en autoridades centralistas (como las monedas fiduciarias). Abreviando, Bitcoin está respaldado por las matemáticas. Con estos atributos, todo lo que necesita esta clase de dinero para mantener su valor es confianza y adopción. En el caso de Bitcoin, podemos medirlo con su crecimiento en usuarios, comerciantes y empresas nacientes. Como

cualquier moneda, el valor del Bitcoin se consigue sola y directamente de la gente que quiere aceptarlo como pago. (Bitcoin.org, 2010, párr.23)

2.2 Blockchain y minería de criptomoneda

Blockchain, originalmente una cadena de datos, es una base de datos distribuida que mantiene una lista cada vez mayor de registros, llamados bloques, seguros de manipulación y revisión. Cada bloque contiene una marca de tiempo y un enlace a un bloque anterior. Por diseño, las cadenas de bloques son intrínsecamente resistentes a la modificación de los datos - una vez registrados, los datos en un bloque no pueden ser alterados retroactivamente. Mediante el uso de una red peer-to-peer y un servidor de estampado de tiempo distribuido, una base de datos blockchain se gestiona de forma autónoma. Blockchain es "un libro abierto y distribuido que puede registrar las transacciones entre dos partes de manera eficiente y de manera verificable y permanente. El propio libro también puede programarse para activar las transacciones de forma automática" (Blockchain.info, 2013, párr.4).

Los bloques Blockchain son seguros por diseño y un ejemplo de un sistema de computación distribuido con alta tolerancia a errores bizantinos. Por lo tanto, el consenso descentralizado puede lograrse con una Blockchain. Esto hace que las cadenas de bloque sean adecuadas para el registro de eventos, registros médicos y otras actividades de gestión de registros, gestión de identidades, procesamiento de transacciones y documentación de procedencia. (Blockchain.info, 2013, párr.6)

La primera cadena Blockchain fue conceptualizada por Satoshi Nakamoto en 2008 e implementada el año siguiente como un componente central de Bitcoin de moneda digital, donde sirve como el libro mayor público para todas las transacciones. La invención de la Blockchain para Bitcoin la convirtió en la primera

moneda digital en resolver el doble problema de gasto, sin el uso de una autoridad de confianza o servidor central. El diseño Bitcoin ha sido la inspiración para otras aplicaciones.

Una Blockchain facilita las transacciones en línea de forma segura. Una Blockchain es un ledger (registro) digital descentralizado y distribuido que se utiliza para registrar transacciones a través de muchas computadoras, de modo que el registro no puede ser alterado retroactivamente sin la alteración de todos los bloques subsiguientes y la colusión de la red. Esto permite a los participantes verificar y auditar transacciones de manera económica. Son autenticados por la colaboración masiva impulsada por intereses colectivos. El resultado es un flujo de trabajo robusto en el que la incertidumbre de los participantes con respecto a la seguridad de los datos es marginal. (Blockchain.info, 2013, párr.7)

El uso de una Blockchain elimina la característica de reproducibilidad infinita de un activo digital. Confirma que cada unidad de valor fue transferida solo una vez, lo cual resuelve el problema de largo plazo del doble gasto. Blockchain ha sido descrito como un protocolo de intercambio de valor. Este intercambio de valor basado en una Blockchain puede completarse más rápidamente, con mayor seguridad y de forma más barata que con los sistemas tradicionales. Una Blockchain puede asignar derechos de título porque proporciona un registro que obliga a ofrecer y aceptar.

Una base de datos de bloque de bloques consta de dos tipos de registros: transacciones y bloques. Los bloques contienen lotes de transacciones válidas que son hash y codificadas en un árbol Merkle. Cada bloque incluye el hash del bloque anterior en la Blockchain, uniendo los dos. Las variantes de este formato se utilizaron previamente, por ejemplo, en Git. El formato no es por sí mismo suficiente

para calificar como cadena de bloque. Los bloques unidos forman una cadena. Este proceso iterativo confirma la integridad del bloque anterior al camino de vuelta al bloque de génesis original. Algunos bloques de blockchain crean un bloque nuevo tan frecuentemente como cada cinco segundos. Conforme crecen los bloques de blockchain en edad, estos llegan a crecer en altura.

A veces se pueden producir bloques separados simultáneamente, lo cual crea un fork temporal. Además de un historial basado en hash seguro, cualquier Blockchain tiene un algoritmo especificado para marcar diferentes versiones del historial en donde una con un valor superior pueda ser seleccionada sobre otras. Los bloques no seleccionados para su inclusión en la cadena se denominan bloques huérfanos. Los pares que apoyan la base de datos no tienen exactamente la misma versión de la historia en todo momento. En su lugar, mantienen la versión de puntuación más alta de la base de datos que conocen actualmente. Cada vez que un compañero recibe una versión de puntuación más alta (usualmente la versión antigua con un solo bloque añadido), amplían o sobrescriben su propia base de datos y retransmiten la mejora a sus compañeros. Nunca hay una garantía absoluta de que cualquier entrada en particular permanecerá en la mejor versión de la historia para siempre.

Debido a que los bloques de blockchain normalmente se construyen para agregar la puntuación de nuevos bloques en bloques antiguos y porque hay incentivos para trabajar solo en extender con nuevos bloques en lugar de sobrescribir bloques antiguos, la probabilidad de que una entrada sea superada disminuye exponencialmente a medida que se construyen más bloques encima de ellos, llegando a ser muy baja. Por ejemplo, en una Blockchain que utiliza el sistema de prueba de trabajo, la cadena con la prueba de trabajo más acumulativa

siempre es considerada válida por la red. Hay una serie de métodos que pueden utilizarse para demostrar un nivel suficiente de cálculo. Dentro de una Blockchain, el cálculo se realiza de forma redundante en lugar de la tradicional segregada y paralela.

2.2.1 Descentralización

Almacenando datos a través de su red, Blockchain elimina los riesgos que vienen con los datos que se sostienen centralmente. Las cadenas bloqueadas descentralizadas pueden utilizar el paso de mensajes ad hoc y la red distribuida. Su red carece de puntos centralizados de vulnerabilidad que los piratas informáticos puedan explotar o cualquier punto central de falla. Los métodos de seguridad Blockchain incluyen el uso de la criptografía de clave pública. Una clave pública (una larga cadena de números al azar) es una dirección en el Blockchain. Los tokens de valor enviados a través de la red se registran como pertenecientes a esa dirección. Una clave privada es como una contraseña que da acceso a su propietario a sus activos digitales o de, otra manera interactuar, con las diversas capacidades asignadas. Los datos almacenados en la cadena de bloqueo se consideran generalmente incorruptibles.

Cada nodo o minero en un sistema descentralizado tiene una copia de la Blockchain. La calidad de los datos se mantiene mediante la replicación masiva de bases de datos y la confianza computacional. No existe una copia "oficial" centralizada y ningún usuario es "de confianza" más que cualquier otro. Las transacciones se transmiten a la red mediante software. Los mensajes se entregan sobre la base de un mejor esfuerzo. Los nodos de minería validan las transacciones, las añaden al bloque que están creando y, a continuación, transmiten el bloque completado a otros nodos. Los bloqueos utilizan varios esquemas de marcación de hora, como prueba de trabajo para serializar los cambios. Los

métodos de consenso alternativos incluyen prueba de estaca y prueba de quemadura. El crecimiento de una cadena bloqueada descentralizada se acompaña del riesgo de centralización de nodos porque los recursos informáticos necesarios para operar datos más grandes se vuelven más costosos.

2.2.2 Apertura

Las cadenas bloqueadas abiertas son más fáciles de usar que algunos registros tradicionales de propiedad, los cuales, aunque están abiertos al público, todavía requieren acceso físico para verse. Debido a que todos los bloqueos tempranos fueron sin permiso, la controversia ha surgido sobre la definición de bloque de bloques. Una cuestión en este debate en curso es si un sistema privado con verificadores encargados y autorizados por una autoridad central debe considerarse un bloque de bloqueo. Los defensores de las cadenas autorizadas o privadas sostienen que el término "Blockchain" puede aplicarse a cualquier estructura de datos que agrupa los datos en bloques con marcas de tiempo. Estos bloques de blockchain sirven como una versión distribuida del control de concurrencia multiversión (MVCC) en bases de datos. Así como MVCC impide que dos transacciones modifiquen simultáneamente un solo objeto en una base de datos, bloques de blockchain impide que dos transacciones pasen la misma salida única en una cadena de bloqueo. Los opositores afirman que los sistemas autorizados se asemejan a las bases de datos corporativas tradicionales, por lo cual no apoyan la verificación descentralizada de datos, y que tales sistemas no se endurecen contra la manipulación y revisión del operador.

2.2.3 Aplicaciones de Bitcoin

La tecnología Blockchain tiene un gran potencial para transformar los modelos operativos del negocio a largo plazo. La tecnología de contabilidad distribuida Blockchain es más una tecnología fundamental -con el potencial de crear

nuevas bases para los sistemas económicos y sociales globales- que una tecnología disruptiva, que típicamente "ataca un modelo de negocio tradicional con una solución de menor costo y supera rápidamente a las empresas establecidas" (Nakamoto S., 2009, p.5).

Blockchain puede integrarse en múltiples áreas. Esto significa que las aplicaciones de bloque de bloques específicas pueden ser una innovación disruptiva, ya que se pueden crear instancias de soluciones sustancialmente de bajo costo, lo que puede interrumpir los modelos de negocio existentes. Los protocolos Blockchain facilitan a las empresas el uso de nuevos métodos de procesamiento de transacciones digitales. Los ejemplos incluyen un sistema de pago y moneda digital, facilitando crowdsales (compra y venta de criptomoneda a inversionistas), o implementando mercados de predicción y herramientas genéricas de gobernabilidad. Blockchain se espera que interrumpan la industria de la computación en nube, aunque cuestiones técnicas prácticas siguen siendo obstáculos.

Blockchain puede ser pensado como un libro de registro automáticamente notariado. Ellos alivian la necesidad de un proveedor de servicios de confianza y se predice que resultará en menos capital atado en disputas. Blockchain tiene el potencial de reducir el riesgo sistémico y el fraude financiero. Automatiza los procesos que antes eran demorados y se hacían manualmente, como la incorporación de negocios. En teoría, sería posible recaudar impuestos, conducir el traspaso y proporcionar la gestión de riesgos con bloqueos.

Las aplicaciones más importantes de Blockchain incluyen las criptomonedas, como Bitcoin, BlackCoin, Dash y Nxt, y las plataformas blockchain como Factom, como un registro distribuido; Gems, para mensajería descentralizada:

MaidSafe,para aplicaciones descentralizadas;Storj, para una nube distribuida, y Tezos, para el voto descentralizado. Cada frecuencia críptica tiene sus propias características y particularidades. Marcos y ensayos, como el del Registro de la Tierra de Suecia, tienen como objetivo demostrar la efectividad de la cadena de bloqueos en los acuerdos de venta acelerada de tierras.

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

La investigación es de tipo evaluativa con una meta clara: el desarrollar un marco de referencia claro para la investigación e identificación de los dueños de las billeteras electrónicas investigadas.

3.2 Alcance Investigativo

Se crea una metodología entregada en la forma de manual, con la definición y técnicas recomendadas para el rastreo e investigación de transferencias y destino del dinero en su modalidad de criptomoneda, tomando como ejemplo la denominada como “Bitcoin”, por lo tanto, tiene un alcance explicativo.

3.3 Enfoque

El enfoque es la identificación de un marco de referencia funcional para el seguimiento del dinero dentro de las plataformas de blockchain hasta la IP del aparato que contiene la billetera electrónica, incluyendo la posibilidad de transferencia a una entidad de cambio a moneda corriente. El tipo de enfoque será cualitativo dado que se este documento tiene como fin mostrar soluciones para contrarrestar ataques cibernéticos usando las diferentes experiencias previas recolectadas durante esta investigación.

3.4 Diseño

El diseño de la metodología será en modalidad de Marco de Referencia con recomendación y/o desarrollo de aplicaciones que utilicen los algoritmos definidos en la investigación. El marco de referencia será el resultado de la serie de investigaciones realizadas, por tanto, el diseño es de forma cualitativa debido al tipo de enfoque seleccionado.

3.5 Población y Muestreo

Al ser una investigación de aspectos técnicos, la población es la de todos los usuarios de criptomoneda y la muestra para la demostración de funcionalidad será de una cuenta discrecional.

3.6 Instrumentos de Recolección de Datos

Se utilizará la investigación académica para recolectar los datos técnicos a utilizar en el desarrollo de la metodología. Se aplicará el análisis de contenido precisamente al estudiar ataques previos, así como la estructura del Bitcoin que permiten encontrar los puntos importantes para generar el marco de referencia.

3.7 Técnicas de Análisis de Información

Básicamente será un análisis cualitativo, donde se extraen los comportamientos de los paquetes que se correlacionen con Bitcoin, y definir una serie de parámetros para encontrar las billeteras culpables, así como los nodos corruptos. El algoritmo será capaz de ayudar con el análisis de esta información.

3.8 Estrategia de Desarrollo de la Propuesta

El desarrollo será primordialmente la generación del “marco de referencia” mencionado, el cual incluirá la metodología y requerimientos al día de la entrega de los métodos necesarios (algoritmos) para el cumplimiento de la obtención de la

información necesaria para la identificación de la cuenta meta y/o IP del aparato que contiene la billetera digital.

Capítulo 4. Análisis del Diagnóstico

Al intentar tener una justificación colegiada para implementar el manual dentro de un organismo investigativo, el enfoque tuvo la forma de mesa redonda, para generar una lluvia de ideas que finalmente dieron como resultado los comentarios y acuerdos que se documentaron en la transcripción incluida a continuación.

Transcripción de conversación sobre manual de rastreo Bitcoin

Participantes

Jonathan Durán

Raúl Morales

Erick Lewis

Charles Hill

La revisión hecha por los ingenieros del departamento de Delitos Informáticos del Organismo de Investigación Judicial (OIJ) arrojó las observaciones que se transcriben a continuación:

1. El formato del documento es altamente técnico, en donde los ingenieros que lo revisaron (Jonathan más a fondo) denotan que el investigador promedio no tiene la capacidad técnica para procesarlo. Aun así, la opinión de ambos es muy favorable ya que identifican que el manual es altamente funcional para la eventualidad de rastrear el dueño de la billetera de criptomonedas.
2. Consulta sobre el lenguaje utilizado para el algoritmo (Python), en donde se propone por ser un lenguaje de programación adaptable a las funciones requeridas en la función de rastreo.
3. Es el sitio de bitcoin.org el único punto de referencia para registrar las transacciones de Bitcoin. Esto debido a que es bitcoin.org al que se le

cargan todas las transacciones que suceden en esta moneda, la cual es el objeto de análisis mayoritario en este estudio.

4. El ingeniero Durán expuso su preocupación en donde manifestamos que las transacciones se pueden rastrear incluso cuando el usuario haya utilizado un servicio de anonimato como lo es Tor. La explicación que le dimos fue que el método a utilizar de deanonimización es altamente capaz de rastrear los "seudónimos" que servicios como el Tor arrojan, por lo que logra que eventualmente el rastreo encuentre la dirección del cliente.
5. Se conversó sobre otros protocolos que utilizan algunas criptomonedas, sin embargo, nuestro enfoque fue claro desde un inicio en que nos íbamos a enfocar en Bitcoin, ya que es la criptomoneda más aceptada y por la que se conoce se han cometido los fraudes más conocidos al momento.
6. El OIJ finalmente ve con buenos ojos esta propuesta y apoya continuar con la iniciativa del manual. Se llega a un consenso de que la interpretación y puesta en práctica de este proyecto está en buen camino. Ellos ofrecen de parte de su departamento de delitos informáticos colaboración en este proyecto, así como contar con los investigadores para consultoría en temas relacionados con el Bitcoin y delitos en general que tengan relación con la ciberseguridad.

Capítulo 5. Propuesta de Solución

Solución propuesta

Se propone un marco de referencia con explicaciones de cada técnica conocida de ofuscación y sus posibles métodos de detección (o contra ofuscación), así como metodología de investigación y posibilidades realistas de éxito.

El marco de referencia, en sí, contiene explicaciones de técnicas que, aunque no forman parte de un modus operandi conocido, pueden ser utilizadas por los antisociales para no ser detectados, y los métodos conocidos para contrarrestarlas.

Solución óptima

La solución óptima para la situación corriente implicaría, además del manual propuesto, un salón de clases, un laboratorio con simulaciones de una red P2P y las herramientas programáticas necesarias para probar las técnicas descritas, asimismo implicaría un curso estandarizado con el conocimiento previo a la aplicación de la metodología.

Usando como referencia las recomendaciones, así como el estado actual del OIJ con respecto al poco personal con el que el departamento cuenta actualmente capacitado para contrarrestar y analizar este tipo de vulnerabilidades y fraudes, se considera necesario que todo el personal del departamento de delitos informáticos sea apropiadamente entrenado con los estándares más altos de Seguridad disponibles en el mercado.

Las diferentes técnicas de ofuscación explicadas en el marco de referencia conllevan un riesgo con respecto a las legislaciones de cada país (como ya fue anteriormente mencionado en el marco teórico). Por tanto, es indispensable que cualquier uso de las técnicas explicadas en el marco de referencia sea debidamente analizado contra el marco legal actual y no se corra el riesgo de violentar algún derecho del potencial usuario afectado.

Como se había mencionado, en el alcance económico del proceso, las Horas hombre de los implementadores sumarían unos $36,000 por unos 4 meses de implementación, pruebas, documentación, entre otros. El software requerido, así como el hardware a implementar, dependerá de las capacidades económicas del

OIJ o algún otro agente investigativo. Las licencias de Python suelen ser código abierto, lo cual haría que la inversión de software sea considerablemente baja.

La prueba de concepto vendría a ser la implementación de estas técnicas por parte de una persona capacitada para llevarlas a cabo, con el marco legal debidamente analizado y con alta sospecha de que el potencial dueño de una cartera Bitcoin cometió o su cuenta fue parte de un fraude o crimen.

5.1 Marco de referencia para rastreo de transacciones por medio de criptomoneda

5.1.1 Introducción

La meta de este manual es describir diferentes tácticas de rastreo de criptomonedas, por esa razón se explorarán tácticas utilizadas por diferentes usuarios para preservar su anonimato; el que se documenten estas técnicas no es excusa para su uso indiscriminado, estas son para uso en situaciones de investigación bajo sospecha de un crimen y con orden judicial al respecto.

Las criptomonedas son certificados digitales que mantienen un valor variable derivado de la oferta y demanda por ellas, con la ventaja de que la identidad de sus poseedores no es evidente para el usuario laico; son intercambiados con registro a una base de datos distribuida y extremadamente segura en cuanto al registro de sus movimientos, pero, en cambio, es totalmente pública y permite la consulta de sus registros en cualquier momento.

El problema se define en cómo reconocer el responsable de cual transacción.

En las bases de datos utilizadas, los usuarios son codificados con una identificación de aproximadamente 34 caracteres, los cuales son letras, números y símbolos, lo que hace su identificación análoga extremadamente difícil, esto aunado

a estrategias de ofuscamiento que son similares a la utilizadas en fraudes bancarios.

Las criptomonedas son generadas en ambientes “P2P” o “peer to peer”, lo cual implica que no existe una entidad centralizada que efectúe alguna especie de control sobre ellas, asimismo en su diseño no hay una manera “nativa” de obtener los datos de identidad de los creadores de una “billetera electrónica”, como se le llama al contenedor donde se registran.

Se adentrará en el ámbito estratégico y técnico que envuelve a esta plataforma y que permite colocar “nombre y apellidos” a las personas que la utilizan.

5.1.2 Técnicas de rastreo

Bitcoin no es anónimo. Cualquiera que haya seguido la “Dark Web” o la regulación continua de la criptografía debe estar familiarizado con esa idea. Si alguien logra vincular una identidad real con una cartera, algo visto como posible, pueden seguir otras transacciones alrededor de la cadena de bloqueo pública para ver dónde ha viajado el dinero de esa persona.

Para esto se puede utilizar una herramienta de código abierto para agrupar las transacciones de criptomonedas, con el fin de identificar que pertenecen a la misma entidad, mercado o persona. No necesariamente revela la identidad del usuario, pero puede mostrar detalles sobre el gasto de la moneda de alguien.

En lugar de ver movimiento por direcciones, se ve movimiento por entidad. Esa entidad podría ser un traficante de drogas, un defraudador o un usuario de criptomonedas ordinario.

En muchos casos, los autores de ransomware -la gente detrás del malware que bloquea una computadora hasta que se paga una recompensa en criptomonedas (Bitcoin en la mayoría de los casos)- dan a cada víctima su propia

dirección de billetera para enviar dinero. De esta manera, los delincuentes pueden hacer un seguimiento de quién ha pagado. Pero si el autor agrupa todo ese dinero en una cartera, entonces se puede ver exactamente cuánto dinero han hecho, porque se puede agrupar estos datos por fecha o cantidad, se puede saber exactamente cuándo la primera víctima les envió dinero.

En cuanto a los mercados de "Dark Web", es posible agrupar las carteras que se están utilizando para los pagos de fideicomiso en cualquier mercado, es decir, el dinero que retiene el mercado hasta que los vendedores cumplan con el fin del trato.

5.1.3 Estructura estándar del paquete de información de la criptomoneda

Las criptomonedas utilizan una base de datos llamada “blockchain” la cual utiliza la clave de hash del bloque anterior para codificar el nuevo bloque de datos.

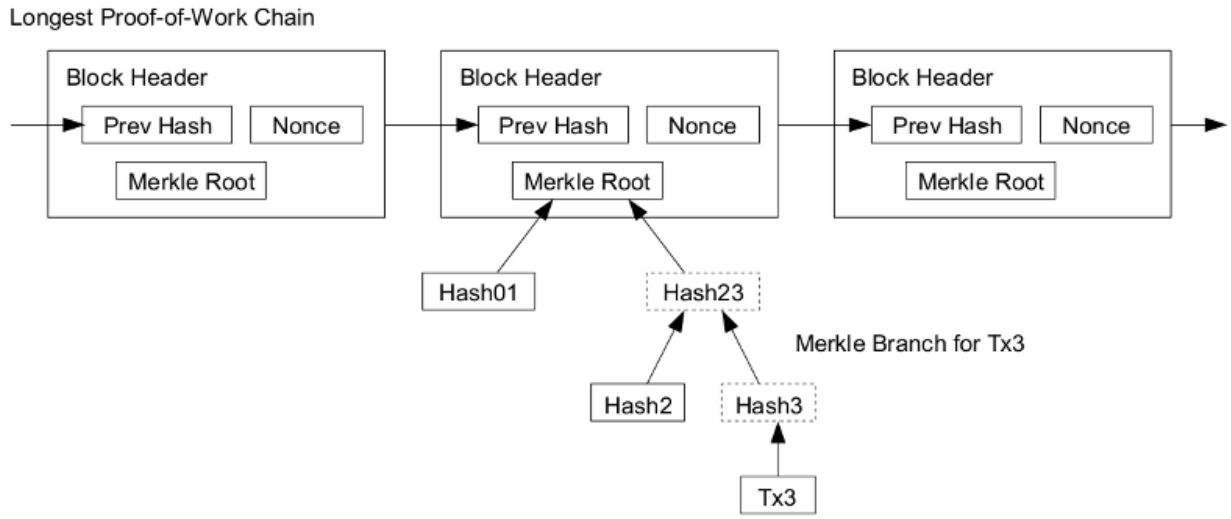

Figura 1. Estructura de Bitcoin

La ilustración anterior muestra una versión simplificada de una Blockchain. Un bloque de una o más nuevas transacciones se recoge en la parte de datos de transacción de un bloque. Las copias de cada transacción son hash, y los hashes son emparejados, hashed, emparejado de nuevo, y hash de nuevo hasta que un hash único permanece, la raíz merkle de un árbol merkle.

La raíz merkle se almacena en el encabezado del bloque. Cada bloque también almacena el hash del encabezado del bloque anterior, encadenando los bloques juntos. Esto garantiza que una transacción no se puede modificar sin modificar el bloque que lo registra y todos los bloques siguientes.

Esta estructura requiere de un tiempo de codificación que aumenta exponencialmente conforme va avanzando en la cadena, lo cual dificulta enormemente su falsificación.

El encadenamiento de bloques hace imposible modificar las transacciones incluidas en cualquier bloque sin modificar todos los bloques siguientes. Como resultado, el costo de modificar un bloque particular aumenta con cada nuevo bloque añadido a la Blockchain, lo cual magnifica el efecto de la prueba de trabajo.

La prueba de trabajo utilizada en Bitcoin aprovecha la naturaleza aparentemente aleatoria de los hashes criptográficos. Un buen algoritmo de cifrado criptográfico convierte los datos arbitrarios en un número aparentemente aleatorio. Si los datos se modifican de alguna manera y se vuelve a ejecutar el hash, se produce un nuevo número aparentemente aleatorio, por lo que no hay forma de modificar los datos para que el número de hash sea predecible.

Para probar que hizo un trabajo extra para crear un bloque, debe crear un hash del encabezado de bloque que no exceda un cierto valor. Por ejemplo, si el valor de hash máximo posible es 2256 - 1, puede probar que intentó hasta dos combinaciones produciendo un valor de hash inferior a 2255.

Una única transacción puede crear múltiples salidas, como sería el caso al enviar a varias direcciones, pero cada salida de una transacción en particular solo puede utilizarse como entrada una vez en la Blockchain. Cualquier referencia

posterior es un doble gasto prohibido, un intento de gastar el mismo satoshis dos veces.

Las salidas están vinculadas a los identificadores de transacción (TXID), que son los hashes de las transacciones firmadas.

Debido a que cada salida de una transacción particular solo se puede gastar una vez, las salidas de todas las transacciones incluidas en la Blockchain se pueden clasificar como salidas de transacciones no gastadas (UTXO) o salidas de transacciones agotadas. Para que un pago sea válido, solo debe usar UTXO como entradas.

Si el valor de las salidas de una transacción excede sus entradas, la transacción será rechazada, pero si las entradas exceden el valor de las salidas, cualquier diferencia de valor puede ser reclamada como una tarifa de transacción por el Minero Bitcoin que crea el bloque que contiene esa transacción. Por ejemplo, en la ilustración anterior, cada transacción gasta 10,000 satoshis menos de lo que recibe de sus insumos combinados, pagando efectivamente una tarifa de transacción de 10.000 satoshi.

Datos de Transacción

Cada bloque debe incluir una o más transacciones. La primera de estas transacciones debe ser una transacción de moneda base, también llamada una transacción de generación, que debe recoger y gastar la recompensa de bloque (que comprende un subsidio de bloque y cualquier comisión de transacción pagada por transacciones incluidas en este bloque).

El UTXO de una transacción de moneda base tiene la condición especial de que no se puede gastar (utilizado como entrada) para al menos 100 bloques. Esto impide temporalmente que un minero gaste los honorarios de transacción y

recompensa de bloque de un bloque que puede ser determinado más tarde ser rancio (y por lo tanto la transacción de moneda base destruida) después de un tenedor de cadena de bloque.

No se requiere que los bloques incluyan transacciones que no sean de coinbase, pero los mineros casi siempre incluyen transacciones adicionales para cobrar sus tarifas de transacción.

Todas las transacciones, incluida la transacción de moneda base, se codifican en bloques en formato de transacción binaria rawtransaction.

El formato rawtransaction se ha creado para crear el identificador de transacción (txid). A partir de estos txidos, el árbol de Merkle se construye emparejando cada txid con otro txid y luego chocándolos juntos. Si hay un número impar de txids, el txid sin un socio es “hasheado” con una copia de sí mismo.

Los propios hashes resultantes están emparejados con otro hash y “hasheados” juntos. Cualquier hash sin un socio es “hasheado” con sí mismo. El proceso se repite hasta que sólo queda un hash, la raíz de merkle.

Direcciones y llaves Bitcoin

El primer paso es crear una dirección Bitcoin. Normalmente se utiliza el software de cliente Bitcoin para crear una dirección y las claves asociadas. Sin embargo, escribiendo un código de Python para crear la dirección, se puede mostrar exactamente lo que sucede detrás de las escenas.

Bitcoin utiliza una variedad de claves y direcciones, por lo que el siguiente diagrama puede ayudar a explicarlos. Comience creando una clave privada aleatoria de 256 bits. La clave privada es necesaria para firmar una transacción y así transferir (gastar) Bitcoins. Por lo tanto, la clave privada debe mantenerse en secreto o bien sus Bitcoins pueden ser robados.

El algoritmo DSL de curva elíptica genera una clave pública de 512 bits de la clave privada. (La criptografía de la curva elíptica se discutirá más adelante.) Esta clave pública se utiliza para verificar la firma en una transacción. Inconvenientemente, el protocolo Bitcoin agrega un prefijo de 04 a la clave pública. La clave pública no se revela hasta que se firma una transacción, a diferencia de la mayoría de los sistemas en los que la clave pública es publicada.

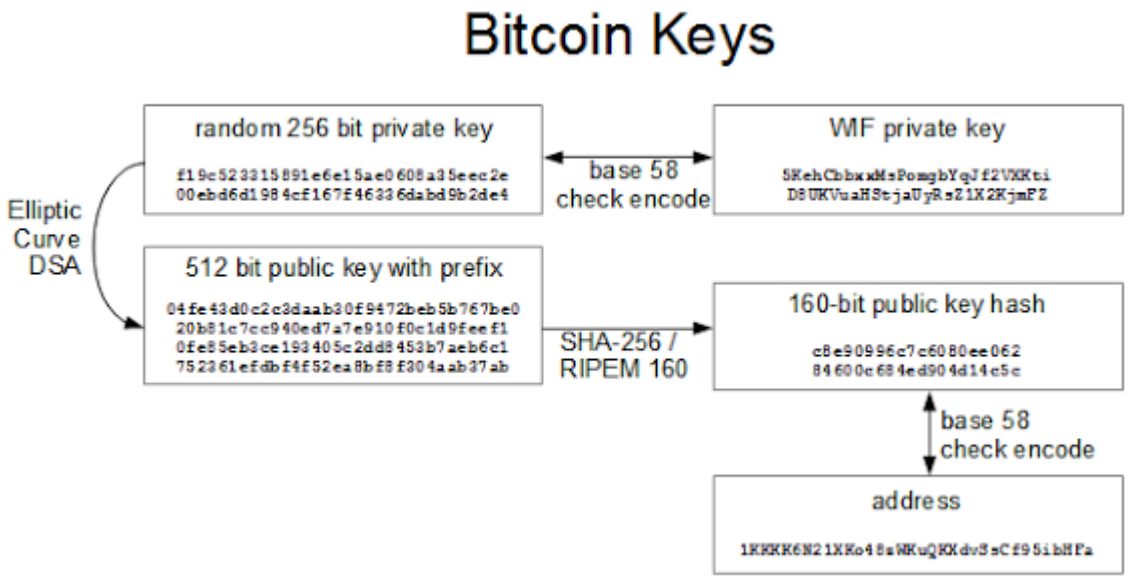

Figura 2. Llave pública y privada

El siguiente paso es generar la dirección Bitcoin que se comparte con otros. Dado que la clave pública de 512 bits es inconvenientemente grande, es “hasheada” hasta 160 bits utilizando los algoritmos de hash SHA-256 y RIPEMD. La clave se codifica en ASCII usando la codificación Base58Check personalizada de Bitcoin. La dirección resultante, como 1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa, es la dirección que la gente publica para recibir Bitcoins. Tenga en cuenta que no puede recuperar la clave pública o la clave privada de la dirección. Si pierde su clave privada (por ejemplo, desechando el disco duro), los Bitcoins se pierden para siempre.

Por último, la clave de formato de intercambio de la carpeta (WIF) se utiliza para agregar una clave privada al software de cartera de clientes. Esto es simplemente una codificación Base58Check de la clave privada en ASCII, que se invierte fácilmente para obtener la clave privada de 256 bits.

Para resumir, hay tres tipos de claves: la clave privada, la clave pública y el hash de la clave pública, y se representan externamente en ASCII usando la codificación Base58Check. La clave privada es la clave importante, ya que se requiere para acceder a los Bitcoins y las otras claves se pueden generar a partir de ella. El hash de clave pública es la dirección de Bitcoin que se ve publicada.

Se muestra el siguiente fragmento de código para generar una clave privada en formato WIF y una dirección. La clave privada es simplemente un número aleatorio de 256 bits. La biblioteca criptográfica ECDSA genera la clave pública de la clave privada. La dirección Bitcoin se genera mediante el hash SHA-256, el hash RIPEMD-160 y, a continuación, la codificación Base58 con suma de comprobación. Por último, la clave privada se codifica en Base58Check para generar la codificación WIF utilizada para introducir una clave privada en el software de cliente de Bitcoin: Nota: esta función aleatoria de Python no es criptográficamente fuerte.

```
def privateKeyToWif(key_hex):
    return utils.base58CheckEncode(0x80, key_hex.decode('hex'))
def privateKeyToPublicKey(s):
    sk = ecdsa.SigningKey.from_string(s.decode('hex'), curve=ecdsa.SECP256k1)
    vk = sk.verifying_key
    return ('\04' + sk.verifying_key.to_string()).encode('hex')
 def pubKeyToAddr(s):
    ripemd160 = hashlib.new('ripemd160')
```

```
    ripemd160.update(hashlib.sha256(s.decode('hex')).digest())
    return utils.base58CheckEncode(0, ripemd160.digest())
def keyToAddr(s):
    return pubKeyToAddr(privateKeyToPublicKey(s))

# Warning: this random function is not cryptographically strong and is just for example
private_key = ''.join(['%x' % random.randrange(16) for x in range(0, 64)])
print keyUtils.privateKeyToWif(private_key)
print keyUtils.keyToAddr(private_key)
```

Dentro de una transacción

Una transacción es la operación básica en el sistema Bitcoin. Se puede esperar que una transacción simplemente mueva algunos Bitcoins de una dirección a otra dirección, pero es más complicado que eso. Una transacción Bitcoin mueve Bitcoins entre una o más entradas y salidas. Cada entrada es una transacción y una dirección que suministra Bitcoins. Cada salida es un Bitcoin de recepción de dirección, junto con la cantidad de Bitcoins que va a esa dirección.

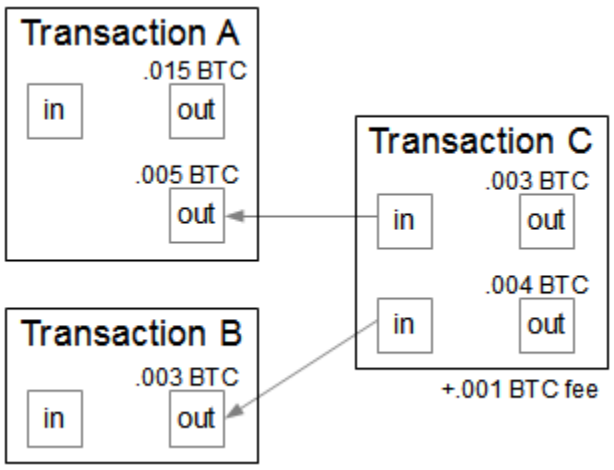

Figura 3. Transacción de ejemplo "C"

El diagrama anterior muestra una transacción de ejemplo "C". En esta transacción, .005 BTC se toman de una dirección en la transacción A y .003 BTC se toman de una dirección en la transacción B (es necesario tener en cuenta que las flechas son referencias a las salidas anteriores, por lo que son hacia atrás al flujo de Bitcoins). Para las salidas, .003 BTC se dirigen a la primera dirección y .004 BTC se dirigen a la segunda dirección. Los restos .001 BTC va al minero del bloque como una tarifa. Se debe tener en cuenta además que el .015 BTC en la otra salida de la transacción A no se invierte en esta transacción.

Cada entrada utilizada debe ser completamente gastada en una transacción. Si una dirección recibió 100 Bitcoins en una transacción y solo se desea gastar 1 Bitcoin, la transacción debe gastar 100. La solución es utilizar una segunda salida para el cambio, que devuelve los 99 Bitcoins sobrantes.

Las transacciones también pueden incluir honorarios. Si quedan residuos de Bitcoins después de sumar los insumos y sustraer los productos, el resto es un honorario pagado al minero. La tarifa no es estrictamente requerida, pero las transacciones sin una tarifa serán una prioridad baja para los mineros y no pueden ser procesadas por días o pueden ser descartadas enteramente. Un honorario típico para una transacción es 0.0002 Bitcoins (cerca de 20 centavos), así que las tarifas son bajas, pero no triviales.

Siguiendo la especificación, la transacción sin firmar se puede montar con bastante facilidad, como se muestra a continuación.

version	01 00 00 00
input count	01

input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	
	scriptSig	script que contiene la firma digital
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00
	script length	
	scriptPubKey	script que contiene la dirección de destino
block lock time		00 00 00 00

Esta transacción es creada por el siguiente código:

```
def makeRawTransaction(outputTransactionHash, sourceIndex, scriptSig, outputs):
    def makeOutput(data):
        redemptionSatoshis, outputScript = data
        return (struct.pack("<Q", redemptionSatoshis).encode('hex') +
        '%02x' % len(outputScript.decode('hex')) + outputScript)
    formattedOutputs = ''.join(map(makeOutput, outputs))
    return (
        "01000000" + # 4 bytes version
        "01" + # varint for number of inputs
```

```
    outputTransactionHash.decode('hex')[::-1].encode('hex') + # reverse
outputTransactionHash
    struct.pack('<L', sourceIndex).encode('hex') +
    '%02x' % len(scriptSig.decode('hex')) + scriptSig +
    "ffffffff" + # sequence
    "%02x" % len(outputs) + # number of outputs
    formattedOutputs +
    "00000000" # lockTime
)
```

Cómo se firman las transacciones de Bitcoin

El siguiente diagrama ofrece una vista simplificada de cómo se firman y enlazan las transacciones. Considerando la transacción media, transfiriendo Bitcoins de la dirección B a la dirección C. El contenido de la transacción (incluido el hash de la transacción anterior) se ha codificado (hash) y firmado con la clave privada de B. Además, la clave pública de B está incluida en la transacción.

Al realizar varios pasos, cualquiera puede verificar que la transacción está autorizada por B. Primero, la clave pública de B debe corresponder a la dirección de B en la transacción anterior, probando que la clave pública es válida (la dirección se puede derivar fácilmente de la clave pública, como se explicó anteriormente). A continuación, la firma de B de la transacción se puede verificar utilizando la clave pública de B en la transacción. Estos pasos garantizan que la transacción sea válida y autorizada por B. Una parte inesperada de Bitcoin es que la clave pública de B no se hace pública hasta que se utiliza en una transacción.

Con este sistema, Bitcoins se pasan de dirección a dirección a través de una cadena de transacciones. Cada paso en la cadena puede ser verificado para

asegurar que Bitcoins se están gastando válidamente. Se debe tener en cuenta que las transacciones pueden tener múltiples entradas y salidas en general, por lo que la cadena se ramifica en un árbol.

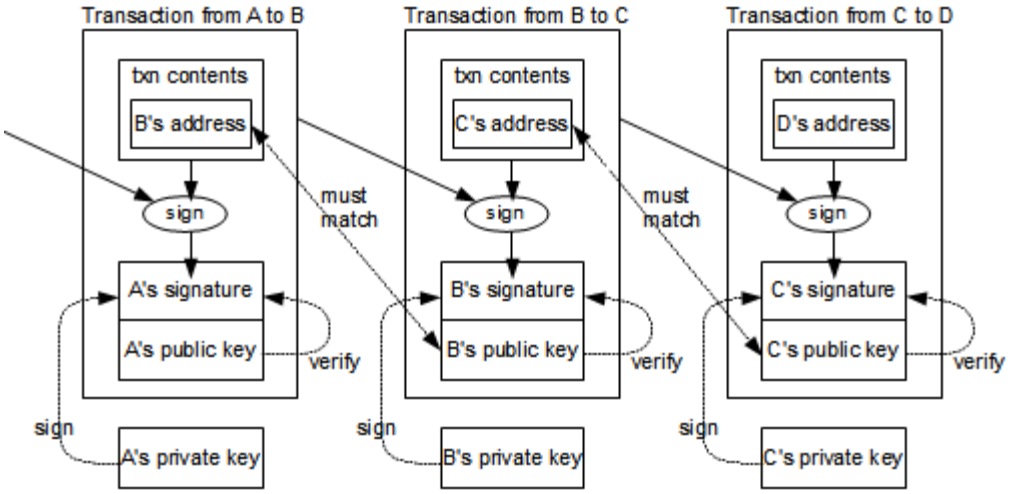

Figura 4. Árbol de transacciones

El lenguaje de secuencias de comandos Bitcoin

Se podría esperar que una transacción de Bitcoin se firme simplemente incluyendo la firma en la transacción, pero el proceso es mucho más complicado. De hecho, hay un pequeño programa dentro de cada transacción que se ejecuta para decidir si una transacción es válida. Este programa está escrito en Script, el lenguaje de script Bitcoin basado en pila. Las condiciones complejas de redención pueden expresarse en este lenguaje. Por ejemplo, un sistema de fideicomiso puede requerir que dos de cada tres usuarios específicos deban firmar la transacción para gastarla. O pueden establecerse diversos tipos de contratos.

El lenguaje Script es sorprendentemente complejo, con alrededor de 80 opcodes diferentes. Incluye operaciones aritméticas, bit a bit, operaciones de cadena, condicionales y manipulación de pila. El lenguaje también incluye las operaciones criptográficas necesarias (SHA-256, RIPEMD, entre otras.) como primitivas. Para garantizar que los scripts terminan, el idioma no contiene ninguna

operación de bucle (como consecuencia, no es Turing-complete). Sin embargo, en la práctica, solo se apoyan algunos tipos de transacciones.

Para que una transacción de Bitcoin sea válida, las dos partes del script de redención deben ejecutarse correctamente. El script de la antigua transacción se llama scriptPubKey y el script de la nueva transacción se llama scriptSig. Para verificar una transacción, se ejecuta el código scriptSig seguido por el scriptPubKey. Si la secuencia de comandos se completa correctamente, la transacción es válida y se puede gastar el Bitcoin. De lo contrario, la transacción no es válida. El punto de esto es que el scriptPubKey en la antigua transacción define las condiciones para pasar los Bitcoins. El scriptSig en la nueva transacción debe proporcionar los datos para satisfacer las condiciones.

En una transacción estándar, el scriptSig empuja la firma (generada desde la clave privada) a la pila, seguida de la clave pública. A continuación, se ejecuta el scriptPubKey (desde la transacción de origen) para verificar la clave pública y luego verificar la firma. Como se expresa en Script, el scriptSig es:

PUSHDATA

Datos de firma y SIGHASH_ALL

PUSHDATA

Datos de clave pública

El scriptPubKey es:

OP_DUP

OP_HASH160

Pulso

dirección Bitcoin (hash clave pública)

OP_EQUALVERIFY

OP_CHECKSIG

Cuando se ejecuta este código, PUSHDATA primero empuja la firma a la pila. El PUSHDATA siguiente empuja la clave pública a la pila. A continuación, OP_DUP duplica la clave pública en la pila. OP_HASH160 calcula el hash de 160 bits de la clave pública. PUSHDATA empuja la dirección Bitcoin requerida. A continuación, el script OP_EQUALVERIFY comprueba que los dos valores de pila superiores son iguales - que el hash de clave pública de la nueva transacción coincide con la dirección en la dirección antigua. Esto demuestra que la clave pública es válida. A continuación, OP_CHECKSIG comprueba que la firma de la transacción coincide con la clave pública y la firma en la pila. Esto demuestra que la firma es válida.

La mayor complicación es que la firma aparece en el medio de la transacción, lo que plantea la cuestión de cómo firmar la transacción antes de tener la firma. Para evitar este problema, la secuencia de comandos scriptPubKey se copia desde la transacción de origen en la transacción de gasto (es decir, la transacción que se está firmando) antes de calcular la firma. A continuación, la firma se convierte en código en el lenguaje de scripts, creando el script scriptSig incrustado en la transacción. Parece que el uso de scriptPubKey de la transacción anterior durante la firma es por razones históricas en lugar de cualquier razón lógica. Para transacciones con entradas múltiples, la firma es aún más complicada ya que cada entrada requiere una firma separada, pero no se entrará en los detalles.

Antes de firmar, la transacción tiene una constante de tipo hash añadida temporalmente. Para una transacción regular, esto es SIGHASH_ALL (0x00000001). Después de la firma, este tipo de hash se elimina del final de la transacción y se anexa a la scriptSig.

Otra particularidad acerca del protocolo Bitcoin es que la firma y la clave pública son valores de curva elíptica de 512 bits, pero están representados de maneras totalmente diferentes: la firma se codifica con codificación DER pero la clave pública se representa como bytes simples. Además, ambos valores tienen un byte adicional, pero se colocan de forma incoherente: SIGHASH_ALL se coloca después de la firma y el tipo 04 se coloca antes de la clave pública.

La depuración de la firma se hizo más difícil porque el algoritmo ECDSA utiliza un número aleatorio. Por lo tanto, la firma es diferente cada vez que lo calcula, por lo que no puede ser comparado con una firma conocida.

```
def makeSignedTransaction(privateKey, outputTransactionHash, sourceIndex,
scriptPubKey, outputs):
    myTxn_forSig = (makeRawTransaction(outputTransactionHash, sourceIndex,
scriptPubKey, outputs)
        + "01000000") # hash code
    s256 =
hashlib.sha256(hashlib.sha256(myTxn_forSig.decode('hex')).digest()).digest()
    sk = ecdsa.SigningKey.from_string(privateKey.decode('hex'),
curve=ecdsa.SECP256k1)
    sig = sk.sign_digest(s256, sigencode=ecdsa.util.sigencode_der) + '\01' # 01 is
hashtype
    pubKey = keyUtils.privateKeyToPublicKey(privateKey)
    scriptSig = utils.varstr(sig).encode('hex') +
utils.varstr(pubKey.decode('hex')).encode('hex')
    signed_txn = makeRawTransaction(outputTransactionHash, sourceIndex,
scriptSig, outputs)
    verifyTxnSignature(signed_txn)
 return signed_txn
```

El script script final contiene la firma junto con la clave pública para la dirección de origen (1MMMMSUb1piy2ufrSguNUdFmAcvqrQF8M5). Esto demuestra que se permite “gastar” estos Bitcoins, haciendo la transacción válida.

PUSHDATA 47		47
signature (DER)	sequence	30
	length	44
	integer	02
	length	20
	X	2c b2 65 bf 10 70 7b f4 93 46 c3 51 5d d3 d1 6f c4 54 61 8c 58 ec 0a 0f f4 48 a6 76 c5 4f f7 13
	integer	02
	length	20
	Y	6c 66 24 d7 62 a1 fc ef 46 18 28 4e ad 8f 08 67 8a c0 5b 13 c8 42 35 f1 65 4e 6a d1 68 23 3e 82
SIGHASH_ALL		01
PUSHDATA 41		41
public key	type	04
	X	14 e3 01 b2 32 8f 17 44 2c 0b 83 10 d7 87 bf 3d 8a 40 4c fb d0 70 4f 13 5b 6a d4 b2 d3 ee 75 13
	Y	10 f9 81 92 6e 53 a6 e8 c3 9b d7 d3 fe fd 57 6c 54 3c ce 49 3c ba c0 63 88 f2 65 1d 1a ac bf cd

Una vez que todos los métodos necesarios están en su lugar, la transacción final se puede montar:

privateKey =
keyUtils.wifToPrivateKey("5HusYj2b2x4nroApgfvaSfKYZhRbKFH41bVyPooymbC6KfgSXdD") #1MMMM

signed_txn = txnUtils.makeSignedTransaction(privateKey,

"81b4c832d70cb56ff957589752eb4125a4cab78a25a8fc52d6a09e5bd4404d48", # output (prev) transaction hash

0, # sourceIndex

keyUtils.addrHashToScriptPubKey("1MMMMSUb1piy2ufrSguNUdFmAcvqrQF8M5"),

[[91234, #satoshis

keyUtils.addrHashToScriptPubKey("1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa")]]

)

txnUtils.verifyTxnSignature(signed_txn)
print 'SIGNED TXN', signed_txn

La transacción final se muestra a continuación. Esto combina el scriptSig y scriptPubKey arriba con la transacción sin firma descrita anteriormente.

Version		01 00 00 00
input count		01
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81

	previous output index	00 00 00 00
	script length	8ª
	scriptSig	47 30 44 02 20 2c b2 65 bf 10 70 7b f4 93 46 c3 51 5d d3 d1 6f c4 54 61 8c 58 ec 0a 0f f4 48 a6 76 c5 4f f7 13 02 20 6c 66 24 d7 62 a1 fc ef 46 18 28 4e ad 8f 08 67 8a c0 5b 13 c8 42 35 f1 65 4e 6a d1 68 23 3e 82 01 41 04 14 e3 01 b2 32 8f 17 44 2c 0b 83 10 d7 87 bf 3d 8a 40 4c fb d0 70 4f 13 5b 6a d4 b2 d3 ee 75 13 10 f9 81 92 6e 53 a6 e8 c3 9b d7 d3 fe fd 57 6c 54 3c ce 49 3c ba c0 63 88 f2 65 1d 1a ac bf cd
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00
	script length	19
	scriptPubKey	76 a9 14 c8 e9 09 96 c7 c6 08 0e e0 62 84 60 0c 68 4e d9 04 d1 4c 5c 88 ac
block lock time		00 00 00 00

Cómo encontrar nodos

El primer paso en el uso de la red peer-to-peer es encontrar un par. La lista de pares cambia poco cada cierta cantidad de segundos, cuando alguien ejecuta un cliente. Una vez que un nodo está conectado a un nodo igual, comparten a nuevos pares intercambiando mensajes del addr cada vez que un nuevo par se descubre. De este modo, los nuevos pares se expandieron rápidamente a través del sistema.

Hay un problema sobre cómo encontrar al primer compañero. Los clientes de Bitcoin resuelven este problema con varios métodos. Varios pares confiables se

registran en DNS bajo el nombre de bitseed.xf2.org. Al hacer un nslookup, un cliente obtiene las direcciones IP de estos pares, y esperemos que uno de ellos funcione. Si eso no funciona, una lista de semillas de los compañeros se codifica en el cliente.

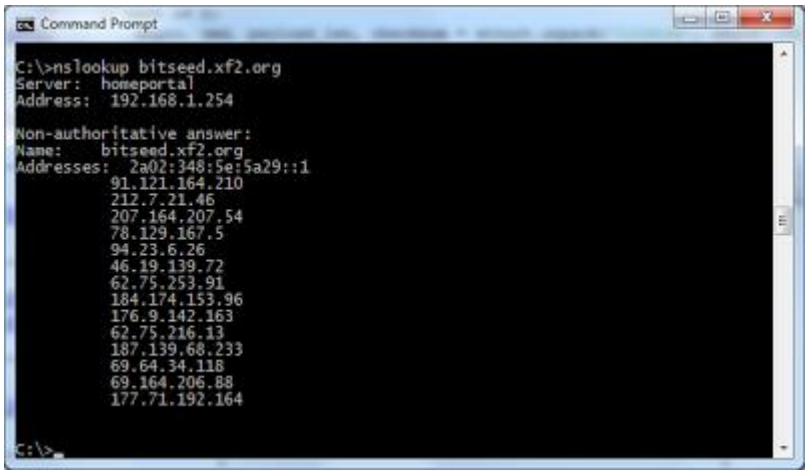

Figura 5. Propiedades de bitseed.xf2.org

Los nodos entran y salen de la red cuando los usuarios comunes inician y detienen a los clientes de Bitcoin, por lo que hay una gran cantidad de rotación en los nodos, por lo que es necesario un mapeo inicial de los nodos enviados al cliente de Bitcoin a usar para verificar su actividad y conectividad.

Una vez que tenía la dirección de un nodo funcional, el siguiente paso era enviar la transacción a la red peer-to-peer. El uso del protocolo peer-to-peer es bastante sencillo. Se abre una conexión de TCP a un peer arbitrario en el puerto 8333. El protocolo Peer-to-peer de Bitcoin es bastante tolerante; los peers mantienen la comunicación incluso si se envían las solicitudes de forma desordenada.

Nota importante: si se desea experimentar, se debería usar Bitnet TestNet, que permite experimentar con Bitcoins "falsos", ya que es fácil perder valiosos Bitcoins si se usan en la red real.

El protocolo consta de unos 24 tipos de mensajes diferentes. Cada mensaje es una burbuja binaria bastante directa que contiene un nombre de comando ASCII y una carga útil binaria apropiada para el comando. El protocolo está bien documentado en el wiki Bitcoin.

El primer paso al conectar a un par es establecer la conexión intercambiando mensajes de la versión. Primero se envía un mensaje de versión con el número de versión de protocolo, dirección y algunas otras cosas. El nodo devuelve su mensaje de versión. Después de esto, se supone que los nodos reconocen el mensaje de la versión con un mensaje verack.

Generar el mensaje de versión no es totalmente trivial ya que tiene una gran cantidad de campos, pero se puede crear con unas pocas líneas de Python. MakeMessage, a continuación, genera un mensaje peer-to-peer arbitrario a partir del número mágico, el nombre del comando y la carga útil. GetVersionMessage crea la carga útil para un mensaje de versión rellenando los distintos campos.

```
magic = 0xd9b4bef9
def makeMessage(magic, command, payload):
    checksum = hashlib.sha256(hashlib.sha256(payload).digest()).digest()[0:4]
    return struct.pack('L12sL4s', magic, command, len(payload), checksum) + payload
def getVersionMsg():
    version = 60002
    services = 1
    timestamp = int(time.time())
    addr_me = utils.netaddr(socket.inet_aton("127.0.0.1"), 8333)
    addr_you = utils.netaddr(socket.inet_aton("127.0.0.1"), 8333)
```

```
    nonce = random.getrandbits(64)
    sub_version_num = utils.varstr('')
    start_height = 0
    payload = struct.pack('<LQQ26s26sQsL', version, services, timestamp, addr_me,
        addr_you, nonce, sub_version_num, start_height)
return makeMessage(magic, 'version', payload)
```

Envío de una transacción: tx

El script envía un mensaje de versión, recibe (e ignora) la versión de los pares y mensajes verack, y luego envía la transacción como un mensaje tx. La cadena hexadecimal es la transacción creada anteriormente.

```
def getTxMsg(payload):
  return makeMessage(magic, 'tx', payload)
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("97.88.151.164", 8333))
sock.send(msgUtils.getVersionMsg())
sock.recv(1000) # receive version
sock.recv(1000) # receive verack
sock.send(msgUtils.getTxMsg("0100000001484d40d45b9ea0d652fca8258ab7caa42
541eb52975857f96fb50cd732c8b481000000008a47304402202cb265bf10707bf493
46c3515dd3d16fc454618c58ec0a0ff448a676c54ff71302206c6624d762a1fcef46182
84ead8f08678ac05b13c84235f1654e6ad168233e8201410414e301b2328f17442c0b
8310d787bf3d8a404cfbd0704f135b6ad4b2d3ee751310f981926e53a6e8c39bd7d3fe
fd576c543cce493cbac06388f2651d1aacbfcdffffffff0162640100000000001976a914c
8e90996c7c6080ee06284600c684ed904d14c5c88ac00000000".decode('hex')))
```

En la siguiente captura de pantalla se observa cómo se muestra el envío de la transacción en el programa de análisis de red de Wireshark. El tipo de mensaje

"tx" está visible en el volcado ASCII, seguido en la línea siguiente al inicio de la transacción (01 00 ...).

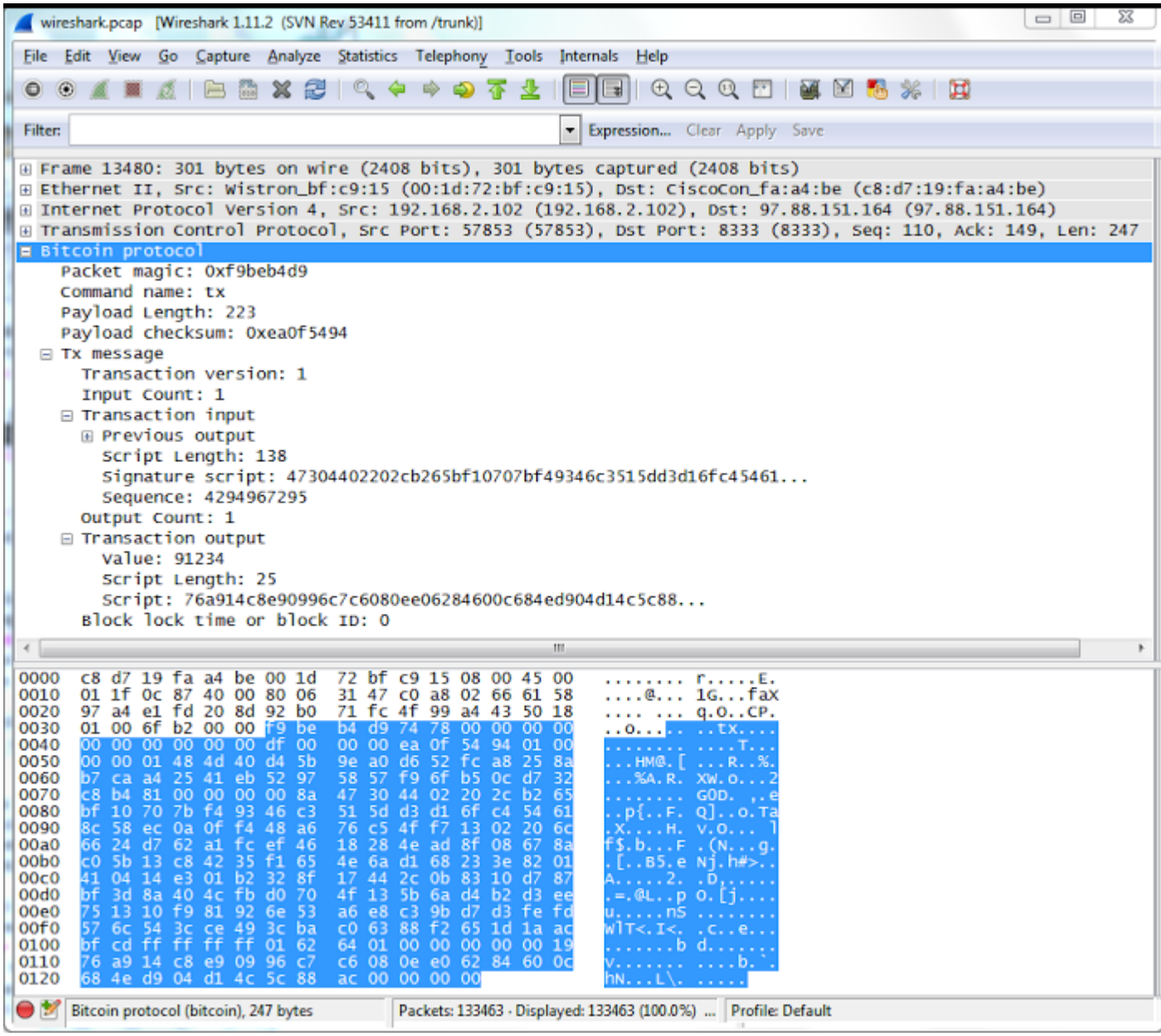

Figura 6. Rastreo de transacción "tx"

La transacción fue extraída por la gran piscina minera GHash.IO, en el bloque # 279068 con hash 0000000000000001a27b1d6eb8c405410398ece796e742da3b3e35363c2219ee.(el hash se invierte en el mensaje inv arriba: ee19 ...). Es necesario tener en cuenta que el hash comienza con un gran número de ceros, encontrar tal literalmente uno

en un valor quintillón es lo que hace la minería tan difícil. Este bloque en particular contiene 462 transacciones, de las cuales esta transacción es solo una.

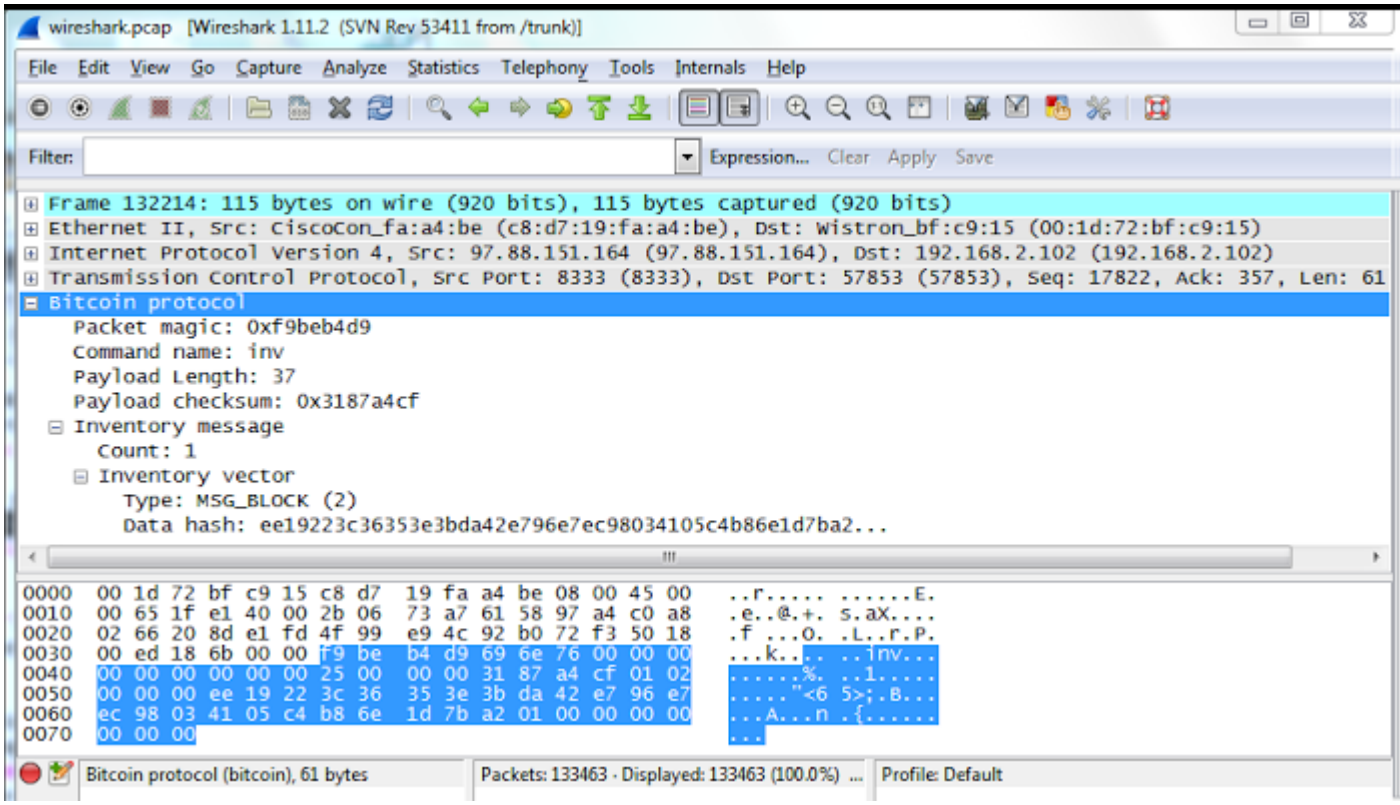

Figura 7. Hashes encontrados en el rastreo

Esto termina con la explicación y demostración del uso del protocolo Bitcoin, esta explicación permitirá una mejor comprensión de las siguientes herramientas, cómo rastrean las diversas transacciones y cómo, eventualmente, es posible utilizar este mismo protocolo para hacer un mapa de la red de nodos Bitcoin (en este caso) y sus IP correspondientes.

5.1.4 Rastreo de transacciones Bitcoin

El primer paso en esta investigación es la de determinar una o varias direcciones Bitcoin como pistas iniciales. Explicado anteriormente, los usuarios de criptomonedas utilizan varias maneras para despistar a sus perseguidores, la finalidad de este paso es determinar cuál o cuáles son las billeteras reales de los responsables de la billetera que recibe el dinero sospechoso.

El capítulo anterior muestra que el protocolo de criptomonedas es lo suficientemente amplio como para crear un script propio en Python y explorar la base de datos blockchain por todos aquellos que envíen dinero a una billetera y sus subsecuentes traslados, la facilidad de estos procedimientos ha propiciado varios proyectos de código abierto que exploran las billeteras como entidades y que permiten ver sus diferentes relaciones, así como su historia.

La primera de las herramientas que se analizará es un website llamado https://blockchain.info/, el cual contiene todas las transacciones registradas en tiempo real, el sitio permite hacer búsquedas simples, la página permite ver una billetera y las transacciones que haya efectuado durante toda su historia.

La búsqueda hecha a través de este sitio carece de profundidad y solo abarca las transacciones de primer nivel, lo que implica que, para una búsqueda de mayor profundidad, hay que hacer varias búsquedas manualmente.

La siguiente herramienta por evaluar sería BitCluster.

BitCluster es una herramienta de código abierto desarrollada por Mathieu Lavoie (@mathieu_lavoie_) y David Décary-Hétu (@ddhetu), que analiza todas las transacciones de Bitcoin y reagrupa las direcciones de la cartera de Bitcoin basándose en sus transacciones entrantes y salientes. Esto permite un mapeo más preciso de las actividades en línea de las entidades, sin importar cuántas direcciones Bitcoin estén utilizando.

Bitcluster agrupa las transacciones de Bitcoin con el fin de identificar cuáles pertenecen a la misma entidad, mercado o persona. No necesariamente revela la identidad del usuario Bitcoin, pero puede mostrar detalles sobre el gasto de Bitcoin de alguien y adónde va.

Esta herramienta también puede reagrupar las direcciones de cartera de Bitcoin en función de sus transacciones entrantes y salientes. Toda esta información se toma de la "Blockchain", que está disponible al público en tiempo real

Por último, y de una manera más visual, se recomienda la herramienta Maltego incluida con Kali Linux, la cual permite visualizar los diferentes intercambios con un modelo de “telaraña”.

Transformaciones que se ejecutan en una dirección de Bitcoin:

(Bitcoin) Get Address Details: esta transformación devolverá información adicional acerca de una dirección Bitcoin específica y agregará esta información a la vista de detalle de la entidad de direcciones.

(Bitcoin) To Addresses [*Received from] - Esta transformación devuelve direcciones Bitcoin que eran entradas a transacciones donde esta dirección era una salida. Esencialmente, esta transformación devuelve direcciones Bitcoin que enviaron Bitcoin a su dirección de entrada.

(Bitcoin) To Addresses [*Sent To] - Esta transformación devuelve direcciones Bitcoin que eran salidas a transacciones donde esta dirección era una entrada. Esencialmente, esta transformación devuelve direcciones Bitcoin que recibieron Bitcoin de su dirección de entrada.

(Bitcoin) To Addresses [Received from][Using Taint Analysis] - La relación de contaminación entre dos direcciones de Bitcoin se representa como un porcentaje e indica cuán estrechamente están relacionadas dos direcciones. Esta transformación permite al usuario especificar un umbral de relación de contaminación (en%) y devuelve direcciones Bitcoin que han enviado Bitcoin a su dirección de entrada con una relación de contaminación más alta que la especificada en la configuración de transformación.

(Bitcoin) To Addresses [Sent To][Using Reversed Taint Analysis] - Esta transformación permite al usuario especificar un umbral de relación de contaminación (en%) y devuelve direcciones Bitcoin que han recibido Bitcoin de su dirección de entrada con una relación de contaminación más alta que la especificada en la configuración de transformación.

(Bitcoin) To Transactions [where address was an OUTPUT] - Devuelve los hashes de transacciones donde la dirección de Bitcoin era una salida de las transacciones (receptor).

(Bitcoin) To Transactions [where address was an INPUT] - Devuelve los hashes de transacciones donde la dirección de Bitcoin era una entrada a la transacción (remitente).

Transformaciones que se ejecutan en una transacción de Bitcoin:

(Bitcoin) To INPUT Addresses - Esta transformación devolverá las direcciones de entrada para la transacción Bitcoin.

(Bitcoin) To OUTPUT Addresses - Esta transformación devolverá las direcciones de salida para la transacción Bitcoin.

(Bitcoin) To IP Address of First Relay - Esta transformación devuelve la dirección IP del nodo que primero transmite esta transacción a BlockChain.info. Esto no significa necesariamente que la dirección IP devuelta es el verdadero origen de la transacción.

Transformaciones que se ejecutan en una entidad de URL:

(Bitcoin) To Bitcoin Addresses on Page - Esta transformación pasará cualesquiera direcciones de Bitcoin encontradas en una página web específica.

Uso de las transformaciones

Por ejemplo, comenzando con la dirección 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX que supuestamente es la dirección de monedas "SilkRoad" incautada. Ejecutar la transformación (Bitcoin) Get Address

Details devuelve la siguiente información sobre la dirección, así como un enlace para abrir la dirección en un explorador de bloque de bloques.

Figura 8. Detalles de obtención de dirección IP

Ejecutando la transformación (Bitcoin) To Addresses [Output to transactions] para obtener todas las direcciones que eran salidas en transacciones donde esta dirección era una entrada. Al ejecutar esto, se devuelve una dirección única que incluye metadatos que indican monedas de subasta de Marshal de los Estados Unidos. Los metadatos para esta dirección también incluyen un enlace que proporciona más información sobre el supuesto propietario de la dirección.

Figura 9. Hashes de envío y recibido

En la vista de detalle de la dirección devuelta, se incluye información adicional sobre la transacción que enlaza estas direcciones.

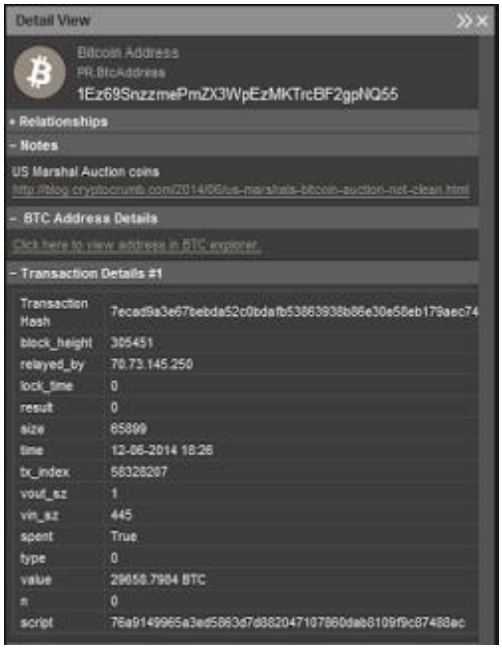

Figura 10. Detalles de dirección encontrada en Bitcoin

Ir directamente de una dirección a otra dirección, como se muestra arriba en la imagen, es un atajo, ya que se pierdela inclusión de la entidad de transacción en el gráfico, que es el enlace entre estas dos direcciones. Un método alternativo sería ejecutar primero la transformación (Bitcoin) To Transactions [Where address is an INPUT] que devolverá una entidad de transacción Bitcoin. Desde la entidad de transacción, se podría ejecutar la transformación (Bitcoin) To Transactions [Where address is an OUTPUT] retorna la misma entidad de direcciones de la subasta Marshal de los Estados Unidos que se tenía previamente.

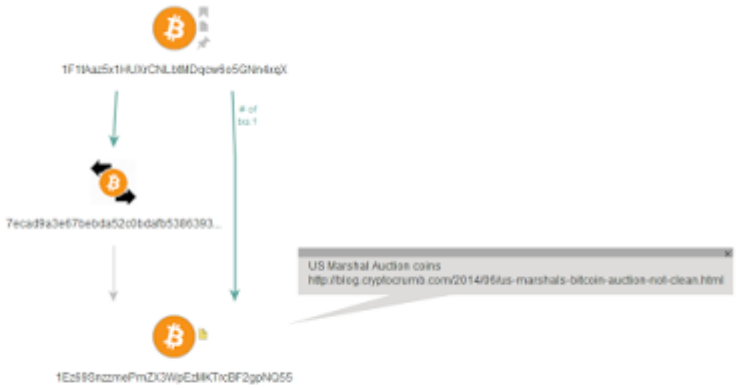

Figura 11. Entidad de transacción Bitcoin

La mayoría de las veces no se estará realmente interesado en tomar el paso intermedio de obtener la entidad de transacción primero y simplemente se puede ejecutar la transformación que lleva directamente de una dirección a otra.
A continuación se retoma la dirección original y se ejecuta la transformación (Bitcoin) To Addresses [Inputs to transactions], que devolverá direcciones Bitcoin las cuales eran entradas a transacción donde esta dirección era una salida.

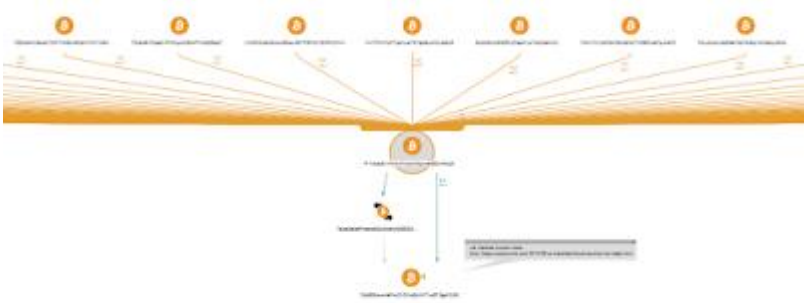

Figura 12. Transacciones bitcoin

Como es de esperar, es posible un gran número de direcciones (en teoría usada en Silk Road). La transformación devuelve la cantidad máxima de entidades de 10 000. Las entidades que se devuelven se ponderan según la cantidad de transacciones en las que estuvieron implicadas con la dirección de entrada, lo que facilita la selección de las direcciones más relacionadas con la entrada. Las entidades más relacionadas aparecerán en la parte superior izquierda del diseño del bloque, mientras que las entidades menos relacionadas se encontrarán en la parte inferior derecha.

Por último, se analizarán las transformaciones que hacen uso de los datos de Taint Analysis de Blockchain.info. Estas transformaciones permiten devolver direcciones que han enviado o recibido Bitcoins hacia o desde una dirección particular. Además, estas transformaciones tienen otro parámetro llamado Taint

Relationship que se mide como un porcentaje y representa lo fuerte que es el enlace entre las direcciones. Se ejecuta la transformación To Addresses [Using Taint Analysis] en esta dirección, mientras que especifica una Taint Relation de más del 1% de resultados en las tres entidades a continuación devuelve.

Figura 13. Vista Taint Relation

API keys para Blockchain.info

Por defecto, el Bitcoin transformer usa una clave de API de Paterva que está sujeta a ser limitada por la tasa Blockchain.info. Si la clave API obtiene una tasa limitada, recibirá un mensaje de la transformación. Para reducir las posibilidades de ser limitada, puede registrarse para obtener una API libre de Blockchain, e ingresarla en el ajuste apikey blockchain.info. Se debe además tomar en cuenta también que el punto final utilizado para Análisis de contaminación está muy limitado.

Es posible instalar el Bitcoin transformer en su cliente Maltego simplemente haciendo clic en Instalar:

Figura 14. Instalacion de cliente Bitcoin

5.1.5 Ataque de deanonimizacion de billeteras

La red Bitcoin consiste en nodos homogéneos y proporciona mecanismos de descubrimiento y reputación de pares para lograr la estabilidad.

La gran mayoría de nodos Bitcoin (los llamamos clientes), alrededor del 90%, se encuentran detrás de NAT y no permiten ninguna conexión entrante, mientras que eligen N conexiones salientes a servidores (Nodos Bitcoin con IP pública). Este capítulo está basado en la tesis de ataque deanonimizador de Alex Biryukov, Dmitry Khovratovich y Ivan Pustogarov, de la Universidad de Luxemburgo.

En una transacción Bitcoin, la dirección del remitente (s) de dinero o receptor (es) es un hash de su clave pública. Se le llama a esa dirección un seudónimo para evitar confusiones con la dirección IP del host donde se generan las transacciones, y a este último se le llama simplemente dirección en todo el texto. En el actual protocolo Bitcoin, todo el historial de transacciones está disponible públicamente para que cualquiera pueda ver cómo Bitcoins viajan de un seudónimo a otro y potencialmente enlazar diferentes seudónimos del mismo usuario.

En este capítulo se descubre un método genérico desarrollado en la Universidad de Luxemburgo para deanonimizar una fracción significativa de usuarios de Bitcoin y correlacionar sus seudónimos con direcciones IP públicas. El método apunta explícitamente a los clientes (es decir, a los pares detrás de NAT o firewalls) y puede diferenciar los nodos con la misma IP pública. Además, este método también maneja el caso cuando los clientes usan servicios de anonimato como Tor. Si un cliente utiliza dos seudónimos diferentes durante una sola sesión, e incluso si no están relacionados en el gráfico de transacciones (de modo que el enlace sería totalmente inalcanzable a través del análisis de gráfico de transacciones) es probable que este método lo capture y pegue los pseudónimos juntos. El método es genérico y puede ser utilizado en otras redes P2P.

Los nodos de la red Bitcoin se conectan entre sí a través de un canal TCP no cifrado. No hay ninguna funcionalidad de autenticación en la red, por lo que cada nodo solo mantiene una lista de direcciones IP asociadas a sus conexiones.

Para evitar ataques de denegación de servicio, el protocolo Bitcoin minimiza la cantidad de información reenviada por sus compañeros.

Los bloques válidos y las transacciones se retransmiten mientras que los bloques no válidos son descartados. Además, Bitcoin implementa un protocolo basado en la reputación con cada nodo manteniendo una penalización para cada conexión.

Cada vez que se envía un mensaje malformado al nodo, este último aumenta el puntaje de penalización de la conexión y prohíbe la dirección IP de comportamiento indebido durante 24 horas cuando la pena alcanza el valor de 100. Aunque el software oficial de Bitcoin no divide explícitamente su funcionalidad entre clientes y servidores, los pares de Bitcoin pueden agruparse en aquellos que pueden aceptar conexiones entrantes(Servidores) y aquellos que no pueden (clientes), es decir, pares detrás de NAT o cortafuegos, entre otros.

De forma predeterminada, los usuarios de Bitcoin (tanto clientes como servidores) intentan mantener 8 conexiones salientes.
Además, los servidores de Bitcoin pueden aceptar hasta 117 conexiones entrantes (teniendo así hasta 125 conexiones en total).

Si alguna de las 8 conexiones salientes disminuye, un nodo Bitcoin intenta reemplazarlas por nuevas conexiones. Si ninguna de las 8 conexiones salientes disminuye, el par permanecerá conectado a ellas hasta que se reinicie.

En caso de un cliente, se llama a los 8 nodos a los que establece nodos de entrada de conexiones. Un servidor Bitcoin acepta cualquier número de conexiones desde una única dirección IP siempre y cuando no se alcance el umbral para el número total de conexiones.

El protocolo Bitcoin implementa un mecanismo de propagación de direcciones para ayudar a los compañeros a descubrir otros compañeros en la red P2P.

Cada par de Bitcoin mantiene una lista de direcciones de otros compañeros en la red y cada dirección recibe una marca de tiempo que determina su frescura. Los nodos pueden solicitar direcciones de esta lista entre sí mediante mensajes GETADDR y publicar de manera no solicitada las direcciones conocidas por ellos utilizando mensajes ADDR.

Cada vez que un nodo Bitcoin recibe un mensaje ADDR, decide individualmente para cada dirección en el mensaje si desea reenviarlo a sus vecinos.

El protocolo comprueba primero si el número total de direcciones en el mensaje ADDR correspondiente no excede de 10 y la marca de tiempo adjunta no tiene más de 10 minutos.

Si cualquiera de estas dos comprobaciones falla, la dirección no se reenvía; De lo contrario la dirección está programada para reenviar a dos de los vecinos del nodo en caso de que la dirección sea accesible y solo a un vecino. Una dirección se considera accesible por un nodo si el nodo tiene una interfaz de red asociada con la misma familia de direcciones. De lo contrario, la dirección está marcada como inaccesible.

De acuerdo con la implementación de referencia actual, los nodos Bitcoin reconocen tres tipos de direcciones: direcciones IPv4, IPv6 y OnionCat.
Limitar el número de vecinos a los que se reenvía una dirección reduce la cantidad total de tráfico en la red Bitcoin P2P.

Para elegir vecinos a los que enviar una dirección, un nodo Bitcoin, para cada uno de sus vecinos, calcula un hash de un valor compuesto de los siguientes elementos: Dirección a remitir, una semilla secreta, día actual y la dirección de memoria de la estructura de datos que describe al vecino.

La expresión exacta del valor hash es de poca importancia para los ataques. Lo único que se debe destacar es que el hash permanece igual durante 24 horas.

El par ordena, entonces, la lista de sus vecinos basándose en los hashes calculados y elige la primera entrada o dos primeras entradas (lo cual depende de la accesibilidad de la dirección).

En el resto del trabajo se llama a estos nodos responsables los nodos para la dirección.

La transmisión real de los mensajes ADDR programados no ocurre inmediatamente. Cada 100 milisegundos un vecino se selecciona aleatoriamente de la lista de todos los vecinos de pares y la cola para los mensajes ADDR salientes se vacía para este nodo solamente.

Se llama al nodo elegido al principio de un nodo rastreador redondo de 100 milisegundos y el procedimiento en su conjunto como goteo.
Supongamos que el nodo n0 recibe un mensaje ADDR con una dirección A0 desde el nodo n3 y que el nodo n0 planifica para reenviarlo a los nodos n1 y n2 (es decir, estos nodos son nodos responsables para la dirección A0).

En la ronda 1, el nodo n1 se elige como nodo de goteo y la dirección se reenvía a este nodo mientras que la entrega de n2 sigue pendiente.

Después de 100 milisegundos en la ronda 2, otro 100 milisegundos en la ronda 3 n2 se elige como el tricklenode y la dirección A0is finalmente se envía a ella.

La elección de un nodo de goteo provoca retrasos aleatorios en cada salto durante una propagación de direcciones.

Por último, para cada conexión, un nodo Bitcoin recuerda direcciones que fueron reenviadas a través de esta conexión. Antes de que un nodo envíe una dirección, comprueba primero si la misma dirección ya fue enviada a través de la conexión.

Esta historia se borra cada 24 horas. Una nota importante es que el historial de direcciones enviadas se mantiene por conexión y no por IP, es decir, si un par Bitcoin se vuelve a conectar, su historial se borrará.

El número total de direcciones que un par de Bitcoin puede almacenar está limitado por 20480. Cada vez que las nuevas direcciones llegan a un par, reemplazan a las viejas (de acuerdo a reglas específicas que están fuera del alcance de este documento).

Asimismo cuando un nodo peer recibe un GETADDR mensajes, que envía de vuelta el 23% del número de direcciones que almacena, pero no más de 2500 direcciones. Después de la puesta en marcha, un nodo Bitcoin descubre sus propias direcciones IP, que incluye no solo sus direcciones de interfaces de red, sino también la dirección IP, ya que se ve desde la Internet (en la mayoría de los casos para los usuarios de NAT que se resuelve a una dirección IP del ISP del igual).

Con el fin de descubrir este último, los pares emiten una solicitud GET a dos sitios web codificados que responden con la dirección. Para cada dirección obtenida por el procedimiento de descubrimiento, el compañero asigna una puntuación.

Las interfaces locales obtienen inicialmente la puntuación 1, la dirección IP externa obtiene una puntuación de 4 (en caso de que la dirección IP externa

coincida con una de las direcciones locales, las puntuaciones se suman). Cuando un cliente establece una conexión de salida con un nodo remoto, primero intercambian mensajes VERSION y el cliente anuncia su dirección con la puntuación más alta.

El par remoto utiliza entonces el algoritmo de propagación de direcciones descrito anteriormente. El cliente repite el mismo procedimiento para las restantes 7 conexiones salientes.

Reenviar una transacción de un par a otro implica varios pasos. En primer lugar, el remitente transmite un mensaje INVENTORY con el hash de las transacciones.

En segundo lugar, el receptor ejecuta varias comprobaciones en la transacción y si las comprobaciones pasan, solicita la transacción real enviando un mensaje GETDATA.

A continuación, el emisor transmite la transacción en un mensaje de TRANSACCIÓN. Cuando el receptor recibe la transacción, lo anuncia a sus pares en un mensaje INVENTORY.

Cuando un cliente genera una transacción, lo programa para enviarlo a todos sus vecinos. A continuación, calcula un hash de un valor compuesto por el hash de transacción y una semilla.

Si el hash calculado tiene dos últimos bits puestos a cero, la transacción se reenvía inmediatamente a todos los 8 nodos de entrada.

De lo contrario, una cola de un vecino para las transacciones salientes se vacía cuando el vecino se convierte en el nodo trickle (lo mismo que con los mensajes ADDR). Obviamente, 14 de todas las transacciones se envían inmediatamente en promedio.

Cuando se recibe una transacción, se programa para la entrega a todos los vecinos de iguales, como se describió anteriormente. Al igual que con los mensajes ADDR, un par de Bitcoin mantiene el historial de transacciones reenviadas para cada conexión.

Si ya se ha enviado una transacción a través de una conexión, esta no se volverá a enviar. Un par de Bitcoin mantiene todas las transacciones recibidas en una agrupación de memoria.

Si el nodo recibió una transacción con el mismo hash que uno en el grupo o en un bloque de la Blockchain principal, se rechaza la transacción recibida.

Desconexión desde TOR

En esta sección se explica la primera fase del ataque. Se muestra cómo prohibir que los servidores de Bitcoin acepten conexiones a través de Tor y otros servicios de anonimato.

Esto da como resultado que los clientes utilicen sus direcciones IP reales cuando se conecten a otros pares y, por lo tanto, estén expuestos a la fase principal del ataque, que correlaciona pseudónimos con direcciones IP.

Esta fase es bastante notable, por lo que un atacante furtivo puede querer saltar y deanonimizar solo los usuarios no-Tor.

En el texto más adelante se discute sobre Tor, pero el mismo método se aplica a otros servicios de anonimato con pequeñas modificaciones.

En pocas palabras, la red Tor es un conjunto de relés (5397 para el tiempo de escritura) con la lista de todos los relés Tor disponibles públicamente en línea. Cada vez que un usuario desea establecer una conexión a un servicio a través de Tor, elige una cadena de tres repetidores Tor.

El nodo final de la cadena se denomina nodo Tor Exit y el servicio ve la conexión como se originó desde este nodo Tor Exit.

Para separar Tor de Bitcoin, se aprovecha la protección incorporada de Bitcoin DoS.

Cada vez que un compañero recibe un mensaje malformado, aumenta el puntaje de penalización de la dirección IP de la que proviene el mensaje (si un cliente utiliza Tor, el mensaje obviamente procederá de uno de los nodos de salida de Tor).

Cuando esta puntuación supera los 100, el IP del remitente está prohibido durante 24 horas. De acuerdo con la implementación de Bitcoin, hay muchas maneras de generar un mensaje que podría causar una penalización de 100 y una prohibición inmediata, p.

Se puede enviar un bloque con lista de transacciones vacías (el tamaño de un mensaje de este tipo es de 81 bytes).

Esto significa que, si un cliente utiliza un proxy para proteger su conexión sobre un repetidor de Tor y envió un mensaje malformado, la dirección IP de este repetidor será prohibida.

Esto permite separar cualquier servidor de destino de toda la red Tor. Para ello se debe conectar a la meta a través de n3, como se elige el nodo de goteo, por lo que no se produce la transmisión real en esta etapa.

Después de tantos nodos Tor como sea posible. Para la época del ataque inicial había 1008 nodos de la salida de Tor. Por lo tanto, el ataque requiere establecer 1008 conexiones y enviar unos MBytes en los datos.

Esto puede repetirse para todos los servidores de Bitcoin, prohibiendo así todas las conexiones Tor durante 24 horas al costo de un millón de conexiones y menos de 1 GByte de tráfico.

En caso de que una dirección IP de un nodo Bitcoin específico pueda ser falsificada, también puede ser prohibida.

Como prueba de concepto, se utilizó el método descrito para aislar el nodo Bitcoin de un conjunto de repetidores de salida Tor.

Posibles contramedidas

Es deseable permitir que los compañeros de Bitcoin utilicen Tor y aun así mantener alguna capacidad de lista negra. Se sugiere que cada conexión de tiempo o de computación consuma para aumentar radicalmente el coste de ataque.
Por ejemplo, cualquier compañero que inicie una conexión podría requerir presentar alguna prueba de trabajo, por ejemplo, un hash de su IP, la marca de tiempo y el nonce que tiene un cierto número de ceros finales.

Si se necesitan 32 bits cero, entonces separar un único par de la red Tor costaría alrededor de 245 cálculos de hash, lo que lleva varios días en un PC moderno.

Se puede argumentar que algunos pools de Bitcoin son lo suficientemente poderosos para permitirse muchas llamadas hash.
Sin embargo, la gran mayoría de la potencia de computación de la piscina está contenida en mineros ASIC personalizados, que implementan solo una instancia específica de SHA-256 y no pueden reconfigurarse para otra función hash, por ejemplo, SHA-3. La fracción exacta de la GPU y la potencia de la CPU de computación es desconocida, pero en el momento en que estas arquitecturas eran dominantes, la potencia total de cálculo era de varios órdenes de magnitud menor que ahora.

Topología del aprendizaje

Suponiendo que se ha descartado el caso de que los usuarios de Bitcoin usan Tor, ahora se debe dirigir a los clientes, es decir, los nodos que no aceptan conexiones entrantes, pero tienen 8 conexiones salientes (por ejemplo) a Nodos de entrada.

En esta sección se muestra cómo aprender estos nodos de entrada. El método se basa en el hecho de que cada vez que un cliente C establece una conexión con uno de sus nodos de entrada, anuncia su dirección Ca como se ve desde Internet.

Si el atacante ya está conectado a un nodo de entrada, con alguna probabilidad (que depende del número de conexiones del atacante), la dirección Ca le será reenviada. Esto sugiere la siguiente estrategia:

1. Conectarse a W servidores Bitcoin, donde W es cercano al número total de servidores.
2. Para cada Ca anunciado, se registra el conjunto E ' de servidores que reenviaron Ca a las máquinas del atacante y lo designan como el subconjunto de nodos de entrada E' Ca.

Hay dos problemas con este método. En primer lugar, el nodo de entrada puede enviar la dirección del cliente a algún par de no atacante. En segundo lugar, un cliente no se conecta a todos sus nodos de entrada simultáneamente, pero hay un intervalo entre las conexiones. En ambos casos, la dirección anunciada llega a las máquinas del atacante a través de pares que no son nodos de entrada, lo que produce entradas falsas (ruidosas) en E 'Ca.

Técnica de reducción de ruido

La estrategia propuesta para filtrar el ruido asume que ya sea el IP del cliente ya estaba utilizado en la red Bitcoin -que es bastante común para los clientes detrás

de NAT o el IP público del cliente- está contenido en una lista conocida de direcciones IP (por ejemplo, dentro de un rango IP de un ISP importante) que un atacante puede usar.

Si un atacante conoce Ca, restringe su propagación usando el siguiente hecho:

• Si la dirección ya se había enviado de A a B, no se reenviará por esta conexión; esto sugiere la difusión (broadcast) Ca (o todas las direcciones bajo investigación) a todos los servidores a los que se esté conectado. Se sugiere repetir este procedimiento cada 10 minutos, aunque podría haber otras opciones. El adversario espera que, cuando el cliente se vuelva a conectar, los nodos de entrada le envíen Ca, e incluso si no lo hacen, la propagación de la dirección se detendrá antes de que llegue al adversario a través de un nodo sin entrada.

Eventualmente, el atacante obtiene la fracción paddr de los nodos de entrada del cliente. El valor exacto de paddr depende del número de conexiones del atacante.Por ejemplo, si un atacante establece 35 conexiones a cada nodo de entrada potencial, que tenía 90 conexiones de antemano, entonces identifica 4 nodos de entrada de 8 en promedio.

Aquí hay algunos detalles adicionales. Cuando el atacante anuncia el Ca, cada servidor de Bitcoin elige dos nodos responsables para reenviar la dirección.

El atacante establece una serie de conexiones a cada servidor de la red esperando que sus nodos reemplacen algunos de los nodos responsables de la dirección Ca.

Cuando el cliente C se conecta a uno de sus nodos de entrada e1, anuncia su dirección.

Si uno de los nodos del atacante reemplazó uno de los nodos responsables, el atacante aprenderá que el cliente C podría estar conectado al nodo e1.

Si los nodos responsables no cambian la dirección, no se propagará más en la red.

Dado que el atacante anunció Ca al nodo e1, los nodos responsables de e1 podrían ser reemplazados por algunos nodos no atacantes y el ataque podría fallar.

Deanonimización

Se ha prohibido que los servidores de Bitcoin acepten conexiones de Tor y se demostró cómo encontrar los nodos de entrada de clientes. Ahora se describe la fase principal del ataque de deanonimización, que consta de cuatro pasos:

1. Obtener la lista S de servidores. Esta lista se actualiza periódicamente.
2. La composición de una lista C de clientes de Bitcoin para la deanonimización.
3. Aprendizaje de nodos de entrada de clientes de C cuando se conectan a la red.
4. Escuchar servidores de S y asignar transacciones a nodos de entrada y luego a clientes.

Finalmente, se crea una lista I = {(IP, Id, P K)}, donde IP es la dirección IP de un nodo o su ISP, Id distingue a los clientes que comparten la misma IP, y P K es el seudónimo utilizado en una transacción (hash de una clave pública). Se van a explicar los pasos en detalle.

Paso 1. Obtener la lista de servidores.

Esta fase del ataque es bastante sencilla. Un atacante primero recolecta toda la lista de pares consultando a todos los compañeros conocidos con un mensaje GETADDR.

Cada dirección P en el mensaje ADDR de respuesta se puede comprobar si está en línea, estableciendo una conexión TCP y enviando un mensaje VERSION. Si lo es, P se designa como un servidor.

Un atacante puede iniciar el procedimiento consultando un pequeño conjunto de nodos de simulación y continuar consultando las direcciones IP recién recibidas. El adversario establece m conexiones a cada servidor (la sugerencia es 50 para el tamaño de la red Bitcoin actual).

Paso 2. Composición de la lista de deanonimización.

El atacante selecciona un conjunto C de nodos cuyas identidades quiere revelar. Las direcciones pueden provenir de varias fuentes.

El atacante podría tomar rangos de IP de los principales proveedores de servicios de Internet, o recopilar direcciones ya anunciadas en la red Bitcoin.

Finalmente, podría tomar algunas entradas de la lista de pares que obtuvo en el Paso 1.

Paso 3. Asignar clientes a sus nodos de entrada.

Ahora el atacante identifica los nodos de entrada de los clientes que se conectan a la red. Equipado con la lista C de direcciones, el atacante ejecuta el procedimiento descrito en la Sección 4.

Se va a estimar cuántos nodos de entrada se necesitan para identificar de forma exclusiva al cliente.

El conjunto de nodos de entrada para P por E P. Se hace hincapié en que es posible que EP16 = EP2 incluso si P1 y P2 comparten la misma dirección IP. Para cada P que anuncia su dirección en la red el atacante obtiene un conjunto de

E 'P⊆ EP

Dado que hay alrededor de 8 · 10^3 posibles nodos de entrada de un total de 105 pares (servidores y clientes juntos), las colisiones en E'P son improbables si cada tupla tiene al menos 3 nodos de entrada:

10^5 · 10^5 / (8*10^3) ^3 tendiendo a 1.

Por lo tanto, 3 nodos de entrada identifican de forma exclusiva a un usuario, aunque dos nodos también lo hacen para un gran porcentaje de usuarios.

Un atacante agrega EP a su base de datos y procede a Paso 4.

Paso 4. Asignar las transacciones a los nodos de entrada. Este paso se ejecuta en paralelo a los pasos 1-3. Ahora un atacante trata de correlacionar las transacciones que aparecen en la red, con los conjuntos E'P obtenidos en el paso 2. El atacante escucha los mensajes INVENTORY con los hashes de transacción recibidos sobre todas las conexiones que estableció y para cada transacción T Ella recoge RT ,las primeras direcciones q de los servidores Bitcoin que enviaron el mensaje INVENTORY.

Luego compara E'P con RT (ver detalles a continuación), y las entradas coincidentes sugieren pares (P, T). En los experimentos efectuados se tomaron q = 10.

Podría haber muchas variantes para el procedimiento de coincidencia, y se sugiere la siguiente versión:

• El atacante compone todas las posibles 3-tuplas de todos los conjuntos E'P y busca sus apariciones en RT.

Si hay una coincidencia, se consigue un par (R, T);

• Si no hay coincidencia, el atacante considera 2-tuplas y luego 1-tuplas. Varias parejas {(Pi, T)} pueden ser sugeridas en esta etapa, pero pueden ser filtradas con transacciones posteriores.

Las 2-tuplas pueden sugerir diversos pares, cada cliente tiene 2^5 2-tuplas de nodos posibles de entrada, mientras el top10 sugiere 2^5.5 2-tuplas. La probabilidad de coincidencia se calcula en 2^-26, lo que implica que el top-10 sugiere 2^(16.5+10.5-26) = 2 clientes en promedio de la regla 2-tupla. La probabilidad para que el cliente correcto sea detectado es del 28% aproximadamente.

Capítulo 6. Conclusiones y Recomendaciones

6.1 Conclusiones

- El marco de referencia permitió documentar de una manera ágil, pero a la vez detallada, distintas técnicas que pueden ser utilizadas por un agente de la ciberseguridad para rastrear potenciales sospechosos de crímenes cometidos por medio de la criptomoneda Bitcoin.
- Se logró, por medio de esta investigación, el entender a fondo el protocolo Bitcoin, así como le metodología Blockchain, los cuales son los elementos esenciales para explicar la funcionalidad de Bitcoin. Además se determinó cómo estos se pueden resguardar, por medio de los conceptos explicados en el marco de referencia.
- Las instituciones nacionales requieren de entrenamiento especializado en investigación técnica de los diversos recursos utilizados por los criminales y sus cómplices.
- El marco de referencia propuesto y desarrollado obtuvo gran aceptación por parte del departamento técnico del OIJ; mas los comentarios recibidos indican recursos muy limitados a la hora de desarrollar herramientas para implementar las técnicas descritas. Asimismo los investigadores expresaron un interés en que se

desarrollara una versión del manual con entrenamiento y herramientas incluidas

- El análisis de la metodología propuesta por los recursos técnicos de la institución policíaca fue satisfactorio, en el tanto que se mostraron muy complacidos e intrigados por el método y la evidencia matemática de los resultados por obtenerse de utilizarse la propuesta.

6.2 Recomendaciones

Dentro de lo que se recomienda a la luz de esta investigación, se identifica lo siguiente:

- El escenario ideal dicta que, para producir un manual más exhaustivo, es necesario un equipo más grande de personas (recursos especializados en el área de seguridad, programación, redes), para lograr un resultado final mucho más ajustado a las necesidades del día a día en estas agencias, y según la realidad del país y del planeta, con respecto a los fraudes cometidos por medio del Bitcoin.
- Conducir una investigación longitunal (a lo largo de más tiempo) para resolver más ataques, así como enfocar el análisis a más criptomonedas. Bitcoin es la más común y la pionera, sin embargo, hoy se deben comprender las vulnerabilidades que puedan surgir con el uso de otras criptomonedas.

Capítulo 7. Reflexiones Finales

Durante la evaluación del proyecto por el departamento de delitos informáticos del OIJ, se demostró una deficiencia en cantidad de recursos que influyó en el tiempo y la cantidad de reuniones que se realizaron, asimismo se

expresó la falta de equipos, tanto humanos como técnicos, para llevar a cabo las simulaciones necesarias para practicar las técnicas descritas.

Es un hecho que, en la cultura del país, no ha sido una prioridad el entrenar a personas de acuerdo con sus roles y más bien depende de actitudes individualistas el desarrollo de habilidades dentro del campo de acción.

Los investigadores consideran que es imperativo el cambiar este modo de actuar, debido a la evidencia del mundo global en que ha venido evolucionado el ambiente, no es una opción mantener a personas con entrenamiento y equipo incompleto en posiciones de tal responsabilidad como la aplicación de la ley.

Capítulo 8. Trabajos a Futuro

De momento el alcance final de esta investigación resulta ser el manual producido, sin embargo, para futuro se desea ampliar la investigación a otras técnicas, así como otras criptomonedas.

Los cibercriminales van ganando en sofisticación, de modo que se requiere estar a la vanguardia en temas de defensa.

Referencias

Birkuyov , A.; Khovratovich, D. y Pustogarov I. (2014). Deanonimización de clientes en una red Bitcoin P2P. Pp.4-53. University of Luxemburg. Tomado de: http://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf

Sameeh T.,(2017). Bitcoin and Money Laundering – Challenges for Law Enforcement Agencies. Tomado de: https://www.deepdotweb.com/2017/03/18/bitcoin-money-laundering-challenges-law-enforcement-agencies/

Shaw, T.,(2015). Proposed Bitcoin Rules Could Make or Break User Privacy. Tomado de: https://iapp.org/news/a/proposed-bitcoin-rules-could-make-or-break-user-privacy/

Weinstein, J.,(2015). Why Bitcoin Is Good for Law Enforcement. Tomado de: https://iapp.org/news/a/why-bitcoin-is-good-for-law-enforcement/

Blockchain.info. (2013). Conformación de los bloques y definiciones. Tomado de: https://www.blockchain.com/

Nakamoto, S.,(2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Pp4-10. Tomado de: https://bitcoin.org/bitcoin.pdf

Apéndices