Facultad de Informática

Trabajo Final Integrador de Especialidad

Título

Análisis del anonimato aplicado a criptomonedas

Carrera

Especialidad en Redes y Seguridad

Tesista

Ing. Ignacio Martín Gallardo Urbini

Directora

Dra. Patricia Bazán

Codirectora

Lic. Paula Venosa

La Plata, Argentina. Año 2017

Índice

Resumen

Este trabajo final integrador muestra un estudio en profundidad de la tecnología Bitcoin, en el cual se aborda un análisis cualitativo de sus funcionalidades y arquitectura. También describe diferentes técnicas y fines de usos que potencialmente un usuario podría llegar a realizar con esta tecnología. Por último presenta un análisis de la posibilidad de aplicación de diferentes prácticas de descubrimiento ante la presencia de una investigación del uso cibercriminal de criptomonedas.

Introducción

El derecho a la privacidad y el anonimato son temas que hoy en día despiertan el interés no solo de empresas particulares, sino que también para cibercriminales o eventos similares a los ocurridos en los últimos tiempos, como conocer detalles delicados acerca de los documentos filtrados por Edward Snowden[3] y las actividades desempeñadas por organizaciones como la NSA[1] o la CIA[2]. Se trata de cuestiones que ponen de manifiesto lo que muchos ya saben cuando navegan por internet: Toda actividad en la red está siendo monitoreada.

Muchas de estas actividades de monitoreo o vigilancia son llevadas a cabo por entidades gubernamentales, cuya finalidad es la de intentar detectar amenazas terroristas, actuar en consecuencia para minimizar su impacto, o tracear la amenaza para ejecutar acciones ofensivas, disuasivas y/o defensivas.

Evidentemente muchas personas obran por tener privacidad y no ser monitoreados, por esto en la actualidad han surgido diferentes herramientas que ayudan a proporcionar privacidad y anonimato en internet. Estas soluciones tecnológicas poseen además de una vía alternativa a los sistemas de monitoreo utilizados por los gobiernos, sistemas de tracking que son utilizados por organizaciones de marketing para perfilar a los usuarios y ofrecer productos acorde a sus patrones de navegación.

Dichas soluciones también suponen una amenaza para la privacidad, ya que se encargan de recolectar datos de navegación, información sobre realización de pagos y análisis de diferentes patrones de uso que cualquier usuario desearía mantener en secreto, ya que evidentemente forman parte de su vida privada. No obstante, el caso en donde este tipo de herramientas adquieren una relevancia mayor, es en países donde restringen el acceso a internet o donde los habitantes no poseen la posibilidad de informar al mundo sobre los abusos que sufren por parte de sus respectivos gobiernos, como por ejemplo, China o Norcorea. Finalmente, estos beneficios que aportan los sistemas de anonimato, también suelen ser utilizados por grupos de activistas o cibercriminales para realizar extorsiones o estafas financieras en la red.

Es útil plantear una distinción básica entre la privacidad y el anonimato en el contexto de las transacciones financieras. Se define una transacción financiera "anónima" al desconocimiento total por parte del contexto hacia el actor que la realiza. Por otra lado, se llama operación financiera "privada", si el producto de compra y su cantidad son desconocidos, pero no sus actores.

El dinero en efectivo o trueque proporcionan máximas características de privacidad y anonimato esencialmente al momento de realizar transacciones. Por otra parte, y de

[1] National Security Agency.

[2] Central Intelligence Agency.

manera contraria, existen las transacciones que no son ni privadas ni anónimas, y esto contempla, por ejemplo, donaciones de cierta cantidad de dinero, compras mediante tarjetas de débito/crédito, pago por transferencias bancarias, etc., en donde la identidad del ente comprador se encuentra almacenada y relacionada con la entidad vendedora junto al detalle de la transacción y, no obstante, ante ciertas situaciones esta información podrá eventualmente ser accedida.

Desde el punto de vista de **Bitcoin**[1], las transacciones no presentan características de privacidad, pero sí de anonimidad, es decir, las identidades no se registran en ninguna parte del **protocolo Bitcoin**, pero cada transacción realizada es visible en un "libro electrónico público" y distribuido, conocido como **blockchain** o **cadena de bloques**[2].

Estas características proporcionadas por **Bitcoin** alteran el principio de la regulación financiera y se convierte potencialmente en un mecanismo de pago generalizado entre los cibercriminales. Es por ello que en muchas ocasiones los investigadores forenses se tienen que enfrentar ante los desafíos que conlleva su investigación debido a la utilización de esta tecnología para el cobro anónimo de extorsiones o de servicios fraudulentos llevados a cabo por algunos grupos de ciberdelincuentes.

Objetivos

Objetivo General

El objeto general del presente trabajo final integrador consiste en abordar un análisis de anonimidad en ***blockchain***[3] aplicado al uso diario de las **criptomonedas**[4]. Se pretende que a partir de un estudio de los conceptos técnicos pertinentes se permita comprender los distintos usos para los que se pueden utilizar estas formas de pago, por ejemplo, en el caso del uso por parte de los cibercriminales en la red y la complejidad que una investigación por parte de las fuerzas de seguridad debería abordar ante la presencia de dicho fenómeno.

Objetivos Específicos

Como objetivos específicos se fijaron los siguientes:

- Introducir y definir teóricamente el concepto de **criptodivisas**, entrando en detalles con **Bitcoin**.
- Describir el funcionamiento de **blockchain**.
- Detallar de forma clara el manejo de **criptomonedas**.
- Explicar el punto de convergencia entre las **criptomonedas** y la ***deep web***[5].
- Analizar la posibilidad de existencia de un método de investigación y traceo ante un ciberdelito por medio del cual se utilizaron **criptomonedas**.
- Proporcionar un material de referencia en español con respecto a este área de conocimientos.
- Aportar conocimientos básicos de los conceptos técnicos a un lector no familiarizado con los términos utilizados en el área.

[3] Cadena de bloques: columna vertebral sobre la cual descansan las arquitecturas de las criptomonedas.

Motivación y Estado del Arte

Los malwares o virus informáticos se presentan de diferentes formas y los ataques que adoptan los mismos se llevan a cabo de manera cada vez más sofisticada y difíciles de identificar. El motivo principal puede ser el de conseguir datos personales, encriptar archivos para luego poder extorsionar o simplemente desestabilizar una organización o gobierno. Los targets[4] principales de estos ataques se clasifican en dispositivos inteligentes de cualquier tipo como: móviles, computadoras, cámaras de vigilancia y vehículos conectados.

De acuerdo a una encuesta realizada a más de 4.000 compañías en Latinoamérica, se considera que, diariamente, casi dos millones de usuarios en el mundo son víctimas de un ataque informático y en lo que va del año, el 49% de las empresas tuvo una infección por malware; el 15 % fue víctima de phishing y el 16% de **ransomware**[5].

Detrás de estos delitos no hay un cibercriminal, ni dos, ni tres; hay toda una industria que trabaja en red. Se trata de un entramado que se mueve en la ***deep web*** donde muchos de "los trabajos" se cobran en **criptomonedas**.

En el nivel más bajo de la pirámide está el ***script kiddie***, un término despectivo para describir a quienes utilizan programas o scripts de otros para vulnerar sistemas informáticos. Ellos no desarrollan malwares, sino que se hacen de archivos o datos que obtienen en foros o por otra vía para realizar sus ataques.

En un nivel más avanzado se encuentran los ***hackers*** con ciertos conocimientos técnicos, algunos, incluso están graduados en alguna carrera de informática o sistemas. Ellos, por ejemplo, se encargan de publicar ***exploits***[6], que son programas que se aprovechan de un agujero de seguridad en una aplicación o sistema. Un exploit no es, en sí, un código malicioso, sino "la llave" o el modo en que se puede acceder al sistema.

Encontrar y vender un exploit es legal siempre y cuando se utilice con fines éticos. De hecho hay empresas como ***Zerodium*** que compran los exploits para desarrollar soluciones de seguridad basada en esa información. El camino ilegal sería vender eso datos a cibercriminales que la utilizan para realizar ataques.

Los ***exploits*** para antivirus hoy en día se encuentran en torno a los 4,43 bitcoins (40 mil dólares) y los que son para sistemas operativos como el de Apple tienen un tope de hasta 166 bitcoins (1,5 millones de dólares).

[4] Objetivo de un ataque.

[5] Software malicioso que al infectar el equipo le da al ciberdelincuente bloquea la PC desde una ubicación remota y encripta los archivos quitando el control de toda la información y datos almacenados, por los cuales se exige un pago extorsivo en Bitcoins.

[6] Software malicioso que busca explotar vulnerabilidades en sistemas informáticos.

También se rentan ***botnets***[7] por entre 0,02 y 0,04 bitcoins (170 y 350 dólares) por hora para enviar ***Spam***[8] o hacer ataques de ***DNS***[9] como el que ocurrió a fines de 2016 y que dejó a los principales sitios web del mundo sin servicio.
La realidad es que es cada vez más fácil y más masivo el acceso y utilización de las criptomonedas para cobros anónimos de dinero, especialmente **Bitcoin**, lo que converge en moneda corriente a la hora de hablar de cibercriminales, pagos extorsivos y lavado de dinero. Por este motivo surge la necesidad de contar con conocimientos y procedimientos al momento de toparse con la necesidad de realizar un análisis activo o pasivo ante un cibercrimen.

Proyectos como los siguientes quieren hacer Bitcoin mucho más accesible y confiable:

- *Wayniloans*: una comunidad latinoamericana de préstamos basada en Bitcoin (P2P Lending).[6]
- *Cubits* y *Kraken*: plataformas para comprar y vender bitcoins, ya sea con euros y dólares, a través de tarjetas de crédito.[7]
- *Xapo*: plataforma que permite gestionar bitcoins con la mayor seguridad financiera, incluso en bóvedas físicas.[8]

Proyectos relacionados con criptomonedas alternativas:

- *Ripple*: es un proyecto basado en un pequeño software libre que persigue el desarrollo de un sistema de crédito basado en el paradigma de compañero a compañero.[10]
- *Litecoin*: criptomoneda de tipo punto a punto que permite realizar pagos instantáneos y de costo casi cero a cualquier parte del mundo.[9]
- *Ethereum*: criptomoneda presentada como una alternativa cercana a Bitcoin.[11]

Casos documentados de pagos extorsivos por medio de criptomonedas y usos cibercriminales:

- *Oficina del Fiscal de Estados Unidos pagó $1400 en bitcoins a extorsionistas de software malicioso.*[12]
- *Extorsión por medio ataques DDOS.*[13]
- *Detención de hacker uruguayo por extorsión mediante bitcoins.*[14]
- *El director del mayor banco de EE.UU. cree que Bitcoin es una moneda para traficantes, criminales y dictadores.*[15]
- *Cómo un día Ransomware y Bitcoin se volvieron socios.*[16]
- *Surcorea en alerta tras extorsión por bitcoins a siete bancos del país.*[17]
- *Deep web y Criptomonedas.*[18]

[7] Conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática
[8] Correo basura o mensaje basura hace referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo).
[9] Sistema de nombres de dominio.

Capítulo 1 - Privacidad y Anonimato

Introducción

La **identidad** es aquella atribución que permite ser únicos como personas en el planeta, proporcionando atributos propios como el aspecto físico, personalidad, origen, nombres, relaciones personales y muchas otras peculiaridades más. Gracias a la **identidad** se puede acceder a infinidades de funciones y beneficios, que se obtienen mediante documentos de identificación que acrediten que una persona es quien dice ser y que todo lo que se le es asignado a la misma sea a esa y no a otra. Estas características gozadas por la **identidad** son las que permiten a las personas a relacionarse con otras, más aún en un mundo donde el delito y la desconfianza perseveran como una constante al momento de entablar cualquier tipo de relación interpersonal. No obstante, en la actualidad el mundo exige a las personas estar suficientemente identificados para salir adelante. Esto permite generar las condiciones jurídicas y de confianza de que el individuo o la persona jurídica que se tiene enfrente, corresponde con lo que dice ser. Es esa certeza la que ofrece el mínimo de convicción en todas las actividades humanas, aquéllas que se llevan a cabo diariamente y las cuales están sustentadas en un sistema jurídico, o en un sistema de normas no jurídicas que constituyen un rol socialmente esperado.
En contraparte se encuentra el **anonimato**, que tiene diversas caras que comienzan en el derecho a la **privacidad**, siguen por las actividades de esa índole, hasta llegar a las delictivas.

Privacidad en el Ciberespacio

Dado a que la información es indispensable al momento de tratar la privacidad en el ciberespacio, surge una pregunta técnica: ¿cómo se entiende la privacidad en términos de información?.
Debido a que desde el punto de vista tecnológico, la diseminación de la información se puede realizar tanto de forma autorizada como no autorizada por el dueño de la misma, y puede hacerse tanto de forma discernida como involuntaria, parte del debate sobre privacidad se realiza en términos de acceso, es decir, que cuanto menos acceso a la información, más privacidad se gozará, y recíproco, cuanto más acceso, menos privacidad.
El control de la información no debe simplemente ser definitorio para la privacidad, es decir, no puede ser su único componente. Su importancia tiene que estar determinada en

otro u otros aspectos que no sean el simple hecho de acceder a información confidencial o privada. Si bien es cierto que este acceso puede suponer una violación de la privacidad y por lo tanto debe ser importante para la misma, también es cierto, que ese mismo acceso a la información puede mantener intacta la privacidad de la persona relativa a la información dada u obtenida. Existe, sin embargo, un desarrollo de la teoría de la privacidad como acceso que afirma que ésta no tiene que ver con el simple control del acceso a la información sino con un acceso restringido a dicha información [19].
La privacidad es uno de los derechos fundamentales incluidos en la declaración universal de los derechos humanos y no solamente es vital que los usuarios sean conscientes de su importancia, sino que también son libres de exigir a los administradores de aquellos servicios que gestionan información confidencial en internet, ya que la "trivialidad" de poseer datos personales de los diferentes usuarios, puede causar la utilización potencial por terceros de forma arbitraria e irresponsable, con las consecuencias que aquello implica para el dueño de la información.

Anonimato en el Ciberespacio

Dado a que la privacidad es indispensable al momento de tratar la anonimidad en el ciberespacio, este último tiene que ver con la atención puesta en una persona o grupo de personas. De esta forma cuando se habla de anonimato en el ciberespacio se podría interpretar como aquella propiedad que uno posee para garantizar que el acceso o conexión de uno mismo a este espacio informacional no se conozca; mientras que con la privacidad se logra la protección de la información por medio del acceso y/o publicaciones en este mismo espacio.
Existen dos tipos de anonimato en el ciberespacio. Por un lado, está el anonimato a nivel dispositivo, por otro, se tiene el anonimato en la red. El primero contempla todo lo que tenga que esté relacionado con los datos/información alojados en el dispositivo principal correspondiente al acceso al ciberespacio. El segundo trata de abarcar todo lo referido a los datos/información que corresponde con los "rastros" dejados en la red (ya una vez accedido al mismo), es decir, que un tercero sepa quien es el que está navegando por el mismo. No obstante, el anonimato en la red es la mejor forma de mantener la privacidad en el ciberespacio.
El ciberespacio ya tiene forma de lugar anónimo. La mayoría de las personas navegan por una red superficial, visible y pública para la mayoría de usuarios y empresas. Pero hoy en día existen herramientas como por ejemplo, la red llamada ***deep web***, que permite a sus usuarios nó solo navegar en la red de forma privada, sino también de forma anónima, por medio de la arquitectura interna y la manera de acceder y conectarse a la red; o las financiaciones por medio de **criptomonedas**, que permiten realizar pagos en todo el mundo prácticamente sin dejar rastros de quienes los realizan o los reciben.

Consideraciones Generales

Como ya se ha nombrado anteriormente, hoy en día existen infinidad de herramientas gratuitas, de muy sencillo acceso y fácil uso, que permiten a los usuarios lograr un alto grado tanto de privacidad como de anonimato en el ciberespacio. Aunque se trata de soluciones de software pensadas para una finalidad completamente defensiva e inofensiva y con el objetivo de ayudar a personas a hacer valer sus derechos fundamentales, también han sido utilizadas por el ciberterrorismo/cibercriminales que hallan en ellas una solución cuasi perfecta para pasar desapercibidos y cometer indiscriminadamente delitos de manera privada y anónima.

La utilización de sistemas que proporcionan anonimidad se ha convertido en estos últimos años en la manera primordial de comunicación por parte de mafias, miembros del crimen organizado, pedófilos, narcotraficantes, ciber extorsionistas, etc. Es por esto que, organizaciones gubernamentales de lucha contra estas fuerzas, centran gran parte de sus esfuerzos en investigaciones forenses para lograr desenmascararlos.

Para finalizar este capítulo, es importante destacar que no existen la privacidad y anonimato absolutos en el ciberespacio, existen soluciones que dificultan ciertos ataques, ayudan a asegurar el canal de comunicación entre los interlocutores, y proporcionan la posibilidad de dejar los menos rastros posibles. Un usuario de estos sistemas puede poseer o no conocimientos profundos de como utilizarlos adecuadamente y emplea su sentido común para hacerlo, por consiguiente, es posible que su anonimato no sea tan robusto como esperaba debido a vulnerabilidades en el software utilizado, errores de configuración del mismo u otros factores no contemplados. Por este y otros motivos, es que existen cuestionamientos y surgen estudios acerca de qué tan robusto es el anonimato/privacidad que proporcionan estos sistemas.

Capítulo 2 - Criptomonedas

Introducción

El comercio en Internet ha llegado a depender casi exclusivamente de las instituciones financieras que actúan como terceros de confianza para procesar pagos electrónicos. Si bien el sistema funciona lo suficientemente bien para la mayoría de las transacciones, todavía sufre las debilidades inherentes del modelo basado en la confianza.
Las transacciones completamente irreversibles no son realmente posibles, ya que las instituciones financieras no pueden evitar disputas mediadoras. El costo de la mediación aumenta los costos de transacción, limitando prácticamente al tamaño mínimo de la transacción y eliminando la posibilidad de pequeñas transacciones eventuales, y hay un costo más alto en la pérdida de capacidad para realizar pagos no reversibles por servicios no reversibles. Con la posibilidad de reversión, la necesidad de confianza se extiende.
Se acepta un cierto porcentaje de fraude como inevitable. Estos costos e incertidumbres de pago se puede evitar en persona mediante el uso de la moneda física, pero no existe ningún mecanismo para realizar pagos sobre un canal de comunicaciones sin una parte confiable.
Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, permitiendo que dos partes interesadas tramiten directamente entre sí sin la necesidad de un tercero confiable. Las transacciones que no son viables desde el punto de vista informático protegerían a los vendedores contra el fraude, y los mecanismos de custodia de rutina podrían implementarse fácilmente para proteger a los compradores. Las criptomonedas, proponen una solución a problemas como el de doble gasto utilizando una arquitectura distribuida (peer to peer) para generar una prueba computacional del orden cronológico de las transacciones. El sistema es seguro siempre que los nodos "honestos" controlen colectivamente más potencia de CPU que cualquier otro grupo cooperante de nodos atacantes[20].
Una criptomoneda es un medio de cambio digital que utiliza además de la arquitectura descrita arriba, una tecnología criptográfica para asegurar la veracidad de las transacciones.
Se puede entender a la transferencia de una moneda digital como el endoso de un cheque, es decir, análogamente a que una persona escriba en el dorso el destinatario del dinero, y este puede a su vez endosarlo nuevamente. También se puede saber si la persona que se lo dió o bien fue el dueño del cheque, o bien fue el último en endosarlo antes que él.
En el ciberespacio, se puede lograr algo similar con firmas digitales y hashes criptográficos, es decir, cuando una persona quiere transferir dinero digital a otra, se crea

una transacción, que no es más que la firma digital del hash criptográfico de la transacción anterior que usó ese dinero y la clave pública del destinatario. De esta forma, el destinatario puede verificar que el emisor era realmente el dueño del dinero, verificando la firma digital contra la transacción con el hash dado, y además, puede volver a transferirla usando él su clave privada.

La primera aparición pública de las criptomonedas tuvo origen con ***Bitcoin***, donde un usuario con el pseudónimo "Satoshi Nakamoto" anunció, el 1 de noviembre de 2008, su investigación en un nuevo sistema de dinero digital, resumiendo sus propiedades y el contenido del artículo original que describía su trabajo, el cual se encontraba disponible en el portal de Bitcoin[1].

El 11 de febrero de 2009, un perfil creado en el portal P2P foundation[21], también con el nombre de "Satoshi Nakamoto", publicó el siguiente mensaje: "Bitcoin open source implementation of P2P currency". En el texto, "Nakamoto" daba a conocer el portal oficial de Bitcoin, las características fundamentales de éste, el artículo donde se describe el diseño e, incluso, el cliente inicial con el que comenzar a participar en la red.

Bitcoin

Antes de entrar en detalles técnicos, resulta útil resaltar que la novedad y éxito de Bitcoin radica en su forma de funcionamiento distribuido y sin una autoridad central que regule la emisión de moneda, o acepte o deniegue transacciones. Básicamente son los nodos pertenecientes a la red los que implícitamente toman estas decisiones de forma "democrática". Por medio de conceptos que serán expuestos a continuación, es posible lograr entender el paradigma a través de los siguientes ejemplos:

- Los usuarios reciben bitcoins a modo recompensa por haber colaborado con la red (más adelante se verá cómo se produce esto). Hasta acá, puede parecer que los usuarios podrían engañar al sistema para aumentar su recompensa pero, por construcción del sistema, la mayoría de los usuarios tendrán que validar posteriormente esa recompensa. Así, si el usuario la aumentase de forma oculta, esa acción sería rechazada por el resto.
- Un usuario A realiza una transferencia de bitcoins a B. Para evitar que posteriormente A vuelva a utilizar esos mismos bitcoins para pagar a un tercer usuario C, en Bitcoin, las transacciones se hacen públicas, no obstante, cuando el resto de la red detecte esta inválida segunda transacción, la rechazará, imposibilitando dicha reutilización de bitcoins por parte del usuario A.

Como se aprecia en estos ejemplos, son los mismos usuarios los que toman las decisiones que normalmente corresponden a una única autoridad central. Esto hace que Bitcoin sea una moneda "democrática". Como en cualquier democracia, su evolución se adapta a lo que la mayoría de la población quiere. Por consiguiente, en este caso no hay una equivalencia de "un usuario = un voto", ya que el peso de cada usuario depende de la

potencia de cómputo que éste dedica a la red. Así, la ecuación anterior en Bitcoin, sería más bien "x% de cómputo = x% de votos". Por lo tanto, siempre y cuando más de un 50% de la potencia de cómputo de la red sea controlada por usuarios honestos, la red seguirá la evolución que estos decidan. La idea puede contemplarse como una "democracia ponderada" en función de las implicancias en el sistema.
Descripto esto, Bitcoin genera un nuevo paradigma económico y social, ya que de adoptarse Bitcoin, o un sistema de criptomonedas equivalente, los gobiernos y autoridades financieras no podrían controlar la evolución del dinero de una forma directa, pero sí influenciar de forma indirecta legislando sobre ella, pero nunca controlar su lógica funcional de negocio. No obstante, una criptomoneda no tiene un carácter nacional, sino internacional. Por lo tanto, legislar sobre ella de manera efectiva es más complicado. Además, considerando esta diversidad de escenarios sin precedentes en la teoría económica, los efectos de una aceptación y uso masivos de la moneda son impredecibles.

El papel de la criptografía

Las soluciones de alta complejidad como ser la implementación de estas criptomonedas, generalmente se respaldan por un conjunto de primitivas avanzadas. Sin conocer las mismas, no es posible comprender cómo se consiguen muchas de las propiedades anunciadas por el sistema. Por consiguiente, una vez adquirido un conocimiento general del sistema y antes de seguir describiendo cómo funciona en su totalidad, es necesario definir las primitivas indispensables que se apoderan del core del funcionamiento[27].
El término criptografía, procedente del griego *kriptos grafein* (escritura oculta), hace referencia al conjunto de técnicas y métodos que tienen como objetivo principal la transformación de información en una codificación que resulte ilegible para todas aquellas entidades que desconozcan alguno de los parámetros involucrados en dicha transformación. Se trata de una necesidad básica en el ámbito de la protección de las comunicaciones, que ha tomado gran importancia con el auge de las redes de comunicaciones.
Los elementos de un sistema criptográfico son los **métodos** utilizados para el cifrado y descifrado de información (los cuales pueden coincidir), la **clave** empleada como parámetro de dichos métodos, y el **espacio** en el cual se encuentran definidos tanto el mensaje a codificar (denominado también texto plano) como su representación codificada (denominada también texto cifrado). En función de que la clave empleada para cifrar coincida o no con la clave utilizada para descifrar, los sistemas criptográficos se agrupan en dos grandes bloques: sistemas criptográficos **simétricos** y sistemas criptográficos **asimétricos**.
La **criptografía simétrica** se caracteriza por emplear la misma clave tanto para cifrar como para descifrar un mensaje. En la mayor parte de los casos, el parámetro que se supone secreto para que la información sea protegida de la interceptación de terceras personas es la clave empleada. Es un hecho contrastado que la seguridad de un sistema criptográfico

no puede recaer en el desconocimiento por parte de la comunidad del funcionamiento interno de los algoritmos de cifrado o descifrado. Un exponente de la robustez del sistema es que dichos algoritmos sean públicos, de forma que su fortaleza pueda ser sometida a juicio público y que la seguridad del mismo recaiga solamente en la no revelación de la clave empleada.

A este tipo de sistemas criptográficos se los conoce también como de secreto compartido, y su correcto funcionamiento recae en la distribución confidencial de la clave a las entidades que formarán parte de la comunicación. Sin embargo, es la propia necesidad de compartir dicho secreto la que limita en muchas ocasiones el uso de este tipo de criptografía a la hora de poner en contacto entidades sin ningún tipo de relación previa. El

uso aislado de la criptografía simétrica queda reducido a aquellos ámbitos en los cuales los participantes disponen de algún tipo de medio de comunicación externo mediante el cual puedan realizar una transmisión confidencial previa del secreto a compartir. Otra posibilidad es emplear los denominados centros de distribución de claves (KDC, Key Distribution Center), los cuales actúan como terceras partes confiables a la hora de suministrar las claves que protegerán las futuras comunicaciones a realizar por parte de las entidades del sistema. No obstante, el uso de KDCs plantea también serios inconvenientes en lo que se respecta a privacidad, suplantación de identidad o disponibilidad.

El hecho de que coincida la clave empleada para cifrar y descifrar lleva también otra serie de limitaciones en la aplicación de este tipo de criptografía. Por un lado, es necesario generar una clave distinta por cada par de entidades que deseen proteger su comunicación. En consecuencia, dado un sistema con **"n"** usuarios finales, el número total de claves necesarias para poner en conectar a todos los usuarios entre sí es del orden **O(n^2)**, lo cual puede llegar a limitar su escalabilidad. Por otra parte, el hecho de que dos usuarios compartan el mismo secreto hace imposible determinar con seguridad quién cifró o descifró una determinada información, lo cual impide que pueda ser utilizada como mecanismo de no repudio o de autenticación de la identidad.

La particularidad de la **criptografía asimétrica** con respecto a la anterior descrita es que las claves no son únicas, sino que forman pares compuestos por una clave privada y una clave pública. Cada usuario del sistema dispone de un par de claves único y, a diferencia de lo que sucedía con la criptografía simétrica, la clave privada no es un secreto compartido sino que debe ser protegida por cada usuario. Sin embargo, la clave pública debe difundirse con el fin de que otras entidades puedan emplearla para proteger las comunicaciones realizadas con el usuario en cuestión. Este tipo de criptosistema se basa en el hecho de que resulta computacionalmente intratable intentar descubrir una clave a partir del conocimiento de la otra, lo cual anula la necesidad de establecer secretos compartidos entre entidades ya que basta con tener acceso a las claves públicas.

Lo que resulta interesante del uso de muchos de los sistemas basados en este tipo de criptografía es que las operaciones realizadas con una de las claves pueden revertirse empleando la otra. Por ejemplo, en el caso de que cierta información se cifre utilizando la clave pública de un usuario ésta podrá ser descifrada empleando la clave privada. Dado

que sólo el usuario tiene acceso a dicha clave, obtenemos de esta forma un medio para proteger la confidencialidad de la información. Por otra parte, el cifrado realizado mediante la clave privada también puede deshacerse empleando la clave pública. Aunque esta operación carece de interés desde el punto de vista de la confidencialidad dado que la clave de descifrado es pública, y por tanto conocida por todos, representa un mecanismo muy robusto de autenticación. La razón es que sólo hay un usuario capaz de cifrar información que podrá ser descifrada posteriormente empleando la clave pública: el poseedor de la clave privada. Esta técnica, combinada con el uso de funciones de resumen digital, es lo que se ha dado a conocer como mecanismo de firma digital, ya que además de autenticación es capaz de proporcionar también los servicios básicos de integridad y no repudio.

Las funciones criptográficas de las que **Bitcoin** hace uso, son responsables principales de que se consigan las propiedades de seguridad esta tecnología persigue. El aspecto más importante de la criptografía que le compete a esta criptomoneda es la **asimétrica** o de clave pública y sus capacidades de **firma digital**.

Bitcoin implementa el algoritmo ECDSA[10][23] para firmar digitalmente las transacciones, utilizando los parámetros recomendados por el Standards for Efficient Cryptography Group (SECG), secp256k1[22]. Las firmas utilizan la codificación DER[24] para empaquetar sus componentes en un único flujo de bytes.

ECDSA ofrece ventajas frente a otros esquemas de firma que lo hacen ideal para su utilización en un protocolo distribuido en Internet, como son: longitudes de clave, de firmas muy cortas, y generación y verificación de firmas muy rápidas.

En los cálculos de hashes realizados en Bitcoin se utilizan los estándares SHA-256[25] y, cuando se requiere que el hash sea más corto, RIPEMD-160[26]. Generalmente el cálculo de hashes se realiza en dos fases: la primera con SHA-256 y la segunda, dependiendo de las necesidades de longitud del resultado, con SHA-256 o RIPEMD-160.

La generación de números aleatorios es esencial para la criptografía y más en la aplicada a Bitcoin. Los ***nonces*** o números aleatorios que sólo se utilizan una vez son utilizados de forma directa para la generación de bloques en la ***blockchain*** de Bitcoin que se verá más adelante.

Las **pruebas de trabajo,** el principal componente de Bitcoin que garantiza que la red tenga un comportamiento legítimo. Básicamente, esta idea hace que validar/calcular nuevos bloques de transacciones conlleve un coste computacional muy elevado, de forma que, para hacerse con el control de la red (y por tanto de qué se valida y qué no), un atacante necesitaría una potencia de cómputo extremadamente difícil de conseguir.

En síntesis, en Bitcoin este control de complejidad en los cálculos para los nuevos bloques se realiza obligando a que el hash de cada nuevo bloque deba comenzar con un número determinado de ceros. Como se verá más adelante, para el cálculo de este hash se combinan datos de bloques anteriores y un nonce. Dado que las funciones hash criptográficas no son invertibles, para encontrar un bloque válido la única alternativa será ir obteniendo diferentes nonce hasta encontrar uno que cumpla el requisito preestablecido.

[10] Elliptic Curve Digital Signature Algorithm - Algoritmo de Firma Digital de Curva Elíptica

Contexto Operativo

Con el objetivo de contextualizar el medio operativo del sistema, es necesario describir los actores que interactúan en el mismo y la forma de cómo se efectúan las transacciones.
En cuanto a los actores que actúan en el sistema, se clasifican en tres tipos:

- **Nodos Normales**: realizan compras y pagos de bienes y servicios utilizando como moneda a los bitcoins, produciendo transacciones en el sistema.
- **Nodos Mineros**: son nodos normales que a parte dedican potencia de cómputo para validar nuevas transacciones, creando lo que se conoce como bloques de transacciones. Este rol, como antes se nombró, recibe recompensas en bitcoins por haber colaborado y proporcionado poder computacional a la red.

Un usuario, equivalente a un nodo, se identifica en el sistema por medio de una o más **direcciones Bitcoin**. Esta misma, se representa como una dirección virtual similar a una cuenta bancaria y se materializa como una clave pública de criptografía asimétrica. Estas direcciones pertenecientes a un usuario se almacenan y gestionan en un **monedero** virtual, que equivale a un monedero físico.
Una **transacción** es una transferencia de dinero de un **usuario** hacia otro, incluso a sí mismo, es decir, representa a la asignación de bitcoins de una **dirección Bitcoin** a otra. La constitución de una **transacción**, consiste en que si un usuario **A** transfiere dinero a uno **B**, el **usuario** de la **dirección Bitcoin** asignante (**usuario A**) firme una transcripción de la **dirección Bitcoin** del **usuario B** con la clave privada asociada a la dirección del **usuario A**, de esta forma se determinará que el nuevo propietario de esos bitcoins transferidos es la **dirección Bitcoin** del **usuario B**.
Estas transacciones, una vez que estén pendientes a confirmar, se agrupan a su vez en un conjunto de transacciones pertenecientes a un **bloque,** el cual será sometido posteriormente al proceso de minería y luego adherido a la **cadena de bloques** o **blockchain**.
La **blockchain,** representa al core del funcionamiento de esta criptomoneda. Es básicamente un registro público de las transacciones validadas en orden cronológico, es decir, cuando un bloque ya fue confirmado por medio del proceso de minería, éste pasa a formar parte de este registro público. La **cadena de bloques,** presenta una característica peculiar que es la de público acceso, distribuida, descentralizada y de sólo modo lectura; esto lo logra gracias a su constitución de **Árbol de Merkle**[22].

Arquitectura de comunicaciones del sistema

Los nodos que integran la arquitectura de **Bitcoin** constituyen un sistema de comunicaciones **P2P** o ***peer-to-peer***. Como ya se ha mencionado, la filosofía aquí es evitar la existencia de autoridades centrales que controlan la red.

Como todo arquitectura **P2P**, **Bitcoin** dispone de una serie de mecanismos para descubrir nuevos nodos en la red, y mantener una lista actualizada de los mismos. Además, distintos clientes de **Bitcoin** pueden también ofrecer mecanismos adicionales, como por ejemplo mensajes de tipo **addr** y **getaddr**, mediante los cuales un cliente envía (o solicita) a otro un listado de clientes actualmente conectados a la red. También, en el código de los clientes se suele incluir un listado de nodos semilla, que se utilizarán para iniciar el proceso de conexión a la red en caso de que el resto de mecanismos fallen.
Además de los mecanismos para descubrir otros nodos en la red, hay otros tipos de mensajes de uso frecuente en **Bitcoin**. Por ejemplo, los mensajes **tx** y **block**, utilizados para enviar datos de transacciones y bloques, respectivamente, de manera que los nodos de la red puedan mantener la sincronía requerida por el protocolo. O los mensajes de tipo **inv**, que se utilizan para anunciar (y retransmitir) nuevas transacciones[29].

Estructuras de datos del sistema

Como se describió con anterioridad, unos de los elementos que hace posible el funcionamiento de **Bitcoin** es la **criptografía asimétrica**. En ella, los distintos algoritmos funcionan a partir de una clave compuesta por dos elementos relacionados de modo que son fácilmente computables en una dirección (cifrado, descifrado y verificación de una firma digital) pero difícilmente computables en la contraria si se desconoce de la información secreta.

Direcciones y monederos

Una dirección **Bitcoin** convencional (P2PKH) es simplemente una cadena de texto codificada en **Base58Check** que tiene hasta 20 bytes de longitud y que consiste en el **hash** de la **clave pública** asociada con la dirección. Este formato es similar al **Base64**, con la diferencia que no solo pretende mantener la información codificada lo más legible posible para el usuario, sino que también permite verificar de forma más eficiente si una cadena arbitraria que satisfaga dicha expresión se corresponde con una dirección real o no, aplicando un mecanismo de validación redundante que ya se emplea en los números de tarjeta de crédito o documentos de identidad.

Versión = 1 byte de ceros
HashDeClave = Version + RIPEMD-160(SHA-256(ClavePública))
Checksum = SHA-256(SHA-256(HashDeClave))
***DirecciónBitcoin** = Base58Encode(HashDeClave + Checksum)*

Ilustración 1: Formato de Dirección Bitcoin

Las direcciones cumplen con las siguientes características:

- Generación en tiempo computacionalmente reducido (milisegundos).
- La clave privada asociada a dicha dirección debe ser un problema computacionalmente complejo, con el fin de ofrecer garantías de que un tercero no logre generar una clave privada asociada a dicha dirección.
- Generación offline, con el fin de proporcionar una capa de seguridad a dicha creación.

Un usuario podría crear una o varias direcciones, no obstante, un conjunto de dichas direcciones constituye un **monedero** Bitcoin, mediante los cuales se realizan las transacciones que se verán a continuación.

Transacciones

Con el fin de representar el flujo de las criptomonedas en la red existe el concepto de transacciones.

Las transacciones en Bitcoin son estructuras de datos firmadas digitalmente que cambian el propietario de unidades de bitcoins asignándolas a otra dirección o propietario.

La estructura de datos de una transacción se encuentra formada por **entradas**, **salidas**, **hash de transacción**, **firma digital del emisor**, **clave pública del emisor**, **total entradas**, **total salidas**, **bloqueo**, **versión:**

- Entradas: registros que referencian los fondos de transacciones previas. Las mismas se encuentran firmadas digitalmente por el "pagador" (proceso necesario y suficiente para desbloquear los fondos transferidos). Campo de tamaño variable.
- Salidas: registros que determinan el nuevo o los nuevos propietarios de las bitcoins transferidas. Estas salidas se utilizan como entradas de transacciones próximas. Campo de tamaño variable.
- Hash de transacción: resumen de toda la estructura de datos.
- Firma digital del emisor: encripción del **hash de la transacción** con la clave privada del emisor.
- Clave pública del emisor: se añade dicha para que se pueda verificar la firma digital cuando la transacción llegue a un nodo de la red que la deba procesar.
- Total entrada y salidas: número que indica cantidad de entrada y salidas adheridas a la transacción. Cada uno de estos campos puede contener entre 1 y 9 bytes.
- Versión: posee 4 bytes e indica el número de versión Bitcoin utilizado para esa transacción.
- Bloqueo: indica la fecha mínima en la cual dicha transacción puede ser agregada a la **cadena de bloques**. Si el valor indicado en este campo está entre cero y quinientos (incluidos ambos) indica la cantidad de bloques que deben agregarse a la cadena de bloques antes de agregar esta transacción; y si indica un valor mayor a quinientos,

entonces se interpreta como una fecha límite en formato UNIX. En una transacción de transferencia de bitcoins, se deben utilizar todas las que se encuentran asignadas a la dirección origen.

Por ejemplo, si A posee 10 bitcoins y desea enviar sólo 5 bitcoins a B, pues entonces las salidas de la transacción van a ser 5 bitcoins para la dirección de B y 5 bitcoins para la dirección de A; donde esta última toma el rol de una "dirección de devolución". Por consiguiente, en una transacción siempre se "gastan" todos los bitcoins asignados.

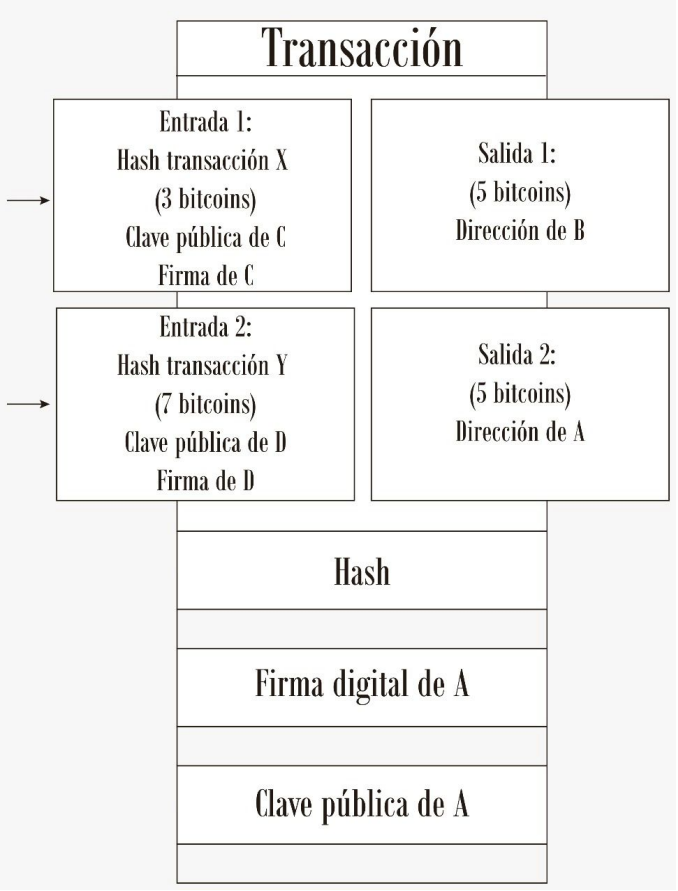

Ilustración 2: Esquema de transacción Bitcoin

Como se visualiza en la *Ilustración 3* el emisor A posee 10 bitcoins que antes los obtuvo por medio de dos transacciones diferentes (la transacción X y la transacción Y), donde tanto la "entrada 1" como la "entrada 2" antes fueron salidas de otras transacciones como la ilustrada (en este caso una transacción Y generada por D hacia A y otra transacción Y generada por D hacia A). Finalmente, A se queda con 5 bitcoins y B con los otros 5, los cuales podrán utilizar estas salidas para generar nuevas entradas en próximas transacciones.

La suma de la totalidad de las entradas debe ser igual o mayor que la suma de la totalidad de las salidas. En el caso de que la cantidad de bitcoins de la entrada sea mayor que la de la salida, la diferencia se considera una "comisión", y quien incluya esa transacción en la

cadena de bloques o ***blockchain*** (base de datos distribuida y descentralizada) puede disponer de esa cantidad. Esta recompensa es una manera de motivar a los nodos **mineros**, que obtienen beneficios por su trabajo en forma de bitcoins. Las transacciones que poseen "comisiones" tienen prioridad por los nodos mineros al momento de elegir cual de ellas procesar primero, y en consecuencia, las transacciones que posean mayor monto en comisiones serán procesadas de forma más veloz en la red.

Cada **salida** y **entrada**, al igual que las transacciones, tienen su estructura interna. Como ya se vió, las **entradas** son referencias o "punteros" a **salidas** anteriores, es decir, cada **entrada** hace referencia a un identificador perteneciente a una **salida** (UTXO, Salida de Transacción Sin gastar) que se encuentra almacenada en la base de datos distribuida. Para gastar una **UTXO**, la **entrada** de la transacción también incluye una condición de desbloqueo que satisface la condición especificada por la **UTXO**. Este código de desbloqueo normalmente consta de una firma la cual prueba la posesión de la dirección que se encuentra especificada en el código de bloqueo de la **UTXO**.

Las **entradas** están compuestas por los siguientes campos:

- Hash de transacción: puntero a la transacción que posee la **salida** perteneciente a esta **entrada**. Posee 32 bytes.
- Índice de la **salida**: índice de la **salida** perteneciente a esta **entrada**, es decir, el índice de la **UTXO** que se quiere gastar. Tiene 4 bytes.
- Tamaño del código de desbloqueo: especifica el tamaño en bytes que tiene el código de desbloqueo. De 1 a 9 bytes.
- Código de desbloqueo: el cual cumple las condiciones del código de bloqueo de la **UTXO**. Tamaño variable.

Las **salidas** están compuestas por:

- Monto: cantidad de bitcoins que se desean transferir. Posee 8 bytes.
- Tamaño del código de bloqueo: tamaño en bytes. De 1 a 9 bytes.
- Código de bloqueo: el cual define las condiciones que se deben de cumplir para poder gastar el monto. Generalmente, el código perteneciente a este campo realiza una transferencia de bitcoin a una dirección parametrizable. Tamaño variable.

Cada transacción crea salidas, las cuales son almacenadas en la base de datos distribuidas. Todas las salidas (excepto una) crean **UTXOs** las cuales son reconocidas por toda la red y están disponibles para que el poseedor haga uso de las mismas.

En síntesis, la transferencia de un monto en bitcoins es básica y sencillamente crear una **UTXO** asignada a la dirección bitcoin de destino.

```
"tx": [
    {
      "hash": "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
      "ver": 1,
      "vin_sz": 1,
      "vout_sz": 1,
      "lock_time": 0,
      "size": 204,
      "in": [
        {
          "prev_out": {
            "hash": "0000000000000000000000000000000000000000000000000000000000000000",
            "n": 4294967295
          },
          "coinbase": "04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c
            6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73"
        }
      ],
      "out": [
        {
          "value": "50.00000000",
          "scriptPubKey":
            "04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f3
            5504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG"
        }
      ]
    }
  ]
```


Ilustración 3: Esquema de Transacción en formato JSON

Códigos de Bloqueo y Desbloqueo

Script es el lenguaje usado para describir los **códigos** de Bitcoin, utilizados para bloquear/desbloquear de las transacciones. Cualquier combinación de un **script** o código de desbloqueo y uno de bloqueo que finalice con un valor de **VERDADERO** indica que la condición de la **UTXO** se cumple y por tanto es válido, en cualquier otro caso es inválido.
Cuando se valida una transacción, los scripts de entrada se concatenan con los scripts de salida y se evalúan. Una buena analogía de cómo funciona esto es que los scripts de salida son rompecabezas que especifican en qué condiciones se pueden gastar esos **bitcoins**. Los scripts de entrada proporcionan los datos correctos para que los scripts de salida se evalúen como verdaderos.
Por ejemplo si se tiene el código de bloqueo **3 OP_ADD 4 OP_EQUAL** éste se puede satisfacer con el script de desbloqueo **1** [33].
El lenguaje tiene las siguientes características:

- Simple
- Limitado. El lenguaje no es Turing completo debido a que no tienen ciclos ni controles de flujo complejos lo cual asegura que siempre termine. Por esta razón no es posible tener bombas lógicas que ocasionen un ataque de denegación de servicio en la red Bitcoin.
- Requiere un procesamiento mínimo.

- Puede ser implementado en una amplia gama de dispositivos.
- No hay un estado anterior o posterior a la ejecución del script. Toda la información necesaria para ejecutar el código debe estar contenida en él.
- Es un lenguaje que accede a la memoria basándose en una pila. Por tanto no hay variables. Para hacer más claro el uso de la pila, han decidido usar notación polaca inversa. Los valores se van metiendo en la pila y los operadores meten o sacan uno o más parámetros de la pila, modifican los parámetros y finalmente pueden meter un resultado en la pila. Por ejemplo la instrucción **OP_ADD** saca dos elementos de la pila, los suma y mete el resultado en la pila. Al final del código, la cima de la pila es el valor de retorno. **Script** puede usar dos pilas: La principal y la alternativa. La alternativa se usa para almacenar datos de cálculos de pasos intermedios de forma similar a la tecla memoria de las calculadoras.
- Su funcionamiento es similar al del lenguaje ensamblador ejecutado sobre una CPU little-endian con un solo registro de memoria de 16 bits. Bitcoin implementa su procesador virtual para interpretar el código máquina **Script**.

En bitcoin existen 5 tipos de combinación códigos de bloqueo/desbloqueo (pay-to-public-key-hash, pay-to-pubkey, pay-to-multisig, pay-to-script-hash y data output) que son las únicas aceptadas por el cliente de referencia y la mayoría de los nodos mineros. Estas combinaciones pertenecen a tipos de transacciones aceptadas en el **protocolo Bitcoin**. Aunque es posible crear códigos de bloqueo/desbloqueo y transacciones que no son estándar, se tiene que encontrar un nodo minero que no siga estas limitaciones para que mine la transacción en un bloque con scripts o códigos no estándares.

Pay-To-Pubkey-Hash (p2pkh)

Pago a hash de clave pública es el script de salida de transacción más comúnmente utilizado. Se usa para pagar a una dirección de bitcoin (como visto antes, una dirección de bitcoin es un hash de clave pública codificado en base58check).

Script de Bloqueo:

scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

Script de Desbloqueo:

scriptSig: <sig> <pubKey>

*Nota: **scriptSig** está en la entrada de la transacción de gasto y **scriptPubKey** está en la salida de la transacción.*

Así es como se procesa cada palabra:

Pila	Código	Descripción
Vacía.	<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	scriptSig y scriptPubKey se combinan.
<pubKey> <sig>	OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Las constantes se agregan a la pila.
<pubKey> <pubKey> <sig>	OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	El elemento superior de pila se duplica.
<pubHashA> <pubKey> <sig>	<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	El elemento superior de la pila se hashea.
<pubKeyHash> <pubHashA> <pubKey> <sig>	OP_EQUALVERIFY OP_CHECKSIG	Se agrega la otra constante.
<pubKey> <sig>	OP_CHECKSIG	La igualdad se verifica entre los dos elementos superiores de la pila.
VERDADERO	Vacío.	La firma se verifica para los dos elementos superiores de la pila.

Explicación detallada:

El remitente **A** solo tiene la dirección de Bitcoin del destinatario **B**, entonces, ¿cómo obtiene el **pubKeyHash** de su dirección de Bitcoin?.
La clave es que el remitente **A** no necesita obtener el **pubKeyHash** de "su" dirección de Bitcoin.
El script **scriptPubKey** está sucediendo primero. **A** crea este script con la dirección de bitcoin de **B** en lugar de su <pubKeyHash>. Ese es el trabajo de **A** hecho, y lo que **A** ha dicho es "1 BTC ahora pertenece a **B** pero, si y solo si **B** puede demostrar que es el verdadero propietario de la dirección de bitcoin agregada en <pubKeyHash>".

B, en su billetera, ve que aparece esta cantidad de 1 BTC. Entonces técnicamente **B** "lo posee". Pero para que **B** lo gaste, es decir, enviarselo a otra persona, **B** necesita probar que la dirección de bitcoin a la que le dió el BTC a **A** era de hecho suya. Acá es donde aparece **scriptSig**. Entonces, la <sig> <pubKey> es responsabilidad de **B** quien conoce todos los parámetros para completar la misma. No obstante, **A** antes de haber enviado el BTC a **B** tuvo que haber realizado el mismo procedimiento.

Pay-To-Pubkey (p2pk)

Los scripts de pago a clave pública son una forma simplificada de p2pkh, pero ya no se utilizan comúnmente en nuevas transacciones, porque los scripts p2pkh son más seguros (la clave pública no se revela hasta que se gasta el resultado).

Script de Bloqueo:
scriptPubKey: <pubKey> OP_CHECKSIG
Script de Desbloqueo:
scriptSig: <sig>

Procesamiento:

Pila	Código	Descripción
Vacío.	<sig> <pubKey> OP_CHECKSIG	scriptSig y scriptPubKey se combinan.
<pubKey> <sig>	OP_CHECKSIG	Las constantes se agregan a la pila.
cierto	Vacío.	La firma se verifica para los dos elementos superiores de la pila.

Pay-To-Multisig (p2ms)

Las salidas multigrado permiten compartir el control de bitcoins entre varios destinatarios. Al crear el script, uno especifica las claves públicas que controlan los fondos, y cuántas de esas claves se requieren para firmar transacciones de gasto para que sean válidas. Una salida con N claves públicas de las cuales se requieren M se denomina salida m-of-n (por ejemplo, 2 de 3, 3 de 5, 4 de 4, etc.)

Script de Bloqueo:
scriptPubKey: <m> <A pubkey> [B pubkey] [C pubkey...] <n> OP_CHECKMULTISIG
Script de Desbloqueo:
scriptSig: OP_0 <A sig> [B sig] [C sig...]

Pay-To-Script-Hash (p2sh)

Las salidas de hash de pago a script son scripts que contienen el hash de otro script llamado ***redeemScript***. Para gastar bitcoins enviados en un resultado p2sh, la transacción de gastos debe proporcionar un script que coincida con el hash del script y los datos que hacen que el script se evalúe como verdadero. Esto permite postergar el revelado de las condiciones de gasto al momento del gasto. También hace posible que el receptor establezca las condiciones para gastar esos bitcoins.

Script de Bloqueo:
scriptPubKey: OP_HASH160 <Hash160(redeemScript)> OP_EQUAL
Script de Desbloqueo:
scriptSig: <sig> [sig] [sig...] <redeemScript>

Data Output

Las salidas de datos se utilizan para insertar datos en la cadena de bloques. Pueden enviarse hasta 40 bytes de manera estándar, pero se pueden usar más datos si un minero decide aceptar la transacción.

scriptPubKey: OP_RETURN <0 a 40 bytes de datos>
(No pueden ser gastados, ya que no posee **scriptSig**)

El Satoshi

Como norma general, el **bitcoin** se divide en 8 partes u 8 dígitos decimales, es decir que si alguien posee 1 bitcoin (BTC) en realidad tiene 1.00000000 BTC, cuando se posee de medio bitcoin o cuarto bitcoin, es cuando se tienen fracciones de bitcoins, siendo para **medio bitcoin** = 0.50000000 BTC y para **cuarto bitcoin** = 0.25000000 BTC.
Existen fracciones aún más pequeñas que se pueden manejar en el mundo Bitcoin, las mayormente usadas son estas tres: mBTC, uBTC y **Satoshis**, pero también existe el cBTC.
El cBTC simboliza el poco usado **centibitcoin**, que es lo mismo que: 0.01BTC = 0.01000000 BTC, es poco usada por los usuarios comunes, pero si muy usada por la comunidad que compran y venden la divisa, ya que no se enfocan mucho en las micro fracciones de esta moneda.

Los mBTC, o también llamada **millibitcoin**, usa la letra "m" como indicativo de 00.000, y que se debe agregar 00000 (5 ceros) al número que esté delante de la letra "m", por ejemplo:

- 1mBTC = 0.00100000 BTC.
- 15mBTC = 0.01500000 BTC.
- 100mBTC = 0.10000000 BTC.

El uBTC, o denominado también **microbitcoin**, y cualquier número que haya delante de la letra "u" tendrá 00 (2 ceros) seguidos, por ejemplo:

- 1uBTC = 0.00000100 BTC.
- 15uBTC = 0.00001500 BTC.
- 100uBTC = 0.00010000 BTC.

Por último, el **Satoshi**, la fracción más utilizada por los usuarios bitcoin, su nombre proviene de su creador y es la unidad de BTC más pequeña que se puede manipular (enviar o recibir), para entender fracciones Satoshis, simplemente se debe contar siete ceros luego de la coma, es decir, 1 Satoshi es igual a: 0.00000001 BTC.

Bloques

Los bloques son estructuras de datos que contienen un conjunto de transacciones ya confirmadas. Cada cierto tiempo (aproximadamente cada diez minutos), un nuevo bloque que incluye y nuevas transacciones se anexan a la cadena de bloques por medio del proceso de minería.

hash	Hash del bloque
ver	Versión del bloque
prev_block	Hash del bloque anterior
mrkl_root	Hash de la raíz del árbol de Merkle
time	Marca el tiempo de creación del bloque
bits	Especificación de la complejidad del bloque
nonce	Nonce que resuelve la prueba de trabajo
size	Número de bytes que siguen, hasta el final de bloque
n_tx	Número de transacciones en la siguiente lista
tx	Lista de transacciones contenidas en el bloque

Ilustración 5: Esquema de Bloque perteneciente a la Blockchain

De los campos anteriores, el campo **versión**, **hash prev block**, **hash merkle root**, **time**, **bits** y **nonce**, pertenecen al header del bloque.
Los campos que comienzan con la palabra "**hash**" del esquema anterior tienen como fin establecer la cadena de bloques.
En el campo **Bits**, se define cual es la complejidad requerida en el momento de generación del bloque para que dicho bloque fue válido. Esta complejidad es variable en función de la capacidad de cómputo total de la red, de forma que cada bloque que se genere cada diez minutos.
El campo **Nonce**, es el número que se resuelve en la prueba de trabajo. Básicamente es un campo que se va variando, y en cada variación calcula el hash del bloque hasta conseguir un hash compatible con la complejidad indicada en el campo **Bits**. Ejemplificando, si el campo **Bits** está en 4, significa que el hash del bloque debería estar compuesto por 4 ceros al principio, no obstante, para lograr ésto se deben calcular sucesivos hashes de este bloque modificando el campo **Nonce,** con el fin de obtener diferentes resultados, hasta llegar a un hash que contenga 4 ceros al comienzo.
Con el fin de optimizar el espacio en disco necesario para almacenar todos los bloques de la cadena de bloques, las transacciones que se incluyen en cada bloque se organizan en forma de árbol de Merkle.
En **Bitcoin**, el primer bloque perteneciente a la gran cadena de bloques se lo denomina **bloque génesis** y cuya recompensa por resolverlo fue de 50 bitcoins y el valor encontrado dentro del campo **hash prev block** es "0".

```
{
  "hash":"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
  "ver":1,
  "prev_block":"0000000000000000000000000000000000000000000000000000000000000000",
  "mrkl_root":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
  "time":1231006505,
  "bits":486604799,
  "nonce":2083236893,
  "n_tx":1,
  "size":285,
  "tx":[
    {
      "hash":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":204,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
            "n":4294967295
          },
          "coinbase":"04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6
            c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73"
        }
      ],
      "out":[
        {
          "value":"50.00000000",
          "scriptPubKey":"04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6b
            c3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
  ]
}
```


Ilustración 4: Bloque Génesis en formato JSON

Minado de Bloques

El proceso de minado consta de la creación de nuevos bloques para la cadena, y es una tarea muy costosa desde el punto de vista computacional.

Los campos del bloque que llevan un papel importante en este proceso son: **ver**, **prev_block**, **mrkl_root**, **time**, **bits** y **nonce**.

Donde en el campo **mrkl_root,** se encuentra detallado el contenido del árbol de Merkle, que permite verificar que el bloque está correctamente incluido en la cadena.

El **hash** del bloque se calcula utilizando los campos de la cabecera, es decir, los nombrados anteriormente. Para determinar qué hashes serán considerados válidos, se utilizará el campo **bits**, en el cual se encuentra una versión codificada del máximo valor que puede

tomar el hash del bloque para ser considerado válido. Para obtener dicho límite, hay que convertir el valor del contenido en hexadecimal y aplicar la siguiente función:
Valor máximo = HEX(bits)*2*(8*(0x19 - 3))
No obstante, cualquier hash con un valor inferior a dicho número hexadecimal, será válido.
Todos estos campos involucrados en la creación del hash son elementos fijos, excepto el **nonce**. Así, este es otro campo que hace que un hash sea válido o no, y es el que los mineros tienen que ir variando hasta encontrar un hash válido. En contexto, cuanto menor sea el límite, más difícil es encontrar un nonce válido (porque se reducen los números que satisfacen la fórmula). Este procedimiento de búsqueda del hash indicado se denomina **prueba de trabajo**.

Recompensas

Dado el proceso anterior una tarea computacionalmente tediosa, el nodo minero que encuentra un nuevo bloque recibe una recompensa.
Dicha recompensa puede percibirse por dos medios. Por un lado, Bitcoin tiene establecido un límite máximo de 21 millones de bitcoins y hasta que se llegue a ese límite, la generación de cada nuevo bloque es recompensada con una cantidad predefinida de bitcoins nuevas. Por ejemplo hasta el 2012, se recompensaba con 50 bitcoins a cada nuevo bloque. Desde entonces, la recompensa es de 25, hasta el 2016 que se redujo a la mitad, es decir 12,5 bitcoins, y así sucesivamente.
Por otro lado, para mantener una motivación similar para los mineros pese al decrecimiento de las recompensas (que potencialmente llegará a cero), existen las tasas de transacción, mediante las cuales, los usuarios pagan una comisión, como ya se describió anteriormente. Este dinero en bitcoins obtenidos de comisión sólo puede ser gastado sí y solo sí existieron 100 bloques por detrás del creado.

Confirmando Transacciones

Aunque una transacción nueva haya sido incluida en un bloque y dicho bloque en la cadena, inicialmente puede ser posible que esa modificación sea revertida. Esto podría pasar cuando se crean dos ramas inicialmente válidas, lo cual puede ocurrir por diversos motivos. Al generarse dos ramas distintas, cada una de ellas será respaldada inicialmente por una cantidad determinada de mineros, que irán extendiéndola. Cuanto más similares sean las capacidades de cómputo de las ramas, más se tardará en resolver la ambigüedad, aunque eventualmente una de las ramas recibirá un nuevo bloque antes que la otra y prevalecerá sobre ella y la descartará. No obstante, esto es un caso posible y dar por válida una transacción no respaldada por nuevos bloques no es correcto. Por esto, es aconsejable esperar un número determinado de bloques hasta considerar una transacción

como confirmada. El número de bloques puede variar dependiendo de la cantidad involucrada en la transacción, y obviamente, en función de las consideraciones personales. Normalmente, se considera que tras 10 bloques nuevos, la transacción será difícilmente revertida y, por tanto, se puede considerar confirmada.
Nótese también que la probabilidad de revertir una transacción decrece exponencialmente por cada nuevo bloque que la respalda.

Consideraciones Generales

En los modelos tradicionales, la confianza se deposita completamente en una autoridad o entidad que controla toda la información. En Bitcoin por medio de Blockchain, por el contrario, no existe dicha autoridad, sino que la información es gestionada por todos los usuarios. De esta forma, siempre y cuando la "mitad más uno" de los usuarios del sistema sean honestos, las "políticas" establecidas por el sistema no podrán saltarse por ninguno de los usuarios deshonestos.
El uso de un sistema criptográfico asimétrico fuerte, como es ECDSA, y de algoritmos de hashing robustos, como SHA-256, garantiza la integridad actual del sistema. Pero teniendo en cuenta que la capacidad de cómputo aumenta considerablemente año tras año, además de producirse nuevos avances en la teoría criptográfica/criptoanalítica, el sistema está diseñado de forma que se pueda modificar el sistema criptográfico a utilizar, utilizando el mismo protocolo de comunicación entre pares y de gestión de transacciones.

Manipulando bitcoins

Para comenzar a manejar *bitcoins* es necesario crear una dirección Bitcoin que podrá ser realizado desde un cliente Bitcoin. En función a este cliente, existirán diversos formatos de almacenamiento de la información asociada a una cuenta. Por ejemplo, en el caso del cliente Bitcoin Core, esta información se almacena en un fichero denominado por defecto *wallet.dat*. De esta forma, las principales *wallets* o carteras disponibles son: las locales, en la nube, almacenamiento en frío y carteras mentales.

Carteras Locales

Son todas aquellas que se instalan en un equipo y que generan y almacenan las claves privadas sin depender de algún almacenamiento externo.
Existen dos tipos de carteras locales, por un lado tenemos las que fueron diseñadas para funcionar de forma independiente como un nodo dentro de la red, por ejemplo: cartera

oficial de Bitcoin (Bitcoin Core), y por otro lado están las que dependen de un tercero de confianza para operar con ella, por ejemplo: Green Address. Este segundo tipo de cartera existe con el fin de agilizar los diferentes pagos y por el cobro del uso de sus infraestructuras y espacio de almacenamiento. No obstante, la implicación de optar por un nodo independiente es la descarga completa de la *blockchain*, donde al día de la fecha el tamaño total de la misma es de aproximadamente 1 terabyte y la descarga y configuración de la misma requeriría al menos dos semanas.
En ciertas circunstancias, la descarga de toda la cadena de bloques se vuelve poco viable, por ejemplo, el caso de los dispositivos móviles, para esto existen clientes especiales que funcionan de una forma diferente, como ser: Electrum, Multibit o Mycelium, que delegan el proceso de validación y notificación de las transacciones en un servicio alternativo.
No obstante, existen tres métodos de validación de transacciones:

- Validación completa: se realiza de forma local con toda la *blockchain* descargada. Este método es el utilizados por los nodos de la red que validan y retransmiten transacciones. Este método es el nativo de Bitcoin y el que presenta mayor seguridad. Ejemplo: Bitcoin Core.
- Validación simplificada: se produce cuando los nodos "livianos" descargan únicamente la cabecera de la cadena de bloques. Estos clientes no verifican los bloques como los nodos completos, sino que utilizan el número de confirmaciones como dato de referencia excluyendo la información completa de la transacción. Ejemplo: Electrum, Copay
- Validación centralizada: acá las validaciones las centraliza un servicio tercerizado, es decir, los usuarios confían en terceros que consultan a la *blockchain* para validar las transacciones. Ejemplo: Green Address.

Utilización de Bitcoin Core

Una vez instalado y ejecutado el cliente Bitcoin Core[11] por primera vez, este comienza a descargar toda la *blockchain* de Bitcoin. Luego de concluir este proceso se podrán realizar diversas operaciones, tanto desde la consola que se presenta en la interfaz gráfica como desde la consola bitcoin-cli.
Generalmente, la acción siguiente a la instalación del cliente es cifrar la cartera. Este proceso es simple y lo permite hacer tanto desde la interfaz gráfica como desde la consola. Este cliente también permite realizar backups de la cartera y volcados de las claves y direcciones, y para realizar cualquiera de estas acciones, primero es necesario desbloquear la cartera con la passphrase configurada en la encripción previa.

[11] www.bitcoin.org

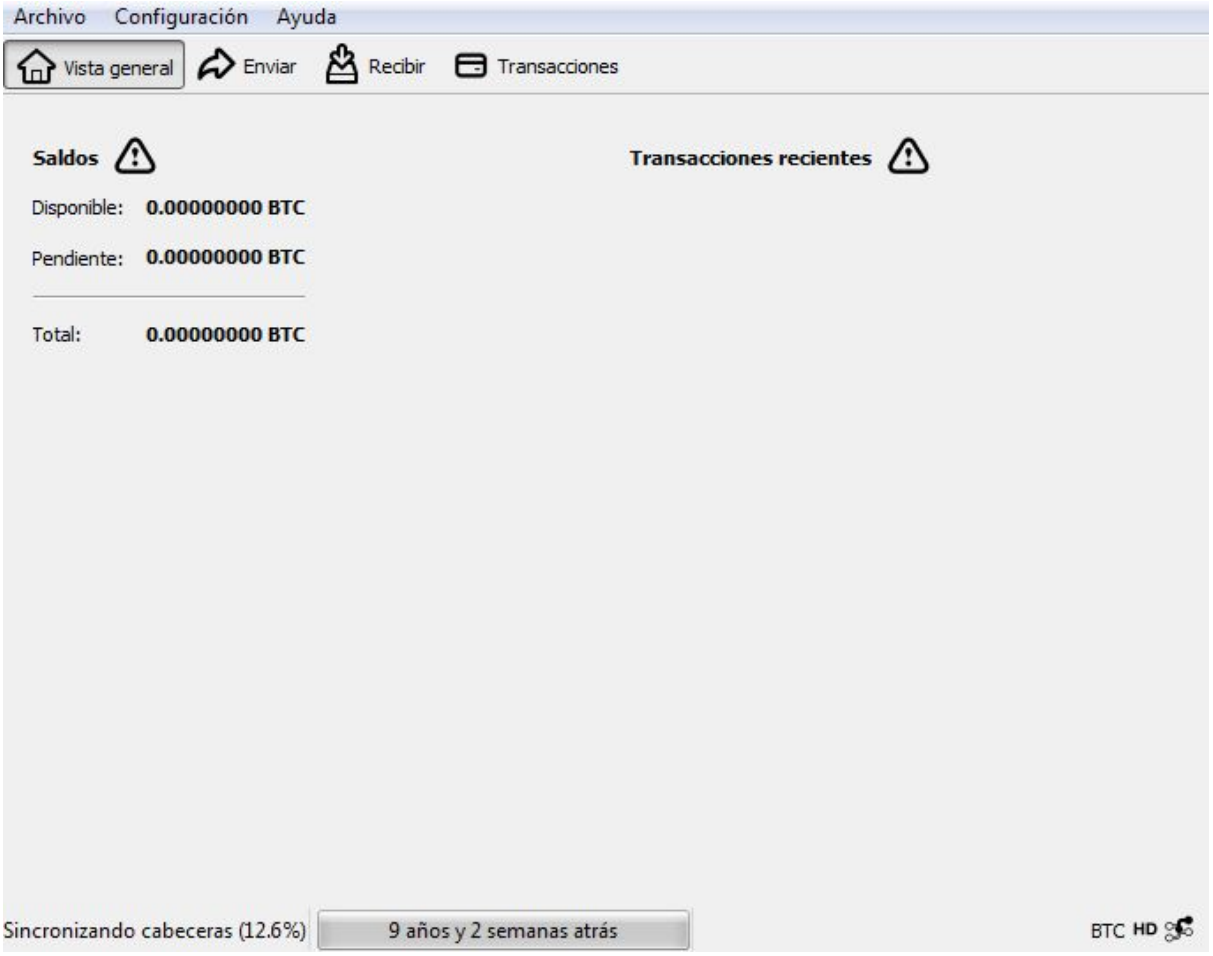

Ilustración 5: Primera ejecución del monedero Bitcoin Core

Como se visualiza en la parte izquierda inferior de la *Ilustración 5*, se encuentra descargando y sincronizando la totalidad de la cadena de bloques (desde el inicio de los tiempos).

En la opción de **configuración** inmediatamente aparecerá un botón para cifrar el monedero por medio de una passphrase, y en la sección de **archivo**, una opción para realizar un backup y copiar el *wallet.dat* en otro directorio.

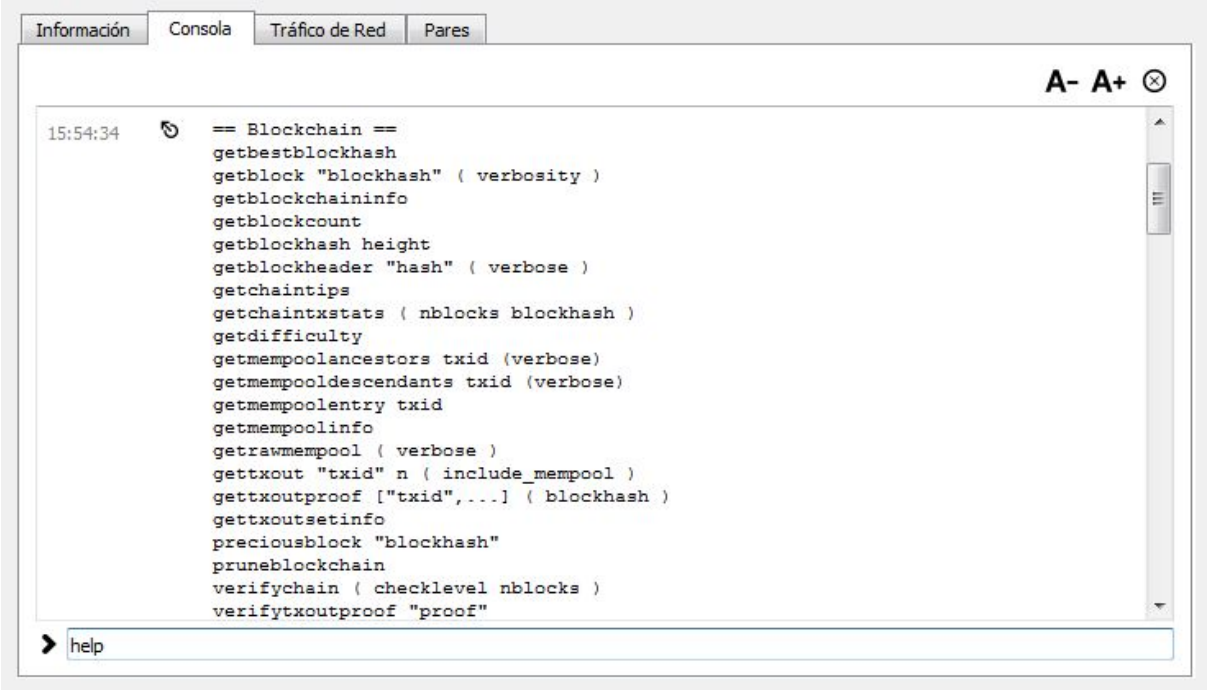

*Ilustración 6: Ejecución del comando **help** en la consola del cliente Bitcoin Core*

Por medio de la opción **recibir** y luego **solicitar pago**, un usuario puede solicitar los pagos de terceros.

Ilustración 7: Opción de solicitar pagos del cliente Bitcoin Core

La dirección presentada en la Ilustración 7, es a donde un pagador podrá destinar los fondos. Y no obstante, se podrá añadir información extra de la operación realizada que se almacenará unicamente en la cartera, como ser nombre del pagador, nombre de operación, etc.
Desde la opción **enviar** se podrán realizar pagos en *bitcoins* simplemente con agregar una dirección de destino, un importe y configurar la comisión a pagar al nodo que mine el bloque en donde se encontrará la transacción. Acá también se podrá añadir información extra de la transacción realizada. Una vez realizado el pago, solo resta esperar a que se agregue la transacción a la cadena de bloques y esperar un número *n* de confirmaciones.
Cada transacción diseminada por la red podrá ser consultada a su vez en la *blockchain* por medio del servicio "www.blockchain.info" sólo agregando el identificador de las mismas (hash de transacción).

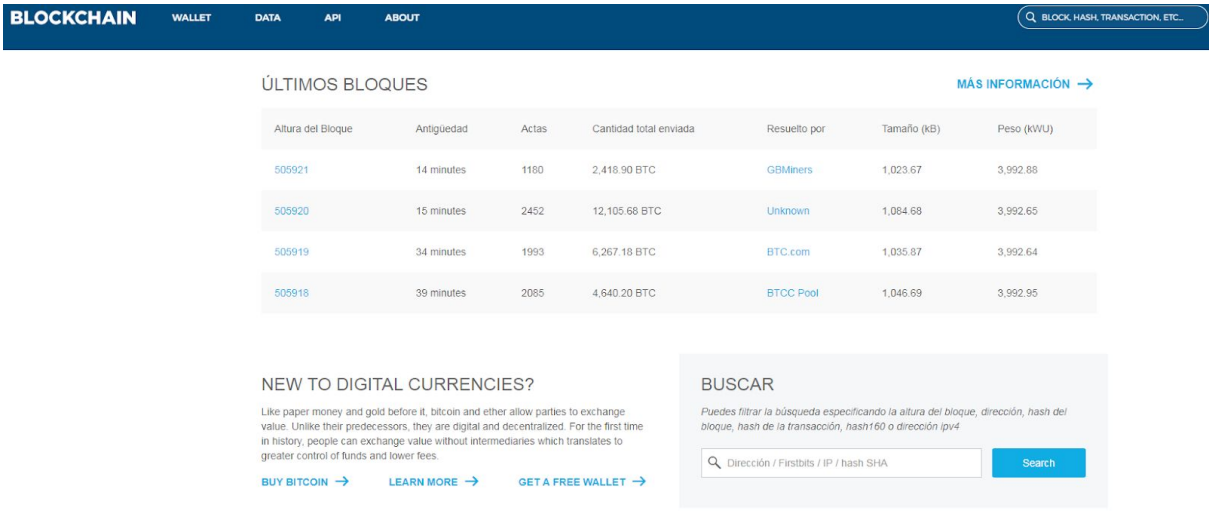

Ilustración 8: Vista sitio web blockchain.info

Carteras en la nube

Otra opción es la confianza en servicios de terceros. Existen varias alternativas en la red que ofrecen monederos online por medio de una plataforma. Estas, son intermediarios innecesarios desde el punto de vista técnico en la estructura del protocolo Bitcoin, pero su existencia tiene sentido por el ofrecimiento de servicios complementarios para los usuarios novatos, por ejemplo: diferentes tipos de cambio entre divisas y criptodivisas, compras y ventas programadas, etc. La desventaja principal de optar por esta opción es que uno no tiene el control total de sus criptodivisas, tiene que confiar en un tercero que centraliza las operaciones y cobra una comisión por la gestión de las mismas.

Almacenamiento en frío

Esta opción pretende un almacenamiento de las criptomonedas en equipos offline, a modo de evitar el riesgo de que los bitcoins almacenados se vean afectados por ataques que se realizan a equipos que se encuentran conectados a Internet.

Carteras mentales

Como la palabra lo indica, una forma de almacenar bitcoins en la mente de su dueño. Permite acceder a los bitcoins por medio de un passphrase que se almacenaron en una *brainwallet* y enviarlos a cualquier persona sin necesidad de exponer las claves privadas fuera de la extensión. Es decir, no es necesario intentar mantener segura la *wallet.dat,* ni almacenar largas e ininteligibles URLs. Desde el punto de vista de la seguridad este tipo de carteras son las menos recomendables ya que cualquiera que conozca la contraseña (determinando por ataques de fuerza bruta o diccionario) en cualquier parte del mundo podría firmar cualquier transacción sin consentimiento del propietario.

Capítulo 3 - Análisis del Anonimato

Introducción

Las diferentes modalidades de extorsión se acercan cada vez más a ambientes de delincuencia organizada que a la de un delito informático común y corriente.
Un claro ejemplo de esto es la explosión de grupos dedicados a extorsionar a grandes objetivos como plataformas de juego online y sectores financieros mediante la amenaza de preparar ataques distribuidos contra su infraestructura.
El uso de las criptomonedas, en especial Bitcoin, permite también la posibilidad de crear escenarios ficticios en los que se simule la realización de otros pagos para hacer creer a sus víctimas que verdaderamente se están generando transacciones hacia sus direcciones con el objetivo de dar una sensación de que otros están pagando para conseguir convencerlos de que paguen también.
Por otro lado, la extorsión por medio de la amenaza del secuestro de bases de datos con información crítica de las empresas se ha convertido en una moda reciente. Los rescates de estas suelen realizarse en *bitcoins* a través de plataformas de compra y venta ubicadas en la *deep web* y creadas como servicios ocultos de las mismas. Paralelamente, las amenazas de filtración de grandes bases de datos con información de usuarios y contraseñas son inhibidas con pagos en *bitcoins*.
Por otro lado, las fuerzas de seguridad son conscientes de que se están produciendo intercambios de material de abuso infantil a cambio de esta criptodivisa a través de plataformas anónimas.
Para finalizar, todos estos casos son formas de obtener un beneficio ilícito cuyo cobro se realiza en *bitcoins* con el fin de anonimizar el rastro de dicho beneficio. Por lo tanto, no existen dudas de que los organismos de seguridad tienen mucho trabajo en este campo ya que muchas investigaciones probablemente hayan quedado frustradas debido al anonimato que proporciona implícitamente el uso de Bitcoin.

Traceando bitcoins

Bitcoin, como visto en el capítulo anterior, es un sistema con una total transparencia en sus operaciones, principalmente porque el histórico global, es decir, la *blockchain* está disponible y redundante en todos los nodos de la red y accesible para cualquier usuario de Internet. Bajo estas circunstancias, es útil resaltar que dada la posibilidad existente de

purgar transacciones para optimizar espacios de almacenamiento, existen también multitudes de nodos, que contienen el histórico completo. Esto resulta funcional para poder verificar con total certeza que no ha habido irregularidades en las transacciones habituales.

Las direcciones en la *blockchain* están pensadas para funcionar como seudónimos con el fin de evitar que el carácter público del historial de transacciones implique de forma directa el poder identificar a alguien, pero eventualmente un usuario que quiera realizar un pago en *bitcoins*, tendrá que proporcionar algún dato identificativo a quien le proporcione el servicio en cuestión, por lo que su identidad quedará enlazada con la dirección que utilice para la realización del pago. En ocasiones similares a ésta, por más que se haya realizado una gestión adecuada de las direcciones Bitcoin, la dirección de pago se podrá utilizar para trazar otras direcciones relacionadas. Por tanto, son varias las fuentes que concluyen que es imposible que una dirección Bitcoin permanezca completamente anónima.

No obstante, desde una mirada criptográfica, esto no se refiere literalmente a que la identidad del propietario de dichas claves permanezca anónima, sino que se refiere a que dichas claves no contienen una identidad real "dentro" de ellas. A pesar de ello, como se ha avanzado y se verá con más detalle a continuación, esto no evita que sea posible (incluso probable, en ocasiones), deducir la identidad real de quien maneja una dirección Bitcoin.

En cualquiera de los casos, resulta relevante destacar que como se ha descripto en el capítulo 2, Bitcoin, no requiere la introducción de datos identificativos y que, a diferencia de los sistemas de comercio tradicionales, no existe una autoridad central a la que se pueda preguntar por la identidad real del propietario de una dirección o *wallet*.

Tracking basado en análisis de tráfico

Es posible mediante el análisis del tráfico TCP/IP descubrir la identidad de quien realiza un pago en Bitcoin. Debido al diseño de Bitcoin, la primera persona en anunciar una transferencia será, con alta probabilidad, el pagador de la misma. Por lo tanto, descubriendo quién fue el primero en publicarla, se podrá deducir con gran probabilidad quién es el pagador de dicha transacción y por tanto el propietario de las direcciones de entrada utilizadas.

También es destacable que este ataque está basado en la naturaleza de Bitcoin (que el primero en anunciar una transacción probablemente sea el pagador). Por ello, a Bitcoin por sí mismo le resulta difícil evitar este ataque. Para solucionarlo, no obstante, bastaría con utilizar algún sistema de anonimización de las comunicaciones, como la *darknet*.

Tracking basado en heurísticas

Otro tipo de análisis que se destaca bastante es el que se basa en las relaciones que se pueden establecer entre direcciones que, en algún momento, aparecen como entradas comunes a una transacción. Y es que, dada la construcción de Bitcoin, el hecho de que una entidad utilice varias direcciones Bitcoin como entrada a una misma transacción es garantía de que dicha entidad controla las claves privadas asociadas a dichas direcciones. Por lo tanto, parece seguro asumir que todas esas direcciones pertenecen a la misma persona.

Análisis de grafo de transacciones

Se crea un grafo τ (T, L), donde T es el conjunto de transacciones en la *blockchain* y L es el conjunto de asignaciones directas (relaciones de entrada salida en transacciones) entre estas transacciones. Cada asignación $l \in L$ lleva un numero de monedas Cl. De forma inherente las transacciones tienen un orden total definido por el *blockchain*, y no pueden existir ciclos en τ .

Análisis de grafo de direcciones

Por medio del grafo de transacciones se pueden determinar los pares de direcciones origen-destino. Por medio de estas relaciones se obtiene el grafo α (A, L0) donde A es el conjunto de direcciones de Bitcoin y L0 es el conjunto de asignaciones directas, pero esta vez conectando direcciones en lugar de transacciones. Opcionalmente se puede transformar a α en un multigrafo al añadir la fecha como un atributo a cada $l \in L0$ para poder distinguir entre multiples asignaciones y un par de direcciones.

Acceso al dispositivo

Para determinar si un dispositivo ha operado con cuentas Bitcoin, es necesario hurgar en en los directorios donde se almacenan las carteras, que si bien la ubicación de las mismas pueden ser configuradas por el usuario, las rutas por defecto estará determinada por el cliente Bitcoin utilizado y el sistema operativo en el que se desplegaron. Por ejemplo:

- Cliente Bitcoin Core con sistema operativo Windows: “C:/Usuarios/<nombre usuario>/AppData/Roaming/Bitcoin”.

- Cliente Bitcoin Core con sistema operativo Linux: "/home/<nombre usuario>/.bitcoin/".
- Cliente Electrum con sistema operativo Linux: "/home/<nombre usuario>/.electrum/wallets".

En fin, una vez ubicadas las carpetas, se deberá realizar una copia del archivo con el objetivo de no manipular el archivo original.

Ya obtenido el duplicado del fichero este podrá o no estar cifrado. En el primer caso conlleva la posibilidad de que se cuente o no con el passphrase de desencripción. En el caso de que el fichero esté cifrado y no se cuente con la contraseña, aún así se podrá obtener cierta información de la misma ya que la única información que permanece encriptada es la clave privada con la que el portador firma las transacciones.

No obstante, la información que brinda el archivo obtenido es la siguiente:

- Historial de transacciones: de acá se podrán extraer las direcciones origen, destino y el monto en *bitcoins*.
- Fichero de la cartera: acá se encontraran las etiquetas/comentarios/información adicional de las transacciones en caso de haberlas agregadas al momento, clave privada genérica y clave pública en Base58Check, si es que ha tenido recepciones de *bitcoins* programadas (monto, partes implicadas y fecha), semillas que permitirán la recuperación de la clave privada (si es que la cartera no fué protegida), tipo de cartera y si está encriptada o no.
- Contraseña: en caso de que el usuario no haya protegido la cartera podría extraerse facilmente la clave privada.

En caso de que la cartera se encuentre cifrada, habrá que recurrir a diferentes métodos como la fuerza bruta, ataques de diccionario o alguna herramienta de cracking de contraseñas cómo ser "JohnTheRipper" que incluye un módulo que permite la utilización de la potencia de la herramienta con carteras Bitcoin. Por ejemplo, en una máquina en la que se tuviese funcionando el cliente Bitcoin Core, se podría utilizar el cliente bitcoin-cli con el comando **walletpassphrase** para realizar búsquedas sucesivas de un número determinado de palabras.

En cualquier caso habrá que determinar si el objetivo de la investigación es la incautación de los fondos que contiene la cartera o no, ya que para el momento de la incautación o acceso al equipo, el propietario de la cuenta bitcoin podría haber realizado un backup y realizar las transferencias de sus *bitcoins* a otra dirección no intervenida.

Identificación de carteras

Los nodos con carteras locales completas necesitan tener conectividad para acceder a información de la red de Bitcoin y mantener sincronizada la *blockchain*. No obstante, al tener información que una máquina está en la red de Bitcoin es un indicio suficiente para determinar que allí hay en circulación bitcoins.

En Bitcoin Core, los nodos más cercanos de la red se identifican en el archivo *peers.dat*. Para que el cliente conozca más nodo, el protocolo de descubrimiento envía a estos nodos una petición para descubrir más nodos. Cuando estos nodos reciban dicha petición, estos informarán de aquellos nodos mas cercanos a ellos, y así sucesivamente.
Existen aplicaciones de acceso público que permiten dimensionar la red a nivel mundial por medio de la utilización de este protocolo de descubrimiento, por ejemplo: *Bitnodes*, que presenta una vista en el mapa mundial de todos los nodos Bitcoin descubiertos.

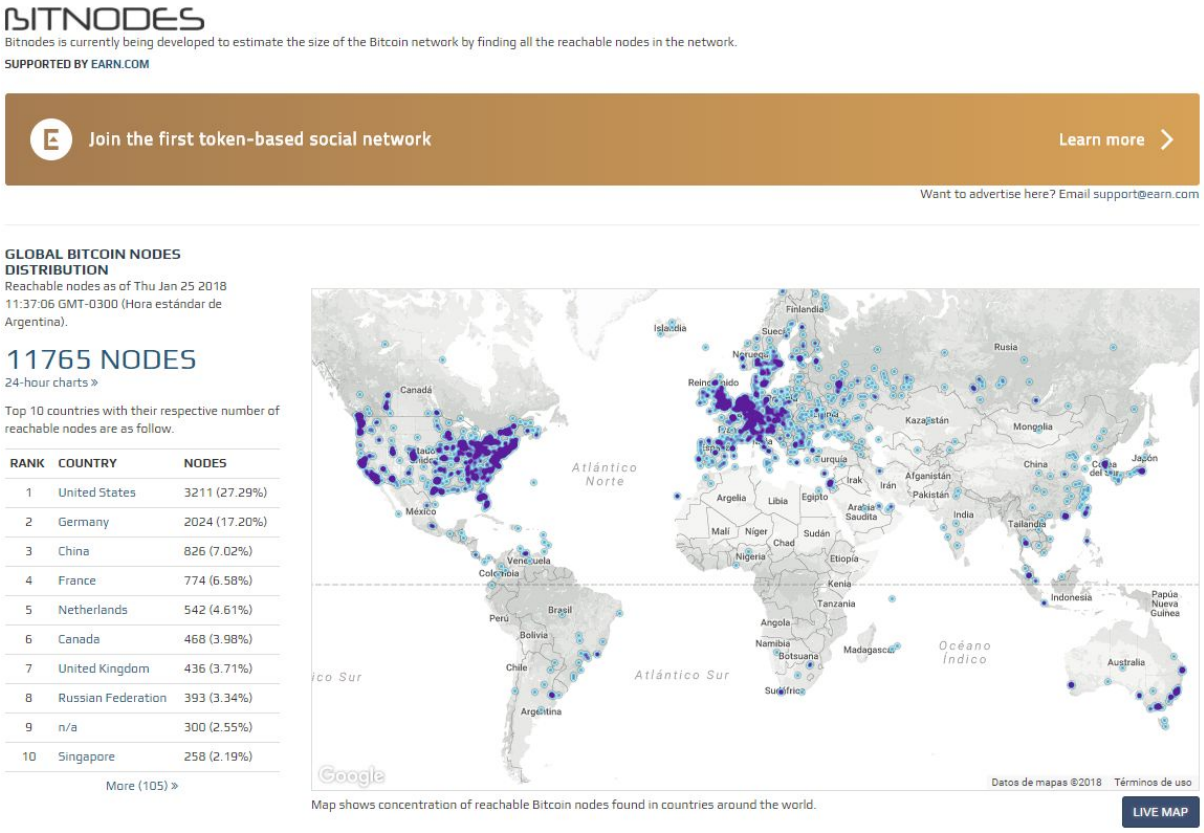

Ilustración 9: Vista sitio web bitnodes.earn.com

Dada una investigación forense, la aplicación web de la *Ilustración 9* podría ser utilizada para determinar a partir de una dirección IP si es que esta conectada a esta red o bien consultar el registro histórico de la misma cruzando los datos con la información proveida de *blockchain.info*.
No obstante, también se podrían cruzar los datos la información proveida por servicios como Shodan[12] o Mr. Looquer[13] sabiendo que en general estos nodos responden como un User-Agent que incluye la palabra Satoshi junto con la versión del protocolo que están ejecutando.
En consiguiente, podrían realizarse búsquedas por puertos por defectos de los diferentes clientes Bitcoin, como es el caso de Bitcoin Core con puertos por defecto en 8332 y 8333.

[12] https://www.shodan.io/
[13] http://mrlooquer.com/

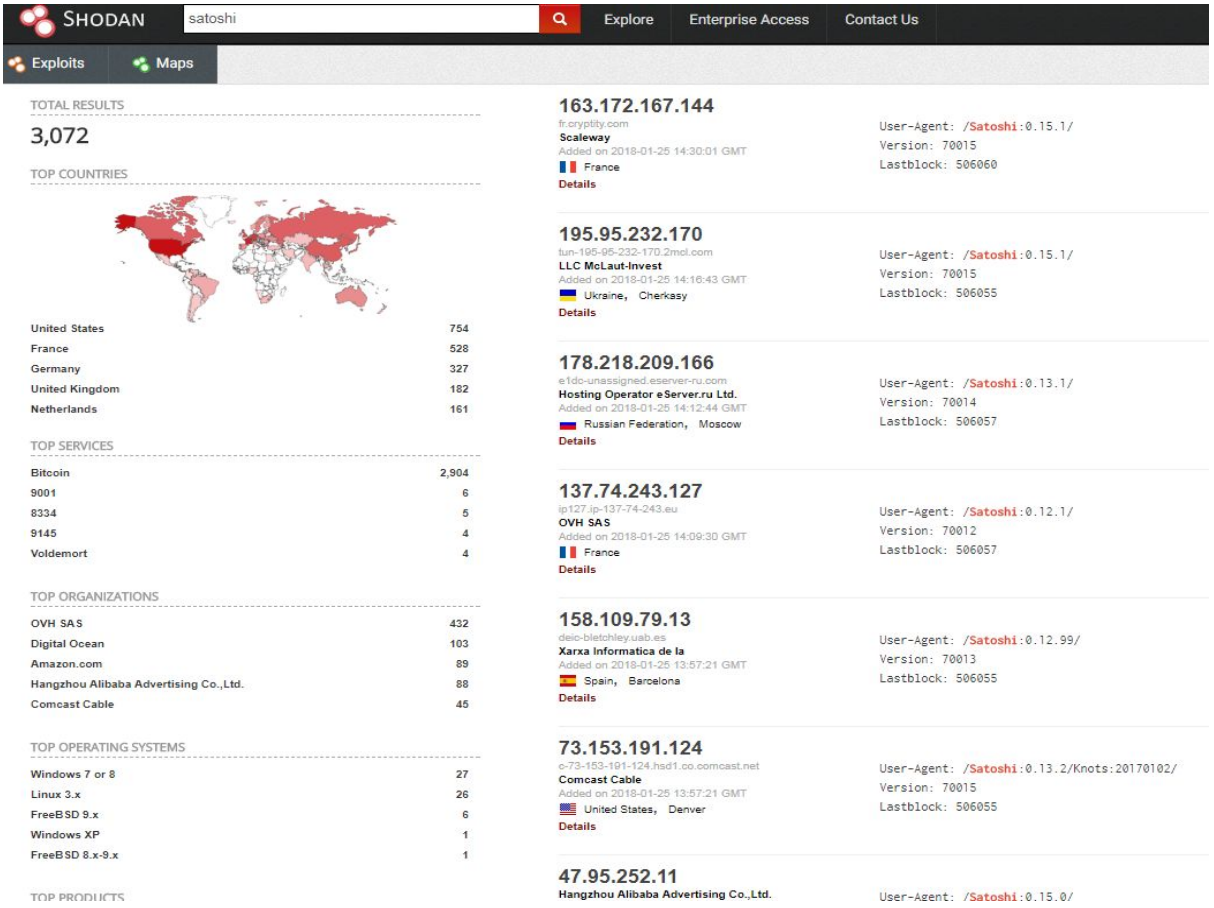

Ilustración 10: Vista sitio web shodan.ioi en búsqueda del termino "satoshi"

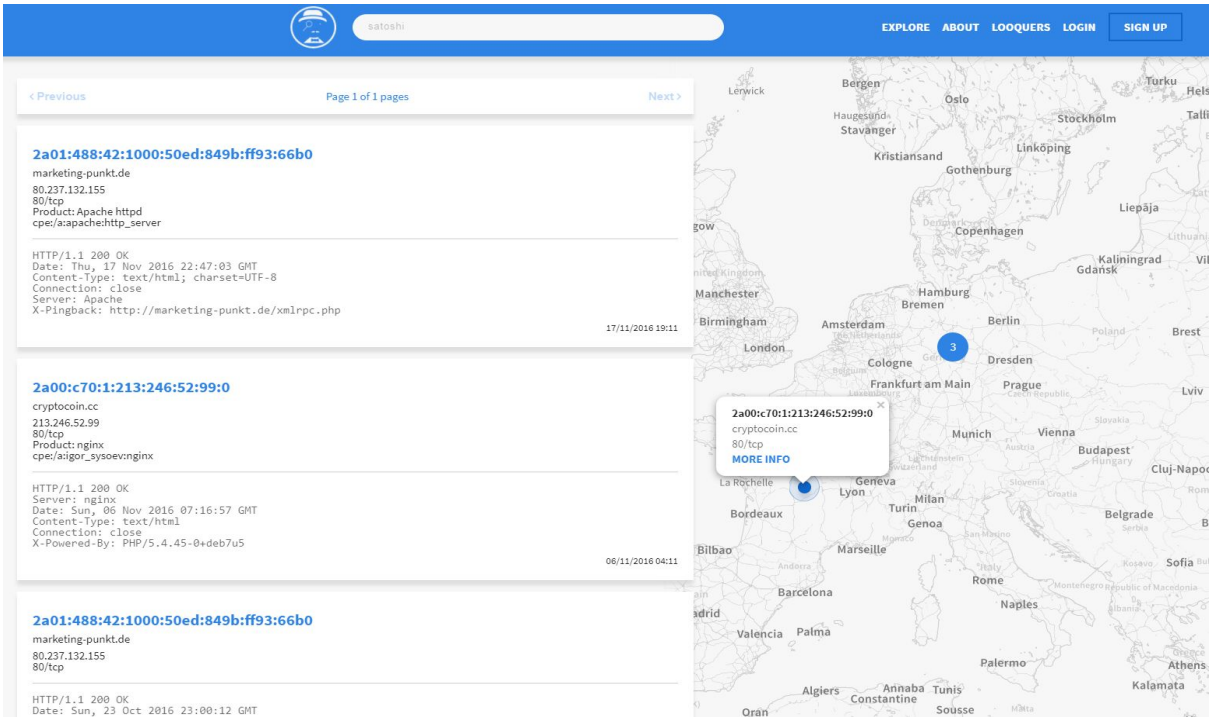

Ilustración 11: Vista sitio web mrlooquer.com en búsqueda del termino "satoshi"

Sin acceso al dispositivo

Generalmente a la hora de realizar investigaciones que tengan que ver con criptomonedas, no se cuenta con acceso físico al equipo, por lo tanto, es conveniente comenzar por las fuentes públicas disponibles, es decir, la *blockchain*.
En función del número de consultas que se desea realizar se podrá optar por diferentes exploradores en Internet, como ser blockexplorer.com o blockchain.info (ya anteriormente nombrado). En el caso que se deseen realizar consultas masivas y automatizadas también es posible y no muy complejo implementar un explorador de la cadena de bloques con una API Rest incluida.

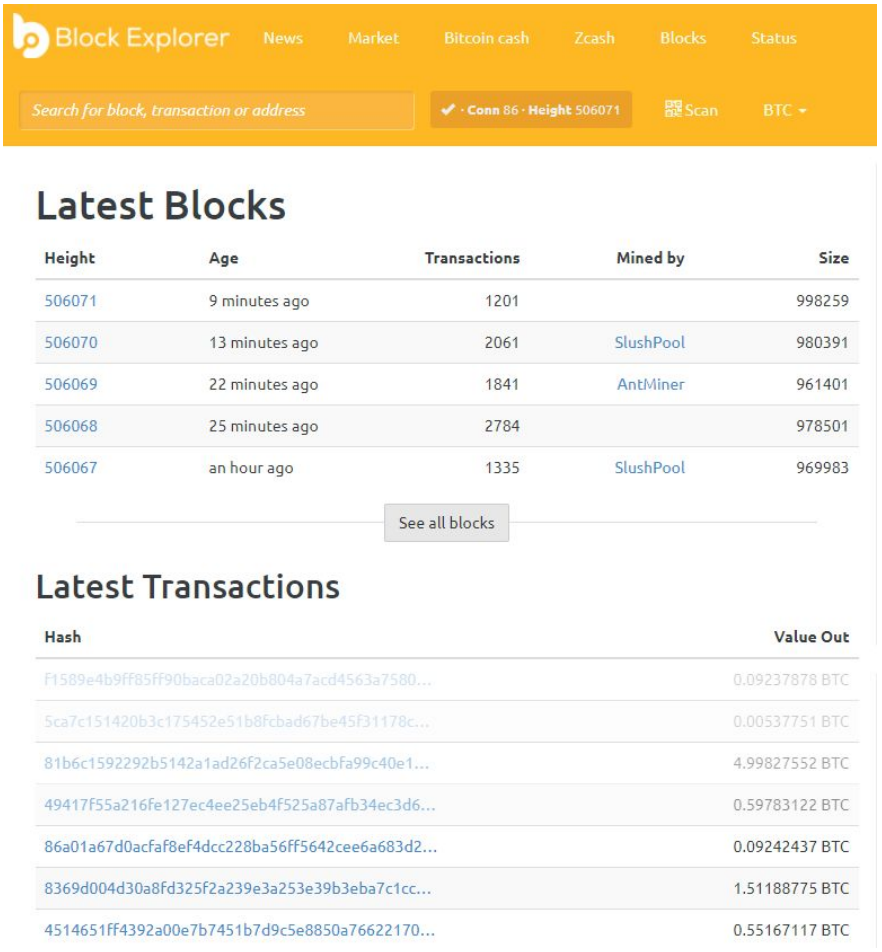

Ilustración 12: Vista sitio web blockexplorer.com

Estos portales de consultas presentan la información de forma más amigable que accediendo en crudo a la cadena de bloques, por lo tanto, se podrán visualizar por medio de filtros los bloques minados recientemente, últimas transacciones en tiempo real, gastos duplicados, transacciones sin confirmar, direcciones más populares, etc.

Dentro del apartado de los bloques minados recientemente se podrá extraer la altura del bloque en la *blockchain*, tiempo transcurrido desde que se minaron los bloques, número de transacciones dentro de cada bloque, cantidad de bitcoins transferidos, nombre del pool de minería que ha resuelto el bloque y tamaño de los mismos.
Existe la posibilidad también de realizar búsquedas más específicas por medio del buscador de la cadena de bloques, por ejemplo: por altura de bloque, dirección Bitcoin, identificador del bloque, identificador de transacción o direcciones IP.
Otra funcionalidad muy interesante que proveen estas páginas de consultas es la categorización de operaciones en base a la información de contexto que se conoce. Estas mismas tienen la capacidad de etiquetar si un bloque fue sido añadido por uno u otro pool de minería en base a las direcciones IP.

Ilustración 13: Vista sitio web blockchain.info generación de grafo de direcciones relacionadas

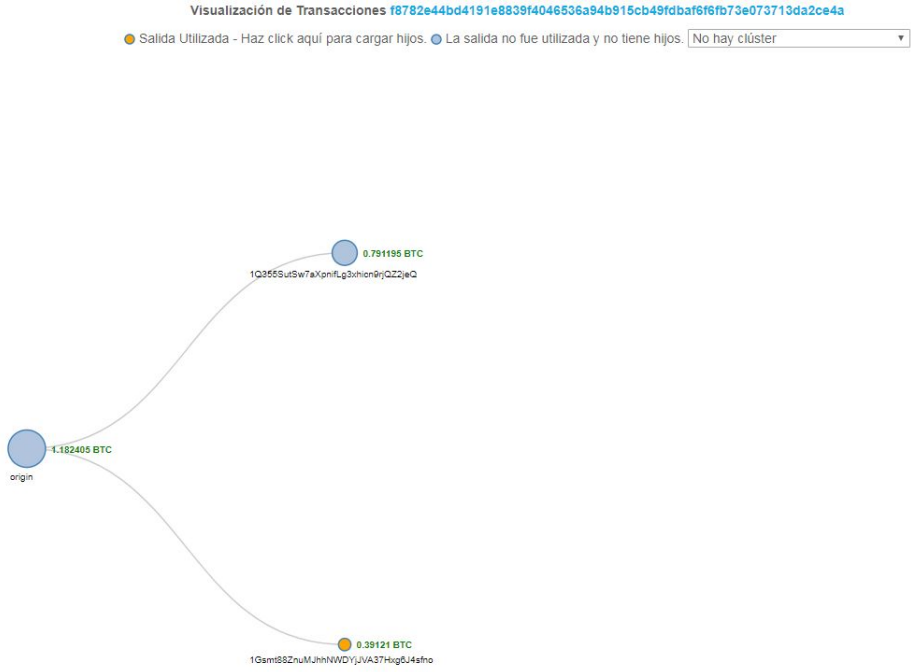

Ilustración 13: Grafo de árbol simple generado por blockchain.info

Pagos en la Deep Web

Una de las soluciones más potentes en el campo de la privacidad y el anonimato, son las redes anónimas y la posibilidad de acceder a servicios que solamente se encuentran disponibles dentro de dichas redes. Actualmente existen algunas soluciones que son interesantes desde el punto de vista de TOR, I2P o Freenet. Se trata de soluciones avanzadas y maduras que existen actualmente en el campo del anonimato y privacidad, en consiguiente, estas tecnologías cuentan con un gran apoyo por parte de la comunidad usuaria.

En la última década el término "deep web" se ha ido popularizando y extendiendo tanto entre la comunidad *hacker*, como entre los usuarios comunes en Internet. No obstante son muchas las premisas erróneas sobre el término en cuestión, ya que en muchas ocasiones se utiliza de forma indistinta a otros términos como "dark web" o "darknet".

El término "deep web" hace referencia principalmente a contenidos que no se encuentran indexados por los más grandes motores de búsqueda en Internet, no obstante, resulta imposible localizarlos. Los motivos por los cuales cierto contenido no se encuentra indexado por los grandes buscadores como Google y Yahoo pueden ser muy variados, sin embargo, generalmente uno de los motivos es debido a que el contenido es demasiado antiguo, existe mejor contenido y mayormente accedido que otro, o simplemente se encuentra protegido por sistemas de encripción y/o autenticación. En la *deep web* el contenido se encuentra en Internet, pero dicho contenido se encuentra accesible por fuera de los motores de búsqueda convencionales, y si dado el caso estuviesen indexados por los mismos, estos serían muy difíciles de hallar.

Por otra parte, el término *dark web* se refiere a contenido no indexable por decisión de los autores, los cuales comparten dicho contenido en otros medios como ser redes privadas o sitios web protegidos por sistemas de autentificación.

Finalmente el término *darknet* pertenece a un subconjunto de *deep web* que representa un espacio protegido por una red privada o al que solamente un número reducido de usuarios autorizados pueden acceder. Estos contenidos no se encuentran indexados por ningun buscador convencional, de hecho, en algunos casos el acceso a algún servicio determinado requiere una configuración especial y poco convencional para acceder a dicha red, por ejemplo el nodo cliente-servidor TOR.

Aunque existe una gran porción de la comunidad que aprovechan estas funcionalidades de privacidad y anonimato para actividades delictivas, como ser pagos con criptomonedas a cambio de algún servicio ilícito, o utilización de estos servicios anónimos para realizar pagos que sean muy difíciles de "*tracear*", estos proyectos fueron llevados a cabo para todo lo contrario, es decir, para que las personas puedan ejercer derecho a la privacidad y libertad en la navegación, sin censuras ni restricciones al momento de acceder a contenidos que se encuentran prohibidos por el país u organización en donde se encuentran.

No obstante, no significa que estas herramientas sean buenas o malas, simplemente aporta los medios para conseguir diversos fines y lamentablemente, en algunos casos dichos fines incluyen actividades ilegales.
Cuando se realizan acciones ocultas en cualquiera de las *darkents* que incluyan por ejemplo tráfico de contenidos ofensivos o denigrantes, lo mejor que se puede hacer es denunciarlo, o también es posible intentar detectar ciertas vulnerabilidades que puedan ser utilizadas por los cuerpos de seguridad o los organismos pertinentes para la identificación de los administradores del sitio en cuestión. Aunque se trata de servicios que se encuentran en la darknet, pueden verse afectados por cualquiera de las vulnerabilidades a las que enfrenta cualquier servicio en Internet, en este sentido no existe ninguna diferencia entre sitios web en Internet y una *darkent*.

Algunos ataques y vulnerabilidades documentadas

- Un hacker de sombrero blanco del grupo "Anonymus", quien durante el mes de febrero cerró un aproximado de 10.613 páginas de la Darknet por comerciar con pornografía infantil [34]
- Un equipo de investigadores de la firma de ciberseguridad italiana descubrió una vulnerabilidad crítica en Tor Browser que pone al descubierto la dirección IP real de los usuarios [35]
- Desarrolló un programa que ayudó a colocar en el mapa a 95.000 personas que habían descargado fotografías y vídeos en los que aparecían niños sufriendo algún tipo de abuso [36]
- Un hacker demostró que la web oscura puede ser fácilmente comprometida y la da de baja por publicar pornografía infantil [37]

Capítulo 4 - Conclusiones y Trabajos a Futuro

Conclusiones

Son cada vez más frecuentes aquellos actos de cibercriminalidad cuyo pagos se realizan mediante monedas virtuales. Como se vió en el desarrollo de este trabajo final, resaltan los diferentes tipos de actos delictivos como los ataques de denegación de servicio distribuidos, cifrado de discos/ robo de información, venta de bases de datos de usuarios y contraseñas, extorsión con contenido sexual, venta de drogas, armas y lavado de dinero.
En el desarrollo de este trabajo se demostró que existe mucha información para extraer desde dispositivos que han estado operando con criptomonedas, no obstante las mismas también suelen utilizarse en mercados ocultos como los ubicados en la *darknet* con el fin de lograr mayor anonimicidad posible de forma tal de dificultar la realización de traceos con resultados positivos por parte de los investigadores forenses.
No obstante, también se demostró que en cualquiera de los casos, siempre es posible intentar verificar si una red o equipo está ejecutando algún tipo de cliente relacionado con criptodivisas aprovechando las características del protocolo de descubrimiento y diferentes herramientas de búsquedas existentes en Internet, así como también determinar si ademas de estar utilizando servicios de criptomonedas están utilizando servicios anónimos como TOR.
Para finalizar, la conjunción *darknet* y **Bitcoin** plantea un reto de gran complejidad desde el punto de vista de la anonimidad y privacidad para las agencias de investigación forense y fuerzas policiales. Su propia naturaleza hace que los procedimientos convencionales sean insuficientes para dicha tarea, siendo imprescindible acomodarlos a un entorno estandarizado para lograr un eficaz y eficiente análisis de las mismas para converger a resultados positivos dado el caso de la ocurrencia de actos criminales.

Trabajos a Futuro

En este trabajo final se hizo hincapié en ciertos clientes de criptomonedas en especial de Bitcoin, pero la realidad es que hoy en día, a los pasos a los que avanza la tecnología y crece la comunidad usuaria, es necesario contar con un conocimiento de análisis forenses en todas las formas de utilización, como por ejemplo: dispositivos móviles, otras criptomonedas y las diferentes implementaciones de clientes de las mismas.
Por lo tanto, entre los trabajos futuros para esta línea de investigación, se identifica la estandarización de procedimientos de análisis forense profundo, no solo para criptomonedas, sino orientado a medios por los cuales se utilizan las mismas, como por ejemplo la *darknet*.

Bibliografía

1. "Bitcoin Project".https://bitcoin.org/es/ . Consultado en Septiembre 2017
2. "Blockchain: Blueprint for a New Economy". Melanie Swan. ISBN 9781491920473
3. https://www.nytimes.com/es/2016/08/03/snowden-y-wikileaks-debaten-por-la-forma-de-divulgar-documentos-secretos/ . Consultado en Septiembre 2017
4. "Bitcoin For Dummies". Pryptor . ISBN 9781119076131
5. "Deep Web". Pablo Allegritti. ISBN 9789876277587
6. "Wayniloans Project". https://www.wayniloans.com/ . Consultado en Septiembre 2017.
7. "Cubits Project". https://cubits.com/ . Consultado en Septiembre 2017.
8. "Kraken Project". https://www.kraken.com/ . Consultado en Septiembre 2017.
9. "Xapo Project". https://xapo.com/ . Consultado en Septiembre 2017.
10. "Litecoin Project". https://litecoin.org/es/. Consultado en Septiembre 2017.
11. "Ripple Project". https://ripple.com/ . Consultado en Septiembre 2017.
12. http://www.diariobitcoin.com/index.php/2016/12/08/oficina-del-fiscal-de-estados-unidos-pago-1-400-en-bitcoins-a-extorsionistas-de-software-malicioso/ . Consultado en Septiembre 2017 .
13. https://hipertextual.com/2017/07/nuevo-modo-extorsion-empresas-ataques-ddos . Consultado en Septiembre 2017 .
14. http://masterhacks.net/noticias/detienen-a-hacker-uruguayo-por-extorsion-a-mutualista-con-bitcoins/ . Consultado en Septiembre 2017.
15. http://es.gizmodo.com/el-director-del-mayor-banco-de-ee-uu-cree-que-bitcoin-1806528213 . Consultado en Septiembre 2017.
16. https://criptonoticias.com/colecciones/especial-un-dia-ransomware-bitcoin-volvieron-socios/ . Consultado en Septiembre 2017.
17. https://criptonoticias.com/sucesos/surcorea-alerta-amenaza-hackers-siete-bancos-pais/ . Consultado en Septiembre 2017.
18. http://eldiariodemadryn.com/2017/05/deep-web-la-via-paralela-y-libre/ . Consultado en Septiembre 2017.
19. Privacidad como acceso restringido a la información. La privacidad en el ciberespacio. Una aproximación filosófica en el entorno digital a partir de un estudio de caso sobre el buscador Google. Ana María Arconada Beasoain de Paulorena. P 90.
20. Bitcoin: A Peer-to-Peer Electronic Cash System . Satoshi Nakamoto
21. http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source. Consultado en Octubre 2017

22. Certicom Research, "SEC 2: Recommended Elliptic Curve Domain Parameters."
23. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf . Consultado en Octubre 2017.
24. http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf. Consultado en Octubre 2017.
25. https://es.wikipedia.org/wiki/Advanced_Encryption_Standard . Consultado en Octubre 2017.
26. https://es.wikipedia.org/wiki/RIPEMD-160 . Consultado en Octubre 2017
27. https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida. Consultado en Octubre 2017
28. https://es.wikipedia.org/wiki/%C3%81rbol_de_Merkle . Consultado en Octubre 2017
29. https://en.bitcoin.it/wiki/Protocol_documentation#Message_types . Consultado en Noviembre 2017
30. La revolución blockchain (Blockchain Revolution), Don Tapscott & Alex Tapscott. Deusto.
31. An Integrated Reward and Reputation Mechanism for MCS Preserving Users' Privacy. Cristian Tanas, Sergi Delgado-Segura, Jordi Herrera-Joancomartí. Febrero de 2016. Data Privacy Management, and Security Assurance. pp 83-99
32. La Revolución de la tecnología de Cadenas de Bloques en la economía: Impacto en los distintos Sectores Económicos, Santiago Moreno Ismael. Marzo de 2017. EAE.
33. https://es.wikipedia.org/wiki/Anexo:Script_(Bitcoin)#cite_note-basurto-1 . Consultado en Noviembre 2017.
34. https://www.criptonoticias.com/colecciones/12-hackeos-mayor-impacto-2017/. Consultado en Enero 2018
35. https://computerhoy.com/noticias/software/vulnerabilidad-critica-tor-browser-filtra-ip-real-del-usuario-70791. Consultado en Enero 2018
36. https://www.genbeta.com/a-fondo/este-hacker-descubrio-que-la-policia-dirigia-un-portal-de-pornografia-infantil-en-la-darknet. Consultado en Enero 2018
37. http://www.cioal.com/2017/02/08/hackean-20-la-darknet/. Consultado en Enero 2018