Análisis del anonimato aplicado a criptomonedas

Ignacio Gallardo [1 2], Patricia Bazan [2], Paula Venosa [2]

igallardo@info.unlp.edu.ar, pbaz@info.unlp.edu.ar, pvenosa@info.unlp.edu.ar

[1] Universidad de la Defensa Nacional - Facultad de Ingeniería del Ejército, Palermo, CABA, Argentina.

[2] Universidad de la Plata - Facultad de Informática - Laboratorio de Investigación de Nuevas Tecnologías Informáticas, La Plata, Argentina.

DOI: 10.17013/risti.n.pi-pf

Resumen: Este trabajo 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.

Palabras-clave: Anonimato; privacidad; criptomonedas; blockchain; bitcoin.

Analysis of anonymity applied to cryptocurrencies

Abstract: *This work shows an in-depth study of Bitcoin technology, in which a qualitative analysis of its functionalities and architecture is addressed. It also describes different techniques and uses purposes that a user could potentially achieve with this technology. Finally, it presents an analysis of the possibility of applying different discovery practices in the presence of an investigation of the cybercriminal use of cryptocurrencies.*

Keywords*:* Anonymity; privacy; cryptocurrencies; blockchain; bitcoin.

1. 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 y las actividades desempeñadas por organizaciones como la NSA o la CIA. 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 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**, 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**.

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.

2. 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 principales de estos ataques se clasifican en dispositivos inteligentes de cualquier tipo como: móviles, computadoras, cámaras de vigilancia y vehículos conectados.

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***, 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).

También se rentan ***botnets*** por entre 0,02 y 0,04 bitcoins (170 y 350 dólares) por hora para enviar ***Spam*** o hacer ataques de ***DNS*** 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.

3. Metodología

Se realizará un estudio en profundidad de la tecnología Bitcoin abordando un análisis cualitativos de sus procedimientos, arquitectura y core de funcionamiento: ***Blockchain*** o **Cadenas de Bloques**.

Se describirán diferentes técnicas y medios de uso, con el fin de determinar los fines con los que potencialmente un usuario podría llegar a utilizar esta tecnología.

Se analizará la posibilidad de poder poder presentar diferentes prácticas a realizar ante la posibilidad de investigar el uso de las criptomonedas.

3. Criptomonedas

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.

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.

El 11 de febrero de 2009, un perfil creado en el portal P2P foundation, 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.

3.1 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.

3.1.1 El papel de la Criptografía

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 para firmar digitalmente las transacciones, utilizando los parámetros recomendados por el Standards for Efficient Cryptography Group (SECG), secp256k1. Las firmas utilizan la codificación DER 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 y, cuando se requiere que el hash sea más corto, RIPEMD-160. 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.

3.1.2 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**.

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.

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.
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)*

Figura 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.

3.1.3 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.

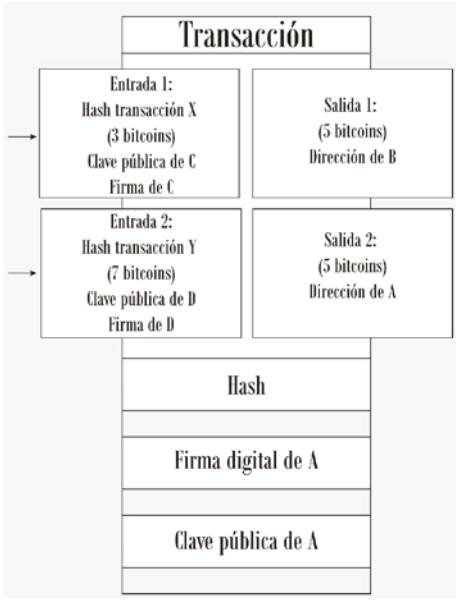


Figura 2 - Esquema de transacción Bitcoin

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.

3.1.4 Manipulación de 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.

3.1.4.1 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.

3.1.4.2 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.

3.1.4.3 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.

3.1.4.4 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.

4. Análisis del anonimato

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.

4.1 Traceando Bitcoins

Bitcoin, como visto en la sección anterior 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 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*.

4.1.1 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*.

4.1.2 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.

4.1.3 Análisis de grafo

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 ∈ L lleva un número de monedas Cl. De forma inherente las transacciones tienen un orden total definido por el *blockchain*, y no pueden existir ciclos en τ .

4.1.4 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 ∈ L0 para poder distinguir entre múltiples asignaciones y un par de direcciones.

4.2 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 encontrarán 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 fácilmente 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.

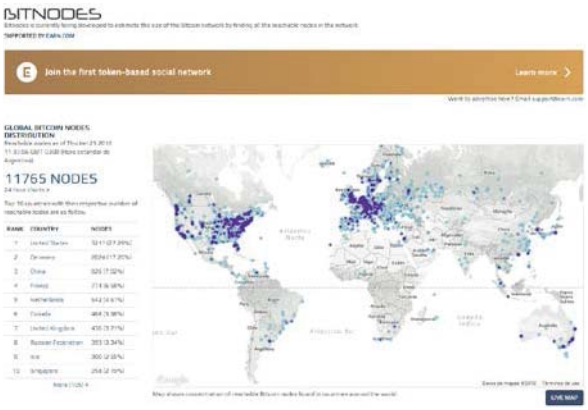
En cualquier caso habrá que determinar si el objetivo de la investigación es la incautación de los fondos que contiene la cartera o no, ya que para el momento de la incautación o acceso al equipo, el propietario de la cuenta bitcoin podría haber realizado un backup y realizar las transferencias de sus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

4.3 Identificando 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 más 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.



Fugura 3 -Vista sitio web bitnodes.earn.com

Dada una investigación forense, la aplicación web de la *Figura 3* 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[1] o Mr. Looquer[2] 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.

4.4 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.

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.

4.5 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

[1] https://www.shodan.io/
[2] http://mrlooquer.com/

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*.

6. Trabajos Futuros

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*.

7. 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 trakings 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 además 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.

8. Referencias Bibliográficas

Adams, M. (2016). *Blockchain: The history, mechanics, technical implementation and powerful uses of blockchain technology*. Matthew Adams.

Antonopoulos, A. M. (2018). *Mastering bitcoin: Programming the open blockchain*. Beijing ; Boston ; Farnham ; Sebastopol ; Tokyo: OReilly.

Bahga, A., & Madisetti, V. (2017). *Blockchain applications a hands-on approach*. Verlag nicht ermittelbar.

Blake, I. F., Seroussi, G., & Smart, N. P. (1999). *Elliptic curves in cryptography*. Cambridge University Press.

Capoti, D., Colacchi, E., & Maggioni, M. (2015). *Bitcoin revolution: La moneta digitale alla conquista del mondo*. Milano: U. Hoepli.

Choi, Kyung-shick, and Toro-Álvarez Marlon Mike. *Cibercriminología: guía Para La investigación Del Cibercrimen y Mejores prácticas En Seguaridad Digital = Cybercriminology: Guide for Cybercrime Investigation and Best Practices in Digital Security*. Universidad Antonio Nariño, 2017.

Finch, V. (2017). *Bitcoin: The only complete quick & easy guide to mastering Bitcoin and digital currencies*. Auva Press. *Mastering bitcoin for beginners*. Publisher not identified.

Hoskinson, Charles (2013), "The Mathematician's Defense of Bitcoin: It's Just Another Option".

Jayawardena, Kasun P. *A Criminological Analysis: Using Real-Time Monitoring to Gather Data on Online Predators*. 2011.

Jenkins, Y., & Jenkins, Y. (2015). *Bitcoin: Millionaire maker or monopoly money?* Publisher not identified.

Johnson, E. C. (2017). *Cryptocurrency: The beginner's guide to investing and trading in cryptocurrency*. CreateSpace Independent Publishing Platform.

Papacharissi, Zizi. *A Networked Self: Identity, Community and Culture on Social Network Sites*. Routledge, 2011.

Satoshi, Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf.

Shane, P. M., & Hunker, J. A. (2013). *Cybersecurity: Shared risks, shared responsibilities*. Carolina Academic Press.

Steinmetz, R.; Wehrle, K (2005). *2. What Is This "Peer-to-Peer" About?*. Springer Berlin Heidelberg. pp. 9-16.

The Dark Web: Breakthroughs in Research and Practice. IGI Global, Disseminator of Knowledge, 2018.

Vacca, J. R., & Vacca, J. R. (2013). *Computer and information security handbook*. Morgan Kaufmann is an imprint of Elsevier.

Vigna, P., & Casey, M. (2015). *The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order*.