A Method for Blockchain Transactions Analysis

V. Macedo, M. Rosales, and G. García, *Members IEEE*

***Abstract*—A *ransomware* is a kind of malware used for digital extortion purposes, where victims must make a payment with a cryptocurrency in exchange of information or compromised systems. This article presents a method to analyze the dynamic of Bitcoin transactions related to ransomware, through the representation of the blockchain as a directed network, and the measurement of the corresponding parameters, as well as statistical analysis and a transaction tracking.**

***Index Terms*—Blockchain analysis, Bitcoin, Payment network, Ransomware, WannaCry.**

I. Introducción

ALREDEDOR del mundo se ha propagado una nueva amenaza cibernética conocida como *ransomware*, un tipo de software malicioso, cuyo objetivo es la obtención de un pago por parte de la víctima a través de métodos de extorsión digital. Aunque su origen se remonta al año de 1989, este fenómeno ha tomado fuerza particular desde 2013 con el ataque perpetrado por *CryptoLocker* [1] [2]. La evolución que han tenido los ataques mediante ransomware desde su aparición hasta la actualidad, permite sugerir una clasificación en tres categorías:

- **De bloqueo:** Ataca principalmente dispositivos IoT, bloqueando el acceso al usuario hasta que se realice el pago correspondiente.
- **De cifrado:** Su objetivo es cifrar los archivos resguardados en los dispositivos que infecta, y exigir un pago a cambio de la herramienta de descifrado.
- **De control:** Interfiere con sistemas completos, tomando el control de éstos y exigiendo el pago a cambio de su liberación.

Actualmente, estos pagos son operados generalmente en el sistema *Bitcoin* [3], que ofrece, además de un alto valor de mercado, un alto nivel de anonimato al operar, debido a que no es necesario asociar los pagos con datos personales del emisor o del receptor, lo cual es una característica deseable en los sistemas de pago [4]. Lo anterior, ha favorecido que este sistema sea aprovechado por ciberdelincuentes para propagar ransomware con la finalidad de obtener ganancias de manera rápida y anónima. Los pagos obtenidos, al igual que todas las transacciones en Bitcoin, se registran en una base de datos distribuida conocida como *blockchain*, cuya información es pública.

Con base en lo anterior, la contribución de este trabajo consiste en una propuesta de método de análisis del blockchain de Bitcoin para identificar la dinámica de las transacciones asociadas a los pagos generados por infecciones de ransomware. Este método considera la medición de parámetros propios del grafo generado a partir de las transacciones estudiadas, con el objetivo de obtener información sobre los métodos de dispersión y de lavado de dinero que utilizan los responsables de un ciber delito. Como caso de estudio, se consideró el ataque global ocurrido el 12 de Mayo de 2017, en el cual se propagó un tipo de ransomware llamado *WannaCry*.

Este documento está organizado de la siguiente manera: en la Sección II el lector encontrará una reseña de los trabajos previos que han abordado el análisis de las transacciones en el blockchain. En la Sección III se describe el método propuesto para realizar el análisis y caracterizar algún fenómeno en esta estructura. Posteriormente, la Sección IV aborda el caso de estudio de esta investigación, un análisis sobre los pagos recaudados por WannaCry. En la Sección V se abordan los resultados y su discusión, y finalmente las conclusiones son presentadas en la Sección VI.

II. Trabajos Relacionados

El blockchain de Bitcoin es el componente de su arquitectura que almacena información de las transacciones válidas generadas. La información está disponible de manera pública, e incluye los montos de las transacciones, la fecha y hora en que fueron procesadas, algunos datos propios del protocolo de Bitcoin y el emisor y receptor del pago, sin embargo, no se registra la identidad de quienes realizan las operaciones, sino que se usan identificadores alfanuméricos, los cuales están desasociados de las entidades físicas a las que pertenecen. Dichos identificadores son conocidos como *direcciones bitcoin* y se clasifican en *direcciones de origen*, desde las cuales se hace un pago, y *direcciones de destino*, es decir, las que reciben el pago. A partir de esta característica, diversos estudios han logrado asociar determinadas direcciones con sus respectivas entidades propietarias, por esta razón, la comunidad científica apunta a que en realidad lo que Bitcoin ofrece es *pseudoanonimato* [5]. A continuación se describen las técnicas de análisis del blockchain que han sido desarrolladas con el objetivo de identificar y asociar direcciones Bitcoin con sus propietarios. El estudio de los ataques a los sistemas blockchain queda fuera del alcance de este artículo, el lector interesado puede consultar el trabajo de Xiaoqi Li *et al*. en [6].

A. Clustering y Asociación de Direcciones con Entidades

Diversas investigaciones se han enfocado en el rastreo de transacciones y asociación de direcciones. Una de las primeras, corresponde a la presentada por Reid y Harrigan en 2013, en la cual propusieron un método para asociar direcciones entre sí, a través de un enfoque en redes, incorporando información de fuentes externas, entre las cuales estaban las direcciones públicamente asociadas a entidades diversas [7]. El mismo año, Meiklejohn *et al.* en [8] describió el proceso de *peeling*

V. R. Macedo corresponding author, vreyesm1102@alumno.ipn.mx.
V. R. Macedo, M.S. Rosales and G. G. García.
Instituto Politécnico Nacional, México

chain, a través de un análisis activo, que consistió en un ataque de reidentificación de bitcoins utilizados como pago en diversos servicios, para posteriormente aplicar técnicas de asociación de direcciones. El proceso de *peeling chain* es iterativo, y consiste en dispersar los fondos concentrados en una dirección, haciendo un pago por una cantidad considerablemente pequeña, para devolver el cambio a una dirección nueva o a la dirección de origen. Posteriormente, en 2015 Zhao y Guan propusieron un método con base en grafos para analizar las propiedades de los flujos de pagos en Bitcoin y así identificar grupos de direcciones. Como caso de estudio tomaron el robo sufrido por la operadora japonesa MtGox [9] .

B. Detección de Ransomware en el Blockchain

En 2013, Michele Spagnuolo presentó una herramienta llamada *BitIodine* cuyo objetivo fue trazar flujos de pago en Bitcoin, así como agrupar direcciones en clusters y etiquetarlos como propiedad de determinado usuario si éste está asociado con alguna de las direcciones. El autor realizó un estudio con esta herramienta sobre una muestra del ransomware *CryptoLocker*, recolectando 2118 direcciones pertenecientes al malware. En total, el autor identificó 771 pagos de rescate cuya suma equivale a 1226 BTC, aproximadamente USD $1,100,000 al 5 de diciembre de 2013 [10] .

Kharraz *et al.* realizaron un análisis al flujo de 1,872 direcciones Bitcoin usadas en un ataque de Cryptolocker en [11]. El análisis de las transacciones demostró que los cibercriminales han adoptado técnicas de evasión con el objetivo de encubrir la actividad sospechosa. Dicho análisis también confirmó que las direcciones Bitcoin usadas en actividades ilícitas tuvieron comportamientos similares como un período de actividad corto, se usaron para transferir cantidades menores de bitcoins y en un número pequeño de transacciones.

Por otro lado, en 2016, Kevin Liao *et al.* llevaron a cabo un análisis de los pagos relacionados con CryptoLocker en [2]. Los autores crearon un cluster de 968 direcciones relacionadas con el ransomware. Con ello identificaron 795 pagos de rescate que sumaban 1,128.40 BTC. Además, analizaron los pagos de manera longitudinal (sobre el período de actividad de CryptoLocker) y transversal (sobre las horas del día) para detectar cambios en la distribución del malware.

En 2018, Danny Yuxing Huang *et al.* en [12], desarrollaron un conjunto de metodologías que permiten un rastreo de transacciones a profundidad, mediante un estudio de dos años de distintas muestras de familias de ransomware, en el cual estimaron un total de $16 millones de dólares en rescates de 19750 víctimas potenciales. Además, lograron identificar una casa de cambio de divisas electrónicas rusa, llamada BTC-e, que al parecer era una pieza clave para convertir el dinero obtenido de los pagos de rescate en dinero físico. En dicho trabajo, los autores obtuvieron direcciones asociadas a ransomware a través de dos medios, víctimas reales que reportaron la infección de sus equipos y la dirección a la que debía pagarse el rescate, y a través de una *generación sintética de víctimas*, mediante la cual ejecutaron el malware en un ambiente controlado.

De los trabajos mencionados, se observa que, a pesar de que Bitcoin es famoso por proveer anonimato, el análisis del blockchain tiene el potencial para convertirse en un aliado para enfrentar diversos delitos en los cuales resulta involucrado este sistema. El método de análisis que se propone en la siguiente sección, aborda el enfoque de estas investigaciones con el objetivo de unificar las diferentes aproximaciones, y proveer un marco común que sirva como base para el posterior estudio de transacciones ejecutadas en blockchain, y asociadas a diferentes fenómenos.

III. MÉTODO PROPUESTO

La Fig. 1 muestra, de manera general, las diferentes etapas del método que se presenta: pre-procesamiento de datos, análisis de datos y análisis de resultados. Como se puede observar, se inicia con la recuperación de la información para tener acceso al historial completo de transacciones en el sistema. Posteriormente el proceso se divide en tres etapas: *pre-procesamiento de los datos*, que se lleva a cabo en dos etapas a las que se ha denominado *extracción de datos* y *filtrado de datos*, después se ejecuta el *análisis* que también se compone de tres procesos paralelos: *rastreo*, *análisis de la red* y *análisis estadístico*. La última etapa del proceso es el diagnóstico del estudio vía análisis de los resultados.

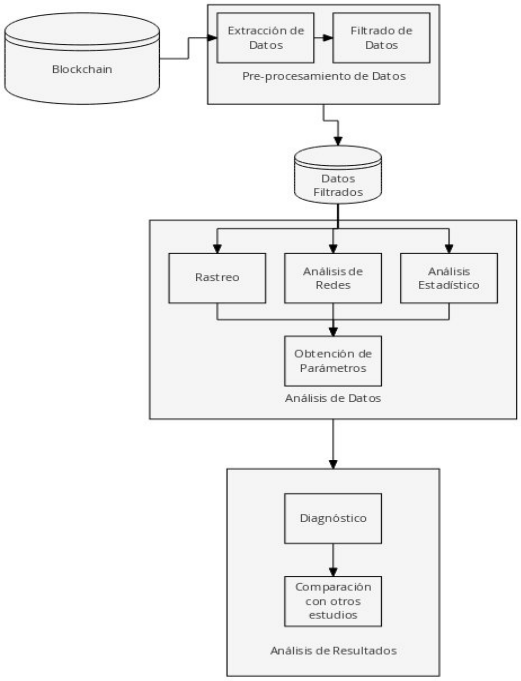


Fig. 1. Método propuesto.

A continuación se describen estas etapas.

A. Pre-procesamiento de Datos

El pre-procesamiento consta de dos etapas, que incluyen la extracción y el filtrado de los datos.

Extracción de Datos: Se inicia con la descarga del blockchain de Bitcoin desde el cliente original BitcoinCore. Con ello se obtiene el historial completo de transacciones del sistema. La estructura de organización de los bloques provee los siguientes campos de información, por cada uno de ellos:

- Número de transacciones
- Altura del bloque (Número del bloque)
- Marca de tiempo o *timestamp*
- Raíz de Merkle
- ID del bloque previo
- Dificultad de minado
- Hash del bloque
- Hash del bloque anterior
- Vector de transacciones
- Factor de aleatoriedad o *nonce*

Así mismo, cada bloque provee la siguiente información sobre las transacciones que contiene:

- **TxID:** Folio de la transacción
- **indexout:** Índice de la transacción
- **value:** Monto de la transacción en BTC
- **scriptPubKey:** Instrucciones para validar la transacción
- **address:** Dirección que recibe el pago.

Filtrado de Datos: Debido a la cantidad de transacciones que se obtienen al descargar el blockchain, es necesario realizar una depuración en función del fenómeno que se estudie, para lo cual se deberán aplicar los criterios más adecuados. De esta manera, es posible proponer como criterio de filtrado, por ejemplo, la fecha de las transacciones, el monto, *direcciones semilla,* entre otros, según sea conveniente. Las *direcciones semilla* se definen como aquellas direcciones de las que se tiene certeza sobre la identidad de su propietario.

B. Análisis de Datos

Con la información reunida, es posible proceder a realizar los tres procesos de análisis anteriormente mencionados; por rastreo, por parámetros de redes e indicadores estadísticos. El objetivo de este proceso, es obtener métricas sobre el movimiento de los pagos en la red Bitcoin, para arrojar información sobre las estrategias que siguen ciertos fenómenos cuyos operadores podrían tener interés en ocultar su rastro. A continuación se aborda la forma en que se sugiere realizar este proceso.

Rastreo:: El rastreo consiste en identificar la forma en que se distribuyen los pagos en la red una vez que han sido enviados a las direcciones semilla. Se espera que una vez depositado un pago en una dirección, ésta lo re-envíe a otra u otras con la finalidad de ocultar su rastro en la propia red. Luego dichos pagos son redistribuidos a través de diversas direcciones asociadas.

Es posible llevar a cabo este rastreo a partir de la información del blockchain, que puede ser consultada en sitios web como `https://blockchain.info`.

Por otra parte, también existen servicios en línea que ofrecen la posibilidad de etiquetar direcciones que de alguna forma está confirmado que pertenecen a alguna entidad en particular, lo cual resulta útil en un análisis de rastreo para identificar servicios como casas de cambio (*exchanges*), servicios de lavado (*laundry*), fundaciones o asociaciones, diversos servicios financieros, sitios de apuestas, por mencionar algunos.

Análisis de la Red: La disposición de los datos de las transacciones permiten visualizar el historial como una red dirigida, en la cual las direcciones serán consideradas nodos y el sentido de los pagos serán considerados como enlaces. El monto de los pagos representa, en este esquema, el peso del enlace. Con ayuda de una herramienta de visualización de redes es posible construir esta red y obtener información sobre el caso de estudio, por ejemplo, la dinámica de las transacciones, los nodos de mayor importancia y las estrategias que siguen los participantes para mejorar el pseudo anonimato de blockchain.

Entre los parámetros de interés, se consideran los sugeridos por Silva en [13], en particular, los siguientes para el caso de estudio:

- **Grado de un nodo:** Es una medida de centralidad que describe la estructura de una red en términos de la conectividad individual de los nodos, es decir, el número de enlaces con los que conecta. Si este valor es mayor respecto a los demás nodos, se considera que el nodo está bien conectado, es decir, se comunica con la red de mejor manera que un nodo con un valor menor. Para el caso de una red de transacciones, se usa la definición de grado de un nodo correspondiente a grafos dirigidos, que consiste en la expresión 1:

$$k_i = k_i^{in} + k_i^{out} \tag{1}$$

  Donde $k_i^{in} = \sum_{j=1}^{n} a_{ji}$ y $k_i^{out} = \sum_{j=1}^{n} a_{ij}$ son los grados de entrada y salida respectivamente para cada nodo.
  Dado que se aplica sobre una red dirigida, este valor indica el promedio de pagos que recibe el *i-ésimo* nodo y el promedio de pagos que envía.
- **Longitud de ruta:** Una ruta en una red es un recorrido a través de la red de vértice en vértice a lo largo de los enlaces. Así mismo, se define la longitud de ruta como el número de enlaces recorridos a lo largo de la ruta. Si suponemos que su longitud es de d_{ij}. Entonces, la longitud media de camino de i a j sobre todos los vértices j de la red se calcula mediante la expresión 2:

$$\iota_i = \frac{1}{n} \sum_j d_{ij} \tag{2}$$

  Para el caso de una red que represente las transacciones en blockchain, este parámetro indica el número promedio de direcciones por las cuales pasa una cantidad de bitcoins, desde que se le paga a la dirección semilla hasta que entra a un *exchange* o a una cuenta concentradora.
- **Componentes conexos:** Este parámetro indica la estructura de la red, es decir, el nivel de conectividad entre los nodos respecto a la red. Un valor alto indica una red aislada, mientras un valor menor indica una red fuertemente conectada en la que se puede acceder a cualquier nodo casi desde cualquier punto.

De manera formal, un grafo está *fuertemente conectado* si cada nodo v_i puede ser alcanzado mediante una ruta tal que $v_j \neq v_i$ para $j = 1, 2, ..., i-1, i+1, ..., n$ [14].

- **Centralidad del eigenvector:** Este parámetro mide la influencia de los nodos en su entorno, un valor alto indica una mayor influencia que un valor bajo. Sea x_i la centralidad del nodo i, entonces se tiene la expresión 3:

$$x_i = \frac{1}{\lambda} \sum_{j=1}^{n} A_{ij} x_j \tag{3}$$

Donde λ es una constante y $x = (x_1, x_2, ..., x_j)$ el vector de centralidades. Con ello es posible identificar las direcciones que sean de mayor importancia, si las hay, ante un fenómeno de estudio en el blockchain.

Análisis Estadístico: El análisis estadístico descriptivo permite conocer características particulares del comportamiento de las operaciones en el blockchain, como puede ser la distribución de las transacciones analizadas y las posibles correlaciones que existan con otras variables, además de las medidas de tendencia central y de dispersión usuales.

En particular, un análisis de este tipo permite además conocer la distribución geográfica y horario de los pagos realizados, lo cual es un indicativo de qué regiones son susceptibles de presenciar determinadas actividades (robo, lavado, extorsión o tráfico que se lleve a cabo usando la criptomoneda) que sean de interés.

Esto es particularmente útil al analizar los montos de las transacciones y los *timestamps* de las mismas, para lograr una caracterización *a posteriori* del fenómeno.

Para ello se lleva a cabo el siguiente procedimiento:

- Elaborar una tabla de distribución de frecuencias de los pagos organizadas respecto a la hora en que fueron efectuados.
- Elaborar una hipótesis sobre la forma en que influyen los horarios en la realización de los pagos.
- Fijar una ventana de tiempo de interés para ubicar los horarios que registran una mayor interacción en el sistema Bitcoin.
- Ajustar la ventana de tiempo de acuerdo con las diferentes zonas horarias alrededor del mundo, contrastando con la hipótesis elaborada.

C. Análisis de Resultados

El análisis de resultados consiste en interpretar las métricas obtenidas en el análisis de datos. Esto dependerá de los parámetros que se hayan considerado en la etapa anterior. Es importante verificar la validez de los resultados obtenidos, lo cual puede ser llevado a cabo mediante la comparación de las mediciones respecto a otras investigaciones, o proponiendo un grupo de control para verificar las variaciones en la medición de los parámetros.

IV. Caso de Estudio: *WannaCry*

Como caso de estudio se eligieron las transacciones generadas a partir del ciber ataque global perpetrado mediante el ransomware *WannaCry*, es decir, el método propuesto se aplicó sobre las transacciones asociadas al malware mencionado.

Esto se hizo con el objetivo de obtener características relevantes del comportamiento de los pagos que realizan las víctimas del ransomware a los responsables de éste, y conocer la forma en la que interactúan en el sistema Bitcoin.

Para el estudio, se descargó el cliente original de Bitcoin, *BitcoinCore.* Con ello se obtuvieron 1632 archivos en formato *.dat* cuya información abarca las transacciones realizadas desde Enero de 2009 hasta el 18 de Agosto de 2017.

A. Pre-procesamiento de Datos

La etapa de pre-procesamiento se compone de dos procesos: la extracción de los datos y su posterior filtrado.

Extracción de Datos: La extracción se llevo a cabo con la herramienta *Rusty-Blockparser*, desarrollada por Michel Spagnuolo [15]. De esta forma se obtuvo un archivo, para visualizar las transacciones, organizado en los siguientes campos:

- **TxID:** Folio de la transacción
- **indexout:** Índice de la transacción
- **value:** Monto de la transacción en BTC
- **scriptPubKey:** Instrucciones para validar la transacción
- **address:** Dirección que recibe el pago.

Filtrado de Datos: Debido a la cantidad de datos, se procedió a filtrar las transacciones mediante la aplicación de los siguientes criterios de filtrado:

- **Fecha:** Se consideraron todas las transacciones que se realizaron durante el período de actividad del ransomware *WannaCry*, el cual abarca del 12 de Mayo de 2017 al 3 de Agosto del mismo año. Se considera como fecha de inicio el día en el que se pagó el primer rescate a una dirección semilla, y como fecha de término el día en el que se transfirieron recursos de una dirección semilla a un *exchange* por última vez.
- **Destino:** Posteriormente, se aplicó un filtro en dos etapas, la primera consistió en ubicar todas las transacciones que recibieron las *direcciónes semilla*. La segunda en ubicar todas las transacciones que efectuaron estas direcciones.

Las semillas analizadas, se muestran en el Tabla I, se obtuvieron de las notas de rescate características del ransomware, que indican a qué dirección se debe de hacer el pago, y fueron publicadas en foros en línea por los usuarios afectados. El resto del análisis depende de la correcta elección de las semillas, y cuánto mayor sea el número de semillas analizadas, mayor información se tendrá respecto a la dinámica de las transacciones.

TABLA I
DIRECCIONES SEMILLA DEL RANSOMWARE *WannaCry* USADAS EN EL CASO DE ESTUDIO

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

B. Análisis por Rastreo

Debido a que en el proceso anterior no se obtiene información sobre las transacciones de origen, es decir, sólo es posible visualizar qué direcciones pagaron a *WannaCry* (las víctimas), pero no es posible verificar cuáles fueron las direcciones posteriores a éstas, se realizó un rastreo usando como herramienta de consulta el servicio que provee el sitio `https://blockchain.info`. Gracias a esto, se pudo hacer un seguimiento de los pagos desde que salieron de las direcciones de las víctimas, se depositaron en las direcciones semilla, se dispersaron en la red y llegaron a cuentas concentradoras que posteriormente dirigieron los fondos a servicios de exchange. Con ello se complementaron los datos para conocer la forma en que el monto recaudado fue disperso en la red. El archivo final consistió en un historial de 731 transacciones indicando el ID, la fecha y hora, el monto, la dirección de origen y la dirección de destino de cada una.

C. Análisis de Redes

La información obtenida en el proceso anterior fue procesada mediante un software libre para visualización de redes, llamado *Gephi*. Con el uso de esta herramienta se obtuvo la Fig. 2, que muestra la red conformada por las transacciones que son objeto de este estudio. De ello, se observa la forma en que los pagos son distribuidos después de llegar a las direcciones semila, mostradas al centro del grafo. Además, a partir de esta red se calculan los parámetros que permiten conocer el patrón de comportamiento y uso de las direcciones Bitcoin involucradas en la transferencia de los rescates obtenidos. Dichos parámetros fueron descritos en la sección III-B, y se presenta la discusión de los resultados en la sección IV-C.

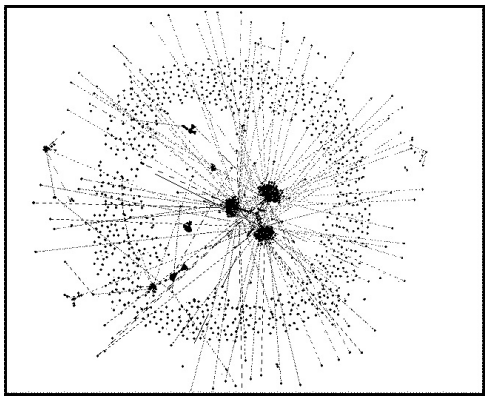


Fig. 2. Visualización de la red de pagos en Bitcoin generada por el ransomware *WannaCry*.

D. Análisis Estadístico

El análisis estadístico se enfocó en describir las características de los pagos de las víctimas a *WannaCry* con un enfoque a posteriori. En particular, este análisis aborda las estadísticas de los pagos que recibió el ransomware de parte de los afectados mediante un análisis descriptivo, que consideró la media aritmética de los pagos, su varianza, desviación estándar, rango y monto mínimo y máximo considerando montos en bitcoin (BTC), en dólares (USD) y el tipo de cambio. De esta manera es posible establecer criterios que indiquen actividad sospechosa en un eventual ataque similar.

También, se consideró la suma total de los montos recaudados por las tres direcciones semillas, para estimar el impacto económico que sufrieron los países afectados, así como la distribución de los pagos en el tiempo, para identificar las áreas geográficas que hicieron la mayor cantidad de pagos.

Además, se hizo un anáisis de correlación para comprobar o desestimar la hipótesis de que un ataque de este tipo incrementa el precio de la moneda digital, o un alza a la moneda fomenta un ataque global. Para ello se utilizó el coeficiente de correlación de Pearson definido en la expresión 4:

$$\rho_{x,y} = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \tag{4}$$

V. Discusión de Resultados

A. Análisis por Rastreo

Entre los primeros resultados destaca la identificación de las empresas involucradas, que prestan el servicio de exchange para convertir el monto de bitcoins en alguna otra moneda, ya sea digital o física, un comportamiento identificado por Yuxing en [16]. La identificación se hizo mediante el servicio del sitio `blockseer.com` que ofrece la facilidad de etiquetar direcciones conocidas. Cabe destacar que estas empresas no necesariamente tienen conocimiento de la identidad de sus clientes, o de sus actividades. A continuación se mencionan las empresas identificadas.

- Bitstamp `https://www.bitstamp.net/`
- HitBTC `https://hitbtc.com/`
- Huobi `https://www.huobi.com/`
- Mercado Bitcoin `https://www.mercadobitcoin.com.br/`
- Poloniex `https://poloniex.com/`
- Shapeshift `https://shapeshift.io/# /coins`
- WhaleClub `https://whaleclub.co/`

Mediante el análisis por rastreo, se identificó el proceso de *peeling chain*, el cual fue descrito por Meiklejohn *et al.* en 2013, mediante el cual los ciberdelincuentes dispersan los fondos obtenidos para incrementar el nivel de anonimato. Este proceso, consiste en realizar pagos por cantidades pequeñas desde las direcciones concentradoras (semillas) y enviar el cambio resultante a direcciones que pueden ser de nueva creación, o previamente usadas, como se describió en la sección II-A. El proceso se ilustra en la Fig. 3 y se discute a profundidad en [8].

B. Análisis de Red

Los siguientes resultados se obtuvieron al utilizar *Gephi* con los datos de las transacciones del caso de estudio.

- **Grado medio de los nodos:**
  Calculado mediante la expresión 1 de la sección III, el valor de grado medio se muestra en la expresión 5:

$$k_i = k_i^{in} + k_i^{out} = 1.053 \tag{5}$$

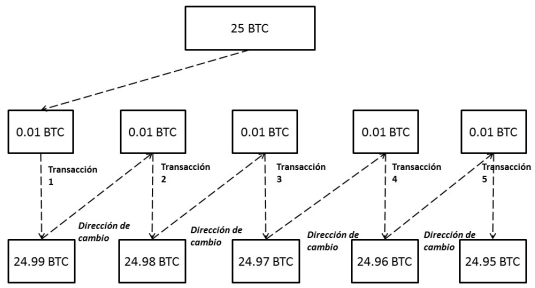


Fig. 3. Proceso de *peeling chain*.

Como se puede observar, el valor del *grado medio* es de 1.053, lo cual al ser una red dirigida, es un indicativo de que en promedio cada nodo tiene un enlace de entrada y uno de salida, lo que lleva a la interpretación de que en general, cada dirección es usada sólo una vez en el sistema, para recibir y reenviar cada pago de rescate y lograr ofuscar los indicios de actividad ilícita.

- **Longitud y Diámetro de la red:**
  Con base en la expresión 2 en la sección III, la expresión 6 representa el valor de la longitud media de la red:

$$\iota_i = \frac{1}{n}\sum_j d_{ij} = 3.9180 \tag{6}$$

  Como se puede observar, la longitud promedio de ruta es de 3.9180, lo que en un contexto práctico, indica que en promedio los pagos pasan a través de 4 direcciones desde que ingresan a la semilla hasta que llega a su punto final en un servicio de exchange. Por otra parte, al considerar el peor caso, es decir, si se maximiza la longitud de ruta del grafo, se obtiene el *diámetro de la red*. En dicha medición el resultado, obtenido a través de la herramienta *Gephi*, indica una longitud de 11 nodos, con lo cual es posible concluir que, a lo más, se requirieron 11 transacciones para transferir los recursos desde alguna dirección semilla hasta el servicio de *exchange*.
- **Componentes conexos:**
  El número de componentes conexos se calculó mediante una búsqueda por profundidad propuesta por Robert Tarjan en [17], la cual dió como resultado un total de 1386 componentes en la red estudiada. El número de componentes conexos muestra a una red poco conectada. Esto indica que los responsables no usaron grandes cuentas concentradoras además de las semillas, sino que una vez recolectados los rescates prefirieron desplazar de manera rápida y fluída los fondos obtenidos para hacerlos líquidos en las empresas mencionadas.
- **Centralidad del eigenvector:**
  De acuerdo con la expresión 3 de la sección III, para este caso el valor de la centralidad del eigenvector se muestra en la expresión 7

$$x_i = \frac{1}{\lambda}\sum_{j=1}^{n} A_{ij}x_j = 0.109218 \tag{7}$$

  El valor relativamente bajo de centralidad del eigenvector demuestra una baja influencia de los nodos de la red respecto a sus vecindarios, por lo que la red no descansa particularmente en ningúno, lo que dificultaría eventualmente identificar direcciones asociadas.

La Tabla II muestra el resumen de los resultados de la medición de los parámetros de interés.

TABLA II
VALORES DE LOS PARÁMETROS OBTENIDOS PARA LA RED DE PAGOS DE *WannaCry*

Parámetro	Valor
Grado Medio	1.053
Diámetro de la Red	11
Longitud Media de Ruta	3.9180
Componentes Conexos	1386
Centralidad del Eigenvector	0.109218

Kharraz *et al.* señalan que el 86.4% de las direcciones asociadas a ransomware procesan a lo más seis transacciones, y que el 68.93% estuvieron activas como máximo 10 días. Además, el 48.9% de las direcciones analizadas recibieron a lo más 2 BTC, monto que coincide con el rescate exigido, además notaron también el proceso de dispersión de fondos a través de nuevas direcciones antes de agruparlos en una nueva. Finalmente señalaron que el 72.9% de las direcciones que analizaron habían registrado sólo dos transacciones, una para recibir un pago y otra para emitirlo [11].

Los resultados obtenidos en este estudio presentaron porcentajes similares, pues el 80% de las direcciones analizadas no registraron más de seis transacciones, el 52% de los pagos analizados corresponden con los pagos de rescate de las víctimas y el 75.36% de las direcciones registraron actividad que señala haber recibido y emitido sólo un pago. Una diferencia radica en el número de días que las direcciones permanecieron activas (número de días entre el primer y último pago registrado por cada dirección), pues mientras en [11] fue un tiempo de 10 días, los responsables del ataque con *WannaCry* mantuvieron la mayoría de las direcciones activas durante 80 días, de manera que las direcciones semilla analizadas recibieron los pagos la primer semana del ataque, del 12 al 20 de Mayo de 2017, y después permanecieron sin actividad hasta el 3 de agosto de 2017.

C. Análisis Estadístico

La Tabla III muestra que el promedio de los pagos realizados fue de aproximadamente 0.1475 BTC, o bien, al tipo de cambio promedio de $1840.86 USD/BTC. Ese monto representó un aproximado de $266 USD por computadora afectada. Resalta que a pesar de haber sido un ataque global de gran alcance, el total de pagos apenas llegó a los 51.92 BTC equivalentes a $93643.91 USD, muy por debajo de los $1.1 M USD que recolectó CryptoLocker en 2013. También se detectó que la mayoría de los pagos se realizaron en la primer semana después del ataque, y los fondos permanecieron sin movimientos hasta el 3 de agosto de 2017.

TABLA III
ESTADÍSTICA DESCRIPTIVA DE LAS DIRECCIONES SEMILLA

Parámetro	BTC	USD	Tipo de cambio
Media	0.14751963	266.083857	1840.86468
Error Estándar	0.007662562	12.64040957	13.74491083
Desviación Estándar	0.143762402	257.8773854	237.155105
Varianza	0.020667628	66500.74592	56242.54384
Rango	1.99899437	3542.058104	1241.351112
Mínimo	0.00000563	0.010000662	1720.4785
Máximo	1.999	3542.068105	2961.829612
Suma	51.92690943	93643.91782	No aplica

TABLA IV
HORARIO DE PAGOS DE RESCATE

Rango de Tiempo	Frecuencia	% Acumulado	% Relativo
00:21:00	0	0.00 %	0.00%
02:41:54	22	6.25%	6.25%
05:02:48	31	15.06 %	8.81%
07:23:42	33	24.43%	9.38%
09:44:36	42	36.36%	11.93%
12:05:30	44	48.86%	12.50%
14:26:24	59	65.63%	16.76%
16:47:18	50	79.83%	14.20%
19:08:12	28	87.78%	7.95%

Para comprobar la existencia de una relación entre el precio de la moneda y la demanda que genera un ataque por ransomware, se hizo un análisis de correlación por medio del coeficiente de Pearson, entre los pagos de rescate y la cotización de Bitcoin. El resultado arrojó un índice de correlación de cero, lo que descarta dicha idea, y podría explicarse como un balance entre la percepción negativa que generó el ransomware sobre Bitcoin y el aumento de la demanda de éste. Dicho cálculo está representado gráficamente en la Fig. 4, que muestra la cotización en dólares de la criptomoneda a través del tiempo, contra la cantidad y el monto de los pagos generados por el ataque de *WannaCry*.

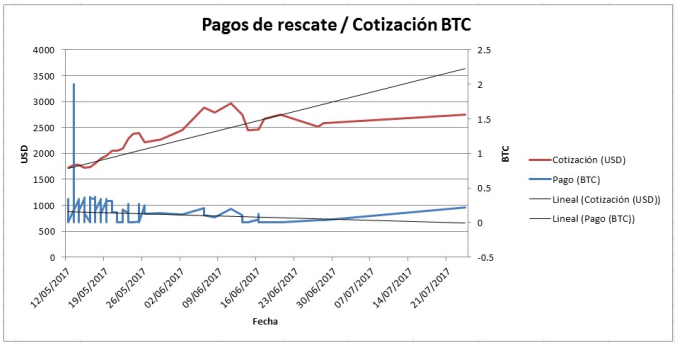


Fig. 4. Relación entre la cotización de Bitcoin y los pagos de rescate.

Posteriormente se hizo un análisis de la información acerca del horario más común en el cual las víctimas realizaron los pagos, con lo cual se obtuvieron los resultados de la Tabla IV, que muestra una tabla de distribución de frecuencias cuyas clases comprenden ventanas de tiempo en formato universal UTC-0 y el número de pagos registrados durante esas ventanas.

Retomando las consideraciones de Liao en [2], se asumió que la mayoría de los pagos se realizaron en horas laborales, tomando una jornada típica de ocho horas desde las 09:00 hrs hasta las 18:00 hrs. Según la Fig.IV, la mayor parte de los pagos se efectuaron entre las 09:44:36 hrs y las 16:47:18hrs, lo cual coincide con la jornada de referencia, por lo que es posible afirmar que dicha proporción de los pagos fue efectuada desde zonas geográficas que coinciden con esa franja de tiempo, de hecho resulta factible suponer que las zonas horarias involucradas corresponden con UTC-1, UTC-0 y UTC+1, lo que llevaría a decir que la mayor parte de los pagos, cerca de un 55.4%, fueron hechos desde: Reino Unido, Irlanda, Islandia, Noruega, Suecia, Alemania, Polonia, España, Portugal, Italia y demás países de la región.

Para ubicar los pagos procedentes de Norteamérica, basta con obtener el equivalente de la jornada de referencia en la región geográfica UTC-5 y UTC-6, la cuál sería de 14:00:00 hrs a 22:00:00 hrs y de 15:00:00 hrs a 23:00:00 hrs respectivamente. Si bien este horario se empalma con la jornada europea desde las 14:00:00 hrs, permite afirmar que aproximadamente el 26.7% de los rescates proceden de esta región. Con un razonamiento análogo, se llega a la conclusión de que China y Japón con UTC-8 y UTC-9 respectivamente, habrían generado un aproximado del 24.43% de los rescates. Esta información se resume en la Tabla V.

TABLA V
PORCENTAJES DE PAGO POR ZONAS GEOGRÁFICAS

Región	Zona Horaria	Porcentaje
Europa Central	UTC-0, UTC+1, UTC-1	55.4%
Norte América	UTC-5, UTC-6	26.7%
China y Japón	UTC-8, UTC-9	24.43%

VI. CONCLUSIONES

En este artículo se presentó un método de análisis de transacciones que se ejecutan en el blockchain de Bitcoin, el cual consiste esencialmente en tres tipos de análisis de las direcciones bajo estudio: rastreo, que permite identificar el flujo de los recursos obtenidos, análisis de redes, para conocer el comportamiento y estrategias que siguen los responsables de un ciberdelito asociado con criptomonedas y análisis estadístico, que permite dimensionar el alcance de un ciberdelito y caracterizarlo. Como caso de estudio, se consideró una red de pagos generada por los usuarios afectados por el ataque del ransomware conocido como *WannaCry*. De los resultados obtenidos, se desprenden algunas de las estrategias que siguen los ciberdelincuentes para ocultar su rastro en el sistema Bitcoin, algunas de las cuales han sido

reportadas en trabajos previos y que pudieron ser confirmadas en este estudio, por ejemplo, la creación de nuevas direcciones para cada movimiento, mantener cada dirección con el menor número de transacciones posible y la distribución de recursos de acuerdo con el proceso de *peeling chain*. Como resultado de la aplicación de este método, también fue posible identificar a las empresas de intercambio de monedas, o *exchange*, que fueron utilizadas para convertir los recursos obtenidos, ya sea en dinero físico o en otra criptodivisa. Se calculó además el monto recaudado por *WannaCry*, así como las medidas de tendencia central que caracterizan a los pagos de rescate de este ransomware y la relación entre el precio de la moneda y el aumento de su demanda a partir de un ataque por ransomware.

Por otra parte, se demostró que los países en los que se registró una mayor cantidad de pagos a *WannaCry* han sido los de la Unión Europea, seguidos por Norteamérica, Japón y China, lo cual coincide con los países mejor posicionados en el ICT Development Index [18], que mide el desarrollo regional y mundial en tecnologías de la información y comunicación.

Aunque el método expuesto está enfocado al análisis de transacciones derivadas de un ataque por ransomware, es posible analizar otros ciberdelitos o actividades que involucren el uso de una criptomoneda basada en un blockchain público. A diferencia de otras propuestas, este método ofrece un análisis en amplitud de la dinámica de las transacciones que se llevan a cabo, lo que permite obtener características útiles para el diseño de estrategias de seguridad. No obstante, no ofrece la posibilidad de identificar plenamente a los participantes, para lo cual se recomienda un análisis en profundidad, como el sugerido por Danny Yuxing en [16].

REFERENCIAS

[1] J. Smith, "Ransomware incident response for law enforcement," Ph.D. dissertation, Utica College, 2017.

[2] K. Liao, Z. Zhao, A. Doupé, and G.-J. Ahn, "Behind closed doors: Measurement and analysis of cryptolocker ransoms in bitcoin," 2016.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] A. P. I. Deya, L. H. Rotger, M. M. P. Capella, and M. M. Puigserver, "Anonymous, fair and untraceable micropayment scheme: Application to lbs," *IEEE Latin America Transactions*, vol. 10, no. 3, pp. 1774–1784, 2012.

[5] J. Herrera-Joancomartí, "Research and challenges on bitcoin anonymity," in *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Springer, 2015, pp. 3–16.

[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[7] F. Reid and M. Harrigan, "An analysis of anonimity in the bitcoin system (2012)."

[8] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 127–140.

[9] C. Zhao and Y. Guan, "A graph-based investigation of bitcoin transactions," in *IFIP International Conference on Digital Forensics*. Springer, 2015, pp. 79–95.

[10] M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bitcoin network," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 457–468.

[11] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: a look under the hood of ransomware attacks," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2015, pp. 3–24.

[12] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, and D. McCoy, "Tracking ransomware end-to-end," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 618–631.

[13] J. S. Silva and A. M. Saraiva, "A methodology for applying social network analysis metrics on biodiversity," *IEEE Latin America Transactions*, vol. 13, no. 9, pp. 3026–3037, 2015.

[14] T. G. Lewis, *Network science: Theory and applications*. John Wiley & Sons, 2011.

[15] rusty-blockparser. [Online]. Available: https://github.com/mikispag/rusty-blockparser

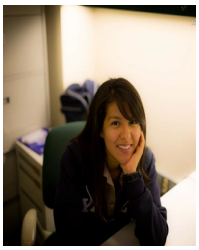
[16] D. Y. Huang, D. McCoy, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, and A. C. Snoeren, "Tracking ransomware end-to-end," in *Tracking Ransomware End-to-end*. IEEE, 2018, p. 0.

[17] R. Tarjan, "Depth-first search and linear graph algorithms," *SIAM journal on computing*, vol. 1, no. 2, pp. 146–160, 1972.

[18] Measuring the information society report. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf

Víctor Reyes Macedo Obtuvo el grado de Ingeniero en Matemáticas por el Instituto Politécnico Nacional, en México. Realizó una estacia de investigación en el CSIRT del Centro de Investigación en Computación del IPN en el área de criptografía, enfocado a la detección de ransomware en el blockchain de Bitcoin. Actualmente es estudiante del programa de Maestría en Ciencias de la Computación en el IPN, en el laboratorio de Ciberseguridad. Sus áreas de interés son la criptografía, la seguridad demostrable y la seguridad en blockchain.

Moisés Salinas Rosales Es profesor investigador del Centro de Investigación en Computación del Instituto Politécnico Nacional, en México. Obtuvo el grado de Ingeniero en Computación, Maestro en Ciencias de Ingeniería en Microelectrónica y Doctor en Ciencias de la Computación por la misma institución. En 2002 realizó una estancia de investigación en el Laboratorio del Profesor Ohta en l aUniversidad de Electro-Comunicaciones en Tokio, Japón. Sus áreas de interés son la criptografía y el análisis de malware.



Gina Gallegos García La Dra. Gallegos es egresada de la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacan, del Instituto Politécnico Nacional en la carrera de Ingeniero en Computación, tiene además el grado de Maestría en Ciencias de Ingeniería en Microelectrónica y Doctora en Ciencias por la misma institución, especialidad en Seguridad Informática y Tecnologías de la Información y Maestría en Ingeniería en Seguridad y Tecnologías de la Información. Realizó un aestancia post-doctoral en la Universidad de Yale en Estados Unidos en el 2011 bajo la supervisión del Profesor Michael J. Fischer, donde trabajó con el tema de protocolos criptográficos de autenticación remota. La Dra. gallegos es miembro del Sistema Nacional de Investigadores, su área de interés es la criptografía.