NOTA DE CONTEXTO INTERNACIONAL

TEMA: Bitcoin y el secuestro digital

I. Monedas virtuales: caso Bitcoin

En la industria de ***micropagos*** se realizan transacciones por vía electrónica (en línea) de pequeñas cantidades de dinero. Con el crecimiento exponencial de los micropagos y la expansión de las redes sociales se generaron las condiciones para que surgieran las llamadas monedas virtuales (Valdés & Hernández-Verme, 2014). De acuerdo con el Banco Central Europeo, ***la moneda virtual es una representación digital de valor que no es emitida por un banco central, una institución financiera o una institución de dinero electrónico, la cual en algunas ocasiones puede ser usada como una alternativa del dinero*** (Central European Bank, 2015). Estas monedas son típicamente emitidas por agentes privados y se pueden intercambiar por otras monedas virtuales e incluso por dinero fiduciario.

La moneda descentralizada más popular hasta ahora es el Bitcoin, la cual es aceptada por diversas empresas como medio de pago, algunas de ellas son Facebook, Amazon y Dell. Dependiendo de la forma de pago (tarjeta de crédito, de débito, efectivo, *PayPal,* etc.), una persona puede comprar Bitcoins con un determinado agente de cambio como *Coinbase* o *BitStamp*. Las transacciones con Bitcoins requieren que los involucrados cuenten con un monedero electrónico a través del cual se les asigna una clave de identificación.

Actualmente, diversas instituciones financieras y empresas en el mundo están interesadas en aprovechar el innovador sistema que rodea al Bitcoin denominado "*blockchain"* por medio del cual se realizan transacciones sin necesidad de un intermediario. Además, dado que el Bitcoin funciona de manera descentralizada, se contempla como un refugio o protección ante políticas que afectan el valor de las monedas nacionales o a los sistemas de transferencia de dinero. De acuerdo con una nota publicada el 24 de marzo de 2017 en

el sitio www.espaciobit.com.ve, la idea del Presidente Donald Trump para gravar el envío de remesas a México podría dar un fuerte impulso al uso del Bitcoin en el proceso de transferencia de remesas.

Algunas ventajas y riesgos del Bitcoin:

Ventajas:

1. ***Privacidad:*** los usuarios se identifican con una clave asignada al adquirir su monedero electrónico por lo que su identidad durante las transacciones se mantiene anónima. Sin embargo, para el registro con los agentes de cambio si es necesario proporcionar información personal que sirva para verificar la identidad.
2. ***Bajo costo de transacción***: Debido a que no hay intermediación financiera su costo de transacción es bajo y no está sujeto a una tasa de interés establecida por un Banco Central.
3. ***Flexibilidad para pagar***: se pueden enviar y recibir Bitcoins a cualquier lugar del mundo en cualquier momento a través de una aplicación móvil.
4. ***Alternativa de pago***: como innovación financiera, el Bitcoin representa una alternativa de pago para los consumidores.

Riesgos:

1. ***Expuesta a actividades ilegales o delictivas***: Por sus características, se ha usado para especular y debido a su dificultad de rastreo también podría ser usada para realizar compras ilegales y otras actividades delictivas como el secuestro digital.
2. ***Volátil***: El Banco Central Europeo señala que las monedas virtuales que crean la oportunidad para especular y/o que pueden ser usadas para comprar bienes y servicios reales son inherentemente inestables debido a la falta de madurez del esquema de monedas virtuales, a la falta de confianza a un sistema en desarrollo, al bajo volumen de monedas comerciadas, a la falta de certidumbre legal, a la especulación y a los ciberataques, etc. (European Central Bank, 2012). Al día de hoy, el precio del Bitcoin supera los 2,000 dólares, lo que puede ser consecuencia del bajo volumen de operaciones que se pueden realizar con el Bitcoin (por su diseño está limitado a un máximo de 7 operaciones por segundo), al aumento de su demanda frente a otras monedas digitales y locales y debido a que está sujeto a actividades especulativas.

3. ***Falta de regulación***: Al no estar delimitado su uso a una región o área monetaria específica, es complicada su regulación. De acuerdo con el Banco Central Europeo (Central European Bank, 2012), la participación en los esquemas de monedas virtuales expone a los usuarios a riesgos de crédito, de liquidez, de operación y legales.
4. ***Consumo de energía***: La red entera del Bitcoin muestra un consumo alto de energía lo que puede representar un riesgo ambiental.

En términos de regulación, en septiembre de 2015, la Comisión para el Comercio de Futuros de Mercados de Estados Unidos (CFTC por sus siglas en inglés), declaró oficialmente que el Bitcoin y otras ***"criptomonedas"*** son consideradas materias primas o ***"commodities"***, por lo que es regulado como parte de dicho mercado. En México, en un artículo publicado por el Financiero en mayo de 2017 se informa sobre la intención de la Secretaría de Hacienda y Crédito Público de comenzar a regular el uso del Bitcoin a través de una iniciativa de ley para regular a las empresas de tecnología financiera que se conocería como la Ley Fintech.

En su reporte sobre monedas virtuales publicado en 2015, el BCE señala que el esquema de monedas virtuales podría afectar la política monetaria, la estabilidad de precios del sistema financiero y del sistema de pagos, lo anterior provocado por el aumento en el número de usuarios y el volumen de transacciones utilizadas en pagos regulares, ya que con esto aumenta su conexión con la economía real involucrando a las instituciones financieras, las cuales requerirán del desarrollo de estructuras que mantengan la estabilidad de los esquema en los que se maneja la moneda virtual.

II. Uso del Bitcoin en el secuestro digital

El pasado viernes 12 de mayo de 2017 fuimos testigos de uno de los ciberataques más grandes de la historia digital provocado por el programa malicioso o virus llamado *WannaCry*, comúnmente conocido como secuestrador de archivos. En el ataque se afectaron más de 200,000 computadoras en alrededor de 150 países. Algunos ejemplos de países e instituciones afectadas son:

- Rusia: red semafórica, metro e incluso el Ministro del Interior
- Reino Unido: gran parte de los centros hospitalarios

- **España**: empresas tales como: Telefónica, BBVA, Gas Natural e Iberdrola

En México las dependencias y organismos gubernamentales, así como empresas privadas no reportaron afectaciones en sus instalaciones. Los daños en México se presentaron mayormente en computadoras de uso personal que no contaban con la última actualización del sistema operativo.

El programa malicioso (o virus) WannaCry utiliza vulnerabilidades del sistema operativo para poder ejecutar código de encriptación de información. Este tipo de programas típicamente utilizan ingeniería social como mecanismo de propagación, engañando a la gente por teléfono o internet logrando que el usuario descargue e instale el programa malicioso o proporcione datos de su cuenta dejando vulnerable su computadora. La propagación de un programa malicioso utilizando ingeniería social no es tan rápida.

La diseminación de WannaCry fue un evento único debido a que los programadores utilizaron una vulnerabilidad del sistema operativo Windows conocida como “EternalBlue”. La vulnerabilidad consiste en enviar paquetes de código malicioso por medio del servidor SMB versión 1 (del inglés Server Message Block). La vulnerabilidad de referencia (EternalBlue) es equivalente a tener una casa con una puerta trasera oculta donde sólo la empresa constructora conoce la existencia de dicha puerta.

El programa WannaCry requiere dos mecanismos para seguir infectando computadoras:

1. **Una forma de difundirse:** explotando la vulnerabilidad EternalBlue y buscando e infectado computadoras vulnerables conectadas a la misma red.
2. **Un software malicioso:** programa de encriptación de archivos que inhabilita su lectura.

Para desencriptar un archivo es necesario contar con una contraseña que sólo es conocida por el programador. La contraseña se ofrece a los infectados a cambio de pagar un rescate por medio de una transacción electrónica. WannaCry pide a los afectados un rescate de 300 Dólares en Bitcoins (1 Bitcoin equivale a 2,273.94 Dólares, tipo de cambio al 23 de mayo de 2017). Las transacciones con Bitcoins son difíciles de rastrear debido a su

naturaleza descentralizada y esto las convierte en la herramienta perfecta para los secuestros digitales.

Recomendaciones para protegerse de los secuestros virtuales

1. Las actualizaciones de software (que normalmente aparecen justo cuando nos vamos de la oficina) son la principal acción para evitar ser afectado por un programa malicioso. Son una analogía de una vacuna para el sistema inmunológico del ser humano, su función es reparar vulnerabilidades del sistema operativo para evitar futuros contagios.

2. Las versiones piratas de Windows son una de las causas de la propagación del programa WannaCry. Una versión pirata no puede realizar actualizaciones convirtiéndola en un objetivo fácil de contaminar. La recomendación es siempre utilizar versiones originales del sistema operativo.

3. Cuando se generan archivos que se consideran importantes (como pueden ser fotos de un viaje, una tesis, un proyecto del trabajo, etc.) la recomendación es almacenarlos en un disco externo o en un servicio en la nube, así evitamos que estén al alance de cualquier programa malicioso.

4. Es recomendable instalar siempre software (ejemplo Adobe Reader, Office, Bases de datos, etc.) desde la fuente original. Descargar software de fuentes no certificadas es peligroso porque no podemos garantizar que el archivo que obtenemos esté libre de software malicioso. Si vamos a instalar un software en una computadora de casa, siempre debemos utilizar fuentes originales, en el caso de computadoras de oficina, la recomendación es solicitar ayuda del equipo de informática.

5. Pagar el rescate de un secuestro digital no garantiza la recuperación de la información encriptada, la recomendación es no pagar el rescate. Si descubres que tu computadora ha sido infectada, necesitas desconectarla inmediatamente de la red y actualizar a la versión más reciente del sistema operativo que se utilice.

III. Consideraciones finales

El uso del Bitcoin es reciente ya que fue introducido en 2009 y viene de la mano con otras innovaciones que han surgido a través del internet. El Bitcoin representa una interesante alternativa como medio de pago, pero con riesgos a considerar como depósito de valor. Su manejo aún genera confusión debido a que está exento del control de las autoridades monetarias y su expansión implicaría un cambio radical en la manera en que funciona la economía actual.

Como se menciona en esta nota, su falta de regulación ha tenido efectos en términos de seguridad a escala global, lo que debe prevenirse por los gobiernos y usuarios de internet de todo el mundo.

IV. Referencias

- https://es.wikipedia.org/wiki/WannaCry
- http://money.cnn.com/2017/05/13/technology/hero-ransomware-malwaretech-cyberattack/index.html
- http://money.cnn.com/2016/08/15/technology/nsa-spy-tools-stolen/?iid=EL
- https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
- Valdes-Benavides, R. & Hernández, P. (2014). Virtual Currencies, Micropayments and Monetary Policy: Where Are We Coming from and Where Does the Industry Stand? *Journal of Virtual Works Research*. 7(3). Págs. 2-8.
- European Central Bank (2012). VIRTUAL CURRENCIES SCHEMES. Frankfurt am Main. Consultado en https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf el 21 de mayo de 2017.
- European Central Bank (2015). Virtual currencies schemes- a further analysis. Frankfurt am Main. Consultado en https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf el 21 de mayo de 2017.
- https://bitcoin.org/en/faq
- https://www.bloomberg.com/quicktake/bitcoins
- https://espaciobit.com.ve/main/2017/03/24/aprendiendo-sobre-bitcoin-parte-ii/
- https://espaciobit.com.ve/main/2017/01/06/sera-el-bitcoin-un-cisne-negro-gracias-a-la-politica-de-donald-trump-hacia-las-remesas-de-mexico/
- http://www.elfinanciero.com.mx/mercados/banxico-se-prepara-para-entender-la-tecnologia-blockchain.html
- http://www.elfinanciero.com.mx/economia/ley-fintech-llegara-hasta-septiembre-shcp.html
- https://fin-tech.es/2014/07/como-se-realiza-una-transaccion-segura.html