Protección contra Hackeo de Criptomonedas

Roger Gregory Ruiz Alvarez
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
msn.rruiz@gmail.com

***Resumen*—La tecnología evoluciona rápidamente con nuevas oportunidades y ventajas, pero también trae consigo nuevos peligros. En el caso del intercambio de valor por medio de la moneda, ahora se utiliza criptomonedas, como una nueva forma de intercambio de valor económico con todos los principios y condicionantes que puede ofrecer y siendo más frecuente, pero también se conoce de ataques que ha sufrido este tipo de moneda culminando en robos de montos significativos. La presente investigación pretende establecer una base inicial para establecer mecanismos de seguridad frente al hackeo de criptomonedas tomando como base investigaciones relacionados al tema, además de normativas y legislaciones locales vigentes. Se toma en cuenta los casos en el ámbito local y países vecinos, que existe una acogida de interés intermedio en comparación con otros más desarrollados lo que muestra también un peligro local para tomar en cuenta.**

Palabras clave—blockchain, bitcoin, criptoactivos, criptomoneda, hacheo, valor de cambio.

I. INTRODUCCIÓN

El uso de la tecnología está muy extendida e inmersa en diferentes áreas de la sociedad, astronomía, física, medicina, construcciones, economía, política, comunicación, simulación, educación, investigación, etc., debido a la gran herramienta que representa en cada área, permitiendo facilitar la operativa diaria con procesos automáticos que facilitan el trabajo.

El dinero que es representado por la moneda de cada país es la unidad de intercambio de valor y/o bienes que permite realizar intercambios entre persona o instituciones, el valor de la moneda con relación a otros países puede tener un valor diferente definido por el tipo de cambio respecto a otra moneda. La economía y el flujo de dinero de forma física o mediante transacciones bancarias en línea implican el uso de un tipo de moneda específicamente.

El uso de una moneda permite ser beneficiario de las ventajas y desventajas que tiene la moneda en términos económicos y de valor de cambio, en el momento de realizar el intercambio o transacción propiamente. El uso de una moneda específica implica estar sujetos a la normativa y limitaciones legales y de convenios internacionales que tiene la moneda, por lo que su valor puede estar sujeto a las variaciones de carácter local o internacional por devaluaciones o cualquier otro efecto económico.

La creciente intercomunicación entre personas en el mundo con intereses y características comunes hacen una nueva forma de sociedad virtual, donde uno socializa, tiene información al día, investiga, etc.; el internet ha permitido la existencia de transacciones bancarias con la creación de la moneda virtual o las criptomonedas como el Bitcoin, Ethereum, Litecoin, Ripple, Dogecoin, además de muchos otros con el mismo objetivo, el intercambio de valor. Estas monedas incluyen sus propias características como el que no están sujetos a una legislación de ningún país o las variaciones del tipo de cambio, por lo que fueron creadas para tener independencia ante cualquier influencia económica, por lo que su control es descentralizado. Utiliza criptografía fuerte y compleja a través de una base de datos descentralizada, normalmente es una Cadena de Bloques conocidas como Blockchain que usa una base de datos pública dedicada al control de transacciones.

Un caso particular es el Bitcoin, el cual fue creado por Satoshi Nakamoto por el año 2008, quien propuso su uso con el algoritmo SHA-256 inicialmente y fue una de las primeras criptomonedas en tener un nivel de seguridad altamente efectiva, aunque matemáticamente es posible algún tipo de ataque a la criptomoneda, pero el costo sería muy alto porque se necesitaría una capacidad de procesamiento computacional con una potencia y capacidad como la que tiene actualmente la empresa Google, equipada con sistemas con algoritmos que se aproximen a los cuánticos, pero a pesar de tener toda la infraestructura disponible, aun así solo se tendría una probabilidad de éxito del 50% de éxito sin la garantía de tener una certeza razonablemente aceptable. Todo esto hace posible el llamado Internet del Valor conocido por las siglas IoV, lo cual hace posible una nueva forma de valoración a los activos de información del mundo digital.

Un concepto importante es la Minería de Criptomonedas, el cual describe minar criptomonedas para obtener el valor de la moneda, este proceso es la verificación de una transacción de criptomoneda, por el creciente número de transferencias de capital electrónico entre cuentas. Los mineros, que son también usuario de estas criptomonedas aprovechan el poder de procesamiento de los ordenadores para mantener la integridad de la Cadena de Bloques (Blockchain) y así verificar estas transacciones. A pesar de esta complejidad se conoce casos de hackeo, por ejemplo, al Bitcoin y Ethereum, por lo que se concluye que, a pesar de su mecanismo de seguridad, estos, no están libres de un posible ataque, y la probabilidad de ocurrencia de un ataque es completamente posible.

En el ámbito local el uso de la moneda virtual no está normado aún, porque de acuerdo a la resolución emitida por el Banco Central de Bolivia en 06/05/2014 y nota de prensa de fecha 29/06/2019 en la cual se verifica que aún no está normado ni autorizado el uso de este tipo de moneda para el intercambio de bienes y servicios. Pero estos aspectos legales no han podido detener a emprendimientos privados que promueven el uso de

Para referenciar este artículo (IEEE):
[N] R. Ruiz, «Protección contra Hackeo de Criptomonedas» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 88-91, 2020.

estos "Criptoactivos", denominación que se usa actualmente mientras no esté regulado o respaldado por parte del estado por medio de la instancia reguladora BCB.

A. *Estudios relacionados*

Existe documentación relacionado a este tema en el ámbito internacional tal como se muestra en los siguientes trabajos, los cuales se toma como base.

- Puvogel Rojas, realiza un análisis desde un aspecto jurídico las ventajas y desventajas de usar una criptomoneda tomando como caso de estudio el Bitcoin, realizando un análisis de aspectos normativos locales y su impacto [1].
- Kaspersky, desde gestiones pasadas la empresa ha reportado la aparición, proliferación y lucha constante contra el ataque de amenazas que atentan la seguridad de la información, también ha reportado casos de ataques asociados a las criptomonedas [3].
- ESET, también ha reportado casos de ataques a criptomonedas desviando fondos a otros destinatarios o extorciones a cambio de criptomonedas traducidos en millones de dólares con el uso de *Ransomwares* [7].
- Castillo Fonseca Diego, propone una alternativa para el envío de remesas a través de criptomonedas tomando en cuenta posibles amenazas con el uso de medidas de apoyo y muestra un breve sustento legal que apoya la propuesta para un entorno local [2].

B. *Objetivos*

La definición de los objetivos principales implica tomar en cuenta los criterios principales que tienen que ser desarrollados hasta la conclusión del presente trabajo, como una herramienta inicial para la implementación de medidas de seguridad con este tipo de activos de intercambio de valor en criptomonedas, por lo que se ha concluido en los siguientes objetivos:

Objetivo principal

Desarrollar un esquema de protección de criptomonedas para casas de cambio.

Objetivos secundarios

- Determinar las vulnerabilidades de las casas de cambio de criptomonedas.
- Elaboración de cada una de las fases del esquema de protección contra el hackeo de las criptomonedas.
- Definición de la estrategia de implementación del esquema de protección contra ataques de hackeo de criptomonedas.

Si se elabora un esquema para la protección de criptomonedas, entonces se minimizará el riesgo de hackeos a las criptomonedas.

Para describir mejor esta hipótesis debemos apoyar con la identificación de las variables que se han considerado:

- Variable independiente: La metodología de protección de criptomonedas.
- Variable dependiente: El impacto de implementar la metodología de protección de criptomonedas.

C. *Antecedente teórico de la propuesta*

La propuesta está justificada por la creciente necesidad de seguridad informática ante posibles ataques a criptomonedas basado en reportes publicados por organizaciones de renombre relacionados a la seguridad como empresas de antivirus que ven necesario implementar sistemas de seguridad que brinden mecanismos de protección, detección y prevención de ataques, en este caso a casas de cambio de criptomonedas.

Un estudio realizado por *Positive Technologies* ha identificado que la mayoría de los ataques de este tipo tienen como objetivo primario la información y las instituciones financieras [4], de acuerdo al siguiente cuadro:

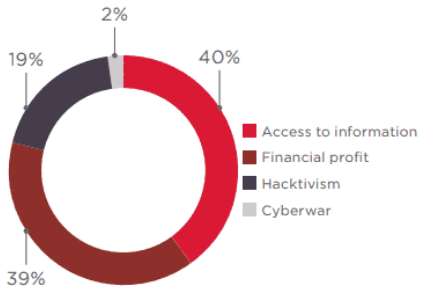

Fig. 1. Objetivos principales de ataques a nivel global 2018. Fuente: Positive Technologies.

Otro estudio realizado por la *Alianza de Amenazas Cibernéticas (CTA)* identifico que en el 2018 hubo un incremento en los ataques a las criptomonedas y/o casa de cambio de acuerdo al siguiente cuadro:

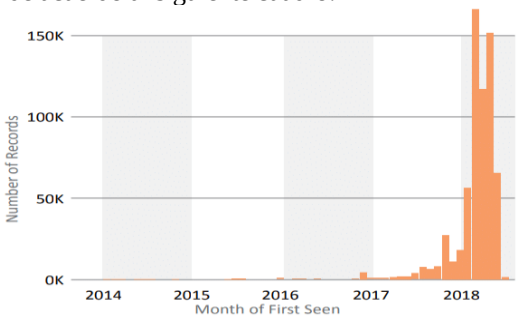

Fig. 2. Incremento de ataques a criptomonedas. Fuente: CTA.

De lo anterior, como un dato curioso se sabe que las formas de ataque solo han usado un 20% de las capacidades de procesamiento de una CPU.

D. *Análisis general*

Existen varios casos de ataques a las criptomonedas deduciendo que se ha intentado vulnerar el sistema de seguridad de las criptomonedas. Algunos de los casos aplicables al presente trabajo son los siguientes:

- La empresa Binance, una de las mayores instituciones Exchange de intercambio de Bitcoin a moneda corriente, fue víctima de un robo de 40 millones de dólares en Bitcoin. El cual se encontraba en un monedero caliente conectado a la red para el intercambio de montos de Bitcoin con otros usuarios.
- La casa de cambio japonesa BITPoint fue víctima de un ataque, como objetivo fueron las criptomonedas por un valor equivalente a 32 millones de dólares, justo cuando había abierto operaciones en Panamá a finales del 2018.

- La firma japonesa *Coincheck* fue víctima de un ataque de con el objetivo del robo de criptomonedas, lo cual ha afectado aproximadamente 260000 clientes.
- La casa de cambio Italiana BitGrail, también fue víctima de un ataque en febrero de 2018, donde se detectó transacciones de criptomonedas no autorizadas por un valor equivalente a 200 millones de dólares, casi el 13% de la criptomoneda circulante.

Existen muchos otros casos de casas de cambio de criptomonedas que fueron víctimas de ataques como ser *Coinsecure, Coinrail, Bithumb, Zaif*. De todas estas empresas dedicadas al intercambio de valor de criptomonedas a monedas corrientes, se puede concluir que también son blancos de ataques. Como resultado de la proliferación de esta forma de ataque ha dado origen a una nueva forma de amenaza, el cual es el *Cryptohacking* a través del uso de herramientas como *CoinHave*.

Evaluación

Entre muchos casos identificados por medio de estudios realizados por diferentes instituciones, se ha identificado los casos más representativos con características comunes entre ellos. Estos ataques a pesar de ser muy variados, en su mayoría se presentan en las siguientes formas:

- El uso de varios tipos de *malwares* que ejecutan procesos de infiltración según el tipo de objetivo.
- El uso de *exploit* de día cero para ejecutar el ataque en el mismo instante en el cual se identifica una vulnerabilidad en el software.
- El uso de la Ingeniería Social, fue, es y será un medio muy usado para determinar contraseñas o accesos, debido a la naturaleza de las personas.

E. Arquitectura de seguridad

Una alternativa de seguridad propuesta para el uso de criptomonedas en el ámbito local, se muestra a continuación:

- *Ámbito de operaciones*: toda operación que implique el intercambio de valor y/o servicios con criptomonedas, debe estar verificado en el origen y el destino.
- *Seguridad*: toda medida de seguridad implementable que apoye el resguardo y minimice el riesgo, deben ser tomados en cuenta con los siguientes criterios: la triada de la seguridad (Confidencialidad, Integridad y Disponibilidad), Descentralización, Criptografía.
- *Privacidad*: implementar plataformas de exchanges descentralizados para mantener la privacidad, mismo que hasta hace poco no era escaso, pero actualmente ya es más frecuente.
- *Respaldo Legal*: al no existir aún una normativa legal solida que rija actividades con este tipo de bienes para el intercambio de valor y/o servicios, es preciso tomar en cuenta los anteriores puntos de forma imprescindible.

II. MÉTODOS

Estrategias Metodológicas

Entre las estrategias y criterios aplicables al desarrollo del presente trabajo, se consideran los siguientes:

Tipo de investigación

El tipo de investigación aplicada en el presente trabajo es de tipo exploratoria, porque al ser un tema relativamente reciente la información disponible y el presente trabajo sirven para el desarrollo de un esquema que esté orientado al uso de las técnicas vigentes.

Universo

El universo de estudio son cualquiera de las instituciones destinadas al intercambio de criptomonedas por moneda de uso corriente como ser casas de cambio o bancos que realicen el intercambio de criptomonedas a moneda corriente y viceversa, como un activo de intercambio de valor económico.

Población

La población elegida del universo anteriormente descrito, comprende aquellas casas de cambio que intercambian criptomonedas por moneda corriente y viceversa.

Técnicas de investigación

Para obtener información necesaria y relacionada a los casos de ataques relacionados con criptomonedas a sujetos con este bien, se utilizará las siguientes técnicas de investigación:

- Revisión de documentación institucional normativo (como políticas de seguridad, normativas internas, nacionales o internacionales, reglamentos, planes de contingencia, respaldos, simulacros, planes de acción y reacción, procedimientos, etc.).
- Cuestionarios (que recopilen información puntual asociado a temas de seguridad concernientes a la tenencia de criptomonedas, o que califiquen o validen estos aspectos).
- Entrevistas con personal responsable, relacionado al área de seguridad y movimientos transaccionales operativos de intercambio de criptomonedas, especialistas, usuario en general u otros involucrados.

III. RESULTADOS

Resultados logrados

De acuerdo a los objetivos planteados se ha formalizado la estructura inicial que permite una mejor protección frente al hackeo de las criptomonedas en las instituciones que así lo requieran para el resguardo del capital disponible para fines operativos y resguardo. Entre algunos de los resultados principales logrados se tiene a los siguientes:

- Al igual que otras metodologías, está sujeto a mejoras, modificaciones y correcciones de acuerdo revisiones y/o validaciones que se necesiten en el tiempo.
- La estructura formal toma en cuenta recomendaciones que la ISO 27000 describe como requisitos mínimos de cualquier sistema de Información en cuanto a seguridad.
- La adaptabilidad a diferentes situaciones es importante, por lo que considera escenarios particulares, como por ejemplo el reglamento interno y procesos operativos.
- La tecnología disponible es importante por lo que se enfatiza su fortalecimiento según necesidades para fines de intercambio de valor económico.

IV. Discusión

El presente trabajo muestra la estructura básica de la arquitectura propuesta que pretende ser el inicio formal de una forma de actuar en los procesos de resguardo y protección de información tomando en cuenta las siguientes características:

- Está orientado a la adecuación y adaptabilidad a normativas vigentes y particulares de cada organización considerando la legislación local vigente.
- Se debe diferencias entre una metodología que pretende abarcar a todas las áreas de la seguridad, por lo que este se especializa en criptomonedas.
- Una característica común que tiene con otros es la posibilidad de mejora continua.

Es posible que existan situaciones que aún no se contemple como la gestión de activos de información debido a que no es parte de la investigación, pero existen otros trabajos mucho más concretos y especializados, pero es posible su implementación si tiene una fuerte relación con el presente tema como parte de la adaptabilidad del presente trabajo.

V. Conclusiones

El uso de las criptomonedas ha coadyuvado en el intercambio de valor en muchos entornos facilitando el intercambio de servicios, bienes y valores en diferentes ámbitos por lo que su uso es muy frecuente. En consecuencia, los beneficios traen consigo amenazas que pueden afectar en gran manera los activos económicos inherentes, en este caso en concreto el activo económico traducido en criptomonedas a causa de los hackeos.

La implementación de medidas de seguridad no siempre garantiza la seguridad de las criptomonedas en concreto, pues también es necesario organizar las medidas de seguridad existentes en una metodología que contemple cada uno de los aspectos que puedan ser tomados en cuenta para la implementación de medidas de seguridad.

Una metodología mejora la eficacia de la implementación, protección, detección y prevención de posibles ataques, y reduce las amenazas a un nivel aceptable y tolerable por la empresa que hace uso de las criptomonedas como otra forma de vida económica.

Referencias

[1] Blockchain y monedas virtuales, aproximación jurídica (2018) Universidad de Chile, Max Puvogel Rojas.

[2] Castillo Fonseca Diego (2017 oct 31), Viabilidad de un sistema alternativo de envío de remesas a través de criptomonedas en Venezuela, Universidad Católica Andrés Bello. Obtenido de: http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/aat4033.pdf

[3] Kaspersky. (2019 oct 10). Kaspersky daily. Obtenido de https://www.kaspersky.es/blog/hardware-wallets-hacked/17653/.

[4] Positive Technologies. (2019 oct 2). Cybersecurity threatscape: Q2 2018. Obtenido desde la dirección https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018-q2/.

[5] Criptonoticias. (2018 oct 20). Ataques cibernéticos relacionados con criptomonedas aumentan en un 459% en el 2018. Obtenido desde https://www.criptonoticias.com/seguridad/ataques-ciberneticos-criptomonedas-2018/.

[6] Criptonoticias. (2018 nov 10). Los hackeos a casas de cambio de criptomonedas más destacados en el 2018. Obtenido de la dirección https://www.criptonoticias.com/seguridad/robo-fraude/hackeos-casas-cambio-criptomonedas-destacados-2018/.

[7] ESET (2018), Eset Security Report Latinoamérica 2019. Obtenido de: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

Breve CV del autor

Roger Gregory Ruiz Alvarez es Licenciado en Informática. Actualmente realiza la Maestría en Informática Forense, Auditoría Informática y Seguridad de la Información en el Postgrado en Informática UMSA. Trabajó en Aduana Nacional, Ministerio de Educación, Banco Central de Bolivia. Su interés investigativo es el desarrollo de software. Email: msn.rruiz@gmail.com.