Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Análisis de seguridad de los principales sistemas de criptomonedas

Trabajo Fin de Máster

Máster Universitario en Ingeniería Informática

Autor: Sitanskiy Stanislav

Tutor: Ripoll Ripoll, José Ismael

2018-2019

Resumen

Dado que el entorno de uso de la criptomoneda se encuentra en la etapa de desarrollo activo y que aún no se ha establecido la “mejor práctica”, su uso (tanto el almacenamiento como la extracción y el pago) está asociado con ciertos riesgos, en particular, los robos. Además, debido a la creciente popularidad de esta tecnología, es posible no solo el robo del dinero sino también de recursos informáticos (tiempo de cálculo) para fabricar nueva moneda. Si la primera concierne a los usuarios directos de las criptomonedas, la segunda amenaza a cualquier compañía que posea computadoras, un usuario común de PC o dispositivos móviles.

Este proyecto aborda el estudio y análisis de las principales amenazas de ambos tipos y, si es posible, dará recomendaciones sobre cómo evitarlas.

Palabras clave: criptomoneda, Bitcoin, amenaza, robo, fraude, hacker.

Abstract

Cryptocurrency environment is still in immature state, which actually is actively developed and improved; there is no established common "best practice". Its usage (its storage, extraction/mining and payment process) is vulnerable to some security threats, in particular to theft. It also opens the possibility to attackers to abuse the computational resources to produce new currency. The first form of theft (the more classic one) affects the end user, but the second one affect the computer infrastructure, which is more relevant for companies or persons dedicated to produce the cryptocurrency.

In the project, the major threats of both types of vulnerabilities will be studied and analyzed, and if possible some recommendations to address the issues will be given.

Keywords : cryptocurrency, bitcoin, threat, theft, fraud, hacker.

Tabla de contenidos

1. Introducción

Documento realizado para el trabajo final del máster en Ingeniería Informática en 'Escola Tècnica Superior d'Enginyeria Informàtica' de la 'Universitat Politècnica de Valencia'.

1.1 Motivación

La reciente evolución tecnológica y económica y la creciente demanda del mercado de métodos de pago confiables, anónimos, "transparentes", descentralizados, independientes y no sujetos a influencia política llevaron a la aparición de criptomonedas.

Sobre la naturaleza económica y el estado legal de la criptomoneda, las discusiones están en curso. En diferentes países, las criptomonedas son consideradas como un medio de pago, un producto específico, puede tener restricciones en circulación (por ejemplo, la prohibición de operaciones con ellos para las instituciones bancarias). En algunos países, y en particular en Japón, hay ejemplos de compañías (GMO Internet Group) que se están preparando para cambiar a un nuevo sistema de salarios, en el que los beneficios de los empleados se pagarán en Bitcoin. Otros lo utilizan para remunerar a los trabajadores extranjeros para simplificar el reclutamiento.

Las criptomonedas ya han tomado firmemente su lugar en el mundo, y se espera un mayor crecimiento en el área de su uso e introducción en la vida cotidiana de los ciudadanos, como lo fue una vez con PayPal.

Dichas tecnologías son una buena alternativa al dinero fiscal tanto para particulares y su uso diario, por que entre otros proponen control personal de los fondos, alto nivel de seguridad y comodidad de pago local e internacional (no hay cambio de moneda), como para las empresas, puesto que ofrecen mayor libertad económica.

1.2 Objetivos

Debido a que el entorno de uso de la criptomoneda se encuentra todavía en la fase de desarrollo activo y que aún no se ha establecido una "mejor práctica", su utilización (tanto el almacenamiento como la extracción y el pago) está asociada con ciertos riesgos, como los robos. Además, debido a la creciente popularidad de esta tecnología, es posible el riesgo de robo de recursos informáticos (tiempo de cálculo) con fines lucrativos. Si la primera concierne a los usuarios directos de las criptomonedas, la segunda amenaza a cualquier compañía que posea computadoras o usuarios comunes de PC o de dispositivos móviles.

Con este documento se pretende:

- Hacer un estudio del estado actual del arte de la tecnología de la criptomoneda y su entorno.

• Describir algunas de las amenazas actuales de ambos tipos: de robo directo de la criptomoneda y de robo de recursos para producir nueva, o influir a otros usuarios del sistema.

• Analizar los principales incidentes de seguridad de últimos años relacionados con la criptomoneda, sus causas de ocurrencia, objetivos principales e influencia.

• Evaluar los riesgos relacionados con uso de criptomoneda o con uso de cualquier dispositivo, que puede ser comprometido con la idea de robo de sus recursos.

• Si es posible, proporcionar recomendaciones sobre cómo evitar dichos riesgos.

Esta información puede ser útil para un gran abanico de personas, como usuarios de criptomoneda, gestores de empresas, desarrolladores de software (no necesariamente asociados con la criptomoneda) y otras personas sin relación con el campo de la criptomoneda, pero que son usuarios de PC o de dispositivos móviles.

1.3 Estructura de la memoria

Este documento tiene siguiente estructura:

- El capítulo 2 se describe en detalle la filosofía, los conceptos teóricos en los que se basa el funcionamiento de Bitcoin, el estado actual del arte de la tecnología de criptomoneda y qué ventajas tiene en comparación con métodos de pago antiguos.
- Capítulo 3 se trata de análisis de amenazas relacionadas con posibilidad de robo de los fondos almacenados en la cartera local, u online (que pertenece a una bolsa de valores, o plataforma de cambio). También se describen las amenazas para la red de sistema de criptomoneda.
- En el capítulo 4 se presentan las amenazas actuales de robo de recursos, el cryptojacking o uso de sus tecnologías como un método de pago.
- En el capítulo 5 se recomiendan varias opciones de guardar criptomoneda y las mejores prácticas.
- En los últimos capítulos se detallan las conclusiones y las líneas de trabajo futuro.

2.Funcionamiento de Bitcoin

El primer lugar en la lista de los principales conceptos erróneos acerca de las criptomonedas lo ocupa la idea de que la criptomoneda es solo otro "trozo de papel", aunque sea electrónico, que solo representa dinero "real". Aquí es donde la mayoría de los otros conceptos erróneos se originan: ya que estos pedazos de papel, no valen nada, pueden ser impresos o destruidos como quieran, pueden ser falsificados o se pueden copiar.

Estas creencias no son más que ilusiones. Por ejemplo, en el origen de la idea de Bitcoin (la primera de las criptomonedas más exitosas y populares con mayor capitalización de mercado) estaba el deseo de crear no solo "trozos de papel" que representaran dinero real, como el oro, sino ser un análogo del oro en sí mismo. Tome esas propiedades del oro, gracias a las cuales es un dinero ideal, y haga una moneda electrónica basada en ellas.

Para comprender los principios de la criptomoneda, tomamos como ejemplo una más común, teniendo la mayor capitalización de mercado de la criptomoneda: Bitcoin.
Bitcoin se asemeja a un reloj mecánico suizo: realiza claramente la tarea desde el exterior, lo que no es difícil de entender. Pero si abre la cubierta trasera, se puede ver un mecanismo complejo, que consiste en un conjunto de engranajes y otros elementos. Sin embargo, es bastante posible que una persona con conocimientos técnicos entienda completamente cómo funciona todo.
Como uno de los usuarios del foro de criptomonedas escribe correctamente: "Bitcoin tiene esta característica: cuanto más lo empieces a entender, más preguntas surgen. Solo hay dos formas de salir: descifrarlo hasta el final o simplemente aprender a usar la interfaz del programa. De lo contrario, no dejará la sensación de que debe haber una incógnita en algún lugar ".
¿Qué es la criptomoneda? En resumen, es una moneda descentralizada con protección contra la reutilización basada en los logros de la criptografía moderna. La idea es que cada transacción sea irreversible y sea confirmada por bloques recién generados que cumplan ciertos requisitos. Estos bloques son calculados por toda la comunidad, están encadenados y están disponibles para que todos los puedan ver como una única base de datos. El procedimiento para calcular bloques se llama minería. Además, algunas criptomonedas permiten la emisión a través de la forja o ICO.
A veces, una nueva criptomoneda aparece como un fork de otra criptomoneda debido a cambios en los parámetros, lo que los hace incompatibles. En este caso, ambas criptomonedas pueden tener un historial de transacciones común hasta que se dividan.

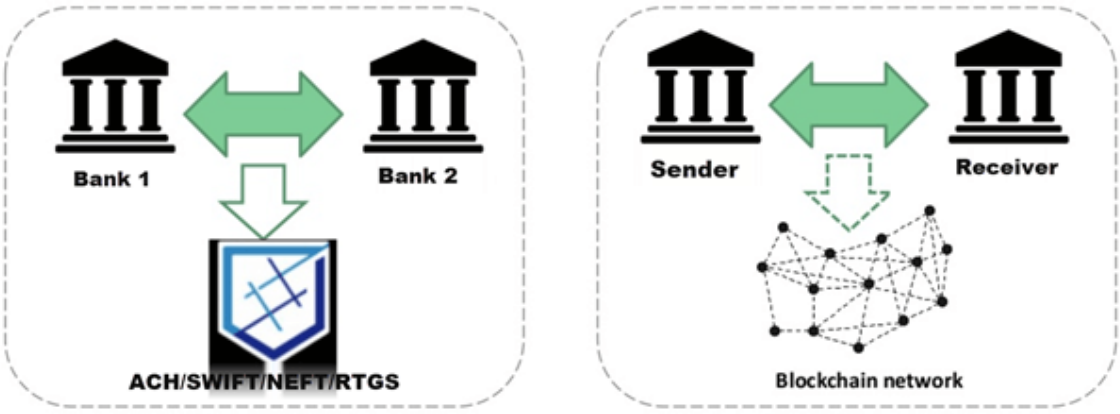

Imagen 1: Diferencia entre una transferencia bancaria y directa con uso de bitcoin.[1]

La red está construida de tal manera que un bloque se ubica en un cierto periodo, independientemente de la potencia de cálculo, es decir, la complejidad de los cálculos se

[1] https://www.guru99.com/blockchain-tutorial.html

autorregula. En el sistema de Bitcoin, el nivel de dificultad se recalcula cada 2016 bloques (aproximadamente una vez cada 2 semanas). Aumenta o disminuye en función de cuánto difiere el tiempo de creación de este lote de bloques de 20160 minutos (2016 * 10). Este mecanismo garantiza la aparición de bloques en promedio cada 10 minutos, independientemente de la potencia total de todos los mineros. En otras criptomonedas, el recálculo tanto del hash como del nivel objetivo de complejidad puede diferir significativamente. En muchos Altkoins (cualquier criptomoneda, que apareció después de bitcoin), el tiempo promedio de formación de bloques es significativamente menor, hasta varios segundos.
Al mismo tiempo, mientras la red crece, cada bloque recién generado también contiene nuevas monedas. En el caso de Bitcoin y algunos otros tipos de criptomoneda, el número de monedas que pueden estar en circulación está limitado a nivel de protocolo, y el número de monedas recién extraídas disminuye gradualmente de manera exponencial, de modo que nunca exceda el límite especificado. Esto asegura que la inflación está bajo control.
Cada usuario que generó el bloque recibe una recompensa fija, además la comisión de transacciones, que confirmó al incluirlos en el bloque.

Las monedas criptográficas tienen la propiedad de materialidad, y esto ya es una propiedad no tanto del oro, sino de cualquier moneda no electrónica. Una barra de oro no se puede cambiar dos veces por un servicio o producto. Es decir, en un momento dado puede ser del vendedor o del comprador.

Este comportamiento es natural para la moneda material, pero no para la electrónica. Para lograr este comportamiento en el dinero virtual, necesitas hacer mucha ingeniería. En Bitcoin, este comportamiento lo proporciona el mecanismo de transacción. Todas las transacciones se fusionan en cadenas. Cada transacción toma monedas de una o más transacciones existentes e indica a quién están destinadas. Por lo tanto, siempre se puede comprobar la validez de toda la cadena.

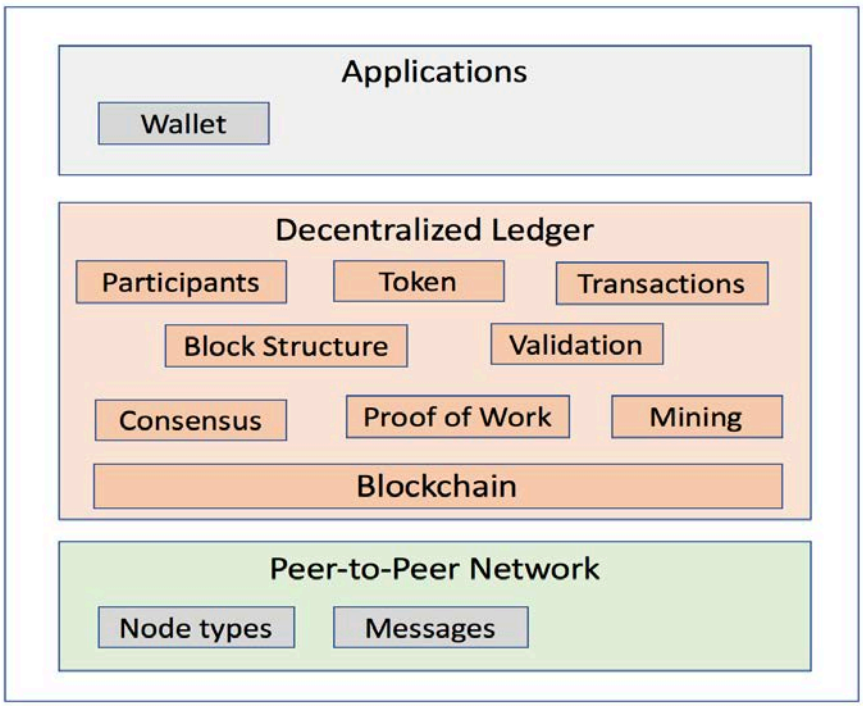

Imagen 2: Modelo de conceptos, usados en Bitcoin[2].

[2] https://luxsci.com/blog/understanding-blockchains-and-bitcoin-technology.html

La complejidad de la minería, los recursos limitados, la materialidad: estas propiedades, más el uso de la criptografía por seguridad, le permiten utilizar Bitcoin como dinero. El núcleo de Bitcoin se basa en ellos. Esto no es solo un arreglo. Todos ellos están incorporados en el sistema por diseño, y de otra manera no funcionará. Ahora se revisará un poco este diseño.

2.1 Cadena de bloques

Cualquier sistema de pago electrónico debe estar en algún lugar y de alguna manera almacenar transacciones. En Bitcoin, toda la información se almacena en una cadena de bloques. Los bloques se transmiten en formato JSON. Cada bloque contiene un título y una lista de transacciones. El encabezado consta de varias propiedades, entre las que se encuentra el hash del bloque anterior. Por lo tanto, toda la cadena de bloques almacena todas las transacciones para toda la operación de Bitcoin.[1]

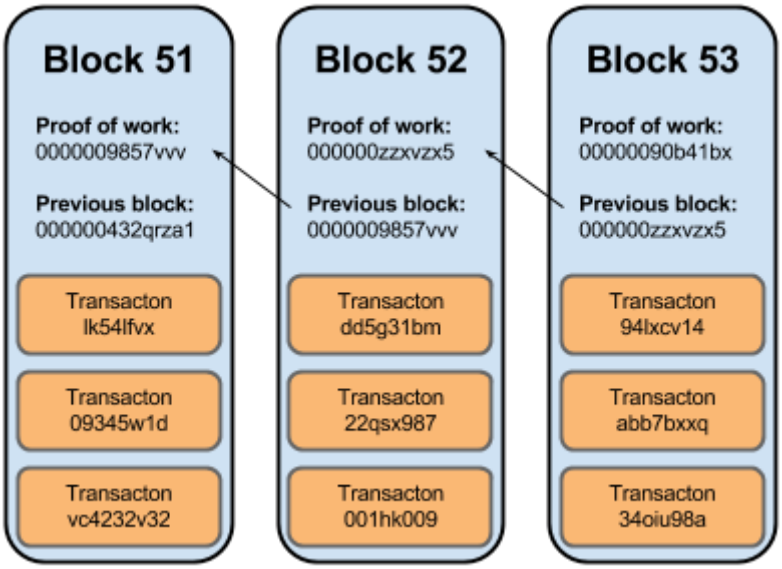

Imagen 3: Esquema simplificada de cadena de bloques[3].

En algunas de las versiones actuales de monederos de Bitcoin, la cadena de bloques se descarga completamente por cada cliente, lo que hace que el sistema esté completamente descentralizado. Los datos no están encriptados y cualquiera puede rastrear manualmente todas las transacciones. Incluso hay un sitio especial, Bitcoin Block Explorer[4], donde puede ver fácilmente toda la información sobre bloques y transacciones.

Al momento de escribir, el número de bloques en la cadena era de 564176 y, este número aumenta aproximadamente cada 10 minutos, lo que significa que algunos de los participantes pudieron crear un nuevo bloque.

Todos los participantes se dividen en dos grupos: aquellos que están trabajando en una nueva unidad y los que no están trabajando. Según las estadísticas, estos grupos se correlacionan de 1 a

[3] https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/
[4] https://blockexplorer.com/

3. Las transacciones se registran en bloques. Cada bloque contiene todas las transacciones que tuvieron lugar en el momento de su creación.

Funciona de la siguiente manera, uno de los clientes crea una nueva transacción y la envía a otros clientes que están ocupados generando el bloque. Añaden esta transacción a su bloque y lo continúan generando. Tarde o temprano alguien podrá generar un bloque. Este se sella (no se le agregan más transacciones) y se envía a través de la red. A continuación, los clientes verifican el bloque y las transacciones dentro de él para la validez. Si no hay problemas, entonces las transacciones se consideran aprobadas. En este punto, un bloque nuevo ya ha llegado a cada cliente y se ha agregado a la cadena. Después de esto, el proceso se repite: los clientes comienzan a generar otro bloque y recolectan nuevas transacciones en él.

2.2 Bloque

Revisaremos los contenidos del bloque y el proceso de su generación con más detalle. Se puede encontrar un ejemplo de un bloque en el mismo Bitcoin Block Explorer. Como ya he mencionado, el bloque consiste en un encabezado y una lista de transacciones. El encabezado consta de las siguientes propiedades[2]:

hash - SHA-256 hash del encabezado del bloque. Este hash es bastante aleatorio, y su tiempo de cálculo es predecible. Quiero señalar que es solo el hash de encabezado, sin transacciones. Por lo tanto, el número de transacciones no influirá mucho en el tiempo de cálculo de hash.

ver - La versión del esquema de bloques.

prev_block - El hash del bloque anterior en la cadena. Debido a esta propiedad, la cadena no puede ser falsificada reemplazando uno de los bloques en ella, ya que el hash del bloque siempre depende del hash del bloque anterior en la cadena. Cambiando uno de los bloques, tendrás que recrear todos los posteriores.

mrkl_root - Merkle root - lista de hashes de transacción. El hash del bloque debe necesariamente depender de las transacciones para que no puedan falsificarse. Pero llevará mucho tiempo calcularlo directamente si el número de transacciones es grande. Por lo tanto, estas se procesan primero y luego se utilizan para calcular el hash de todo el bloque.

Puede parecer absurdo, por qué calcular el hash del mismo. Pero el hecho es que el hash de transacción se actualiza solo cuando se agrega una nueva transacción al bloque, y el hash de encabezado de bloque se recalcula varios miles de veces por segundo. Además, cuanto más cerca esté el tamaño del encabezado en una constante, más exactamente podrá predecir el tiempo para calcular su hash.

time - uint32_t que representa el tiempo de creación del bloque. El año máximo permitido es 2106.

bits - Una de las propiedades más importantes. Es la forma abreviada del valor hash de destino. Se considera que un bloque se genera (válido) cuando su hash es menor que este valor objetivo. El valor objetivo determina la dificultad de crear un bloque. Cuanto más pequeño es, menos probable es que encuentre un hash adecuado en una iteración. Esta propiedad se actualiza cada dos semanas.

Sucede lo siguiente. El número de bloques generados para las últimas dos semanas se calcula y se compara con el estándar (1 bloque cada 10 minutos). Si hay demasiados bloques, entonces la complejidad aumenta. Si los bloques son demasiado pequeños - disminuye. De este modo, el sistema se adapta al aumento en el número de usuarios y, como resultado, a la capacidad total de sus computadoras.

nonce - Un número que, comenzando desde cero, se incrementa después de cada iteración del cálculo de hash. En realidad, esta es la forma en que se realiza la búsqueda hasta que el hash es menor que el valor objetivo. Para que cada nuevo hash difiera del anterior, al menos una de las propiedades del encabezado de bloque debe ser diferente.

Por ejemplo, la versión nunca cambia. El hash del bloque anterior se actualiza cuando alguien se nos adelanta y genera un nuevo bloque. Merkle root se actualiza cuando se agrega una transacción. El tiempo o frecuencia de esta actualización es cada pocos segundos. El tiempo de actualización de Bits (el valor objetivo, la complejidad), cada dos semanas. Todo esto es demasiado largo. No se puede esperar hasta que una de las propiedades se actualice y exista.

Considere una situación hipotética. Se verificaron todos los valores de nonce y ninguno de ellos encaja. Durante este tiempo, ninguna otra propiedad ha cambiado. Se produce un desbordamiento nonce y comienza desde cero de nuevo. Resulta que se repetirán más hashes. Para evitar estas situaciones, después de desbordar el espacio, cambia la propiedad especial de una de las transacciones. Después de eso, Merkle root se actualizará y los hashes del encabezado de bloque ya no se repetirán.

n_tx - El número de transacciones en la lista.

size - el tamaño del bloque en bytes.

2.3 Transacciones

Las transacciones están contenidas en bloques como una lista. Estas, como bloques, están alineadas en cadenas. Cada transacción debe indicar de dónde toma el dinero (de la transacción existente) y dónde se envía.

Para indicar el destinatario, se utiliza su clave pública. Para que este utilice el dinero recibido, debe crear una nueva transacción que tome dinero del anterior propietario y lo redirija a una dirección diferente. Para probar que una persona usa su dinero para la transferencia y no el de otros, debe dejar su firma digital en su transacción. En cualquier momento se podrá asegurar que todas las transacciones en el sistema son válidas.

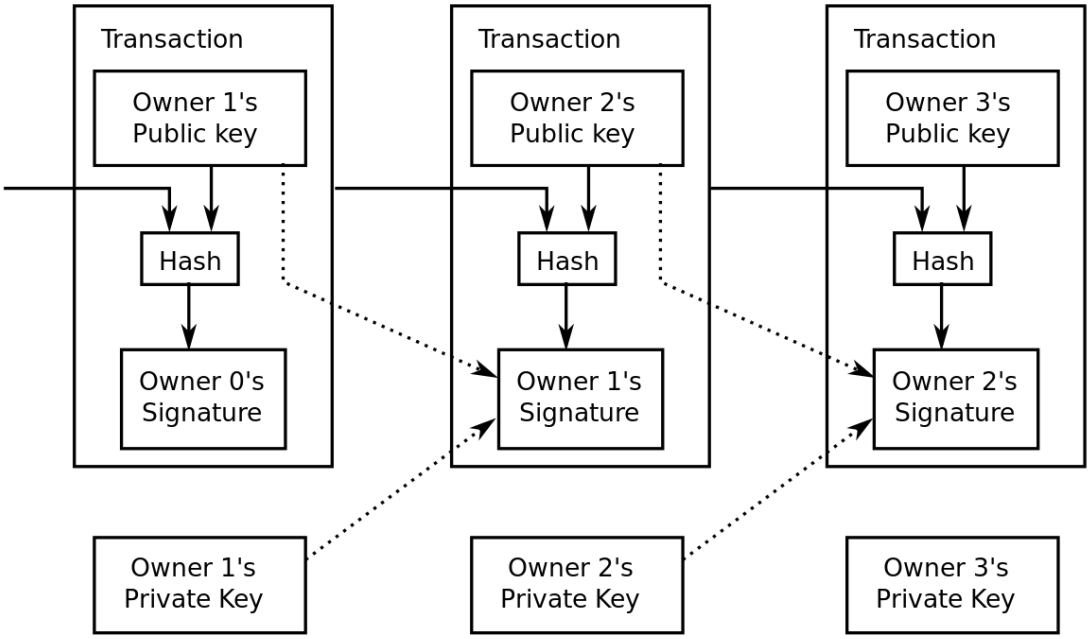

Imagen 4: Esquema de transacciones[5].

En la práctica, todo esto se implementa utilizando las siguientes propiedades[3]:

hash - Hash de toda la transacción. Las transacciones son hash dos veces. La primera vez calculando el hash de transacción. La segunda vez, durante el cálculo del hash de bloque. Además, cada bloque se refiere al hash del anterior, y cada transacción se refiere al hash de la transacción anterior (o transacciones). Si cambia una transacción y el hash no se rompiera (que es poco probable), todos los demás hash lo harán y la cadena de bloques modificada será rechazada por todos los clientes.

ver - Versión del esquema de transacción.

vin_sz - El número de transacciones anteriores de las cuales el dinero se transfiere a nuevas direcciones. Uno o más.

vout_sz: La cantidad de direcciones a las que se transfiere el dinero. Uno o más.

lock_time: Se basa en la idea de crear transacciones pendientes para que no se agreguen al bloque generado actual y de manera posterior (como por ejemplo al siguiente bloque). Esto implica que dicha propiedad indica la cantidad de bloques que una transacción debe omitir antes de agregarse. Así se hace posible que durante algún tiempo cambie la transacción y volver a firmarla.

size - Tamaño de la transacción en bytes, está en formato JSON.

en: Contiene la lista de entradas (fuentes) de la transacción. Como entradas se utilizan las salidas de transacciones anteriores (prev_out). Cada salida tiene las siguientes propiedades:

hash - El hash de la transacción anterior.

[5] https://en.wikipedia.org/wiki/Bitcoin_network

n - Una transacción puede tener varias salidas y se debe especificar de cuál de ellas se toma el dinero. Para esto existe esta propiedad. Contiene el número de secuencia de la salida de la transacción anterior, comenzando por 0.

scriptSig: En esta propiedad, el remitente debe probar que transfiere exactamente su dinero y no a extraños. Para ello, especifica la clave pública del destinatario de la transacción anterior, es decir, su clave (puesto que debe ser este). Además, agrega la firma ECDSA de la misma transacción, que se realiza con su clave privada. Esto prueba que él maneja su dinero, no el de un extraño.

Después de la lista de entradas de la transacción (entrada), se indica la lista de salidas (salida), los destinatarios. Cada salida tiene las siguientes propiedades:

value: Contiene la cantidad de dinero que se transferirá a la nueva dirección. Se toma de transacciones anteriores. Por lo tanto, este número no debe exceder su suma. Por ejemplo, queremos tomar 10 monedas de una transacción y 20 de otra y enviar 25 a una nueva dirección. Las 5 monedas restantes no se pierden, nos las enviamos a nosotros mismos, como si fuera el cambio. Por lo tanto, en nuestra transacción habrá dos destinatarios. El valor siempre se indica en nanomonet para evitar números fraccionarios.

scriptPubKey: Esta propiedad, junto con el *scriptSig*, compone un script en un lenguaje similar a Forth. ScriptPubKey contiene las declaraciones de idioma y el hash de la clave pública del destinatario de la transacción. La secuencia de comandos comprueba la transacción para la validez. El uso de tal escenario ofrece muchas posibilidades para describir las condiciones con las que recibir el dinero por parte del destinatario. Por ejemplo, puede forzar al destinatario a especificar una contraseña en lugar de ECDSA.

La cantidad total de dinero en la entrada de una transacción siempre es igual a la cantidad total en la salida. De lo contrario, sería como si el dinero surgiera del aire o desapareciera de la circulación.

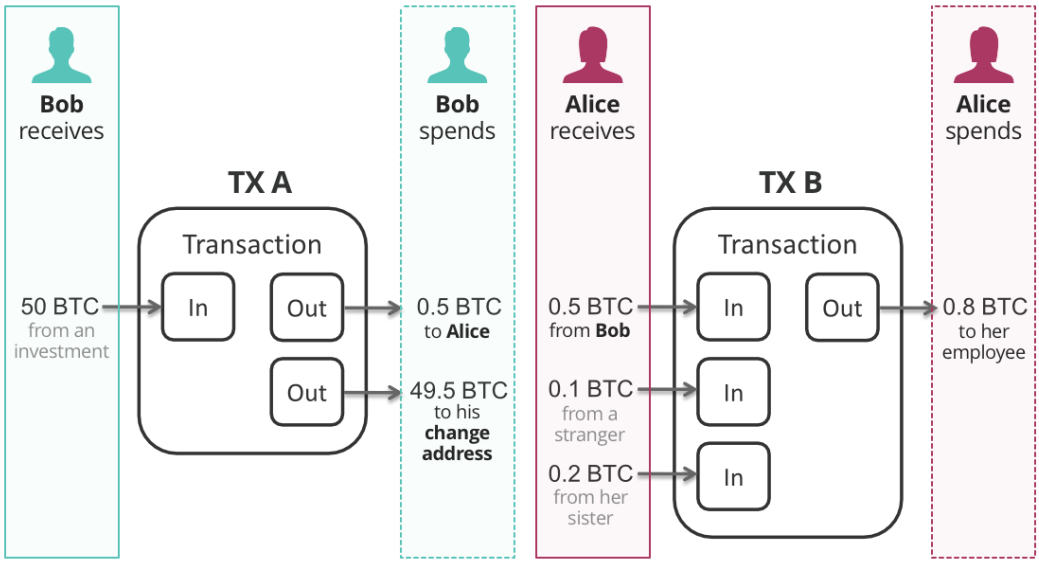

Imagen 5: Esquema de transferencia de dinero por transacciones A y B[6].

[6] https://freedomnode.com/guides/17/how-bitcoin-works

La emisión del dinero es simple y elegante. En cada bloque, la primera transacción en la lista es una transacción especial. Siempre tiene una entrada, que tiene la propiedad *coinbase* en lugar de la propiedad *scriptSig*. Esta propiedad puede contener cualquier cosa.

La salida de la transacción también es siempre la misma. Actualmente redirige 12.5 monedas a la que generó el bloque. Es una recompensa por el tiempo y los recursos dedicados a generar el bloque. Al crear un nuevo bloque en la cadena, el cliente contribuye al trabajo de Bitcoin.

Cada cuatro años, esta recompensa se reduce a la mitad, por lo que el número total de monedas en circulación se estabiliza. Después de eso, incluso si el atacante crea un bloque utilizando una versión modificada del programa y se asigna 12.5 monedas a sí mismo, este bloque no se agregará a la cadena, ya que será rechazado por otros "clientes honestos", que deberían ser la mayoría.

La estabilidad del sistema se basa en la cantidad de usuarios que tienen un cliente oficial en ejecución. Mientras que la mayoría de los usuarios lo utilicen, Bitcoin no se verá amenazado.

2.4 Prueba de trabajo

El resultado de un trabajo que es difícil de lograr, pero fácil de verificar. La red Bitcoin se basa en este principio. Puede verificar el hash (el resultado del trabajo) en una fracción de segundo. Y para recogerlo, se necesita mucho esfuerzo.

La prueba de trabajo[4] implica la exploración de un valor que tiene un hash con cero inicial. El trabajo requerido en un promedio está creciendo rápidamente en la cantidad de cero bits requeridos y puede verificarse ejecutando un solo hash. Para bitcoin, se implementa la prueba de trabajo incrementando un 'nonce' en el bloque hasta que se encuentre un valor que le dé al hash del bloque los bits cero requeridos. Una vez que se ha gastado el esfuerzo de la CPU para que satisfaga la prueba de trabajo, el bloque es inalterable a menos que se vuelva a hacer el trabajo. A medida que los bloques de progreso del trabajo se encadenan después, para cambiar el bloque se requeriría rehacer todos los bloques después de él.

La prueba de trabajo también resuelve el problema de determinar la representación en la toma de decisiones mayoritarias. One-IP-address-one-vote no es una solución óptima; cualquiera podría asignar muchas IP. Entonces, la prueba de trabajo es esencialmente una CPU-un-voto. La cadena más larga representa la decisión mayoritaria, que tiene el mayor esfuerzo de prueba de trabajo, invertido en ella y esto se encuentra en los nodos honestos, que controlan la mayoría de la potencia de la CPU y crecerán más rápido y superarán a las cadenas de la competencia. Requeriría hacer la prueba de trabajo del bloque y todos los bloques después de cualquier intento de cambiar un bloque completado, y luego violar los nodos honestos. Alternativamente, para evitar cualquier desbordamiento de hardware, la dificultad de la prueba de trabajo está determinada por un promedio móvil que apunta a un número promedio de bloques por hora. Si se generan demasiado rápido, la dificultad aumenta.

Aquí puede recordar ahora la analogía con el oro, cuya extracción requiere mucho tiempo y recursos. Pero puede entender que el oro está frente a usted de manera casi inmediata. En este sentido, Bitcoin también tiene su valor. Pero no entienda esto como el precio en dólares o en las facturas de electricidad que usó la computadora durante la selección del hash.

El precio en dólares es un poco diferente. No está incorporado en Bitcoin y está determinado únicamente por el mercado. Después de todo, el oro en sí no le garantiza un precio determinado en dólares. Está garantizado solo por una persona que quiere intercambiar oro por dólares.

El valor inicial del oro fue determinado únicamente por aquellos que lo extrajeron, intentando compensar con este precio el esfuerzo empleado. Y después de eso, el mercado comienza a influir en el precio del oro.

Una vez que Bitcoin ha llegado al mercado, su valor se determina únicamente por el nivel de confianza en el sistema. Cuanto más confíe la gente, más comprará Bitcoin, más dinero invertirán en él y, por consiguiente, más costoso será Bitcoin.

Antes de que la gente pueda confiar en Bitcoin, se debe averiguar si este sistema tiene un grado de seguridad suficiente y si se puede usar como dinero, es decir, si tiene las propiedades del dinero, que se enumeraron al principio. Para saber esto con seguridad, se deben comprender los principios de funcionamiento de Bitcoin.

3.Amenazas: robo de criptomoneda

El robo en la sociedad humana ha existido desde tiempos inmemoriales. Se puede abordar desde una perspectiva global o más individual, incluso personal. El problema del robo en la sociedad es extremadamente complejo. Por otra parte, se cree que es prácticamente imposible de erradicar. A los defensores de esta teoría les gusta dar un ejemplo clásico: cuando en la Edad Media los cuatreros fueron condenados a ejecuciones públicas en la plaza, sus compañeros de trabajo se abrieron paso entre la multitud y cortaron las bolsas de monedas de los espectadores que fueron a observar la ejecución. Por lo tanto, ni la crueldad del castigo de los ladrones, ni su publicidad, se convirtieron en una edificación para otros ladrones y no los alejaron del crimen.

La popularidad de Bitcoin y el nacimiento de otras 1.500 monedas digitales han atraído a los piratas informáticos al área de la criptomoneda, lo que aumenta las oportunidades de delincuencia y fraude. “Los ciberdelincuentes están siguiendo el dinero, y ahora ven en el mundo no regulado y en gran parte inseguro de las monedas digitales la capacidad de dirigirse a personas, negocios e intercambios y ganar dinero de manera rápida y fácil”, dijo Rick Holland, vicepresidente de estrategia para Digital Shadows.[7]

La naturaleza descentralizada de la criptomoneda y de blockchain es, sin duda, una ventaja sobre la financiación tradicional, pero también lo es para los piratas informáticos. Y, la ausencia de transacciones reversibles y el aumento del anonimato, así como la novedad y la insuficiente atención de los usuarios al problema de la seguridad, los hacen aún más atractivos para ellos. Varios informes de la ICO (Initial Coin Offering, forma de atraer inversiones en forma de venta a inversionistas de un número fijo de nuevas unidades de criptomoneda recibidas por una emisión única o acelerada) afirman que el 10% de todos los fondos de los primeros inversores fueron robados por ellos.

Curiosamente, la mayoría de los ataques de hackers no son cometidos por solitarios, sino por “jugadores de equipo”. Según un estudio reciente realizado por la compañía analítica Chainalysis, dos grupos de piratas informáticos gastaron el 60% de todos los robos registrados y robaron criptomonedas por un valor de más de mil millones de dólares[5]. Los investigadores identificaron los grupos de hackers como “Alpha” y “Beta”. Alpha es una organización gigantesca y estrechamente controlada que persigue no solo objetivos monetarios. Beta es menos organizada, monitorea la seguridad peor y está completamente enfocada en el dinero. Ambos grupos operan con criptomonedas robadas de manera diferente. Alfa transfiere las monedas inmediatamente después de la piratería, Beta, dentro de un periodo de 18 meses. Los piratas informáticos esperan al menos 40 días para que desaparezca el interés en el robo, después de lo esto, intentan cobrar las monedas lo más rápido posible: el 50% de todos los fondos robados se cobran dentro de los 112 días. Por lo general, los piratas informáticos roban monedas por 90 millones de dólares a la vez, pero el número de “robos menores” ha aumentado entre 20 y 30 millones dólares. Después del robo, en promedio, pasan la criptomoneda robada unas 5000 veces a través del sistema de carteras, intercambiadores y transacciones entre pares antes de cambiarlos por moneda fiduciaria. Incluso los intercambios regulados que siguen procedimientos estrictos de ALD (procesos contra el lavado de dinero) a veces se usan para cobrar. Rastrear el dinero robado o lavado es difícil: el

[7] https://www.reuters.com/article/us-cryptocurrency-cybercrime/cybercriminals-target-booming-cryptocurrencies-report-idUSKBN1FL5Q7

origen del dinero solo se puede conocer después del hecho, pero no en tiempo real. Los investigadores creen que es probable que ambos grupos sigan activos.

Sin embargo, la experiencia de luchar con la red oscura muestra que el estado es capaz de combatir la ciberdelincuencia, y el anonimato de las criptomonedas sigue estando muy vigente, pero el intercambio de dinero de forma anónima es cada vez más difícil. Los servicios de seguridad pueden asociar transacciones con un usuario específico, que incluso las monedas anónimas no salvan. En tales condiciones, la criptomoneda es un enlace intermediario superfluo, porque el efectivo es más difícil de rastrear. Según los analistas, en los últimos 2 año, los 13-16,7 mil millones de dólares en fondos, que giran en el mundo de criptomonedas, se pueden calificar de delincuentes de manera muy general. Mucho o poco depende del tamaño de la capitalización del mercado criptográfico. Con una capitalización de 700 mil millones de dólares, esto es solo el 2%, con una capitalización de cien mil millones, ya del 13% al 16%. Pero es obvio que, en el contexto de miles de millones de dólares en negro, este es un valor insignificante.

El dinero fiduciario es usado por criminales cientos de veces más, pero esto no es una razón para su prohibición. Está claro que la criptomoneda se ve como una posible herramienta del crimen, pero es mucho menos versátil y conveniente que sus contrapartes tradicionales.

A continuación, se revisarán varios vectores de ataque que pueden ser utilizados por los piratas informáticos.

3.1 Vulnerabilidades de clientes y clientes ficticios.

Las carteras en el contexto de la seguridad del almacenamiento de criptomonedas se pueden dividir en tres tipos:

1) Carteras "frías". No solo almacenan datos privados, sino que también descargan la criptomoneda blockchain en una computadora. Ocupan gigabytes y terabytes, y el espacio que requieren está en constante crecimiento debido al crecimiento de la cadena de bloques. Pero tal cartera usa Internet solo para completar una transacción, sin recurrir a recursos de terceros.

2) Carteras "calientes". Son un programa que, como en el caso anterior, almacena datos de cuentas privadas en una computadora. Pero el blockchain no descarga tal cartera, y por tanto tiene que utilizar recursos de terceros durante cada operación. En teoría, el acceso a los datos privados se cierra antes de que se ejecute una llamada a un tercero, por lo que no se anuncia en ninguna parte.

3) Carteras en línea. Representan una cuenta en el recurso de Internet, similar a las cuentas en sistemas de pago electrónico. Todos los datos del usuario se almacenan en este recurso, y el usuario puede acceder a ellos desde cualquier lugar, donde haya Internet, simplemente ingresando un nombre de usuario y contraseña.

Una de las principales preocupaciones del propietario de la cartera criptográfica es garantizar su seguridad y protección contra intrusos que pueden robar fondos. Cuando esto sucede, en algunos casos el propietario de la cartera es el culpable y en otras ocasiones, los desarrolladores son los que no han completado suficientemente el sistema de protección.

Los hackers pueden encontrar vulnerabilidades en el software criptográfico y crear programas especiales (exploits) que pueden penetrar en el sistema del dispositivo a través de brechas de seguridad y realizar acciones que son ventajosas para los intrusos.

Los exploits son un problema para los desarrolladores de soluciones de protección y uno de los obstáculos más graves para garantizar la seguridad de los sistemas y el almacenamiento de datos. Los exploits son un subtipo especial de malware que contiene datos o código ejecutable que puede penetrar en el sistema a través de vulnerabilidades en el software.

Por ejemplo, si el navegador tiene alguna vulnerabilidad que permita la ejecución de "código arbitrario", entonces un pirata informático, sin el conocimiento del propietario del PC, puede instalar y ejecutar un programa malicioso en su sistema y programar silenciosamente el sistema para obtener beneficios.

Del mismo modo, los exploits buscan vulnerabilidades en el software instalado en las carteras de criptomonedas.

Para demostrar un ejemplo de estado fatal de situación: En 2017, la empresa Solar Security presentó los resultados del estudio[6], durante el cual analizó varias carteras móviles de bitcoin para su seguridad.

Los resultados fueron decepcionantes. Se encontró que muchas carteras son vulnerables a varios tipos de exploits y otros tipos de ataques.

Nivel de seguridad de las versiones de Android de las billeteras bitcoin

Billetera	Vulnerabilidades criticas	Vulnerabilidades de nivel medio	Nivel de seguridad
Bread	0	3	4.4/5.0
BitPay	2	205	2.9/5.0
Copay	2	205	2.9/5.0
Luno	6	412	2.1/5.0
Blockchain	12	447	1.5/5.0
Coinbase	12	266	1.5/5.0
Coins.ph	11	424	1.5/5.0
Airbitz	17	715	1.1/5.0
Xapo	19	482	1.1/5.0
Mycelium	25	274	0.9/5.0

Imagen 6: Nivel de seguridad de las billeteras Bitcoin para Android[6]

La protección insuficiente contra los exploits significa que las carteras no están 100% protegidos contra la piratería y el robo de fondos. En algunos casos, los desarrolladores trataron sus tareas de manera descuidada y no se ocuparon de una protección confiable.

Durante el uso de la cartera, hay que tener en cuenta, que no solo la cartera actual tiene valor para los atacantes, también las copias de seguridad [7]. Una copia antigua de una cartera con contraseña antigua a menudo se puede recuperar fácilmente creando un programa de recuperación (por ejemplo, Apple Time-Machine): restaurar una cartera vieja con una contraseña restaurará la

cartera actual y la contraseña actual. Por lo tanto, los cambios frecuentes de contraseña no son una garantía de seguridad completa. Para solucionar este problema, los creadores de la criptomoneda deben hacer cambios para que al cambiar la contraseña de la cartera se cree automáticamente una nueva cartera con una nueva contraseña, y los ahorros acumulados se transfieran automáticamente a la nueva cartera. En este caso, si intenta restaurar una copia de su cartera y contraseña antiguas, se desactivará. Por otro lado, los usuarios que no entienden las complejidades técnicas de crear carteras no podrán recuperar los datos de su criptomoneda de ahorro y perderán Bitcoins junto con la cartera.

También existe otra amenaza en el uso de cliente de cartera. Los hackers no solo intentan utilizar vulnerabilidades de aplicaciones oficiales de carteras, también hacen sus propias aplicaciones y las publican en sitios web, Google Play o Apple AppStore.

Así, en noviembre de 2018, Lukas Stefanko (un investigador de malware que trabaja para ESET) descubrió un grupo de las aplicaciones maliciosas en el catálogo Google Play, disfrazadas de servicios de criptomoneda legítimos que pretendían robar las credenciales de los usuarios[8]. Los atacantes actuaron de dos maneras diferentes:

- La aplicación MetaMask (Ethereum cryptocurrency wallet) funcionó de acuerdo con el esquema de phishing clásico. Después de la instalación y el inicio, se le solicitó al usuario que ingresara una clave privada y una contraseña de su cartera de criptomonedas. Si la víctima estaba de acuerdo, estos datos estaban a disposición de los intrusos. Después de eso, la aplicación agradeció la activación y cerró.
- El segundo esquema, estaba asociado con carteras falsas. De esta manera, actuaron las aplicaciones NEO y Tether, creadas por el mismo autor (o grupo de autores). Las carteras de criptomonedas reales generan una clave privada para el usuario y una dirección pública para transferir fondos. Las falsificaciones mostraron al usuario la dirección pública de la cartera de los atacantes. La criptomoneda transferida a dicha dirección no podía devolverse sin una clave privada, cuyo acceso en última instancia se mantuvo solo con los atacantes.

Para aumentar la protección de fondos y minimizar la posibilidad de robo al usar carteras de escritorio en un PC, o dispositivo portátil, se recomienda usar la versión oficial y actual de una de las carteras fiables, descargada del sitio oficial, actualizar regularmente el sistema y el software antivirus, no abrir archivos sospechosos de remitentes desconocidos (pueden contener exploits). O utilizar recomendaciones, que se encuentran en el artículo 5 de este documento.

3.2 Vulnerabilidades y ataques a Plataformas de cambios y Bolsas de valores de criptomonedas.

La versión de la cartera en línea se implementa en las bolsas de valores y en las plataformas de cambios, pero a menudo de manera reducida.

Al registrarse en la bolsa de valores, el usuario crea una cuenta en sus servidores. Los números de carteras, las claves de ellos y otra información se almacenan en el mismo lugar. El usuario puede acceder a los fondos desde cualquier lugar donde haya Internet al iniciar sesión en la cuenta en la bolsa con un nombre de usuario y contraseña (y/u otros datos).

La única diferencia con una cartera en línea es que las carteras pueden proporcionar más oportunidades al realizar transacciones, y las bolsas de valores se utilizan para el intercambio y la negociación, por lo tanto, generalmente no se proporciona una gran cantidad de funciones para la transferencia de dinero.

Las criptomonedas llegan al saldo del usuario de tres maneras: de su propia cartera, de otra persona o a través de un programa de minería para extraer monedas, que indica la dirección de la cartera.

El dinero fiduciario se pone en el saldo mediante sistemas de pago como el mismo Webmoney (u otros sistemas similares) o tarjetas bancarias, por ejemplo.

La principal razón por la que no se recomienda a los usuarios de criptomonedas mantener fondos en las bolsas de valores y en las plataformas de intercambios es su mayor inseguridad y vulnerabilidad.

Según el Grupo IB, CipherTrace, Carbon Black[9], en 2018, los piratas informáticos robaron criptomonedas por un valor de 1,1 a 1,7 mil millones de dólares, de los cuales 960 millones provinieron de bolsas de valores y sistemas de pago. El número de casos de este tipo aumentó 3,5 veces en comparación con 2017, y 7 veces en comparación con 2016. El 56% del robo criptográfico ocurrió en las bolsas de valores de Corea del Sur y Japón. El mayor robo en 2018: 532 millones de dólares de Coincheck, 60 millones de dólares de Zaif, 40 millones de dólares de Coinrail y 31 millones de dólares de Bithumb.

Además de atacar directamente el cambio, o cartera en línea, los hackers pueden utilizar vulnerabilidades de sus páginas para robar credenciales de los usuarios. Uno de los métodos más comunes de este tipo de ataque es CSRF.

CSRF[10] (Cross Site Request Forgery en inglés - “falsificación de solicitud de sitio”, también conocida como XSRF) es un tipo de ataque a los visitantes del sitio web que utiliza las desventajas del protocolo HTTP. Si la víctima ingresa al sitio creado por el atacante, se envía secretamente una solicitud a otro servidor (por ejemplo, al servidor del sistema de pago), realizando algún tipo de operación maliciosa (por ejemplo, transfiriendo dinero a la cuenta del atacante, o cambiar algunos datos personales). Para llevar a cabo este ataque, la víctima debe estar autenticada en el servidor al que se envía la solicitud, y esta solicitud no debe requerir ninguna confirmación por parte del usuario, que no puede ser ignorada o falsificada por el script de ataque.

Las carteras en línea pecan por las mismas razones, por lo que tampoco son populares. Las carteras “propias” (que no son en línea) se consideran más confiables por las siguientes ventajas:

Almacenan datos privados en el dispositivo del usuario, ya que a estos datos no pueden acceder terceros. Las bolsas de valores y las plataformas de cambios almacenan datos en sus servidores. Los fundadores del recurso generalmente declaran la confiabilidad del almacenamiento del servidor, su seguridad, tanto física como de software, aunque es imposible de verificar. Además, no importa cuán perfecta sea la protección del servidor, los fundadores del recurso tienen acceso a los datos. Hay razones para confiar en ellos o no: pero su dispositivo, al que nadie más tiene acceso, parece más confiable. Finalmente, cuando se piratea una cartera en línea, si los datos privados son realmente almacenados solo por el usuario, es poco probable que el hacker los reciba. Hackear la bolsa de valores significa obtener acceso a los datos privados de todos los usuarios.

Al piratear los servidores de la cartera, el usuario se queda con su dinero y puede retirarlos. Cuando se trata de la bolsa, él administra su dinero en la medida en que los dueños de esta lo permiten. Si hay una fuga de fondos, los propietarios pueden bloquear todas las cuentas, devolver parte del dinero a las víctimas a expensas de otros usuarios, y así sucesivamente.

La cartera propia, al ser un software completo, implica más oportunidades para la implementación de la protección que la bolsa de valores o la plataforma de cambio. Estos son grandes recursos donde se realizan demasiadas funciones, por lo que no se les puede prestar la misma atención a un problema de seguridad como en un programa separado. Además, ellas están destinadas a realizar otras operaciones.

3.3 Fake ICO, Phishing y Scam.

Según diversas fuentes, desde la mitad al 80% de los ICO se crearon inicialmente como fraudulentos[11]: sus organizadores son conscientes de la imposibilidad de realizar el proyecto y gran parte de los fondos recaudados se destinan a fines personales o publicitarios. Al mismo tiempo, en 2017, a expensas de ICO, se atrajeron de 5,6 a 6,2 de dólares mil millones. Dado que los ICO no están regulados en absoluto, sus organizadores no tienen responsabilidad hacia los inversores. Según el Centro Europeo para el Análisis de Delitos Cibernéticos de la UE, en los proyectos de estafa de 2017-2018 se produjo una pérdida de 1,4 mil millones de dólares por parte de los inversores. Quizás el ejemplo más sorprendente de fraude de ICO en 2018 es el proyecto estadounidense “Centra”. En primavera, un proyecto que anunciaba al boxeador Floyd Mayweather y otras celebridades, por engaño, recaudó 32 millones de dólares, después de lo cual el líder intentó huir del país. En el noviembre de ese mismo año, ocurrió un incidente “divertido” con el proyecto de la estafa de Pure Bit: el administrador inicial se escapó con 2,7 millones de dólares, luego se arrepintió y devolvió el dinero a los usuarios. Este año, las llamadas "letras nigerianas" también fueron populares en Twitter, un tipo de fraude, cuando las páginas de celebridades falsas prometían distribuir monedas gratis a cambio de un pequeño pago, los cuales continúan a día de hoy. El fraude se reveló rápidamente, pero las falsificaciones pueden ganar unos pocos miles de dólares, y toda la "industria", según algunas estimaciones, aumenta de 50.000 a 100.000 de dólares por día.

Otro esquema muy popular para engañar a los usuarios es el phishing. Los profesionales de la esfera moderna de blockchain definen la frase "phishing de criptomoneda" como un cuadro muy común, frecuentemente encontrado, fraudulento. A juzgar por los datos[12] de Kaspersky Lab, cada trimestre, los delincuentes roban de esta manera de 2 a 3 millones de dólares. El significado de este método es simple: está minando de varias maneras los datos secretos del usuario. Los ladrones luego usan la información robada (contraseñas, frases iniciales, inicios de sesión, etc.) para penetrar en la cartera criptográfica o en las cuentas de cambio de moneda virtual para vaciar las cuentas.

Típicamente, los atacantes que utilizan phishing recurren a una técnica relativamente simple, pero a menudo efectiva: envían correos electrónicos a los usuarios que contienen diversos datos atractivos, con un enlace obligatorio al recurso, imitando a la oficial, que es necesario seguir.

Este esquema no es nuevo y existió mucho antes de la llegada de Bitcoin, ethereum y otras criptomonedas. Desde el momento en que apareció el "dinero electrónico", los estafadores tomaron posesión de códigos secretos y contraseñas de sus propietarios mediante acciones

activas, después de lo cual la moneda fiduciaria desapareció instantáneamente de las carteras electrónicas, cuentas y tarjetas bancarias.

Muchas personas descuidadas y demasiado confiadas, "picotearon" el cebo que se les presentó, sucumbiendo a la tentación de obtener beneficios gratuitos. Aquí están en cualquier etapa, intoxicados por la felicidad repentina, dejando la contraseña y su inicio de sesión. Según los detalles del fraude, los usuarios proporcionaron datos para tarjetas bancarias, cuentas de carteras electrónicas y cuentas personales entre otros. Los ladrones, más tarde, del lugar de almacenamiento de fondos retiraron cada centavo. La víctima descuidada e imprudente luego informa que le han robado. Sin embargo, les dio a los estafadores un código con un inicio de sesión con sus propias manos, es decir, que fue como darles el dinero.

La situación en el presente mercado criptográfico es similar: los delincuentes de Internet intentan extraer información secreta relacionada con los depósitos de monedas digitales y las cuentas de bolsas de valores y plataformas de cambio. Más a menudo, los phishing se esfuerzan por obtener claves privadas de las carteras para recoger los cryptoactivos que se encuentran allí.

Los ladrones, que usan phishing en monedas virtuales, siguen estrictamente un esquema de acciones elaborado. El conjunto estándar de actividades de estafas se compone de una secuencia con varias etapas:

1) Objetivo de búsqueda. Aquí hay una selección de la criptomoneda y también se estudian las características de los criptógrafos actuales y las plataformas descentralizadas que son necesarias.

2) Identificar el público objetivo. El estafador, decidido a cometer el robo, concentra sus esfuerzos para recopilar la máxima cantidad de información sobre las personas que utilizan la plataforma elegida y el repositorio de monedas. Un ladrón necesita personas que contengan criptomonedas en sus carteras, de lo contrario, desperdiciaría su energía. Se busca el grupo objetivo de forma relativamente rápida en recursos especializados por vía tópica: comunidades, foros, grupos, salas de chat, etc.

3) La formación de la letra-cebo. Aquí es necesario que el estafador emita un mensaje elaborado para que las dudas del usuario desaparezcan de inmediato al ver la formalidad inspirada y la seriedad ilusoria. Las personas cautelosas que temen los virus, con un pequeño borrón o un error cometido por el autor, enviarán rápidamente este mensaje a la carpeta de SPAM sin hacer clic en el enlace.

4) Construye un recurso web falso. Aquí los estafadores hacen un sitio web falso donde los usuarios que utilicen el enlace proporcionado se moverán. Los creadores le dan especial importancia a la calidad de copiar un recurso web falso para minimizar las diferencias con respecto a un proyecto de la vida real.

5) Enviar cartas de cebo a un grupo seleccionado de personas. Cuando la víctima, sin dudar, utiliza los enlaces indicados y cree en el cebo de los estafadores, en algún momento se produce el secuestro de inicios de sesión y contraseñas con programas especiales. Por ejemplo, la estafa más elemental tiene una estructura similar a esta:

- En la carta felicitan con la cesión de cryptomoneda;
- El usuario está feliz haciendo clic en el enlace;

- La cantidad de 10 BTC brilla en la pantalla, se reproduce música y aparece un mensaje como "El Crypto Trader XXXX le ha transferido monedas, vaya a la cartera para acreditar la cantidad ...";
- Al regocijarse con un regalo de promoción sólido, la persona comienza rápidamente a ingresar una contraseña, un nombre de usuario y las claves, sin darse cuenta del significado de las acciones realizadas;
- Después de abrir un repositorio digital, el sitio con felicitaciones se cierra repentinamente, supuestamente debido a un fallo en la web;
- El usuario angustiado decide repetir todo después y se va.

En la etapa final, cuando se abrió la ventana criptográfica, el programa de software espía grabó los datos necesarios y apagó el sitio.

6) El estafador, después de haber recibido los datos secretos, vacía disimuladamente la cartera virtual de la víctima.

Consejos sobre cómo evitar el phishing de criptomonedas:

- No abrir correos electrónicos y otras formas de mensajes enviados desde direcciones desconocidas, sospechosas o raras.
- No activar enlaces en mensajes que no se esperaban.
- Usar (si es posible) para iniciar sesión en la cartera, en la bolsa de valores o en la plataforma de intercambio un ordenador o un dispositivo separado en el que esté activa una potente protección antivirus.
- Muestre prudencia y elimine instantáneamente cualquier correo sobre ganancias, reposición repentina de cuentas, transacciones de premios, etc. No hay regalos, suerte ni fortuna, especialmente en las áreas relacionadas con el dinero.
- Utiliza el correo en Gmail, este servicio filtra el 99,9% de los correos electrónicos fraudulentos a la carpeta Spam.

Además del phishing, los esquemas de Scam que usan redes sociales como Twitter tienen un gran éxito. Por lo general, los estafadores se hacen pasar por miembros influyentes de la comunidad y prometen multiplicar varias veces la cantidad de monedas que los inversores están invitados a enviar a la dirección especificada.

Según el portal Bleeping Computer, en febrero de 2018 unos estafadores recibieron más de 5000 dólares en criptomoneda Ethereum durante una noche usando cuentas de Twitter falsas de personas famosas que enviaban mensajes a los usuarios con una propuesta para participar en la "distribución de criptoactivos"[13].

Las “celebridades” ofrecieron a los usuarios transferirles una pequeña cantidad de criptomonedas, prometiendo en respuesta proporcionar una suma de diez veces la cantidad enviada. Todos los mensajes se componen de una plantilla. Las diferencias se encuentran solo en las cantidades y direcciones indicadas de los criptomonedas. Como ejemplo de mensaje típico puede servir:

¡Donamos 200 Ethereum a la comunidad ETH! Las primeras 50 transacciones de 0.2 ETH enviadas a la dirección a continuación recibirán 2.0 ETH a la dirección de la cual provienen 0.2 ETH.

Los hackers crearon cuentas falsas de varias personas famosas, como Warren Buffet, Vitalik Buterin, John McAfee e Ilon Musk. Además, se crearon cuentas falsas de los intercambios Coinbase y CoinMarketCap, Nano Cryptocurrency y OmiseGo.

Ahora los atacantes además utilizan cuentas verificadas para sus estafas para hacer que su propuesta se vea más convincente.

Según Buzzfeed News, una cuenta verificada fraudulenta de la Tron Foundation, el desarrollador de la moneda en criptomoneda TRON (TRX), fue descubierto recientemente en la red[14]. Para crearla, los piratas informáticos robaron otra cuenta verificada en propiedad de la compañía estadounidense Literacy Bridge.

Después de eso, cambiaron la imagen en el perfil, arreglaron el tweet como en la cuenta original de la Fundación Tron, cambiaron el nombre de usuario a "tronfoundationl" y dejaron un mensaje debajo del tweet de Justin San, el fundador de Tron, solicitando donaciones. Este mensaje obtuvo alrededor de 200 "likes" y "retweets", lo que probablemente contribuyó al estado de la cuenta.

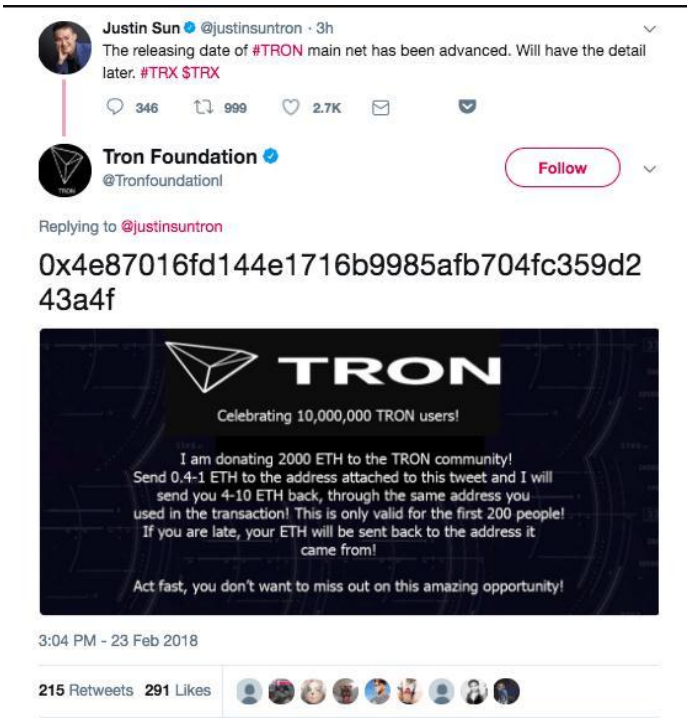

Imagen 7: Ejemplo de mensaje scam[14]

Twitter no explicó por qué, después de cambiar el nombre de usuario, las cuentas permanecen verificadas.

Solo un conjunto de precauciones, atención y conocimientos de los riesgos reales le permitirá evitar perder monedas debido a la implementación exitosa de esquemas de suplantación de identidad en la criptomoneda por parte de los estafadores. Debe tenerse en cuenta correctamente la demanda actual, la popularidad de las monedas digitales y comprender el enfoque obvio de la

guerra cibernética en las cuentas criptográficas de otras personas, las cuentas de las bolsas de valores y el almacenamiento de dinero virtual.

Las precauciones de phishing y Scam son rudimentarias y sencilas, por lo que siempre es fácil ejecutarlas. Cada usuario mediante la previsión y la inteligencia podrá proteger sus propios Bitcoins o Altcoins.

3.4 Vulnerabilidad de la cartera cerebral

Como regla general, la dirección de una cartera Bitcoin es una cadena de 26 a 35 caracteres que desempeña el papel de una identificación o, si lo desea, un nombre de usuario. El segundo número asociado con la cartera es una clave secreta que ya se ha utilizado por el usuario para completar transacciones. La pérdida de esta clave significa para el usuario la pérdida de acceso a la cartera. La mayoría de las veces, la clave secreta es una larga secuencia generada aleatoriamente. Recordar todo esto resulta francamente difícil. Aquí entonces entra en juego la técnica de la cartera cerebral (o “cartera en la cabeza”), diseñada para ayudar al usuario a recordar su clave secreta, así como a mejorar la seguridad: robar la llave almacenada en la cabeza de la víctima es más difícil de lo habitual.

La técnica de las carteras cerebrales ofrece crear y recordar una frase de contraseña significativa, que luego, utilizando el algoritmo hash SHA-256, debe convertirse en una secuencia, que se convertirá en la clave secreta. Sin embargo, este método de almacenamiento de información tampoco puede considerarse seguro. Los atacantes, estafadores adivinando las contraseñas, pueden verificar si coincide con algún alijo de alguna cartera cerebral mediante la búsqueda de la clave pública resultante en una cadena de bloques que registra todas las transacciones.

El documento de “Bitcoin Brain Drain Examining the Use and Abuse of Bitcoin Brain Wallets”[15] publicado en 2017, presentó el primer análisis a gran escala de la Cartera entre los usuarios de Bitcoin. Los investigadores replicaron un ataque de adivinación de contraseñas al verificar contraseñas incompatibles para descubrir aquellas que se han utilizado como una dirección de Bitcoin en la cartera cerebral.

Los investigadores crearon un gran grupo de contraseñas que se obtuvieron de diversas fuentes en línea. Consistieron en filtraciones de contraseñas anteriores, incluyendo Yahoo!, Rockyou, LinkedIn; palabras y listas de frases derivadas, incluyendo Wikiquote y Wikipedia en inglés; Y la información obtenida en los foros de la comunidad Bitcoin, principalmente Bitcointalk.org. En conjunto, al adivinar las ideas de Bitcoin, se usó un promedio de 300 mil millones de contraseñas.

Después de eso, la contraseña SHA256 se usó como clave privada, y la clave pública correspondiente se generó usando las aceleraciones en la biblioteca de curvas secp256k1. Luego, todas las direcciones únicas de Bitcoin se recuperaron a través del bloque analizador znort987. A continuación, las direcciones encontradas se agregaron al filtro “Bloom” para la búsqueda, y se creó una lista para detectar resultados falsos positivos. Todas las direcciones de Bitcoin que se crearon a partir de contraseñas crackeadas se compararon con el filtro de "bloom", y los resultados positivos se confirmaron en las listas ordenadas. Después de detectar todos los códigos de carteras de bitcoin utilizados, esta información se complementó con una solicitud de dirección utilizando la API blockchain.info para obtener marcas de tiempo precisas para todas las transacciones.

Los investigadores descubrieron 884 carteras diferentes con 845 contraseñas únicas, comenzando con el lanzamiento de Bitcoin hasta agosto de 2015. Todas estas carteras tenían 1806 BTC. A pesar de que la mayoría de ellas tenía poco dinero en efectivo, 10 carteras cerebrales tenían el 85% del total.

Curiosamente, 863 carteras de las 884 encontradas fueron destruidas por atacantes (97.6%), lo que refleja la vulnerabilidad de las carteras cerebrales. El 50% se fusionó en menos de 21 minutos y casi todas las carteras se drenaron en menos de 24 horas. Puesto que la dirección de la cartera está formulada a partir de una contraseña, un atacante puede piratearla y fusionar todas las monedas.

El 98% de las carteras cerebrales destrozadas se agotaron al menos una vez. Fueron los investigadores quienes descubrieron 1.895 eventos de drenaje separados que afectaron a 863 carteras; el 69% se fusionó solo una vez, el 19% se secó dos veces y el 1,9% se atacó al menos una docena de veces. Los robos se producen rápidamente debido al uso de bots por parte de los atacantes para monitorear las nuevas monedas colocadas en carteras previamente conocidas. Además, el atacante enviaría instantáneamente monedas a su dirección, encontrando una cartera cerebral vulnerable, a menudo con altas tarifas de minería, para que confirmen rápidamente la transacción.

Los usuarios suelen tener frases muy simples de contraseña, lo que se traducen en un efecto lamentable en el resultado. Peor aún, se estimó que al usar una cuenta regular de Amazon EC2 y su poder, los atacantes potenciales podrían pasar por 500.000 contraseñas de Bitcoin por segundo. Por lo tanto, la verificación de billones de contraseñas costará a los hackers solo 55,86. dólares. Esta es una forma increíblemente barata de hackear.

3.5 Malware

El nombre “malware” proviene de dos palabras: “malicious” y “software”. También hay sinónimos de malware - badware, computer contaminant, crimeware. En la vida cotidiana, todos los programas maliciosos a menudo se denominan virus informáticos, aunque esta sería una terminología incorrecta. Los programas maliciosos incluyen cualquier software que obtenga acceso no autorizado a equipos informáticos. La tarea de dichos productos es interrumpir la computadora, el robo de datos personales, etc. Las plagas se crean para dos propósitos principales. Uno de ellos es beneficiarse de la introducción en la computadora de la víctima. Por ejemplo, un atacante logra la capacidad de controlar una computadora, roba información secreta y realiza extorsiones. El segundo objetivo no se basa en la obtención beneficios materiales, sino más bien en su uso de manera recreativa. La utilización de malware puede ser una manifestación del deseo del autor que creó el programa, de confirmar sus habilidades, el vandalismo común o incluso una broma. Para los propietarios de la criptomoneda, los virus son una amenaza grave, ya que pueden llevar a la pérdida de acceso a la cartera, o a robo de parte o de todos los ahorros.

Como ejemplo “bastante elegante” - un trojan CryptoShuffler[16]. A diferencia de otros programas maliciosos, funciona de manera muy sencilla y, como escriben los analistas, "lo hace sin efectos especiales".

Al infectar otro sistema, CryptoShuffler se esfuerza por no llamar la atención. El malware se sienta en silencio en la memoria y observa todo lo que cae en el portapapeles de una máquina infectada. Tan pronto como CryptoShuffler se da cuenta de que la dirección de la cartera de

criptomoneda o algo similar aparece en el portapapeles, reemplaza cuidadosamente el número de la cartera con otro.

El reemplazo en sí se realiza utilizando conjunto de funciones de API *OpenClipboard\GetClipboardData\SetClipboardData*

La búsqueda del monedero correspondiente en la cadena obtenida del portapapeles se realiza mediante expresiones regulares. La mayoría de las carteras de criptomonedas populares tienen una constante fija al comienzo de una línea y una longitud concreta; no es difícil crear expresiones regulares para ellas. Por ejemplo, la dirección de una cartera bitcoin se reconoce fácilmente por el número “1” o “3” al comienzo de la línea.

Como resultado, la transferencia de la criptomoneda realmente desaparece, y es por la cantidad que ingresó el usuario: solo este dinero se envía a los atacantes que crearon CryptoShuffler.

Los investigadores de Kaspersky Lab escribieron[17] que el malware está igualmente interesado en Bitcoin, Ethereum, Zcash, Dash, Dogecoin y otras criptomonedas. Las más exitosas fueron la sustitución de las carteras de Bitcoin, los atacantes ganaron un poco más de 23 bitcoins, es decir, unos 80.000 euros a la tasa actual. En las carteras de otras criptomonedas pertenecientes a los creadores de CryptoShuffler, también se encontraron cantidades de varias decenas a varios miles de euros.

Otro grupo de malware, que puede ser una amenaza grande son keyloggers. Keylogger es un programa pequeño, cuyo propósito principal es el monitoreo oculto de las pulsaciones del teclado y el registro de estas pulsaciones. Esta definición en realidad no es del todo correcta, ya que los keyloggers pueden usarse como software, hardware y keyloggers acústicos. Junto con la fuga de llave privada de la cartera puede provocar perdida de todos los fondos almacenados en la cartera. Hay diferentes tipos de keyloggers:

- Hardware keylogger

  Los keyloggers de hardware son externos, se parecen a los equipos informáticos comunes e internos, que se instalan directamente en el teclado. El keylogger puede funcionar por un tiempo ilimitado, ya que no se necesita una fuente de alimentación adicional para su funcionamiento. Este tipo de keylogger de hardware puede almacenar hasta 20 millones de pulsaciones. Los keyloggers de hardware son mucho menos comunes que sus homólogos de software, ya que requieren acceso físico a la computadora de la víctima. Para proteger nuestros datos confidenciales, hay que evitar que terceros tengan acceso a nuestro ordenador.

- Registrador de teclas acústico

  Este tipo de keyloggers utilizan servicios secretos, espías y exploradores. Dichos keyloggers son dispositivos de hardware de un tamaño bastante grande que graban los sonidos creados por el usuario en la computadora cuando presionan las teclas del teclado, luego los analizan y los convierten a formato de texto.

- Software keylogger

Los keyloggers de software son los keyloggers más comunes en el mercado. Cuestan poco y son muy fáciles para encontrar y comprar en internet. Las aplicaciones ordinarias pueden interceptar las pulsaciones de teclas en el teclado y, a menudo, se utiliza para invocar funciones de aplicación desde otro programa mediante teclas de acceso rápido o, por ejemplo, para cambiar la disposición del tecladoa una incorrecta (como se implementó en Punto Switcher y Keyboard Ninja). Para instalar el keylogger y recibir informes, no se requiere acceso físico a la computadora. Algunos keyloggers están en la base de datos de firmas del antivirus y son identificados por ellos como malware, que puede ser eliminado durante el proceso de trabajo.

3.6 Amenazas de red

El objeivo de estos ataques en un entorno de registro distribuido no se limita solo al robo directo de fondos. También, el daño indirecto se debe a la limitación del campo de acción para los usuarios, que impide el acceso a los servicios, a la realización de operaciones.

3.6.1 DDoS

Un conocido ataque en Internet, denominado DoS (Denegación de servicio), en un sentido práctico, DDoS (Denegación de servicio distribuido) se organiza para interrumpir el intercambio de información al enviar solicitudes inútiles al nodo de destino para agotar los recursos para proporcionar acceso a los usuarios.

- Se lleva a cabo de acuerdo con esquemas conocidos:
- Ataque por desbordamiento de un nodo con paquetes.
- Implementar y ejecutar código inútil en un servidor que consume recursos informáticos (SYN flood).
- Bloqueo de espacio libre en el servidor con archivos de registro sin sentido.
- Agotamiento de recursos de cola o portapapeles.

Hoy en día, rara vez se lleva a cabo desde una estación de trabajo, más a menudo se usa una red de bots desde muchas computadoras infectadas que atacan simultáneamente al host objetivo.

En las redes P2P, los nodos individuales están deshabilitados, lo que resulta ser cortado y, en consecuencia, no acepta ni valida las transacciones. Esto interrumpe el correcto funcionamiento de la red, pero por lo tanto es difícil "colocar" una estructura de cadena de bloques avanzada. Otro objetivo de este ataque son los servicios de infraestructura de soluciones blockchain: intercambios de criptomonedas, carteras frías y calientes para almacenar criptomonedas. Es fácil imaginar cómo usar un ataque DDoS puede "desactivar" un solo recurso, afectando así la reputación y causando pérdidas materiales debido a problemas de acceso.

3.6.2 Ataque de Sybil

Otra base para la exposición de la red es el Ataque de Sybil. En comparación con el caso anterior, este tipo de ataque es más típico de las redes P2P. Su nombre se debe al nombre del personaje del

protagonista del mismo libro de 1973, que, al ser una entidad única, puede aparecer en diferentes caras simultáneamente. El atacante actúa de manera similar: se crean varios nodos separados, hasta decenas de miles. Parecen desconectados, pero resuelven un problema común.

En un determinado momento, puede surgir una situación en la que la información que recibe un usuario en particular pertenece a la misma fuente. Realizar un ataque de Sybil le da a un atacante capacidades avanzadas de administración de red y en algún momento otros usuarios solo podrán conectarse a los bloques creados para el fraude. Esto se implementa de la siguiente manera:

- El atacante bloquea las transacciones de otros usuarios al desconectarte de la red pública.
- El atacante te conecta solo a los bloques que crea en una red separada. Como resultado, aparecerán transacciones que reenviarán dinero (doble gasto).
- El atacante puede ver todas sus transacciones con la ayuda de programas especiales.

Con respecto a la cadena de bloques de Bitcoin, se cree que el consenso de Nakamoto no deja espacio para estos ataques, ya que requiere poder computacional y evidencia de trabajo para realizar cambios en el registro. Las cuentas se crean, pero aún tienen que ser compatibles con la potencia de cálculo. Sin embargo, con respecto a las redes de blockchain de tamaño más pequeño y funcionalidad diferente, este tipo de ataque conlleva una amenaza.

3.6.3 Ataque de Eclipse

Externamente, Eclipse es similar a Sybil Attack, pero internamente se diferencia de esta. El participante está "eclipsado" en la red real, cayendo en una estructura paralela formada por intrusos. Por lo tanto, Sybil se enfoca en la red en general, mientras que Eclipse se enfoca en usuarios individuales.

Las siguientes son acciones fraudulentas:

- Conectar el poder de cómputo de otra persona a sus recursos usando código malicioso.
- Información errónea sobre el estado y envío de transacciones.

Lo más difícil es redirigir al usuario a una red comprometida. Esto se logra mediante un ataque DDoS dirigido o cambiando la hora del sistema en la computadora de la víctima. Por ejemplo, la cadena de bloques Ethereum rechaza automáticamente los paquetes que llegan con un retraso de 20 segundos o más, lo que deja a la víctima fuera de la red correcta.

Las cadenas de bloques de criptomonedas están parcialmente en riesgo de los ataques de Eclipse que se implementan a través de vulnerabilidades. Los desarrolladores de Ethereum prueban constantemente la plataforma para determinar la resistencia a Eclipse, y periódicamente hay informes sobre la detección de amenazas potenciales.

3.6.4 Ataque de enrutamiento

El ataque a los protocolos de enrutamiento también apareció hace mucho tiempo, tomando su lugar como una amenaza en la red peer-to-peer de blockchain. El propósito del ataque es

comprometer a un miembro o grupo de la red al afectar los protocolos de conexión a Internet y los paquetes transmitidos. Para ello, utiliza:

- Falta de infraestructura necesaria de un proveedor separado.
- La inseguridad de los nodos de enrutamiento, con el resultado de que el atacante obtiene el control.
- Enrutamiento dinámico de paquetes sin algoritmos especiales.
- Vulnerabilidad de los canales para escuchar y cambiar la información transmitida.
- El escenario del comportamiento del atacante se ve así:
- Reenvío de paquetes a través de un nodo dado ("man in the middle").
- Paquetes de escucha (ataque pasivo).
- Sustitución de rutas por phishing o introducción de código malicioso.
- Desbordamiento de la tabla de enrutamiento por lo que la creación de nuevas rutas sería imposible.

Este tipo de ataque está dirigido a un usuario específico, una amenaza similar para toda la red sigue siendo el argumento de una película de ciencia ficción.

3.6.5 Ataque de 51%

Control sobre la mayor parte de la potencia de cómputo de la cadena de bloques, con la que puede confirmar de forma independiente los nuevos bloques, las transacciones, dejando que el resto de los participantes de la red trabajen sin beneficios, en primer lugar, amenaza a la criptomoneda con una ligera tasa de hash. Estos ataques ocurren regularmente. Como regla general, los activos nuevos e inmaduros que aún no se han hecho populares.

Estos incluyen tokens de ERC-20 Krypton y Shift. Un caso similar ocurrió con la criptomoneda Verge, cuando, gracias al control de la potencia y el error en el código, los atacantes lograron establecer un nuevo tiempo de generación para los bloques (1 segundo en lugar de 30), y en 3 horas de ataque generon el 99% de los nuevos bloques y produjeron al menos 250.000 XVG.

El ataque del 51% en Ethereum Classic, que tuvo lugar a principios de enero de 2019, eclipsó este caso: por primera vez, la reorganización fraudulenta de la cadena de bloques recibió una criptomoneda del TOP-20, y la cantidad de gastos dobles como resultado del ataque fue de 1,1 millones de dólares. Sorprendentemente, durante el ataque, la tasa de ETH se mantuvo casi sin cambios.

El 51% de ataque le da al atacante:

- Aproveche para confirmar transacciones y determine, a su discreción, qué transacciones incluir en bloques.
- Rollback" de bloques previamente confirmados por reorganización.
- Realizando doble gasto con la única cancelación de las transferencias ya confirmadas.
- Monopolizando el premio minero.

Es importante recordar que, por sí mismo, poseer el 51% de la potencia de cálculo no significa un ataque. Se detecta únicamente sobre la base de fraude. La minería de PoW (Proof of Work) es más vulnerable: a menudo no es rentable para los mineros de PoS (Proof of Stake) manipular transacciones y realizar otras acciones destructivas.

3.7 “Amenaza” cuántica

El análisis criptográfico mediante una computadora cuántica que, según algunos investigadores, puede descifrar una firma digital utilizando una clave abierta (pública) tanto en SHA-256 como en otros algoritmos criptográficos comunes basados en curvas elípticas y la complejidad del rendimiento inverso de la función de logaritmo discreto excita de la sociedad.

Escriben que "varias computadoras cuánticas de tamaño mediano piratearán toda la red de Bitcoin en unas pocas horas" (algoritmo de Shor), e incluso se asigna menos tiempo a Ethereum.

No está claro qué considerar como una "computadora cuántica de potencia promedio". Según declaraciones oficiales, la NASA tiene una muestra de 2000 qubit, adecuada "solo para cálculos con un enfoque limitado". Google tiene un modelo de 72 qubits, y el IBM informó sobre el lanzamiento de la computadora cuántica con una capacidad de 50 qubits[18].

Se han realizado intentos para crear un aparato de este tipo desde la década de 1980, y es obvio que su implementación en la práctica está plagada de grandes dificultades. Una de ellas es que la "superposición cuántica", en la que se depositan grandes esperanzas, existe solo “en el papel”: cuando intentas leer información, inevitablemente se convierte en código binario.

Parece que si dicho enfoque se implementa en un modelo realmente funcional, no ocurrirá pronto, y se verá como muestras modernas de computadoras cuánticas, como la computadora de Alan Turing creada durante la Segunda Guerra Mundial para descifrar los códigos alemanes. “Enigma” es similar a las computadoras personales modernas. Eso es un poco menos que nada.

Y, si asumimos que un modelo informático cuántico aparecerá en un futuro cercano, sería en una situación bastante optimista:

Los algoritmos de criptografía post-cuántica existen y se están desarrollando activamente, haciendo inútil el uso de una computadora cuántica para el criptoanálisis activo ("códigos de corrección de errores", "celosías", sistemas cuadráticos multidimensionales, isogenia supersingular).

Hackear una firma digital, por ejemplo, en una computadora cuántica SHA-256, requiere el conocimiento de la clave pública, que se genera directamente durante la transacción. En consecuencia, la ventana de tiempo es de 10 a 20 minutos (en el caso de Bitcoin). Desde el momento de recibir la clave pública hasta la 1ª confirmación de la transferencia. Las carteras inactivas no pueden romperse porque no generan claves públicas.

Lo que importa es el ancho de banda de la red y las restricciones de tráfico, así como el seguimiento del estado de la cadena de bloques por parte de muchos jugadores. Solo el Chainalysis puede detectar cualquier actividad inusual. Pero todavía hay Diar y muchas otras empresas.

Se puede añadir aquí la falta de software para computadoras cuánticas, así como el hecho de que los desarrollos no están acompañados por una abundancia de información, y solo podemos adivinar las características reales (así como el grado de utilidad).

En general, SHA-256 es un algoritmo confiable. La seguridad de almacenamiento de la criptomoneda y las operaciones con ellos se está acercando gradualmente al 100%, sujeto a la

exclusión del factor humano. La mayoría de los tipos de ataques son amenazas potenciales. El desarrollo de otros es detectado y bloqueado por la comunidad (como sucedió con Ethereum Classic, cuando se impusieron restricciones adicionales después del descubrimiento de un doble desperdicio).

La cooperación de los desarrolladores, la comunidad, los especialistas en seguridad, junto con la infraestructura de los proyectos de blockchain que se desarrollan con BUIDL todos los días no dejarán espacio para otros problemas importantes, como garantizar la fiabilidad y la seguridad del entorno para los usuarios.

4.Amenaza: robo de los recursos

4.1 Cryptojacking

Desde septiembre de 2017, se ha observado el fenómeno llamado cryptojacking. Cryptojacking es el uso de recursos de un dispositivo comprometido para generar criptomoneda sin el conocimiento de su propietario. La minería se puede realizar con la ayuda de un programa malicioso instalado en una computadora y sin el método de archivo[8].

La pregunta controvertida es si las Herramientas de Cryptojacking se consideran maliciosas. No dañan su computadora y depende del tipo puede funcionar sin nada almacenado en su disco duro, por lo que en este sentido no pueden considerarse maliciosos. Sin embargo, pueden denominarse "Greyware", lo que significa que están identificados como software molesto, especialmente cuando están configurados para consumir toda la potencia de su procesador. Por otro lado, aumentan el consumo de energía de la computadora que está siendo operada, lo que conlleva pérdidas financieras para pagar las facturas. Entonces, en los EE.UU., hubo un precedente con una declaración de TidBit que afirma que usar el poder de un procesador central sin consentimiento se considera acceso ilegal a la computadora de esta persona: esto significa que los culpables pueden sufrir los mismos cargos y multas que cualquier otro pirata informático.

4.2 Cryptojacking en Internet

Sin embargo, las mismas tecnologías se pueden utilizar de una manera completamente legal: como la monetización de los servicios de sitios de Internet. No es una gran noticia que el soporte y el desarrollo de sitios a veces requiere un patrocinio bastante grande. Y si el sitio no es un subproducto de las actividades de la compañía, entonces debería, como mínimo, recuperar los costes. Actualmente, este problema a menudo se resuelve colocando publicidad de recursos de terceros pagada por estos. El abuso de la misma a menudo conduce a saturar la página con banners molestos y obliga al usuario a aislar información útil entre ellos. Esto llevó al hecho de que la mayoría de los usuarios actualmente usan activamente los complementos de navegadores que bloquean los anuncios. Eso, a su vez, conduce a una disminución en las ganancias obtenidas por los propietarios de sitios por la publicidad. Como alternativa a los anuncios molestos, se pueden usar las tecnologías utilizadas por los piratas informáticos en uno de los tipos de cryptojacking: minería en el navegador. En este caso, el visitante, mientras está en el sitio, "pagará" los servicios proporcionados por este, parte de su tiempo de procesador, extrayendo la criptomoneda para él. A su vez, esto permitirá a los propietarios de sitios rechazar la publicidad, lo que debería mejorar su usabilidad. En este caso, la regla del buen tono es la notificación a los usuarios sobre el uso de esta forma de monetización del sitio.

La historia de la cryptojacking en los sitios web comenzó con el hecho de que la compañía Coinhive lanzó una nueva tecnología para la extracción de Monero en un navegador web. El script está escrito en JavaScript (JS), por lo que es fácil de incrustar en cualquier página web. Cabe

[8] Definicion de KasperskyLab https://encyclopedia.kaspersky.com/glossary/cryptojacking/

señalar que esta tecnología fue demostrada en 2013 por un grupo de ex alumnos del MIT que crearon una empresa llamada TidBit para distribuir BitCoin Miner en un navegador web.

Esto llevó a algunos investigadores a preguntar por qué usan Monero. De acuerdo con las Preguntas Frecuentes de Coinhive, eligieron Monero (XMR), porque el algoritmo utilizado para calcular los hash es pesado, pero más adecuado para la CPU, especialmente cuando se compara con otras criptomonedas, donde el uso de procesadores de gráficos trae una diferencia significativa. Señalaron que la ventaja de usar una GPU para Monero es aproximadamente 2x, donde para BitCoin/Ethereum es 10.000x. Además, Monero tiene otra ventaja para los piratas informáticos, ya que no permite rastrear carteras (lo cual es posible en Bitcoin). Esto significa que Monero también les da una capa extra de anonimato.

La desventaja de usar JavaScript en un navegador web, incluso usando las últimas tecnologías web, como WebAssembly, es que el rendimiento es un 35% más lento que el de su propia aplicación de minero.

Por estado del año 2018 Coinhive producia Monero por 250.000$ al mes. Los operadores de Coinhive conservan el 30% de su producción y el resto lo reciben los clientes del servicio. Aunque hay otros servicios similares, además de Coinhive, se mantiene en la cima con un gran margen.

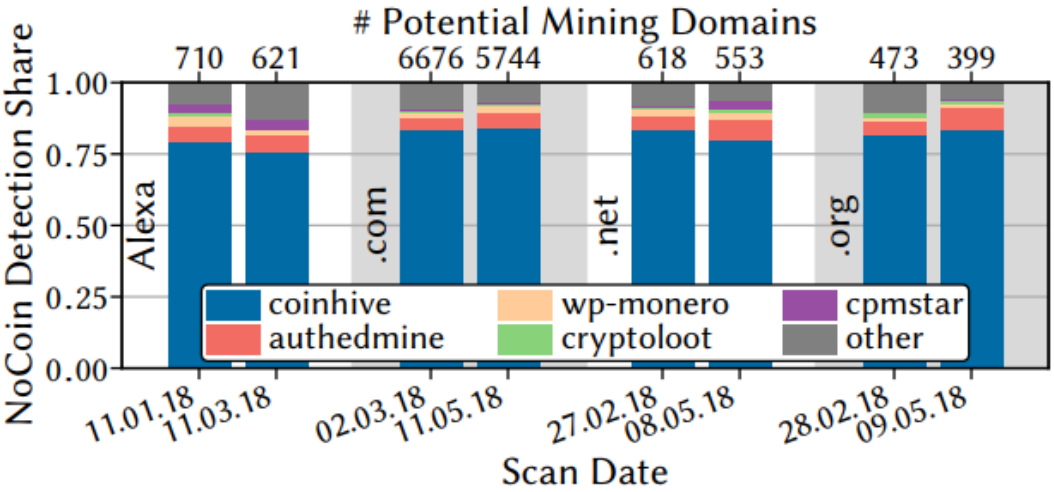

Imagen 8: Mineros detectados por No Coin en los dominios Alexa Top 1 M y .com / .net / .org [19]

Otro caso más curioso de esta tegnologia fue anunciado por los analistas de Votiro y los expertos en el portal de Bleeping Computer[20]. Ellos advirtieron que los mineros ocultos pueden trabajar no solo en sitios web y a través de un navegador. El código malicioso de JavaScript también se puede ejecutar dentro de documentos de Word, ya que más recientemente, Microsoft Word permite a los usuarios incrustar videos directamente en archivos de documentos. Los expertos de la compañía israelí Votiro dicen que, junto con el video del iframe, puede integrar un minero oculto en el documento, que "minará" Monero a la espalda del usuario.

De tal forma, se puede incrustar un iframe en un documento desde prácticamente cualquier fuente, es decir, no hay una lista blanca de servicios o dominios de "confianza". Peor aún, la ventana (popup) que aparece de esta manera es una versión truncada de Internet Explorer.

Como resultado, un atacante puede colocar un video en su dominio, asegurándose de que, junto con un videoclip, se incruste en el documento un script de minería de cifrado. Por lo tanto, cuando la víctima abre el documento malicioso de Word y lanza el video incorporado, IE también lanzará el minero de criptomoneda Monero.

Afortunadamente, es poco probable que este tipo de cryptojacking sea beneficioso para los atacantes. El hecho es que la minería oculta produce beneficios tangibles solo si los usuarios pasan mucho tiempo en el sitio infectado por el minero. Es por eso que los scripts de cryptojacking se pueden encontrar con mayor frecuencia en sitios de noticias, pornografía, recursos de transmisión "pirateados", etc. Mientras que, en este caso, el tiempo de extracción es limitado, y primero se debe persuadir al usuario para que abra el documento de Word y comience el video.

Sin embargo, el problema descubierto puede usarse no solo para la minería oculta. Los atacantes pueden usar contenido incrustado para agregar páginas de phishing directamente a archivos de Word, por ejemplo, al hacer que el video esté disponible solo para usuarios autorizados (es decir, obligar a la víctima a ingresar las credenciales de una cuenta).

La compañía de Microsoft, se negó a reconocer esta funcionalidad como problemática. Según las pruebas realizadas por expertos de Bleeping Computer, después de lanzar el video integrado en Word, muchas soluciones antivirus detectan el script de minería y bloquean su trabajo. Entonces, si los delincuentes comienzan a explotar esta funcionalidad para los ataques, al menos algunos de los usuarios estarán protegidos.

Pero esta etapa de la vida del cryptojacking ya se está convirtiendo en historia. Coinhive anunció que se está cerrando. Las razones de esta decisión fueron una caída drástica del valor de ciptomoneda, su hardfork y actualización del algoritmo de minería. Todo esto llevo al proyecto al ser un servicio no económicamente viable. El cierre no tiene efecto inmediato, pero tampoco está demasiado lejos. La actualización del algoritmo y la bifurcación dura vencen el 9 de marzo, y Coinhive cerrará sus puertas el día anterior.

Coinhive cayó en desgracia cuando se encontró su código de minería en el fondo de sitios web que no habían informado a los visitantes de su presencia. Esto es algo que muy probablemente contribuyó a la caída del valor. Otra razón de caída puede ser el comienzo de bloqueo activo del proceso de mineo con los antivirus. Al comentar sobre los cryptominers, Luis Corrons de Avast security dijo[21]:

> *Si bien existe la criptominación no maliciosa, la verdad es que la gran mayoría se utiliza para drenar los recursos de las computadoras de los usuarios sin su conocimiento. El año pasado en Avast, comenzaron a detectar y bloquear todo el proceso de cifrado. Si una persona realmente quiere explotar criptomonedas, él o ella tiene una opción para permitirlo. Pero por defecto lo bloquean todo.*

Según los expertos de la Universidad Técnica de Rhine-Westphalian, solo 10 usuarios son responsables de publicar el 85% de los enlaces relacionados con el servicio de minería Coinhive[22]. Recopilaron estadísticas sobre los millones de los recursos más populares de la versión de Alexa y los dominios .org para descubrir todos los scripts de Coinhive y asociarlos a cuentas específicas. El hecho es que un token especial debe estar incrustado en el código del script, debido a que se calculan los pagos. Al final resultó que, los distribuidores más activos de

Coinhive son solo 10 clientes del servicio que reciben el mayor beneficio de sus actividades. Un tercio de todos los enlaces son creados por el mismo usuario, y aproximadamente el 85% de todos los enlaces son creados por solo 10 personas.

4.3 Cryptojacking con uso software con un miner implementado.

Ahora, los desarrolladores de aplicaciones móviles están probando una forma similar en la sección anterior para obtener ingresos adicionales. En una serie de juegos para teléfonos inteligentes, los usuarios pueden recibir bonos utilizando la moneda del juego. Los desarrolladores de algunos juegos han agregado una nueva forma de obtener dicha moneda por parte del usuario: la minería. Tarde o temprano, el desarrollador, especialmente indie, tendrá que monetizar las aplicaciones. Lo más razonable es vender el juego, el contenido, etc. El segundo punto es, por supuesto, la publicidad. Muchos usuarios están muy descontentos con la publicidad, pero en aplicaciones y juegos antiguos que están al borde de la rentabilidad, no se puede hacer nada. Ya sea un montón de anuncios, o abandonar completamente y no apoyar. Hay varios métodos para implementar esta idea. Algunas aplicaciones extraen monedas de forma secreta durante el uso, como la aplicación PlacarTV para transmitir videos de fútbol que se han descargado más de 100.000 veces. El minero Coinhive se construyó en él, el cual, mientras navegaba, extraía la criptomoneda Monero en busca de estafadores. Es bastante difícil darse cuenta: en primer lugar, el usuario simplemente no está al día durante el partido, en segundo lugar, el video también calienta el teléfono y descarga la batería, como el minero. Algunas aplicaciones también pueden realizar un seguimiento de la temperatura y el nivel de carga del teléfono. Y en base a los datos obtenidos, pueden pausar la minería a tiempo, no permitiendo que el dispositivo se sobrecalentara o se descargue, y que su propietario sea sospechoso. Otros notifican al usuario que obtendrán una criptomoneda, ofreciendo varias bonificaciones. Por ejemplo, moneda de juego interna en juegos. El módulo integrado en el juego comienza a tener criptomoneda al comienzo del juego. Las monedas, respectivamente, obtienen al desarrollador, y el usuario agregó puntos de bonificación o dinero en el juego. Otros usan otro método: por la noche, cuando el usuario carga el teléfono, la aplicación espera hasta que el teléfono esté completamente cargado y el minero comience a funcionar. Gana poco, pero en general, si hay muchos clientes, resulta ganar de un dólar a tres por cada mil usuarios. El jugador recibe a cambio bonos de juego (propinas, monedas, etc.) dependiendo de cuánto se utilizó el teléfono. Como resultado, tenemos ventajas: el jugador recibe bonificaciones sin gastar nada (solo electricidad por la noche), el desarrollador recibe el dinero. El desarrollador recibe ingresos incluso cuando el usuario no está jugando. Algunos jugadores usan el segundo teléfono solo para ganar monedas de juego, que permanecen conectadas a la carga constantemente.

Según el representante de "Kaspersky Lab", estas herramientas no pueden llamarse maliciosas, ya que se advierte al usuario sobre la minería y comienza el juego por su propia cuenta. Sin embargo, el programa de minería de criptomonedas utiliza casi la totalidad de los recursos disponibles del dispositivo móvil en el que se está ejecutando el minero.

Según Trend Micro, los criptógrafos móviles incrustados en dispositivos móviles difícilmente pueden llamarse maliciosos. Y los primeros casos de minería de juegos y aplicaciones de criptomoneda para teléfonos inteligentes se dieron a conocer hace varios años. Ahora estamos hablando del hecho de que los casos de adición de módulos de minería por parte de los desarrolladores de software se han vuelto más frecuentes. Según los expertos de Trend Micro, una cantidad significativa de producción de cryptomonet de cualquier tipo de dispositivo móvil

no puede hablar. Sin embargo, la duración de la batería de la batería del teléfono inteligente se reduce significativamente debido al hecho de que los recursos del teléfono se utilizan para la minería.

En las tiendas de aplicaciones oficiales, los programas que te permiten extraer criptomonedas fueron prohibidos en el verano de 2018. Del mismo modo, la situación con el software, que contiene módulos criptográficos que no son la parte principal de dicha aplicación. Ahora, una serie de catálogos de aplicaciones han introducido dicha prohibición, pero aquellos que quieren ganar una pequeña cripta en los teléfonos inteligentes de los usuarios no han disminuido. Es cierto que los mineros "limpios" se han vuelto raros, en lugar de ellos comienzan a aparecer en aplicaciones de entretenimiento de manera oculta.

La mayoría de estos programas se descargan en Google Play, por lo que los usuarios del sistema operativo Android están en riesgo. El hecho es que si un usuario permite descargar aplicaciones no verificadas, entonces los desarrolladores de programas de minería tendrán una buena oportunidad de convencer de alguna manera al propietario del teléfono inteligente para que descargue un juego u otro programa con un minero.

Para evitar que el siguiente minero, enmascarado como una aplicación fiable, ingrese a su dispositivo móvil, debe utilizar los métodos habituales. Durante la instalación, vale la pena ver cuántas veces se ha descargado el programa, verificar los permisos solicitados por las aplicaciones y lea los comentarios de otros usuarios que ya han probado el programa en funcionamiento.

4.4 Cryptojacking con malware

Otro tipo de cryptojacking, que ya no tiene aplicación positiva, como lo de web, es el cryptojacking en base de malware. Una computadora o dispositivo móvil infectado comienza a ralentizarse terriblemente y deja de hacer frente normalmente incluso con tareas simples, sin mencionar los programas que utilizan muchos recursos. Y el problema ya no se soluciona con solo cerrar la página web. La computadora es lenta debido a la gran carga que el minero tiene en el procesador o en la tarjeta de video. Bajo la alta presión de un programa malicioso, el equipo se sobrecalienta y produce sus recursos más rápido. En general, con el tiempo, debido a una explotación tan despiadada, un servidor, una computadora de escritorio o una computadora portátil infectados fallarán prematuramente. Una computadora portátil con un sistema de enfriamiento débil será vulnerable, su potencia no será suficiente para enfriar el calor de una tarjeta de video o procesador sobrecargados.

En la mayoría de los casos, el minero llega a la computadora con la ayuda de un programa malicioso especialmente creado, el llamado cuentagotas, cuya función principal es instalar secretamente otro software. Estos programas generalmente se disfrazan como versiones pirateadas de productos con licencia o como generadores de claves de activación para ellos, todo lo que los usuarios buscan. Por ejemplo, en los sitios de intercambio de archivos y descargan deliberadamente. Solo a veces lo que descargaron no es exactamente lo que querían descargar. Otra forma de instalar mineros es mediante los instaladores de adware que se distribuyen a través de la ingeniería social. Pero hay opciones más sofisticadas, como la propagación de vulnerabilidades como EternalBlue. En este caso, como la víctima se elige un servidor, lo que es especialmente beneficioso para los atacantes debido a su mayor rendimiento.

Después de ejecutar el archivo descargado en la computadora de la víctima, se coloca el instalador, y él ya descarga un minero y una utilidad especial en el disco, enmascarándolo en el sistema. Además, junto con el programa se pueden suministrar servicios que garantizan su inicio automático y personalizan su trabajo.

Por ejemplo, dichos servicios pueden suspender el trabajo del minero, si el usuario inicia algún juego popular: dado que el minero usa la potencia de la tarjeta de video, el juego puede comenzar a disminuir y el usuario puede sospechar algo.

Además, dichos servicios pueden intentar desactivar el antivirus, suspender el trabajo del minero si el programa se está ejecutando para monitorear la actividad del sistema o los procesos en ejecución, y restaurar el minero en caso de que el usuario lo elimine.

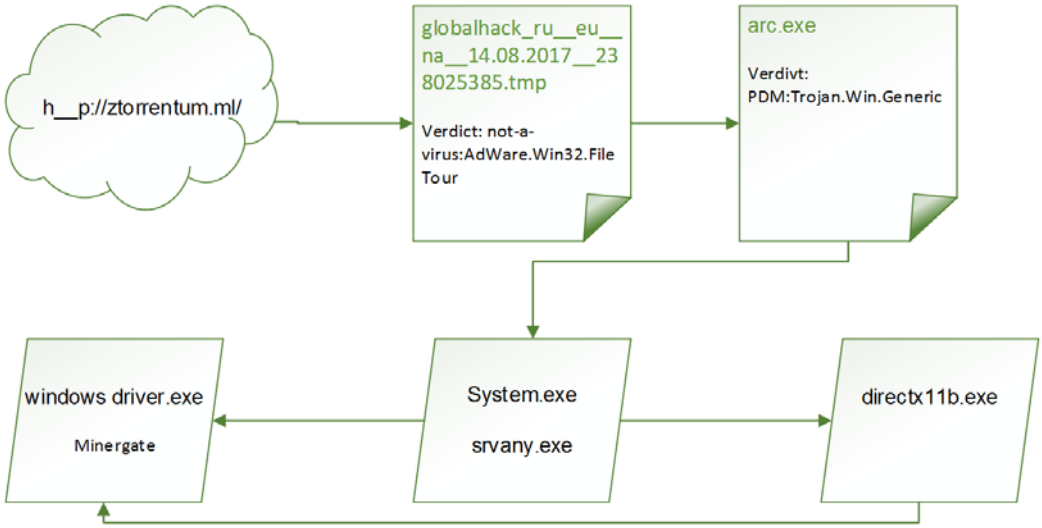

Imagen 9: Proceso de instalacion de un minero malware[9]

4.4.1 Proceso de infección con un miner malware

Proceso de infección con un miner:

1. El usuario descarga el instalador del servicio de alojamiento de archivos bajo la apariencia de software o claves libres para activar productos con licencia;
2. Después de ejecutar el instalador, carga el gotero del minero en la máquina de la víctima (exe);
3. Dropper escribe en el disco Minergate y en la utilidad "srvany.exe", mediante el cual el minero se ejecuta en el inicio del sistema como un servicio llamado "windows driver.exe";
4. Dropper crea un servicio adicional (exe), que garantiza el funcionamiento continuo de Minergate y, en caso de eliminación, lo restaura en el disco;

[9] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/08/07171315/170829_miners-rise-4.png

Dichos programas se distribuyen entre los atacantes como un servicio; por ejemplo, en el mensajero de Telegram, en los canales dedicados a ganar dinero en Internet, puede encontrar anuncios que ofrecen una versión de prueba de dicho paquete para distribuir el minero oculto.

Los objetivos más atractivos para los hackers son los servidores (aún más, si son servidores específicos para el mineo de criptomoneda). Esto se debe a la mayor potencia de cómputo, el ancho de banda de las interfaces de red, el acceso a la infraestructura de información de la compañía y la posible fuga de datos sensibles. También, esto explica su valor más alto para una botnet. Debido a la creciente complejidad del algoritmo de búsqueda hash, la minería de bitcoins y las criptomonedas más conocidas comenzaron a requerir demasiados recursos. Y aunque ya no es posible extraer una moneda en las computadoras del hogar, tal botnet distribuida puede ser muy rentable para sus propietarios.

A finales de enero de 2018, Proofpoint, una empresa de ciberseguridad, anunció[23] el descubrimiento de un nuevo botnet Snominru monero que infectó a más de medio millón de computadoras utilizando el exploit EternalBlue. Anteriormente, la misma vulnerabilidad, que se atribuye a la Agencia de Seguridad Nacional de EE.UU., fue explotada por el cifrado sensacional WannaCry.

La botnet, Smominru (o Ismo), que utiliza el exploit EternalBlue (CVE-2017-0144) y EsteemAudit (CVE-2017-0176) en los sistemas operativos Windows para extraer la criptomoneda de Monero. El código de vulnerabilidad y código ejecutable fue publicado por el grupo de hackers The Shadow Brokers el 14 de abril de 2017.

Para el período comprendido entre mayo de 2017 y enero de 2018, Smominru infectó más de 526 mil computadoras, principalmente servidores que usan versiones de Windows sin las actualizaciones necesarias. Se observa que la mayoría de los sistemas infectados se encuentran en Rusia, India y Taiwán. Usando los recursos de los sistemas infectados, una botnet extrae aproximadamente 24 monedas por día (8500$ en el momento actual). En total, recibieron 8.900 monedas, alrededor de 3,6$ millones según valor de la moneda en ese momento.

También vale la pena señalar que la infraestructura de Smominru se basa en el servicio de protección DDoS de SharkTech, cuyos creadores fueron notificados de uso indebido, pero aparentemente ignoraron esta información.

Como la salida para poder darse cuenta de lo que está sucediendo: varias veces los expertos de empresas dedicadas a ciberseguridad descubrían las redes de bots que constan de varios miles de computadoras en las que se instaló en secreto el minero. Con la mayoría de ellos, los atacantes no extraen el popular Bitcoin, sino principalmente aquellas criptomonedas que le permiten ocultar transacciones y quién es el dueño de la cartera. Por ejemplo, estos son Monero (XMR) y Zcash (ZEC). Según las estimaciones más modestas, la red de bots de minería puede traer a sus propietarios mas de 300.000$ por mes.

La cantidad de estos casos en 2018 aumentó 4 veces, aproximadamente, 13 millones de dispositivos se infectaron con virus. Al principio, el criptodopaje se usaba para la minería y, con el tiempo, también se utilizaba para llevar a cabo ataques DDoS y otros delitos informáticos. Las principales víctimas de la cryptojacking son las empresas. Según los datos de Carbon Black[24], los ataques a empresas representaron una quinta parte de todos los ataques de piratas informáticos.

Los atacantes aprovechan cada oportunidad para obtener ganancias por medios ilegales, y las formas de hacerlo están en constante evolución. El desarrollo del mercado de la criptomoneda también ha contribuido al rápido crecimiento en el número de casos en que los mineros se instalan sin el conocimiento de los usuarios. Este suceso puede explicarse por el hecho de que en la etapa del "nacimiento" de la criptomoneda, minear (y por lo tanto ganar dinero) es mucho más fácil. Los delincuentes están buscando formas de obtener el poder del equipo de otra persona y, a menudo, sus víctimas son usuarios normales.

4.5 Amenazas para los mineros.

Aún más vulnerables son las personas involucradas en el proceso de minería de criptomonedas. No solo pueden perder dinero en caso de fuga de sus datos o robo de la cartera, también los atacantes tienen mucho interés en dispositivos de minería. Esto explica la eficiencia brutal de las computadoras especificas en el proceso de minería.

Hace unos años, era posible extraer la criptomoneda en una computadora normal. Tales ganancias llegaron a probarse en muchos empresarios en línea, y pronto los nuevos mineros literalmente rellenaron la web global. Pero con el tiempo, la complejidad de la minería ha aumentado. Además, el aumento de la competencia en el campo de la criptografía contribuyó a la aparición de equipos especiales para la extracción de monedas virtuales. En principio, incluso hoy en día es posible realizar operaciones de minería en una computadora doméstica, siempre que tenga una potente tarjeta de video GPU, y preferiblemente una granja de 4 a 8 tarjetas de video. Pero, sin embargo, la efectividad de tal trabajo no puede compararse con la minería, llevada a cabo con el uso de ASIC. La principal diferencia es la velocidad de resolución del hash. Y si el minero ASIC le da la oportunidad de obtener ingresos de miles de dólares, entonces en una PC normal, las ganancias se limitan a cien dólares al mes. La única razón por la que las granjas de las tarjetas de video siguen siendo relevantes es porque para muchos algoritmos no se desarrollan ASIC, su uso excluye el algoritmo de minar estas monedas. Por lo tanto, para la extracción de altcoins (cualquier criptomoneda excepto Bitcoin), las tarjetas de video y las granjas de GPU siguen siendo relevantes.

Los mineros de ASIC son el único equipo de minería Bitcoin rentable. La minería de BTC en el GPU no lo es.

ASIC (aplicación específica integrada) es un circuito integrado especializado para resolver un problema específico. A diferencia de los circuitos integrados de propósito general, los circuitos integrados especializados se utilizan en un dispositivo específico y realizan funciones estrictamente limitadas que son características solo de este dispositivo; como resultado, las funciones se realizan más rápido y, en última instancia, más baratas. ASIC Miner es una pequeña instalación utilizada para una sola tarea: la minería de criptomonedas. ASIC no resuelve ningún otro problema. Pero lo hace muy bien. Algunos modelos de ASIC-miners pueden calcular hasta 14 terahashes por segundo.

Así, si un hacker toma el control sobre los dispositivos dedicados a minear de una persona, o empresa, podría reconfigurar y aprovecharlos para ganar beneficio. Además, por su uso específico, la cantidad de personas y empresas, que los usan, no es tan grande, eso afecta a nivel de desarrollo y madurez de tecnologías, que provoca más agujeros en su defensa.

Además, muchos usuarios no son lo suficientemente serios en lo que respecta a la configuración de sus dispositivos. Lo absurdo se debe al hecho de que, en agosto de 2017, el conocido

especialista en seguridad de la información y director de la organización de la Fundación GDI, Victor Gevers, descubrió en la red 2893 dispositivos de minería de bitcoin que estaban disponibles para todos a través de Telnet. No se requería contraseña. Gevers escribio que todos los ASIC trabajaron con un grupo y, al parecer, pertenecían a un propietario de la empresa que, a juzgar por las direcciones IP, se encontraba de alguna manera conectado con el gobierno chino. El especialista sugirió que había encontrado todo un "parque" de dispositivos ZeusMiner THUNDER X3.

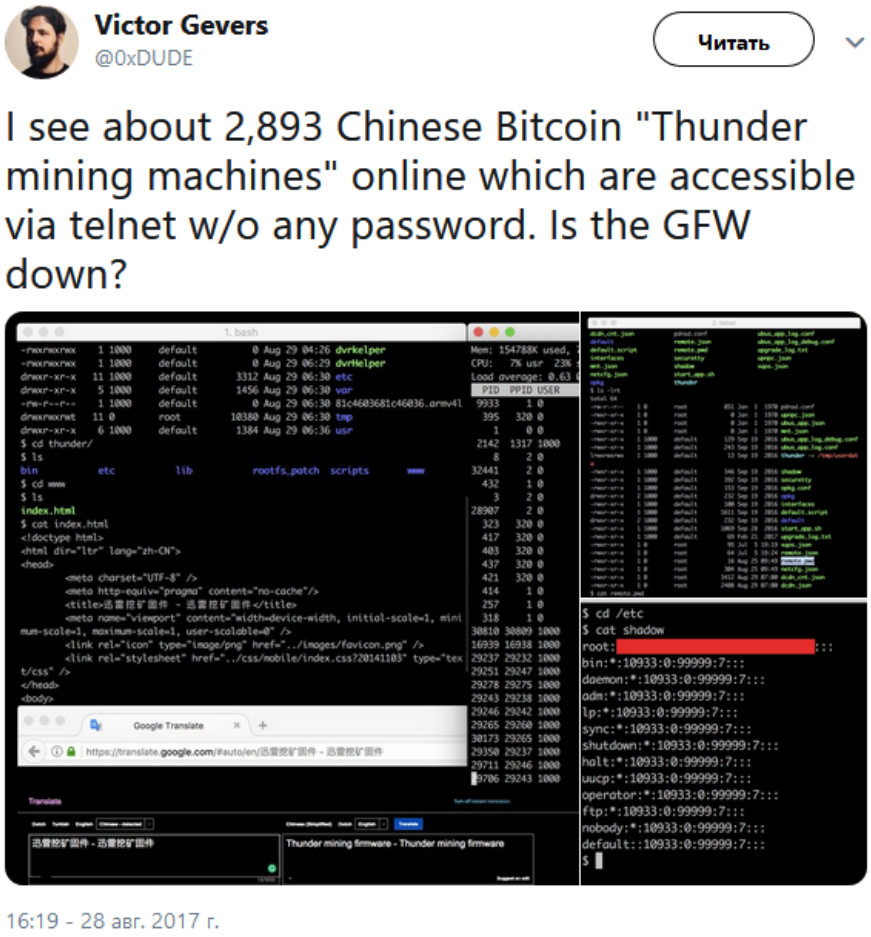

Imagen 10: Un mensaje de twitter sobre dispositivos no protegidos con contraseña[10]

Un par de dispositivos de minería es una cosa, pero 2.893 dispositivos que operan en un grupo pueden aportar sumas considerables.

[10] https://twitter.com/0xdude/status/902309613516808199

5.Cómo guardar las criptomonedas

Cuando se utilizan recursos o servicios online para el almacenamiento, los fondos se confían a un tercero. Esta es una transferencia automática de la capacidad de perder tus fondos a otros participantes. Ya ha ocurrido en varias situaciones, por ejemplo, con la lonja BTC-e.

El propietario de esta lonja fue acusado de violar la ley y el proyecto fue cerrado. El volumen diario de operaciones fue de 50 millones de dólares. Y todos estos medios se volvieron inaccesibles después de la detención. El siguiente mensaje apareció en los medios de comunicación: “Hace unas horas, un ruso fue arrestado en Grecia, acusado de blanquear 4 mil millones$, se encontró vinculado al intercambio BTC-E.”[11]

Para evitar estas consecuencias, es mejor utilizar almacenamiento en frio de criptomoneda.

Esto es recomendable si trabaja constantemente con criptomonedas y una cantidad “decente”. En general, el almacenamiento en frío requiere algo de tiempo y tiene algunos inconvenientes, pero esto se compensa con una alta confiabilidad.

5.1 Almacenamiento en frío con Electrum y Tails

Este método tiene un buen nivel de seguridad. Esto se debe al hecho de que trabajaremos a la vez con dos tipos de carteras: la primera se colocará en la unidad flash de arranque y la segunda se colocará en la máquina en funcionamiento. Esta opción le permite minimizar el riesgo de piratería. No es necesario ingresar una cartera privada en ningún lugar, y las operaciones se pueden firmar y guardar en un archivo, sin estar conectado a Internet.

La unidad de arranque funcionará en base al sistema operativo Tails. Tails es una distribución de Linux, la principal prioridad de los autores al crearla es la privacidad del usuario. Este sistema fue utilizado por el residente más famoso de Rusia (después del Presidente, por supuesto), Edward Snowden. Sobre esto puedes encontrar mucha información en la red. Lo principal es que admite el cifrado, tiene la capacidad de almacenar datos de forma permanente y tiene una cartera Electrum en su ensamblaje.

5.2.1 Instalación de Tails

Para instalar, necesitas dos unidades flash USB. Primero se necesita formatear los dispositivos en el sistema FAT32. A continuación se debe descargar la imagen del sistema operativo Tails. Para montar, se puede usar el Universal USB Installer. Para montar, simplemente se selecciona la imagen y el sistema operativo Tails.

Seguidamente, se debe arrancar desde esta unidad flash e iniciar el sistema. Después de esto, se tiene que insertar una unidad flash USB formateada e instalar el sistema donde se almacenará a largo plazo. Para hacer esto:

[11] https://www.diariobitcoin.com/index.php/2017/07/26/alexander-vinnik-de-btc-e-arrestado-por-lavar-4-mil-millones-de-dolares-enlace-con-caso-mt-gox/

Applications->Tails->Tails Installer

Posteriormente, se debe elegir nuestra segunda unidad flash y comenzar la instalación. El proceso no es lo suficientemente complicado. Después de la instalación, se debe reiniciar desde la nueva unidad flash de arranque.

5.2.2 Configuracion de Tails

Después de arrancar desde el sistema operativo instalado, se debe crear un lugar para el almacenamiento permanente de datos. Para ello, se va al menú:

Aplicaciones-> Tails-> Configurar volumen persistente

Se tienen que seleccionar todos los elementos. A continuación, se debe reiniciar configurando la contraseña que se utilizará. Automáticamente el sistema cifrará los datos almacenados. Después de eso, se puede empezar a trabajar con la cartera. El sistema está completamente listo para funcionar.

5.2.3 Trabajar con la cartera de Electrum

Luego puede encontrar la cartera Electrum en la lista de aplicaciones. Después de comenzar, se debe crear una cartera estándar. Durante el proceso de registro, deberán ingresarse una contraseña, recordar la frase de recuperación y guardar una clave privada. Para estos fines, puede usar un dispositivo separado, pero también puede guardar estos archivos en la partición raíz, ya que está cifrado y el acceso solo se puede obtener con una contraseña.

Después de eso, puedes usar la cartera. Primero debemos guardar nuestra clave publica o dirección, para trabajar con la cartera en modo “watch only”. Eso será suficiente. Para enviar dinero, se debe usar la pestaña con pagos y seleccionar enviar. Para llevar a cabo la operación, se tiene que ingresar la cartera del beneficiario, la cantidad de dinero, la nota y también determinar el tipo de comisión. Después de eso, se firma la operación y se tiene que guardar en la unidad flash USB. Con la ayuda de una cartera “watch only” en una máquina en funcionamiento, esta operación se puede realizar. En principio, esto es suficiente para recibir y recibir operaciones.

Brevemente, se describirá cómo crear una cartera “watch only”. Para hacer esto, se necesita bajar una de las versiones en Electrum (sitio oficial). Varias versiones están disponibles para descargar.

Después de eso, se tiene que descargar la versión necesaria, al instalar, se selecciona *Importar direcciones de Bitcoin o claves privadas*. A continuación, ingresamos nuestra dirección. Seguidamente, se puede usar la cartera en modo de solo visualización. También es posible descargar y realizar transacciones firmadas utilizando dicha cartera.

Para realizar la operación, desde el sistema operativo principal en el menú de la cartera, se selecciona *Load transaction from file*, se debe descargar la transacción firmada desde la unidad flash USB y en último lugar, hacer clic en *Broadcast*.

Por lo tanto, una transacción firmada se envía a la red desde la cartera “watch only”, y su clave privada se filtra al 100% a su Tails.

Este método es bastante confiable. Lo más importante es no conectarse a Internet y no realizar varias actividades en una unidad flash USB de arranque con una cartera de clave privada. El uso solo para almacenamiento en frío y operaciones de firma reduce la posibilidad de piratería a cero.

5.2 Almacenamiento hardware de Bitcoin

Las carteras de hardware son dispositivos electrónicos físicos que se utilizan para almacenar criptomonedas. La esencia principal radica en el hecho de que, para el funcionamiento del dispositivo, debe estar conectado al ordenador, teléfono inteligente o tablet. Esta es una de las formas de almacenar la criptomoneda de manera más segura.

Dichos dispositivos mantienen las claves privadas separadas de la computadora. Esto reduce la posibilidad de un ataque. Las operaciones clave se realizan en un entorno protegido, lo que dificulta la intercepción de la información en una computadora infectada o desprotegida.

Las carteras de hardware están protegidas por un código PIN, que las defiende contra la transferencia de dinero en caso de pérdida física. Si el dispositivo se pierde, se puede restaurar con un código especial.

Algunos de ellos tienen una pantalla, siendo una medida de seguridad adicional. Muestra información importante y permite verificar las transacciones. En un PC, puede reemplazar los datos o falsificarlos, pero es bastante difícil hacerlo en un dispositivo de hardware. Por lo tanto, puede consultar la cartera y la información de la transacción.

Hay varios modelos de carteras de hardware:

Imagen 11: Dispositivo Ledger Nano S[12]

Ledger Nano S es la cartera de hardware más económica con una pantalla. Su coste es de 63 dólares. El desarrollador de la empresa es Ledger. Bastante bien conocido en la comunidad criptográfica. Se encuentra en el mercado desde 2016.

[12] https://www.ledger.com/

Imagen 12: Dispositivo Trezor[13]

TREZOR es la primera cartera de Bitcoin lanzada en 2014. Su cómoda utilización y la alta seguridad que ofrece son sus beneficios clave.

Imagen 13: Dispositivo Keepkey[14]

La cartera KeepKey se lanzó al mercado en septiembre de 2015 y es considerada la segunda cartera en la historia equipada con una pantalla. La pantalla grande KeepKey permitió a los desarrolladores agregar varias medidas de protección nuevas de las que carecen el Nano S y Trezor.

[13] https://cryptowiki.ru/wp-content/uploads/2017/10/08f1a8996350c6bcf3d325c35c74e303.jpg
[14] https://shapeshift.io/keepkey/

Imagen 14: Dispositivo Ledger HW.1[15]

Ledger HW.1 se considera una de las carteras de hardware más baratas. No tiene pantalla y, por lo tanto, no puede considerarse tan seguro como las tres carteras anteriores.

5.3 Almacenamiento en frío con Bitcoin Core

En general, esta cartera no es muy diferente de otras, pero es un poco más segura. Tiene una función de control de entrada, puede cifrar los datos y establecer una contraseña para ingresar a la cartera. Pero, su principal inconveniente es el entorno de instalación.

Se trata de uno de los métodos de almacenamiento que requerirán aproximadamente 160 GB en el disco. Aunque, este tamaño está aumentando constantemente. Si los dos métodos anteriores tienen como objetivo la protección contra la intercepción y la piratería mediante una PC infectada, entonces este método es más vulnerable a ataques. Por lo tanto, la opción ideal es utilizar una máquina separada solo para las operaciones. Esto es bastante problemático, pero en teoría se puede implementar utilizando una máquina virtual o acceso remoto a una computadora.

Puedes elegir una cartera en la web oficial. La instalación llevará mucho tiempo, lo principal es descargar el archivo con toda la historia en bloques. La sincronización puede durar desde varias horas hasta días enteros.

5.4 Recomendaciones sobre cómo guardar criptomonedas

La opción más segura y barata es Electrum y Tails. Para hacer esto, se necesita una unidad flash USB de arranque, con la cual se puede realizar una operación, firmarla y guardarla como un archivo en una unidad flash USB. Esta distinción reduce el riesgo de perder criptomonedas a cero. Lo siguiente en términos de confiabilidad son las carteras de hardware, pero cuestan un poco más que las unidades flash, aunque también hay un alto nivel de confiabilidad. Bitcoin Core es una buena opción en comparación con los servicios e intercambios en línea.

Es mejor usar métodos comprobados que confiar el dinero a un tercero.

[15] https://www.ledger.com/

6.Conclusiones

Este proyecto describe el estado actual de la tecnología de la criptomoneda, sus conceptos básicos, importantes para decidir la necesidad de su utilización y riesgos relacionados con el uso de la criptomoneda o del dispositivo que puede ser comprometido con la idea de robo de sus recursos.

Se han evaluado las distintas formas y vectores de ataque y abuso de las criptomonedas, desde el robo directo hasta el robo de recursos informáticos para producir nuevas, o el influir de manera negativa en otros usuarios del sistema.

Por otra parte, se demuestran los principales incidentes de seguridad de últimos años relacionados con la criptomoneda, los motivos principales de los atacantes, las tecnologías utilizadas y la influencia provocada en el usuario y en el entorno.

Se proponen recomendaciones para varios perfiles, que se encuentran o pueden hacerlo, en la "zona de riesgo", como usuarios de criptomoneda, gestores de empresas, desarrolladores de software (no necesariamente asociados con la criptomoneda) y otras personas que no tienen relación con este campo, pero que son usuarios de PC o de dispositivos móviles. También, recomendaciones para el almacenamiento de la criptomoneda, su segura utilización y para reducir el riesgo de abuso de sus recursos de cálculo.

Las criptomonedas ya han afianzado firmemente su lugar en el mundo, y se espera un mayor crecimiento en el área de su uso e introducción en la vida diaria de los ciudadanos gracias a los beneficios que representan. En este nuevo mundo de "dinero virtual", cualquier persona debe conocer al menos los conceptos básicos de la utilización de la criptomoneda y de las tecnologías relacionadas para maximizar la eficiencia de uso de sus recursos y reducir las amenazas que provoquen pérdidas.

6.1 Relación del trabajo desarrollado con las asignaturas cursadas

Este proyecto ha sido un gran desafío intelectual debido a la gran variedad de temas e información a tenerse en cuenta como:

- Identificar los riesgos potenciales gracias a "Ciberseguridad".
- Conocimientos de conceptos de funcionalidad de la red, necesarios para sistema de criptomoneda gracias a "Redes y seguridad".
- Arquitectura distribuida general, protocolos y patrones de comunicación, alto nivel de concurrencia gracias a "Servicios y aplicaciones distribuidas" y "Computación de altas prestaciones".
- Evaluar diseño y los resultados de ejecución del código malware gracias a "Sistemas empotrados y ubicuos".
- Uso de software requerido, conocimiento de sistemas de virtualización e identificación de riesgos técnicos, amenazas para la infraestructura de empresa gracias a "Configuración y optimización de sistemas de cómputo".

7.Líneas de futuro

La inmadurez de la tecnología de la criptomoneda de momento da mucho espacio a los delincuentes para sacar beneficio de la gente. Se produce una carrera entre los desarrolladores, que intentan mejorar el software y los conceptos del sistema para subir el nivel de seguridad y los hackers, que intentan buscar y utilizar agujeros en la defensa para su uso malicioso. Y esta nunca se acabará.

No es posible crear una defensa perfecta, la cuestión radica solo en el esfuerzo y los recursos, que hay que gastar para sobrepasarla. Esta evolución continua de tecnologías obliga a las personas que pueden ser afectadas por las amenazas informáticas siempre a estar al día con tendencias y métodos de protección actuales.

Los futuros trabajos posibles dependen mucho del camino de crecimiento que vaya tomando la criptomoneda y de la reacción a su uso por parte de los gobiernos de los países, pero también de sus motivos de control y su uso para lograr objetivos nacionales.

Bibliografía

[1] “An Architectural Assessment of Bitcoin” Procedia Computer Science 44:527-536,12.2015

[2] Documentacion para los desarolladores de Bitcoin https://bitcoin.org/en/blockchain-guide

[3] Documentacion para los desarolladores de Bitcoin, Guía de Transacciones https://bitcoin.org/en/transactions-guide#introduction

[4] “Comparison Between PoW and PoS Systems Of Cryptocurrency” Indonesian Journal of Electrical Engineering and Computer Science Vol.10, No.3, June2018, pp. 1251~1256

[5] “Crypto crime report: Decoding Hacks, Darknet Markets, and Scams” January 2019

[6] “Cryptocurrency Mobile Wallet Security Survey” https://rt-solar.ru/upload/iblock/3c3/report_incode_crypto_wallet.pdf

[7] Las vulnerabilidades de Bitcoin https://en.bitcoinwiki.org/wiki/Bitcoin_weaknesses

[8] “Fake cryptocurrency wallets found on Play Store” Lukas Stefankoon 13.11.2018 https://lukasstefanko.com/2018/11/fake-cryptocurrency-wallets-found-on-play-store.html

[9] “Cryptocurrency Gold Rush on the Dark Web” Carbon Black, junio 2018 https://www.carbonblack.com/wp-content/uploads/2018/06/Cryptocurrency_Gold_Rush_on_the_Dark_Web_Carbon_Black_Report_June_2018.pdf

[10] Cross-Site Request Forgery (CSRF) https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

[11] “Cryptoasset market coverage initiation: network creation” Satis group 11.07.2018 https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

[12] “Spam and phishing in Q2 2018” Maria Vergelis, Nadezhda Demidova, Tatyana Shcherbakova, Kasperskylab 14.08.2018, https://securelist.com/spam-and-phishing-in-q2-2018/87368/

[13] “Ethereum Scammers Make $5,000 in a Night by Impersonating Celebs on Twitter” https://www.bleepingcomputer.com/news/cryptocurrency/ethereum-scammers-make-5-000-in-a-night-by-impersonating-celebs-on-twitter/

[14] “Twitter Is Still Allowing Scammers To Hijack Verified Accounts To Take People’s Money” Charlie Warzel y Ryan Mac BuzzFeed News 23.02.2018 https://www.buzzfeednews.com/article/charliewarzel/twitter-allowed-cryptocurrency-scammers-to-hijack-verified#.upzaoXDde

[15] “The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets” Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith, Tyler Moore (https://link.springer.com/chapter/10.1007%2F978-3-662-54970-4_36)

[16] “Tales from the blockchain” Sergey Yunakovsky, Kasperskylab https://securelist.com/tales-from-the-blockchain/82971/

[17] “CryptoShuffler: Trojan stole $140,000 in Bitcoin” Kaspersky daily, 31.10.2017 https://www.kaspersky.com/blog/cryptoshuffler-bitcoin-stealer/19976/

[18] “IBM Raises the Bar with a 50-Qubit Quantum Computer” Will Knight, 10.11.2017 https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/

[19] “Coinhive Mints Quarter Million Dollars in Monero a Month, Report Reveals” The BlockChain Feed, 15.08.2018 http://theblockchainfeed.com/bitcoin-news/coinhive-mints-quarter-million-dollars-in-monero-a-month-report-reveals/

[20] “THINK YOU ARE JUST WATCHING A VIDEO? THINK AGAIN!” Votiro Inc 20.02.2018 https://www.votiro.com/think-you-are-just-watching-a-video-think-again/

[21] “Coinhive buzzes off” Avast blog, 1.03.2019 https://blog.avast.com/coinhive-shutters-due-to-drop-in-crypto-value

[22] “Digging into Browser-based Crypto Mining” Jan Rüth, Torsten Zimmermann, Konrad Wolsing, Oliver Hohlfeld Communication and Distributed Systems, RWTH Aachen University, Germany https://arxiv.org/pdf/1808.00811.pdf

[23] “Smominru Monero mining botnet making millions for operators” Proofpoint, 31.01.2018 https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

[24] “$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do” Kate Rooney CNBC, 07.06.2018 https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html