USAL
UNIVERSIDAD
DEL SALVADOR

Facultad de Ingeniería de la Universidad del Salvador

Seguridad y Protección para los Usuarios de Criptomonedas

Proyecto Final de Ingeniería Informática

Año: 2019

Alumno: Gonzalo Paraje

Profesores: Horacio Lurati, Joaquín Zajac

1 Abstract

A lo largo de los primeros seis meses del año 2019, siete empresas de intercambio de criptomonedas, que tienen más de cientos de miles de usuarios, han recibido ataques en sus sistemas a gran escala ocasionándoles pérdidas por decenas de millones de dólares. La seguridad nunca ha sido tan importante de lo que es ahora, especialmente considerando lo costosos que han sido algunos de los ataques recientes en varias plataformas de empresas de intercambio.

Las criptomonedas ciertamente tienen sus beneficios pero muchos usuarios aún desconocen lo que son debido a las preocupaciones sobre la seguridad y sobre cómo funciona su tecnología. Es una industria emocionante en la que participar, pero se basa en la confianza. Por lo tanto, es muy importante que las empresas de criptomonedas hagan todo lo posible para proteger sus sistemas y minimizar las posibilidades de violaciones de seguridad que pueden ocasionar el robo de las criptomonedas de sus usuarios.

Dado que las transacciones en redes blockchain públicas como Bitcoin y Ethereum se pueden rastrear debido a la estructura descentralizada de su cadena de bloques o blockchain, se determinará como las principales empresas que brindan servicios de intercambio de criptomonedas están trabajando con firmas de análisis para mantener una base de datos de transacciones y billeteras sospechosas.

En este trabajo de investigación se plantea el objetivo de analizar y describir los mecanismos para garantizar la protección de las criptomonedas de los usuarios ante posibles amenazas en las plataformas de intercambio, tomando como casos de estudio aquellas plataformas de intercambio de criptomonedas que han sido vulneradas en los primeros seis meses del año 2019.

Esta investigación será de carácter cualitativo, con la utilización de fuentes primarias y secundarias, y con el análisis de los resultados obtenidos mediante el empleo de herramientas de software con las que serán realizadas las distintas pruebas durante el desarrollo del marco metodológico.

2 Índice

3 Introducción

Tan innovador y avanzado como Bitcoin y las criptomonedas, hay una serie de riesgos que alguien corre cuando decide invertir en esta clase de activos digitales. Uno de los riesgos más importantes y prominentes que ha estado encabezando las noticias últimamente es la amenaza de violaciones de seguridad y robos en las plataformas de intercambio de criptomonedas (Reuters, 2019).

Durante el primer trimestre de 2019 los ciberdelincuentes robaron más de $ 356 millones de dólares de plataformas de intercambio y usuarios de criptomonedas (CipherTrace, 2019). A pesar de los esfuerzos de estas empresas, que comercializan criptomonedas, para incrementar las medidas de seguridad y mejorar sus sistemas de administración internos, los ciberdelincuentes han podido implementar métodos cada vez más sofisticados y avanzados de ingeniería social para engañar a los usuarios y así obtener accesos no autorizados a billeteras corporativas y cuentas de usuarios de estas plataformas, con el objetivo de robar sus fondos e información confidencial.

Si Bitcoin continúa con su tendencia de crecimiento, podemos esperar que surjan más ataques, por lo tanto las empresas como los usuarios de criptomonedas siguen siendo vulnerables a estos ataques. La preocupante tendencia en el mercado de intercambios de criptomonedas es que, en los primeros seis meses de 2019, la industria ha visto la misma cantidad de ataques que en todo el año 2018, y las brechas de seguridad en 2019 fueron experimentadas principalmente por grandes intercambios y como consecuencia ha desanimado a muchos a invertir (CoinTelegraph, 2019). Tan rápido como se puede recibir una criptomoneda cuando se compra, se puede perder todo en muy poco tiempo si no se protege adecuadamente.

Las criptomonedas han traído muchas posibilidades interesantes, pero también están llenas de riesgos y peligros para los inexpertos, por lo que es muy importante educarse y educar a los que nos rodean. Debido a la problemática descripta anteriormente y a la escasez de información, sobre todo en idioma español, es que se buscará mediante esta investigación, junto con mi experiencia personal en ciberseguridad y utilizando Bitcoin y otras criptomonedas, describir los mecanismos y herramientas de software para poder brindar una mejor comprensión y garantizar la seguridad y protección a los usuarios de criptomonedas ante posibles ataques a las plataformas de intercambio.

Teniendo en cuenta el contexto definido se buscará dar respuesta a la siguiente pregunta:

¿Como contribuye la implementación de mecanismos de seguridad para garantizar la protección de las criptomonedas de los usuarios ante posibles amenazas en las plataformas de intercambio?

El *objetivo general* de esta investigación será el de analizar y describir los mecanismos para garantizar la protección de las criptomonedas de los usuarios ante posibles amenazas en

las plataformas de intercambio, tomando como casos de estudio aquellas plataformas de intercambio de criptomonedas que han sido vulneradas en los primeros seis meses del año 2019.

Para ello se buscará responder a los siguientes *objetivos específicos* que se desarrollarán en el marco metodológico:

- Analizar y describir los mecanismos de seguridad vulnerados en los ataques a las plataformas de intercambio de criptomonedas Binance y Dragonex.

- Analizar y describir la herramienta de software de la firma Chainalysis para realizar un seguimiento de los fondos robados a las plataformas de intercambio de criptomonedas Binance y Dragonex.

- Analizar y describir un conjunto de implementaciones en seguridad para garantizar la protección de las criptomonedas y de las cuentas de usuario en la plataforma de intercambio Binance.

4 Marco Teórico

4.1 Criptomonedas

4.1.1 Concepto de criptomonedas

Las criptomonedas son un medio de intercambio basado en internet que utilizan funciones criptográficas para realizar transacciones financieras, a través de la tecnología blockchain para poder garantizar descentralización, transparencia e inmutabilidad. La característica más importante de una criptomoneda es que no está controlada por ninguna autoridad o ente central. La naturaleza descentralizada de la cadena de bloques o blockchain hace que las criptomonedas sean inmunes a las formas de control e interferencia de un gobierno o institución financiera.

Las criptomonedas son descentralizadas porque su cadena de bloques subyacente se compone de nodos distribuidos alrededor del mundo con una copia de todo el historial de transacciones. Son transparentes ya que cualquiera puede acceder a ese registro de transacciones por ser público. Y son inmutables debido a que una vez realizada una transacción no se puede deshacer o anular (Blockchain Summit LA, 2018).

Las criptomonedas se pueden enviar directamente entre dos partes mediante el uso de claves privadas y públicas. Estas transferencias se pueden realizar con tarifas de procesamiento mínimas, lo que permite a los usuarios evitar las altas tarifas cobradas por las instituciones financieras tradicionales (Visa, Paypal). En la actualidad las criptomonedas se han convertido en un fenómeno global conocido por la mayoría de las personas.

¿Cómo funciona una criptomoneda?

Las criptomonedas han surgido como un producto secundario de otro invento. Satoshi Nakamoto, el creador anónimo o desconocido de Bitcoin, la primera y más importante criptomoneda, nunca tuvo la intención de inventar una moneda. En su anuncio de fines del año 2008, definió a Bitcoin como "Una forma de dinero en efectivo electrónico puramente peer-to-peer debería permitir enviar pagos online directamente entre las partes y sin pasar a través de una institución financiera" (Satoshi Nakamoto, 2008).

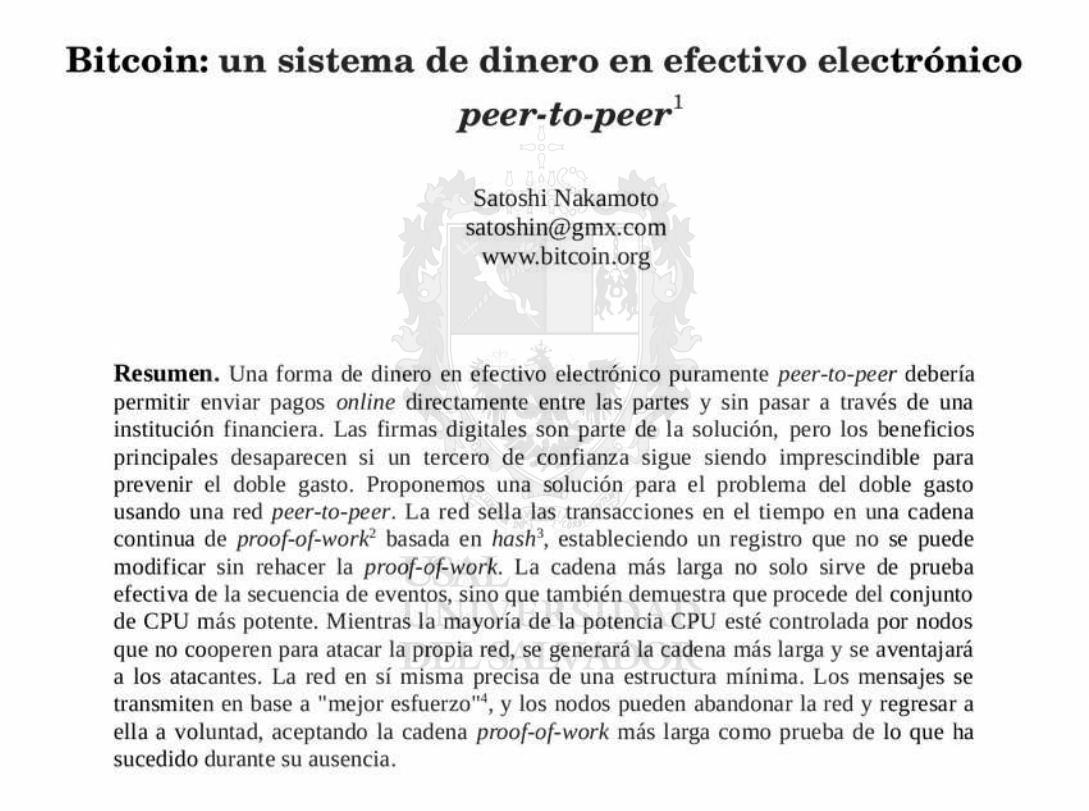
Su objetivo era inventar algo que muchas personas no lograron crear antes del dinero o "*cash digital*". La parte más importante de su invención fue que encontró la manera de construir un sistema de dinero digital descentralizado. En los años noventa, hubo muchos intentos de crear dinero digital, pero todos fracasaron.

Para obtener dinero digital, se necesita una red de pagos con cuentas, saldos y

transacciones. Un problema importante que toda red de pagos tiene que resolver es evitar el llamado "*doble gasto"*, es decir, evitar que alguien gaste la misma moneda dos veces. Por lo general, en los sistemas de pagos tradicionales, esto lo realiza un servidor central que mantiene un registro sobre los saldos.

En una red descentralizada, no se tiene este servidor central, ya que los nodos que forman parte de la red están distribuidos alrededor del mundo. Por lo tanto, se necesita que todas las partes de la red realicen este trabajo. Todos los pares de la red deben tener una lista con todas las transacciones para verificar si las transacciones futuras son válidas o es un intento de duplicar un gasto. Si los pares de la red no están de acuerdo sobre un solo saldo menor, todo se rompe. Se necesita de un consenso absoluto.

Figura 1. Whitepaper de Bitcoin



Bitcoin: un sistema de dinero en efectivo electrónico

peer-to-peer[1]

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Resumen. Una forma de dinero en efectivo electrónico puramente *peer-to-peer* debería permitir enviar pagos *online* directamente entre las partes y sin pasar a través de una institución financiera. Las firmas digitales son parte de la solución, pero los beneficios principales desaparecen si un tercero de confianza sigue siendo imprescindible para prevenir el doble gasto. Proponemos una solución para el problema del doble gasto usando una red *peer-to-peer*. La red sella las transacciones en el tiempo en una cadena continua de *proof-of-work*[2] basada en *hash*[3], estableciendo un registro que no se puede modificar sin rehacer la *proof-of-work*. La cadena más larga no solo sirve de prueba efectiva de la secuencia de eventos, sino que también demuestra que procede del conjunto de CPU más potente. Mientras la mayoría de la potencia CPU esté controlada por nodos que no cooperen para atacar la propia red, se generará la cadena más larga y se aventajará a los atacantes. La red en sí misma precisa de una estructura mínima. Los mensajes se transmiten en base a "mejor esfuerzo"[4], y los nodos pueden abandonar la red y regresar a ella a voluntad, aceptando la cadena *proof-of-work* más larga como prueba de lo que ha sucedido durante su ausencia.

Fuente: Natoshi Nakamoto (2008)

Una criptomoneda como Bitcoin consiste en una red de pares. Cada par tiene un registro del historial completo de todas las transacciones y, por lo tanto, del saldo de cada cuenta o dirección. Se denominan criptomonedas porque el proceso de mantenimiento del consenso está asegurado por una criptografía sólida. Las criptomonedas se basan en la criptografía. No están aseguradas por personas o por la confianza, sino por las matemáticas.