UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO DE SISTEMAS

CARRERA:
INGENIERÍA DE SISTEMAS

TEMA:
“PROPUESTA DE UNA ARQUITECTURA PARA AUMENTAR LA CONFIABILIDAD DE LAS MONEDAS VIRTUALES MEDIANTE TECNOLOGÍA BLOCKCHAIN”

AUTOR:
FLORES CARRILLO JORGE RAFAEL

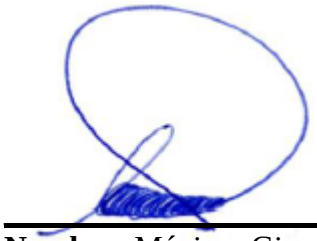
TUTOR:
Msg. MÁXIMO TANDAZO ESPINOZA

Abril 2021
GUAYAQUIL-ECUADOR

DECLARATORIA DE RESPONSABILIDAD

Yo, **FLORES CARRILLO JORGE RAFAEL**, declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del/los autor/es.

Nombre: Jorge Rafael Flores Carrillo
CI. 0924414337



Nombre: Máximo Giovani Tandazo Espinoza
CI. 0916028921

Propuesta de una arquitectura para aumentar la confiabilidad de las monedas virtuales mediante tecnología Blockchain

Máximo Tandazo-Espinoza [1[0000-0001-9907-7048]] and Jorge Flores-Carrillo [1[0000-0001-5981-594X]]

[1] Universidad Politécnica Salesiana, Guayaquil, Ecuador
mtandazo@ups.edu.ec, jfloresc2@est.ups.edu.ec

Abstract. Se analizaron los modelos de seguridad para un sistema de monedas virtuales en las referencias para las gestiones de comercio en el uso de monedas digitales. El problema es que las monedas virtuales al ser un modelo descentralizado, los usuarios no se sienten seguros en las transacciones ante un posible ataque, la confidencialidad del sistema es el problema principal. El objetivo es proporcionar una arquitectura para aumentar la confiabilidad de las monedas virtuales mediante tecnología blockchain. Se utilizó el método empírico analítico, de tipo cuasi experimental con enfoque cualitativo para el análisis de las referencias. Resultó una arquitectura para la gestión de seguridad para la transacción de monedas virtuales, un algoritmo de seguridad para la transferencia de monedas virtuales, una estructura lógica de almacenamiento de datos y un diagrama de secuencia del sistema de seguridad de intercambio o transacciones de monedas virtuales. Se concluyó que el algoritmo de seguridad que hemos propuesto para un manejo exitoso en el intercambio de monedas virtuales proporciona resultados óptimos ante el sistema descentralizado; de acuerdo con las simulaciones realizadas en el sistema se obtuvieron valores promedios de 99.07% en las transaccione realizadas durante la simulación.

Keywords: Monedas virtuales, blockchain.

1 Introducción

Las monedas virtuales son un sistema monetario que está en pleno desarrollo en la actualidad con el fin de reemplazar el sistema financiero tradicional y unificar el sistema monetario de los países; el modo en que se realizan las transacciones no proporciona seguridad a los gobiernos que buscan implementar un nuevo sistema de transacciones; al ser una moneda descentralizada, no es administrada por un gobierno o entidad[1].

Los gobiernos al no administrar la monetización se sienten inseguros de las personas que usan el sistema; algunas personas pueden hacer uso indebido de las monedas virtuales para el lavado de dinero, realizar las transacciones de manera ilegal sin dejar rastro de sus movimientos[2], las empresas o personas que a menudo usan este sistema no tienen un modelo constante del valor de las transacciones; esto afecta el intercambio

de moneda de un sistema tradicional hacia una moneda virtual, su valor incrementa y aumenta el riesgo de ataques a las transacciones[3].

El uso de una moneda virtual de acuerdo con los estándares de gestión de claves actuales implica grandes costos para las empresas que buscan implementar un sistema transaccional con fines comerciales; la seguridad en un sistema de complejo conlleva a perdidas de activos por lo que la confiabilidad es uno de los factores que se estudian en la actualidad[4].

La moneda virtual cuyo funcionamiento es similar al modelo tradicional de finanzas con la diferencia de ser una moneda digital sin ningún intermediario como una entidad bancaria; son totalmente descentralizadas, las transacciones se realizan entre clientes, por medio de nodos; estos nodos se conservan públicamente por medio de un sistema de cadena de bloques; cada nodo se registra en los bloques, por lo que la verificación se realiza de acuerdo con las transacciones realizadas a cada momento[5].

La cadena de bloques es una tecnología de almacenamiento de bloques cifrados, su cambio es constante lo que implica una verificación del nodo actual con el nodo anterior; el sistema garantiza privacidad y seguridad en las transacciones y es adyacente a las monedas virtuales[6], el mercado de moneda digital es descentralizada por lo que un ente regulador no es intermediario, en su lugar la gestionan dos partes, y una red de computadoras; en el momento que se desea realizar una transacción, se envía desde el usuario origen hasta el destinatario[7].

Los modelos de transacciones de las monedas virtuales son compartidos por partes no confiables y al ser un modelo descentralizado; la información de las transacciones son filtradas por medio de una etiqueta que contiene la información del bloque anterior; el modelo de transacción de monedas virtuales son realizadas entre dos personas, transacciones realizadas entre diferentes países con la protección del sistema de cadena de bloques ante la manipulación de atacantes[8], por lo general los problemas que se presentan, son relacionado con la poca confiabilidad del sistema de transacción a través de la red; la implementación de un modelo de bloques cifrados para mejorar los sistemas de transacciones y obtener seguridad ante un inminente ataque en la cadena de bloque[9].

El problema es que las monedas virtuales al ser un modelo descentralizado, los usuarios que usan el modelo no se sienten seguros en las transacciones; la confiabilidad del sistema es el problema principal por el que algunos Países no adoptan el sistema al ser un modelo P2P; no existe intermediarios en las transacciones por lo que los usuarios o empresas se sienten preocupados por un inminente ataque cibernético que intercepte el intercambio de bienes a través de un sistema de monedas virtuales.

2 Materiales y métodos

2.1 Materiales

Los autores propusieron un análisis del uso incorrecto de las monedas virtuales de manera general y presentaron recomendaciones a quienes realizan estas acciones; se identificó un factor que les permitieron la movilización de monedas virtuales a cualquier dirección de su sistema de cadena de bloques; ellos analizaron los delitos más

comunes que van desde el uso de programas generadores de monedas virtuales, ataques de denegación de servicio, programas que atacan otros procesos transaccionales; los delitos cometidos causaron un daño a la propiedad hasta un mal funcionamiento del sistema económico de un país[1].

En este articulo los autores propusieron un modelo de seguridad en múltiples capas para mitigar los ataques maliciosos en los servicios de intercambio de monedas virtuales; se determinaron los ataques de robo de identidades, vulneración de la privacidad que realizan los atacantes en transacciones de monedas virtuales; se diseñó un sistema de seguridad para mitigar los problemas, con el análisis obtuvieron modelos para identificar las vulnerabilidades en aplicaciones; se recomendaron cambios en aplicaciones de intercambios de monedas virtuales más populares para evitar un posible ataque[2].

Los autores propusieron un enfoque sobre el entendimiento de la moneda virtual y su aportación en el ámbito financiero, gestión social y en aplicación con fines no comercial; se realizó el análisis de los mercados de comercialización tradicional y se lo comparó con el mercado de monedas virtuales; se determinaros los comportamientos de manera comercial entre los tres son similares; se identificó que el mercado de monedas virtuales no es muy seguro de acuerdo con la estructura en que se implementen; como resultado del análisis se determinó que la aceptación de la moneda virtual como medio comercial dependió de su sistema[3].

Los autores propusieron un esquema de gestión de monedas virtuales en un ambiente descentralizado para el almacenamiento de claves de manera segura; se realizaron copias de seguridad en la red que representaron las transacciones de los nodos que intervinieron; se identificó de acuerdo con la ejecución de los nodos en el sistema en un determinado tiempo y se minimizo el rendimiento del esquema; se comparó la fiabilidad de los esquemas estudiados con el planteado, se mostraron los indicadores de fiabilidad del sistema; el esquema permitió usar los recursos que brindaron confiabilidad a los usuarios de la red[4].

En este articulo los autores analizaron los conceptos de monedas virtuales y las amenazas en el sistema de cadena de bloques sufre en las transferencias; se determinaron los tipos de transacciones que se realizan entre las diferentes tipos de monedas, la diferencia de dependencia entre los sistemas financieros tradicionales; se detectaron los problemas que el sistema sufrió en su evolución y ataques de denegación de servicio, al usar la red como medio de transferencia; como resultado se identificaron sus usos prácticos, monetarios y de bienes o servicios[5].

Los autores propusieron un análisis de los sistemas de cadena de bloques y el uso de las monedas virtuales para la implementación de un modelo de capas; en base al análisis realizado, se permitió mantener el libro mayor actualizado y compartido para usuarios que desean sincronizarse; se identificó a los dispositivos que realizan transacciones autónomas, las aplicaciones mejoraron el uso de las transacciones entre los clientes que manejan su cartera de monedas virtuales[6].

Los autores propusieron una arquitectura en base al modelo de cadena de bloques para la seguridad en el comercio exterior; se realizaron procesos de registros de la información generada para que la comercialización se establezca por un medio de comunicación segura; se realizaron procesos que minimizaron los riesgos de acuerdo con los resultados captados en la información de los comerciantes; se usó el algoritmo de

registros para mantener el sistema de cadena de bloque; se obtuvo un sistema que permitió solventar problemas de perdida de información[7].

Los autores en este articulo propusieron un estudio que permitió un aprendizaje de los conjuntos de datos y detección de anomalías de transacciones maliciosas de criptomonedas; se analizaron carteras para detectar anomalías, se visualizaron las transacciones de las carteras; se utilizó un programa que ayudo a detectar las transacciones anómalas, se realizaron grupos que identificaron las carteras estudiadas que usaron clasificación binaria para categorizar las carteras; como resultado se obtuvo un algoritmo que clasifico las transacciones de las carteras por clúster separados identificados como transacción anómala[8].

Los autores propusieron un análisis para adoptar el modelo de cadena de bloques en el comercio electrónico para aumentar la eficacia en las transacciones; se realizaron cálculos para la medición de las transacciones realizadas por el modelo de cadena de bloques que determinaron si se realizó correctamente la transacción hacia el destino; los procesos que se realizaron durante el análisis se necesitaron autenticación que son validadas por un administrador; el uso de cadena de bloques para el comercio electrónico con la aplicación de medidas de seguridad para que una transacción sea segura[9].

Los autores realizaron un estudio de la evolución modelo financiero tradicional hasta la moneda digital y propusieron un análisis del modelo para mejorar la privacidad del usuario; se comparó el modelo de transferencia habitual con el banco como intermediario para un sistema físico, con el uso de monedas virtuales, cada usuario tenía control de su monedero; en el análisis se determinaron los modelos de las transacciones normales que se realizan con dinero en efectivo; el modelo descentralizado provoco dudas en el funcionamiento del sistema monetario virtual; el sistema de conocimiento cero proporciono anonimato en las transacciones de los usuarios[10].

Los autores propusieron un análisis del algoritmo de minería de modelo de cadena de bloques existentes para la implementación de un algoritmo asíncrono; se evaluaron perdidas de rendimiento y se implementaron nuevas instrucciones en el núcleo, se determinaron los resultados por medio del algoritmo expresado; se realizaron comparaciones con los resultados entre los algoritmos expuestos y se determinó un cambio en el valor promedio del rendimiento; se determinó que el algoritmo de monedas virtuales mejorado en el núcleo resolvió los problemas de minería que incrementaron su productividad[11].

Los autores realizaron un estudio del modelo de cadena de bloques para la aplicación en las áreas de investigación y las tecnologías del modelo; se identificó que las transacciones en el modelo fueron verificadas en comercializaciones realizadas en el comercio exterior; se analizó la confiabilidad de la seguridad en las transacciones mediante la firma digital única, se obtuvo integridad en la información manejada y sin manipulación; como resultado del estudio se determinó que el modelo de cadena de bloques fue implementado en otras áreas y no se limita solo en finanzas[12].

Los autores propusieron el desarrollo de un modelo estadístico de pérdidas de bloques en la red en el modelo implementado con bitcoins; se realizó un sistema que registraba la información entendible para los usuarios, el sistema registraba los eventos de los usuarios, se monitorearon los bloques de los eventos; en los bloques ocurrieron algunas perdidas, el modelo ayudo a reconstruir los bloques de acuerdo con el número de transacciones para recuperar correctamente el bloque; se identificó la tasa de pérdidas diarias en la red de acuerdo con las sesiones creadas[13].

Los autores propusieron una aplicación de los conceptos de minería y programación lógica sobre incidentes con monedas virtuales; se realizaron secuencias en los eventos para detectar los elementos atacados, los elementos mencionados y las actividades de los atacantes; ellos obtuvieron altas probabilidades de que ocurra problemas con monedas virtuales, se determinaban el área en etiquetas que eran asignadas por la programación; como resultado se identificaban las amenazas que ocurrían a los comerciantes de monedas virtuales[14].

Los autores propusieron un análisis en las transacciones de monedas virtuales para la seguridad de un sistema de bloques de identificación de direcciones sospechosas; de acuerdo con el número de transacciones entrantes se visualizaron perdidas en una fecha determinada, se identificaron las conexiones de direcciones sospechosas; el modelo detecto la dirección de las direcciones de transacciones de monedas virtuales; como resultado del análisis se centraron en la detección del movimiento de las transacciones de las monedas virtuales y su origen[15].

Los autores propusieron un esquema de intercambio y de seguridad en la información para la aplicación a un sistema de cadena de bloques para mejorar la seguridad en las transacciones; ellos mejoraron el sistema de cadena de bloques, se registraban las transacciones con el administrador y se generaba claves pública y privada; al término de la transacción se almacenaba el evento y la información en la cadena de bloques; como resultado los datos almacenados son llamados por otros usuarios que solicitaran la información, se mejoró el intercambio de información de origen a destino[16].

Los autores realizaron un estudio del sistema de cadena de bloques y su aplicación en los sectores comerciales y sociales por medio de la moneda virtual; se determinaron métodos de utilización del modelo de cadena de bloques en la transferencias de activos para la comercialización con la moneda virtual; se identificaron una desconfianza en el sistema de transacción descentralizada que utilizaron las monedas virtuales en comparación con una transacción realizada por cadena de bloques; como resultado se obtuvo los beneficios de contar con un sistema que permita transacciones de acuerdo a la necesidad de la entidad[17].

Los autores en este articulo propusieron una herramienta de código abierto para el análisis de trazas forenses relacionadas con las monedas virtuales; se usaron herramientas de programación para la creación de un programa que centralizó las tareas de control y módulos que integraron la utilización de diferentes modelos; en los módulos se identificaron las transacciones y claves de registros de sistemas que manejaban monedas virtuales; por medio de los módulos forenses ayudaron a visualizar indicadores para acceder a un monedero virtual[18].

Los autores propusieron un prototipo de modelo de seguridad para un sistema de comercio con dinero electrónico; se realizó un modelo de visualización para identificar al usuario que interactuaban con el sistema; se implementó un modelo de seguridad para el pago electrónico con un modelo de claves de seguridad agiles; se implementó un algoritmo de integridad de los datos que determinaban los pasos a seguir del sistema de transacción de dos partes; como resultado se determinó una adopción al modelo de claves de seguridad para las transacciones de dos usuarios[19].

Los autores propusieron un modelo de aprendizaje automático para un sistema de cadena de bloques que ayudaron en la seguridad, privacidad y rendimiento de los bloques; se determinaron los autores que intervinieron en la red propuesta, los actores proporcionaban sus libros contables para la transparencia de datos; se recopilaban los

pesos globales de los actores, luego se ordenaron de acuerdo con su peso y se compartieron los registros de errores; se obtuvo un escenario con menor complejidad de tempos en comparación con otros modelos basados en cadena de bloques[20].

En este articulo los autores propusieron un modelo de minería de monedas virtuales para usuarios de acuerdo con sus intereses; el modelo se desarrolló para que los usuarios puedan implementar modelos para la minería, mientras que otros usuarios eligieron los caminos creados; de acuerdo con los resultados de cada modelo, se determinó los caminos más viables en el sistema de cadena de bloques; como resultado del modelo, los actores obtuvieron más porcentajes en resultados de la minería en relación a la minería habitual[21].

Los autores propusieron un esquema de monetización basado en cadena de bloques para pago automatizado con monedas virtuales; se implementó una aplicación en base al entorno de un sistema de cadena de bloque Ethereum; el cliente accedió por medio de un algoritmo a los servicios del contrato inteligente para la verificación de saldo; se determinó un modelo de seguridad que permitió al nodo tener el control de la sesión; como resultado el modelo permitió un mecanismo de intercambio y comercio automatizados por los contratos inteligentes[22].

Los autores propusieron un modelo matemático de seguridad en los sistemas de cadena de bloques y una comparación con otros modelos; se ejecutaron probabilidades de fallo de acuerdo con un rango expuestos por otros modelos; se clasificaron los resultados de los protocolos usados en clases para medir la seguridad en la red de cadena de bloques; como resultado se determinaron medidas de seguridad de acuerdo con el número medio de fallas en la ejecución del protocolo habitual con el modelo implementado en el sistema[23].

Los autores propusieron una arquitectura para la validación de calidad de las fuentes, confidencialidad entre los modelos de un centro de confianza en el sistema de cadena de bloques; se desarrollaron modelos de confiabilidad en el que dependieron del tipo de transacción; se implementaron métodos de predicción de daños, los bloques afectados fueron restaurados a su estado anterior de acuerdo con las operaciones realizadas; como resultado se obtuvo una protección de la información que se almacenaban en el sistema de cadena de bloques para las transacciones[24].

Los autores propusieron un diseño de un modelo basado en contratos inteligentes y un algoritmo para el análisis del rendimiento de seguridad del modelo; se determinó el modelo que ayudó al sistema de cadena de bloques a una posible reescritura en los bloques, con Ethereum se implementaron funciones que describen los movimientos de registro o visualización por medio de los contratos inteligentes; de acuerdo con el modelo de transacción, el modelo aseguró que los registros no cambien, el contrato inteligente verificó la validez de los datos que se encuentran en todo el sistema de cadena de bloques[25].

Los autores propusieron un modelo de aplicación descentralizado en el modelo de cadena de bloques con uso de programación para el almacenamiento en una base de datos; se realizó una simulación de una red de transferencia de dos usuarios con una aplicación web independiente para cada nodo; el modelo grafico permitió que la recuperación fuera de manera óptima con el fin de recuperar los bloques de manera eficiente; se desarrolló un modelo de cadena de bloques que permitieron una fácil integración de tecnologías para mejorar la seguridad en los bloques[26].

En este articulo los autores desarrollaron un modelo seguro de cartera de monedas virtuales de manera eficaz; el sistema permitió a los usuario, realizar el registro de sus cuentas en un servidor, se generaron los tokens para una visualización oportuna de la cartera; se implantaron medidas de recuperación de claves generado por los usuarios; se simulo un escenario para identificar los posibles robos de contraseñas de los usuarios y se implementó un sistema de encriptación para solucionar los errores encontrados; la aplicación permitió a los usuarios tener más seguridad en sus transacciones y manejo de sus monedas virtuales[27].

Los autores propusieron un modelo de seguridad en un sistema de transacciones de monedas virtuales para mitigar ataques; se generó claves a los usuarios por medio de algoritmos, se obtuvo un beneficio en los costos de las transacciones de origen a destino; con la implementación de un esquema de monedas virtuales proporcionaron seguridad en los modelos de minería de las monedas digitales; los usuarios obtuvieron una privacidad en las claves en comparación con los usuarios de moneda virtual original y el sistema evito problemas con atacantes[28].

Los autores propusieron una mejora en la funcionalidad de los contratos inteligentes en u sistema de cadena de bloques; se desarrolló una tecnología que permitió la integración con los libros contables y que extendieron la funcionalidad del contrato inteligente; en el sistema se permitió realizar el proceso de transacciones controladas en los bloques registrados por un identificador; se simularon varios escenarios que permitió el uso de varias monedas virtuales para uso comercial por medio del uso de los contratos inteligentes[29].

Los autores propusieron una arquitectura para contratos inteligentes para evitar el riesgo en la emisión de monedas virtuales; en el desarrollo se identificaron a los actores del modelo, los usuarios que realizaron las transacciones se almacenan en un libro contable en los bloques del sistema; se midieron las dependencia entre la ejecución de la transacción que el usuario emite hacia el comerciante y la latencia de la transacción; el modelo permitió a los usuario tener confiabilidad durante la transacción sin afectar la fluctuación del valor de las monedas virtuales[30].

Los autores propusieron un modelo de seguridad para un sistema de cadena de bloques en las transacciones de monedas virtuales en el área financiera; los datos se almacenaron en el servidor centralizado a los bloques, la información se almacenó en la nube y el cliente obtuvo una clave de autenticación para acceder; con el acceso los usuarios accedieron a la página para realizar las transacciones, en el análisis se identificó la seguridad del modelo, se simuló un ataque y el atacante obtuvo la mitad de la clave[31].

Los autores realizaron un análisis del riesgo en las transacciones y dinámica en el mercado de las monedas virtuales; se identificaron la competencia del modelo de moneda digital en comparación con un modelo financiero habitual, se determinó un sistema inestable para el uso de monedas virtuales; se identificaron los cambios en los valores en el mercado de las monedas virtuales que perjudicaron la confiabilidad del uso del sistema; como resultado del análisis se mostraron herramientas de verificación en el mercado de monedas digitales[32].

Los autores propusieron una simulación en el proceso de transacciones de monedas virtuales con algoritmos de criptografía; se comparó el tiempo de ejecución de los modelos de cifrado de claves de acceso para un sistema de cadena de bloques; se utilizaron registros para las transacciones con un identificador para cada bloque, este

modelo permitió a los mineros detectar errores en las transacciones de monedas virtuales; como resultado de la implementación se logró un sistema seguro en las transacciones de minería de monedas virtuales[33].

2.2 Métodos

Para llevar a cabo la implementación del modelo de seguridad, se realizó el análisis de los artículos con la finalidad de presentar un modelo de negocio basado en monedas virtuales.

Se estudiaron los modelos de seguridad en un sistema de economía electrónica; le propuesta para un modelo de seguridad se basa en mejorar el sistema de intercambio de monedas virtuales en los sistemas ya existentes, también crear un modelo que permita confiabilidad en los usuarios de extremo a extremo en el sistema.

En los artículos revisados se presentan modelos de transacciones para los usuarios que realizan intercambios de monedas por medio de un sistema de cadena de bloques[24]; los modelos descentralizados permitieron a los usuarios realizar las transacciones son necesidad de un ente regulador[26]; por medio de los modelos revisados en los artículos se representó el siguiente modelo.

La Fig.1 representó el modelo de gestión en las transferencias de monedas virtuales, los usuarios se prepararon para realizar un pago de monedas virtuales; el primer usuario tiene en su posesión, una cartera de criptomonedas que contienen direcciones y que se encontraron encriptados; el segundo usuario para receptar el pago, completo el proceso de creación de una nueva dirección, esta dirección se encontraba vacía con el fin de agregar la transacción de la dirección del primer usuario; en la creación de la nueva dirección se crean las claves pública y privada para que la transacción entre los dos usuarios se realicen con normalidad[8], [10].

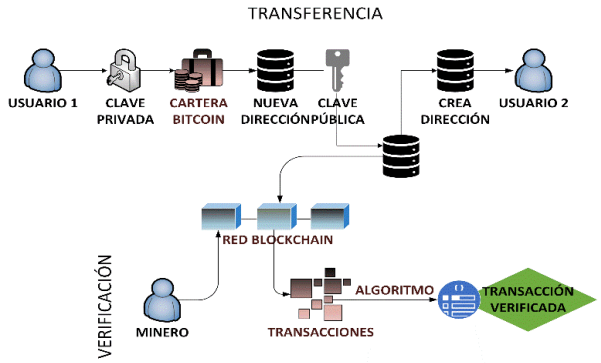


Fig. 1. Modelo de gestión comercial en monedas virtuales.

El modelo de verificación está a cargo de otros usuarios que se denominan mineros; ellos se encargan de visualizas los bloques de los últimos diez minutos en un nuevo bloque de transacciones; por medio de un algoritmo de funciones criptográficas,

las transacciones se cargan en forma de caracteres alfanuméricos de longitud fija; las cadenas de transacciones con el nuevo valor de combinaciones son calculados por las combinaciones anteriores; los minadores no pueden predecir qué valor produciría, por lo que se crean muchas combinaciones hasta dar con el valor correcto; los minadores contienen registros de la transacción de los usuarios y de las nuevas transacciones realizadas en la red de un sistema de cadena de bloques[25][31].

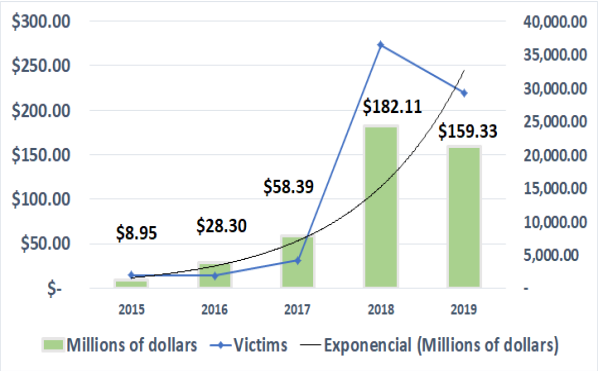


Fig. 2. Víctimas y Dólares perdidos en moneda virtual

La cantidad de víctimas está basada en la cantidad de denuncias realizadas. En la Fig.2, el eje X son los años del 2015 al 2019, el eje Y primario son los millones de dólares perdidos, el eje Y secundario es la cantidad de víctimas que denunciaron el fraude; cada barra representa la cantidad de millones de dólares americanos; la línea azul representa la cantidad de víctimas; la curva negra representa la tendencia de millones de dólares[34]–[35].

En la cantidad de víctimas: en año 2015 hay 1920 víctimas; en año 2016 el incremento es -0.83%; en año 2017 el incremento es 117.38%; en año 2018 el incremento es 781.30%; en año 2019 el incremento es -19.64%; en los años 2016 y 2019 la cantidad de víctimas disminuyó.

En los millones de dólares perdidos: en año 2015 la perdida fue 8.95 millones de dólares; en año 2016 el incremento es 216.16%; en año 2017 el incremento es 106.31%; en año 2018 el incremento es 211.87%; en año 2019 el incremento es -12.51% termino con 159.33 millones de dólares; existe una clara tendencia al alza anual; la curva negra desde 2015 al 2019 indica que existe una tendencia exponencial en los fraudes por moneda virtual.

Los alcances para esta investigación fue el modelo de mercado de monedas digitales; como propuesta por nosotros para mejorar el sistema de transacciones o un modelo de intercambio habitual.

Emplear una arquitectura de seguridad que permita aumentar la confiabilidad para el intercambio de monedas digitales a través de encriptación; adoptar un algoritmo de seguridad para el modelo de encriptación de los datos antes de ser enviados por la cadena de bloque; definir los pasos para la ejecución de la gestión de seguridad; definir un modelo de diagrama para la ejecución de paso a paso de un modelo de intercambio de monedas virtuales.

3 Resultados y discusión

3.1 Resultados

Los resultados en esta fase son los siguientes:

- Arquitectura de seguridad para aumentar la confiabilidad de las monedas virtuales.
- Algoritmo de seguridad para la transferencia de monedas virtuales.
- Estructura lógica de almacenamiento de datos.
- Diagrama de secuencia del sistema de seguridad de intercambio de monedas virtuales

3.1.1 Arquitectura de seguridad para aumentar la confiabilidad de las monedas virtuales

Se propuso una arquitectura que está conformada por cinco capas con la finalidad de realizar una transacción de cambios de criptomonedas entre dos entidades o usuarios; en la arquitectura definimos lo siguiente:

Capa de usuario encontramos los dispositivos finales que usaron las entidades, que solicitan un nuevo pago o transacción de monedas virtuales; los usuarios usaron varios medios que se podrán conectar para realizar las transacciones, estos son portátiles, computadoras de mesa, celulares o tabletas que tengan acceso a la aplicación de la arquitectura.

Capa de aplicación definimos las aplicaciones que se asociaran para realizar la transacción de las monedas virtuales, son accedidas por cualquier medio que el usuario utilice; se necesitaron conectividad a la red para el uso de las aplicaciones, las aplicaciones se las encontraron como un ambiente web o una aplicación instalada en el equipo o celular.

Capa de base de datos se encuentran las bases de datos transaccionales, estas bases almacenan los movimientos de los usuarios que utilizaron las aplicaciones, se almacenan los datos de los usuarios y registros habituales; también se almacenaron los nodos de la cadena de bloques, esta base constó de un modelo integrado que hizo más fácil la filtración de la información.

Capa de encriptación y desencriptación se encontraron los procesos de encriptación de datos que se almacenaron en la base de datos antes de enviarse a los bloques; contienen un registro de las claves públicas y privadas que se crean al momento de iniciar una transacción entre dos usuarios o entidades; realizaron el proceso de desencriptación antes de que la transacción llegue a su destino, de tal manera que la información no sea vulnerada en el camino por parte de los atacantes.

Capa de Blockchain contienen el sistema que gestionara la seguridad en las transacciones de los usuarios, manejara la información encriptada para ser enviada a los destinos que se presentaron en la red; la gestión de seguridad mantuvo la privacidad de las transacciones en varios bloques.

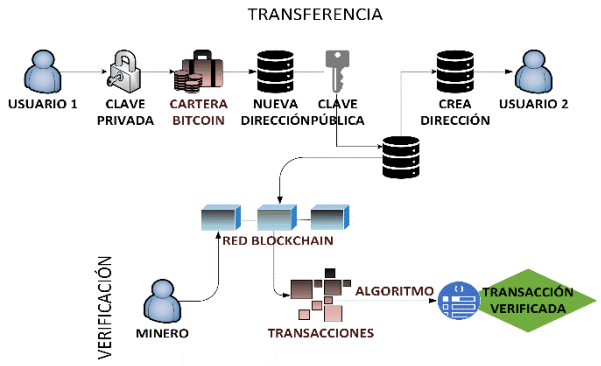


Fig. 3. Arquitectura de seguridad en intercambio de monedas virtuales

En la Fig. 3 se presenta la arquitectura de seguridad en las transacciones o movimiento de carteras de criptomonedas; está compuesta por un modelo de aplicación con conexión a la base de datos integrada con acceso a una red de cadena de bloques.

El fundamento matemático, para la arquitectura esta expresada en la formula (1):

$$\mathrm{Pr}_{arq} = \frac{(TS - TF) * (nUser + App)}{Ttotal * \sqrt{Reg}} * 100\% \qquad (1)$$

Aquí:

- nUser es la cantidad de usuarios que interactúan en el sistema.
- TS es la cantidad de transacciones exitosas en el sistema por los usuarios.
- TF es la cantidad de transacciones que tuvieron errores en el sistema.
- Ttotal es la cantidad total de transacciones que se presentaron en el sistema.
- App es la cantidad de veces que la aplicación es usada por los usuarios.
- Reg es la cantidad de registros que se almacenan en la base de datos.

Para determinar la probabilidad de aceptación de la arquitectura se estableció la formula antes mencionada de acuerdo con los usuarios que interactuaron con el sistema; esta simulación se determinaron los valores de las variables con valores aleatorios; para la cantidad de usuarios que interactuaron en el sistema el rango esta entre 40 a 70 usuarios de acuerdo a las conexiones habituales; se determinaron los valores de las transacciones totales de acuerdo con las transacciones exitosas con un rango entre 500 a 800 transacciones; las transacciones con errores encontrados con un rango de 150 a 500 de acuerdo a los intercambios o validación de información de la cartera de criptomoneda; los valores de los registros almacenados en la base de datos de acuerdo con las interacciones con valores de 100 a 900 registros; el uso de la aplicación por los usuarios de acuerdo a la conexión con un valor de entre 40 a 70 interacciones que el usuario realizó durante un tiempo establecido.

Para la simulación se usaron las variables antes mencionadas, de acuerdo con los usuarios que usaron las aplicaciones; se presenta la siguiente simulación:

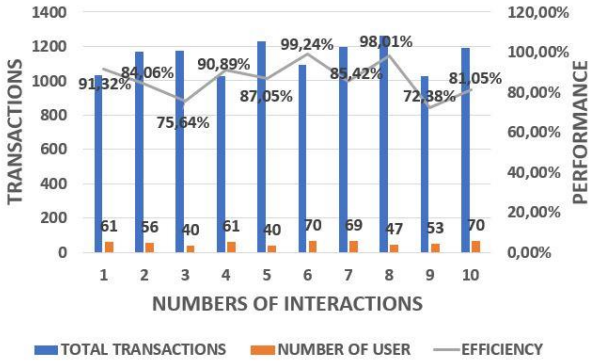


Fig. 4. Análisis de la probabilidad de la arquitectura de seguridad de intercambio

En la Fig. 4 se visualiza una simulación de 10 escenarios en la que los usuarios interactuaron; en el primer escenario con una aceptación de un 91.32% con una interacción de 61 usuarios, 626 transacciones exitosas, 408 transacciones con errores presentados y 887 registros; el sexto escenario con una aceptación de 99.24% con una interacción de 70 usuarios, 665 transacciones exitosas, 427 transacciones con errores y 879 registros en la base de datos; el décimo escenario con una aceptación de 81.05% con una interacción de 70 usuarios, un total de 700 transacciones exitosas; 492 transacciones con errores presentados y con 870 registros en la base de datos.

De acuerdo con las pruebas realizadas hay un rango de aceptación de entre 72.38% hasta un 99.24%; se muestran los valores de aceptación de acuerdo con los estudios de la arquitectura; se realiza el cálculo del promedio de aceptación con la formula (2):

$$Avr_{Pr} = \sum_{i=1}^{n} Pr_i \tag{2}$$

Se calcula el promedio de los resultados del cálculo de la formula establecida para la arquitectura; en la simulación dio como resultado un promedio de 86.50% de aceptación en el sistema.

3.1.2 Algoritmo de seguridad para la transferencia de monedas virtuales

En los estudios realizados de acuerdo con un modelo de transacción de criptomonedas, el manejo de las monedas digitales lo realizaron los usuarios; el proceso de las aplicaciones para encriptar las transacciones ayudó a los usuarios tener confiabilidad en el sistema.

Propusimos el siguiente algoritmo en el proceso de transferencia en el comercio de monedas virtuales, mediante este algoritmo, se proporciona una gestión de transferencia con un modelo de autenticación; en la Fig. 5 se presentan los pasos del algoritmo propuesto realizado en técnicas de diagrama de flujo.

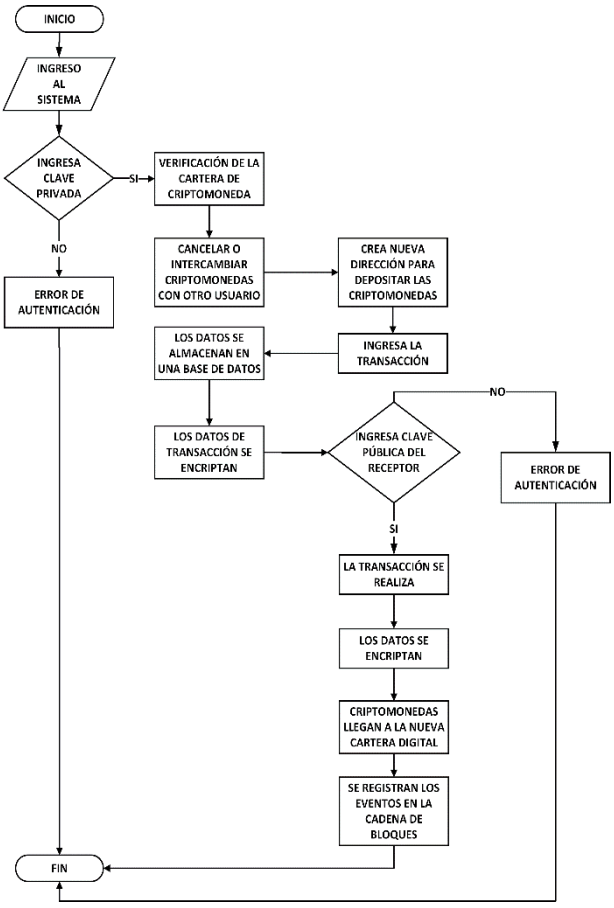


Fig. 5. Algoritmo de seguridad para la transferencia de monedas digitales

En este algoritmo se presenta un modelo de autenticación para el ingreso a la aplicación para la visualización de la cartera de criptomonedas; el sistema valida con una clave privada de acceso a la cartera, de acuerdo con el monto en el monedero digital se realizaron las trasferencias o intercambio de monedas virtuales; se proporcionaron los datos del usuario y el monto a transferir para almacenarlos y encriptarlos antes de enviarlos, la información del usuario se registra en la base de datos; el sistema solicita la clave publica del usuario receptor para realizar la transacción, si las claves proporcionadas son las correctas, la transacción se realizar con normalidad con los datos encriptados a través de la red de cadena de bloques; luego de que la transacción se realice con éxito, los movimientos fueron almacenados en un sistema de registro o libro contable electrónico en la red de cadena de bloques.

El fundamento matemático para el algoritmo esta expresado en la formula (3):

$$C_{ALG} = \left(\frac{\sqrt{Cr * nUser} + PromT}{TotalT} \right)^{\frac{1}{Tsuccess}} * 100\% \quad (3)$$

Aquí:

- Cr es la cantidad de criptomonedas que el usuario utiliza en la transacción.
- nUser es la cantidad de usuarios que se presentan en el sistema de intercambio.
- TotalT es la cantidad de transacciones en el sistema.
- PromT es el promedio de transacciones que se calcula representada en la formula (4)

$$PromT = \frac{TSuccess}{TSuccess + TFail} \quad (4)$$

En la formula (3) se calcula la carga del sistema de acuerdo con las transacciones realizadas en el algoritmo propuesto.

Para determinar la carga del sistema de intercambio de monedas digitales se identificaron las entradas de los usuarios al sistema; en la simulación se realizaron con valores aleatorios, de acuerdo con las transacciones realizadas por los usuarios y el número de monedas virtuales usadas en la transferencia o intercambio; para la simulación se usaron los valores para el usuario que están entre 10 a 150 usuarios que ingresan al sistema con la clave privada; número de criptomonedas que van desde 100 a 1800 unidades de monedas virtuales; total de transferencias que se dividen entre las transacciones realizadas con éxito que van desde 500 a 1000 y transferencias erróneas que van desde 200 a 800; con el fin de determinar la carga de interacciones que el sistema presenta de acuerdo con los usuarios conectados en el sistema.

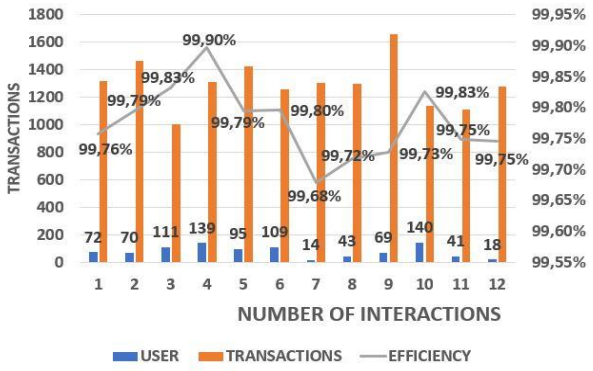


Fig. 6. Análisis de la efectividad del algoritmo de seguridad para la transferencia de monedas digitales

En la simulación de la Fig. 6 se presentan doce escenarios de la interacción de acuerdo con el algoritmo para el intercambio de criptomonedas; en el primer escenario

se visualizó una interacción de 72 usuarios que realizaron el intercambio de monedas, el total de monedas virtuales intercambiadas en el sistema fueron 1253 unidades y con una eficiencia de 99.76%; para el cuarto escenario se realizaron un intercambio de 1682 criptomonedas, los usuarios que interactuaron fueron 139 y con una eficiencia de 99.90%; en el onceavo escenario se intercambiaron un total de 1676 monedas virtuales, los usuarios que realizaron el intercambio fueron 41 con una eficiencia de 99.75%.

Como resultado de las simulaciones realizadas, se determinó un sistema robusto de acuerdo con la media de efectividad con un total de 99.77% de efectividad en el intercambio de monedas virtuales.

3.1.3 Estructura lógica de almacenamiento de datos.

Nosotros propusimos una estructura lógica para el almacenamiento de los registros en el sistema propuesto; esta estructura ayudo a los usuarios que mantienen un intercambio de monedas virtuales con otros usuarios, registrar los movimientos que se realizan durante su transacción; mediante la estructura lógica se muestran las relaciones de las tables que interactúan con el sistema.

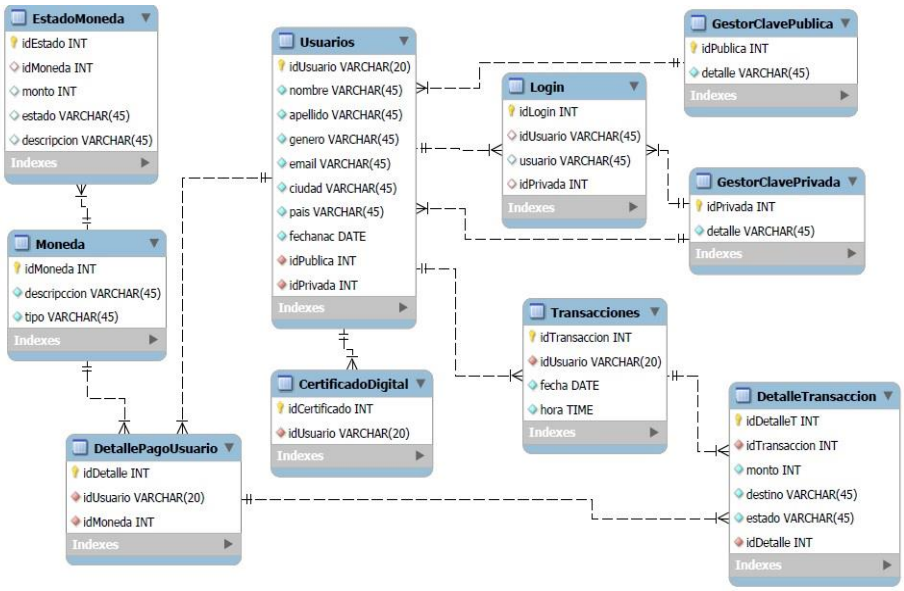


Fig. 7. Estructura de almacenamiento de datos

En la Fig. 7 se muestra el grafico de la estructura propuesta por nosotros; las tablas creadas contienen información de las transacciones y las relaciones entre ellas; la tabla usuario contiene el registro de todos los usuarios que interactúan en el sistema propuesto; la tabla login contiene el listado de usuarios y está conectada con la tabla de gestor de claves privada; la tabla de gestor de claves publica contiene el registro de las claves publicas ya usadas en el sistema para tener mejor respuesta al volver a realizar la transacción; el gestor de clave privada contiene todas la claves de la cartera de

monedas virtuales de los usuarios para acceder al sistema; la tabla transacciones contiene el registro de las transacciones realizadas y se conecta con la tabla detalle de transacciones que contienen el detalle de las transacciones realizadas por los usuarios, contiene el monto trasferido, la fecha en que se realizó y el método de pago; la tabla moneda contiene el registro de las monedas de los usuarios y que tipo de moneda virtual usa el usuario para realizar la transacción; la tabla estado de moneda contiene el registro del estado de las monedas virtuales de los usuarios; la tabla certificado digital contienen la clave cifrada de los usuarios que es utilizada para la seguridad de los datos de origen a destino de cada transacción, esta clave es única por lo que no se puede repetir en cada transacción.

El fundamento para medir la estructura de almacenamiento esta expresado en la formula (5):

$$E = 1 - \frac{EntiUs + Atrib}{Transacc * (CertAu + \sqrt{RegDB})} * 100\% \quad (5)$$

Aquí:

- EntiUs es la cantidad de usuarios conectados en el sistema.
- Atrib es la cantidad de atributos registrados en la estructura propuesta.
- Transacc es la cantidad de transacciones que los usuarios realizaron en el sistema.
- CertAu es la cantidad de claves encriptadas utilizadas por los usuarios en el sistema.
- RegDB es la cantidad de registros almacenados en la base de datos de acuerdo con las interacciones de los usuarios.

Para determinar la eficiencia en la que los registros dentro de la estructura son almacenados, se propuso la formula (5); los valores que hemos tomado para el cálculo de la eficiencia fueron de manera aleatoria de acuerdo con los estudios de las transacciones habituales en una empresa; para los usuarios conectados en el sistema el valor va desde los 100 hasta 1500 usuarios; para la cantidad de atributos registrados los valores desde 100 a 1000; la cantidad total de transacciones realizadas por los usuarios con valores de 100 a 1000 transacciones; la cantidad de claves generadas y registradas en la base de datos con un valor de 100 a 700 claves encriptadas y los registros de la base de datos que tienen valores de 200 hasta 1500 de acuerdo con las interacciones de los usuarios conectados.

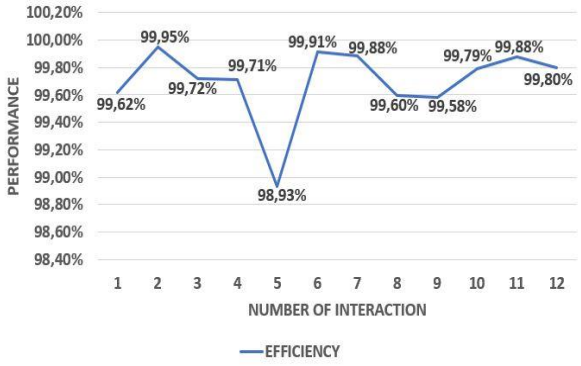


Fig. 8. Análisis de la eficiencia de la estructura de almacenamiento de datos

En la simulación de la Fig. 8 se presentan doce escenarios de la interacción en la estructura de almacenamiento de datos; en el primer escenario se visualizó una interacción de 539 usuarios que se conectaron en el sistema, que realizaron 450 registros en la base de datos y con una eficiencia de 99.62%; en el quinto escenario se mostraron una interacción de 1465 usuarios conectados en el sistema, con un total de 231 registros presentados y con una eficiencia de 98.93%; en el último escenario los usuarios que se conectaron al sistema fueron 383, realizaron un total de 234 transacciones y con una eficiencia de 99.80%.

3.1.4 Diagrama de secuencia del sistema de seguridad de intercambio de monedas virtuales

Propusimos un diagrama de secuencias para visualizan la interacción de los usuarios al momento de realizar una transacción de monedas virtuales en nuestro sistema.

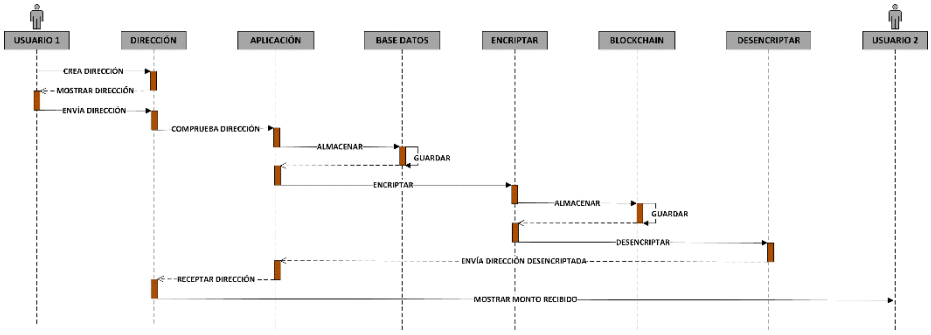


Fig. 9. Estructura de almacenes de datos

En la Fig. 9 se muestra los diferentes actores que interactúan en el diagrama y se detalla el funcionamiento del diagrama; el usuario 1 realizo el proceso de creación de dirección para almacenar las criptomonedas que desea enviar; el monedero virtual

le muestra la nueva dirección creada y es enviada a la aplicación para ser procesada; la aplicación comprueba la dirección recibida y lee los datos del usuario que requiere realizar la transacción; los datos y el monto son almacenados en la base de datos para el registro de los movimientos; los datos son enviados y se realiza el proceso de encriptación, los datos son encapsulados y son enviados a un bloque para el registro público; los datos encriptados se envían a través de la red de acuerdo con la clave publica del receptor escrita en la aplicación para la transacción; el conjunto de datos encriptados llegan al destino y son desencriptados para ser leídos por la aplicación; la aplicación comprueba los datos de origen, la dirección desencriptada es almacenada en el recipiente de criptomonedas del usuario 2; la aplicación le envía un mensaje al usuario 2 acerca del monto transferido del usuario 1; este diagrama realiza métodos de comprobación y almacenamiento de datos desde que se registra la transacción, en el momento en que se envían los datos encriptados y termina en la visualización del monto transferido al remitente.

El fundamento matemático para evaluar el diagrama de secuencia esta expresado en la formula (6):

$$Arrive = \frac{nUser + Transacc}{nApp + nDir} \tag{6}$$

$$PromReg = \frac{RegBD}{\sqrt{RegBC}} \tag{7}$$

$$Losses = \frac{Arrive}{PromReg} * 100\% \tag{8}$$

Aquí:

- nUser es la cantidad de usuarios que interactúan en el modelo de intercambio de criptomonedas.
- Transacc es la cantidad de transacciones verificadas en el sistema.
- nApp es la cantidad de veces que se usó la aplicación en el modelo propuesto.
- nDir es la cantidad de direcciones creadas por los usuarios.
- RegBD es la cantidad de registros almacenados en la base de datos.
- RegBC es la cantidad de registros encriptados almacenados en la cadena de bloques.

Para determinar la perdida en las transacciones que los usuarios realizaron, hemos propuesto la formula (8); se realizó una simulación con valores aleatorios para el cálculo de las perdidas; se utilizaron un rango de usuarios que están desde 100 a 1000 usuarios que realizaron el intercambio; las transacciones que realizaron los usuarios que van desde 100 a 1000 transacciones; el número de veces que el usuario utilizó la aplicación con un rango desde 20 a 100; el número de direcciones creadas por los usuarios con un valor de 30 a 300 ocasiones; la cantidad de registros en la base de datos con un rango de 100 a 1000 y la cantidad de registros en la cadena de bloques con un rango de 100 a 800 registros presentados en el diagrama.

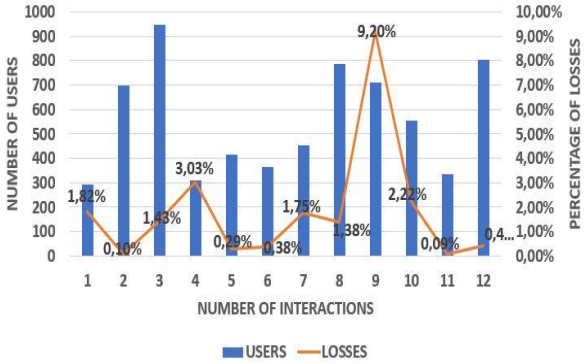


Fig. 10. Análisis de las perdidas en intercambios de monedas virtuales

En la Fig. 10 se mostraron las pérdidas que sufrió el sistema de intercambio, de acuerdo con la perdida de conexión o transacción fallida; en el primer escenario se muestran 292 usuarios que ingresaron al sistema y realizaron 378 transacciones con una pérdida de 1.82%; en el noveno escenario se muestra una interacción de 709 usuarios en el sistema, realizaron 487 transacciones en total con una pérdida de 9.20%, esto debido a un problema con la conexión entre partes; y el ultimo escenario con una interacción de 804 usuarios con una total de 868 transacciones y presentaron una pérdida de 0.41% en la conexión o intercambio de monedas virtuales.

El promedio de perdidas calculada en el sistema es de 1.84% de acuerdo con los datos obtenidos en la simulación realizada.

3.2 Discusión

De acuerdo con los resultados obtenidos por los modelos de seguridad propuesto por nosotros, el análisis de la arquitectura; el sistema de seguridad se manejó de acuerdo con la conexión de los usuarios que interactuaron durante las simulaciones; se aplicaron modelos de transmisión de datos e intercambio de monedas virtuales que proporciono integridad entre los usuarios que realizaron las transferencias.

El algoritmo de seguridad y el diagrama de secuencia proporcionaron una seguridad en el modelo de intercambio propuesto de acuerdo con el modo de transferencia dada; la arquitectura de seguridad y el algoritmo de seguridad mostraron el modo de uso de las aplicación de intercambio y la manera de encriptación de las transacciones antes de ingresar a la cadena de bloque; la arquitectura y la estructura lógica de los datos proporcionaron la manera en cómo los datos son registrados de acuerdo al movimiento de la información propuesta en la arquitectura.

En los análisis que nosotros realizamos, el sistema dependía de la estabilidad en la red por parte de los usuarios; los modelos de transacciones aseguraron el correcto intercambio de monedas virtuales, la confiabilidad en el sistema para los usuarios que lo utilizaron; de acuerdo con la administración de la base de datos, los registros se almacenaron para la oportuna visualización de los usuarios que solicitaron un historial de

movimientos; la seguridad implementada en los resultados permitieron al administrador del modelo tener seguridad en todo el trayecto de la transacción entro los usuarios.

En los modelos propuestos no se determinan el valor monetario de la implementación del sistema; los recursos que el sistema requiera se determinaran de acuerdo con los países que desean adaptar el sistema de monedas virtuales.

En los artículos [1] y [9] se analizó el uso correcto de las monedas virtuales y realizaron una propuesta de recomendaciones para administrar el modelo de intercambio de monedas virtuales; en los artículos [7] y [24] se utilizaron modelos de arquitectura para la seguridad de las transacciones en la cadena de bloque; en los artículos [15] y [27] se propusieron modelos de gestión de monedas virtuales en sistemas descentralizados para la administración de intercambios de monedas digitales; en los artículos [13] y [22] se presentaron modelos de pérdidas de transacciones y propusieron un modelo de almacenamiento de monedas virtuales para proporcionar seguridad en los modelos.

Los modelos de seguridad para el intercambio de monedas virtuales, es necesario una implementación de un sistema de gestor de usuarios para la rapidez de las transacciones; de esta manera los modelos de gestión de intercambio facilitarían una agilidad y confiabilidad en los sistemas de gestión comercial electrónico.

Monitorear la red de cadena de bloques ante un posible ataque y mitigarlos de una manera eficaz; el estudio de los modelos de negocio electrónico para la evaluación de los puntos más vulnerables proporcionó estrategias para el control de transacciones.

4 Conclusiones

Se concluyó que el algoritmo de seguridad que hemos propuesto para un manejo exitoso del comercio de monedas virtuales proporciona resultados óptimos ante el sistema descentralizado; de acuerdo con las simulaciones realizadas en el sistema se obtuvieron valores promedios de 99.70% en las transacciones realizadas durante la simulación.

Con el diagrama de secuencias del modelo de intercambio, proporcionan un historial de transacción y resultados de las pérdidas que se presentaron en todo el sistema; los datos obtenidos en las simulaciones dependieron de la conexión de los usuarios; las perdidas proporcionadas en el sistema fueron de 1.84% de acuerdo con las interacciones realizadas en las pruebas.

Los registros almacenados en la estructura lógica proporcionan a los usuarios un registro ordenado de las transacciones que se realizan; los registros que se almacenan en la cadena de bloque de acuerdo con los códigos de selección lograron ser de ayuda a los usuarios de minería en la red de cadena de bloque; la estructura lógica proporciono un mejor manejo de los registros en todo el sistema.

Referencias

1. Rustem, M., Sergey, K., Anastasia, K., Muhamat, G., Venera, G., Aleksey, K.: Problems of criminal responsibility for illegal circulation of cryptocurrency. Proc. - Int. Conf. Dev.

eSystems Eng. DeSE. October-20, 996–999 (2019). https://doi.org/10.1109/DeSE.2019.00185
2. Takahashi, H., Lakhani, U.: Multiple layered security analyses method for cryptocurrency exchange servicers. 2019 IEEE 8th Glob. Conf. Consum. Electron. GCCE 2019. 71–73 (2019). https://doi.org/10.1109/GCCE46687.2019.9015245
3. Liang, J., Li, L., Chen, W., Zeng, D.: Towards an Understanding of Cryptocurrency : A Comparative Analysis of Cryptocurrency , Foreign Exchange , and Stock. 2019–2021 (2019)
4. He, X., Lin, J., Li, K., Chen, X.: A Novel Cryptocurrency Wallet Management Scheme Based on Decentralized Multi-Constrained Derangement. IEEE Access. 7, 185250–185263 (2019). https://doi.org/10.1109/ACCESS.2019.2961183
5. Rahouti, M., Xiong, K., Ghani, N.: Bitcoin Concepts , Threats , and Machine-Learning Security Solutions. IEEE Access. 6, 67189–67205 (2018). https://doi.org/10.1109/ACCESS.2018.2874539
6. Yuan, Y., Wang, F.Y.: Blockchain and Cryptocurrencies: Model, Techniques, and Applications. IEEE Trans. Syst. Man, Cybern. Syst. 48, 1421–1428 (2018). https://doi.org/10.1109/TSMC.2018.2854904
7. Toapanta Toapanta, S.M., Mafla Gallegos, L.E., Guaman Villalta, M.G., Mora Saltos, N.S.: A hyperledger technology approach to mitigate the risks of the database in foreign trade management. In: Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020. pp. 313–319 (2020)
8. Baek, H., Oh, J., Kim, C.Y., Lee, K., Laundering, A.M.: A Model for Detecting Cryptocurrency Transactions with Discernible Purpose. 713–717 (2019)
9. Moisés Toapanta Toapanta, S., Monserrate Moreira Gamboa, D., Enrique Mafla Gallegos, L.: Analysis of the blockchain for adoption in electronic commerce management in Ecuador. Adv. Sci. Technol. Eng. Syst. 5, 762–768 (2020). https://doi.org/10.25046/aj050295
10. Herskind L., Katsikouli P., Dragoni N.: Privacy and Cryptocurrencies - A Systematic Literature Review. IEEE Access. 8, 54044–54059 (2020). https://doi.org/10.1109/ACCESS.2020.2980950
11. Sukharev P. V., Silnov D. S.: Asynchronous Mining of Ethereum Cryptocurrency. Proc. 2018 Int. Conf. ' 'Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2018. 731–735 (2018). https://doi.org/10.1109/ITMQIS.2018.8524929
12. Nayak A., Dutta K.: Blockchain: The perfect data protection tool. Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017. 2018-Janua. 1–3 (2018). https://doi.org/10.1109/I2C2.2017.8321932
13. Imtiaz M. A., Starobinski D., Trachtenberg A., Younis N.: Churn in the bitcoin network: Characterization and impact. ICBC 2019 - IEEE Int. Conf. Blockchain Cryptocurrency. 431–439 (2019). https://doi.org/10.1109/BLOC.2019.8751297
14. Almukaynizi M., Paliath V., Shah M., Shakarian P.: Finding cryptocurrency attack indicators using temporal logic and darkweb data. 2018 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2018. 91–93 (2018). https://doi.org/10.1109/ISI.2018.8587361
15. Wu Y., Luo A., Xu D.: Forensic analysis of bitcoin transactions. 2019 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2019. 167–169 (2019). https://doi.org/10.1109/ISI.2019.8823498
16. Liu X., Wang Z., Jin C., Li F., Li G.: A Blockchain-Based Medical Data Sharing and Protection Scheme. IEEE Access. 7, 118943–118953 (2019). https://doi.org/10.1109/access.2019.2937685
17. Monrat A. A., Schelen O., Andersson K.: A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. IEEE Access. 7, 117134–117151 (2019). https://doi.org/10.1109/access.2019.2936094

18. Zollner S., Choo K. K. R., Le-Khac N. A.: An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems. IEEE Access. 7, 158250–158263 (2019). https://doi.org/10.1109/ACCESS.2019.2948774
19. Toapanta Toapanta S. M., Sotomayor Balladares A. A, Huilcapi Subia D. F., Mafla Gallegos L. E.: Prototype of a security model to mitigate risks in the management of electronic money in Ecuador. Proc. 3rd World Conf. Smart Trends Syst. Secur. Sustain. WorldS4 2019. 87–93 (2019). https://doi.org/10.1109/WorldS4.2019.8903959
20. Kim H, Kim S. H., Hwang J. Y., Seo C.: Efficient privacy-preserving machine learning for blockchain network. IEEE Access. 7, 136481–136495 (2019). https://doi.org/10.1109/ACCESS.2019.2940052
21. Cheng S., Lin S. J.: Mining strategies for completing the longest blockchain. IEEE Access. 7, 173935–173943 (2019). https://doi.org/10.1109/ACCESS.2019.2956168
22. Debe M., Salah K., Ur Rehman M. H., Svetinovic D.: Monetization of services provided by public fog nodes using blockchain and smart contracts. IEEE Access. 8, 20118–20128 (2020). https://doi.org/10.1109/ACCESS.2020.2968573
23. Hafid A., Hafid A. S., Samih M.: New mathematical model to analyze security of sharding-based blockchain protocols. IEEE Access. 7, 185447–185457 (2019). https://doi.org/10.1109/ACCESS.2019.2961065
24. Lugan S., Desbordes P., Brion E., Ramos Tormo L. X., Legay A., Macq B.:Secure Architectures Implementing Trusted Coalitions for Blockchained Distributed Learning (TCLearn). IEEE Access. 7, 181789–181799 (2019). https://doi.org/10.1109/ACCESS.2019.2959220
25. Zhang S., Lee J. H.: Smart Contract-Based Secure Model for Miner Registration and Block Validation. IEEE Access. 7, 132087–132094 (2019). https://doi.org/10.1109/ACCESS.2019.2940551
26. Tsoulias K., Palaiokrassas G., Fragkos G., Member G. S., Litke A.: A Graph Model Based Blockchain Implementation for Increasing Performance and Security in Decentralized Ledger Systems. IEEE Access. 8 (2020). https://doi.org/10.1109/ACCESS.2020.3006383
27. He S., et al.: A Social-Network-Based Cryptocurrency Wallet-Management Scheme. IEEE Access. 6, 7654–7663 (2018). https://doi.org/10.1109/ACCESS.2018.2799385
28. Gao Y. L., Chen X. B., Chen Y. L., Sun Y., Niu X. X., Yang Y. X.: A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain. IEEE Access. 6, Part Ii. 27205–27213 (2018). https://doi.org/10.1109/ACCESS.2018.2827203
29. Fujimoto S., Higashikado Y, Tekeuchi T.: ConnectionChain the Secure Interworking of Blockchains. 2019 Sixth Int. Conf. Internet Things Syst. Manag. Secur., 514–518 (2019). https://doi.org/10.1109/IOTSMS48152.2019.8939267
30. Hu Y., Lee T, Lam T.: A Risk Redistribution Standard for Practical Cryptocurrency Payment in 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). 89–99 (2019). https://doi.org/10.1109/DAPPCON.2019.00020
31. Farheen S.: Blockchain based Data Security for Financial Transaction System. 2020 4th Int. Conf. Intell. Comput. Control Syst., no. Iciccs. 829–833 (2020). https://doi.org/10.1109/ICICCS48265.2020.9121108
32. Liang J., Li L., Zeng D., Zhao Y.: Correlation-based Dynamics and Systemic Risk Measures in the Cryptocurrency Market. 2018 IEEE Int. Conf. Intell. Secur. Informatics. April. 43–48 (2018). https://doi.org/10.1109/ISI.2018.8587395
33. Ichsani Y., Deyani A., Bahaweres B.: The Cryptocurrency Simulation using Elliptic Curve Cryptography Algorithm in Mining Process from Normal , Failed , and Fake Bitcoin Transactions. *2019 7th Int. Conf. Cyber IT Serv. Manag.* 7, 1–8 (2019). https://doi.org/10.1109/CITSM47753.2019.8965370.

34. Coleman R. C.: FBI/IC3 2015. Fed. Bur. Investig. 233 (2015)
35. Internet Crime Complaint Center. FBI 2019 Internet Crime Report. Fed. Bur. Investig. - Internet Crime Complain. Cent. 1–28 (2019) [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf.