FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso

PARA OPTAR EL TÍTULO PROFESIONAL

DE INGENIERO DE SISTEMAS

Autor

Bach. Lopez Vallejos Rober Yubelder
ORCID: https://orcid.org/0000-0002-2079-8510

Asesor

Dr. Tuesta Monteza Víctor Alexci
ORCID: https://orcid.org/0000-0002-5913-990X

Línea de Investigación

Infraestructura, Tecnología y Medioambiente

Pimentel – Perú

IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN ASOCIANDO USUARIO Y DISPOSITIVO PARA MEJORAR LA SEGURIDAD EN LA AUTENTICACIÓN DE CREDENCIALES DE ACCESO

Aprobación del jurado

DR. ATALAYA URRUTIA CARLOS WILLIAM

Presidente del Jurado de Tesis

DR. VASQUEZ LEYVA OLIVER

Secretario del Jurado de Tesis

MG. ARCILA DIAZ JUAN CARLOS

Vocal del Jurado de Tesis

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la DECLARACIÓN JURADA, soy egresado (s) **Lopez Vallejos Rober Yubelder,** del Programa de Estudios de **Ingeniería de Sistemas** de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autor del trabajo titulado:

IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN ASOCIANDO USUARIO Y DISPOSITIVO PARA MEJORAR LA SEGURIDAD EN LA AUTENTICACIÓN DE CREDENCIALES DE ACCESO

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y auténtico.

En virtud de lo antes mencionado, firman:

LOPEZ VALLEJOS ROBER YUBELDER	DNI: 75860716	

Pimentel, 30 de marzo de 2024.

Dedicatoria

El presente trabajo de investigación
dedico a mis padres Roberto Lopez Saucedo,
María Esther Vallejos Núñez y hermanos
porque se convirtieron en mi soporte principal
en todo este camino universitario de cinco años.
Gracias a su apoyo fue posible
completar uno de mis más grandes anhelos de vida
y dedico este logro a mi hermano Nelver en el cielo.

Agradecimientos

Agradezco a Dios por brindarme
la fortaleza y capacidad para enfrentar
obstáculos en los diferentes ámbitos de la vida,
Gracias a mi familia por brindarme apoyo
para lograr mis metas,
gracias a mis amigos por hacer que esta
experiencia universitaria sea inolvidable,
gracias a los profesores por compartir
su sabiduría y conocimiento.

índice

Índice de Tablas, figuras y fórmulas:

Índice de Figuras:

RESUMEN

Los métodos de autenticación actualmente presentan vulnerabilidades para identificar a un usuario verídico, las modalidades de fishing e ingeniería social son los más comunes para robar datos de usuario, contraseña y hackear cuentas en plataformas del ciberespacio. Debido a esto para mejorar la seguridad de autenticación es necesario implementar caracteristicas que permitan asociar los datos del usuario con sus dispositivos, por lo que se propone en la presente investigación la incorporación de nuevas caracteristicas para los formularios estándar de login, donde además de usuario y contraseña se necesitaría de la dirección Mac del dispositivo asociado a la cuenta para lograr acceder. La metodología permite que la información por seguridad y transparencia se registre en una blockchain de manera cifrada, la cadena de bloques brindará la ventaja de que cualquier alteración en las credenciales registradas son visibles causando suspensión de acceso hasta volver a identificar al usuario verídico a través de biometría por intermedio de la huella dactilar. La incorporación de estas caracteristicas permitirá que los usuarios obtengan un control total de los dispositivos que tienen permitido acceder a sus cuentas. La implementación de estas caracteristicas logró un resultado en usabilidad de 9.67 de una escala de 0/10, una tasa de éxito de sesión del 92% y un 98.67% de efectividad para autentificar a un usuario verídico y el dispositivo asociado a la cuenta. Por lo que se concluye que asociar las caracteristicas de usuario, contraseña y dirección Mac para una sola cuenta incrementa la seguridad del 44% al 96% en autenticación de credenciales.

Palabras clave:

Cifrado de credenciales, Exploit, Login, Usuario Verídico, Dirección Mac.

Abstract

The authentication methods currently present vulnerabilities to identify a real user, fishing and social engineering are the most common methods to steal user data, passwords and hack accounts in cyberspace platforms. Due to this, to improve authentication security it is necessary to implement features that allow associating user data with their devices, so it is proposed in this research the incorporation of new features for standard login forms, where in addition to username and password, the Mac address of the device associated with the account would be needed to gain access. The methodology allows the information to be recorded in an encrypted blockchain for security and transparency, The blockchain will provide the advantage that any alteration in the registered credentials are visible causing suspension of access until the true user is re-identified through biometrics by means of the fingerprint. The incorporation of these features will allow users to gain full control of the devices that are allowed to access their accounts. The implementation of these features achieved a usability score of 9.67 on a scale of 0/10, a session success rate of 92% and 98.67% effectiveness in authenticating a real user and the device associated with the account. Therefore, it is concluded that associating the user, password and Mac address characteristics for a single account increases security from 44% to 96% in credential authentication.

Keywords: Credential Encryption, Exploit, Login, User Veridical, Mac Address.

I. INTRODUCCIÓN

1.1. Realidad problemática

La digitalización del mundo real es inminente, más procesos están migrando a medios digitales y la identificación de un usuario en internet será fundamental para evitar suplantación de identidad, porque cada vez es más difícil detectar si ciertos procesos realmente son ejecutados con el permiso y razonamiento de un ser humano, en este contexto es necesario implementar medidas de autenticación y seguridad.

En una publicación realizada por la Oficina de Seguridad del Internauta, explica una forma que existe para vulnerar la autenticación de doble factor o autenticación en dos pasos, una técnica denominada SIM Swapping, que permite a un atacante utilizar los datos de la víctima para obtener una nueva tarjeta SIM con el mismo número, para posteriormente obtener los códigos de verificación [1]. Métodos de ingeniería social, fuerza bruta y diccionario de datos representan la mayor vulnerabilidad para las contraseñas en las organizaciones a nivel mundial [2]. Según reportes realizados por la empresa Kaspersky, el año 2020 en relación 2019 se identificó un incremento del 34% al 54% en el robo de cuentas bancarias [3].

La BBC publicó un artículo en 2019 donde se reportaron 223,163 casos de robos de identidad a través de internet, representando un incremento promedio del 5% anual desde el año 2015 [4] En un reporte anual realizado por la agencia We Are Social y Hootsuite sobre el uso de redes sociales y tendencias digitales del 2021 publicaron que: 1.3 millones de nuevos usuarios se unieron a redes sociales, con un promedio de 15 usuarios nuevos por segundo, representando un incremento interanual de más del 13% respecto al año anterior, estadísticamente más del 53% de la población mundial que utiliza las redes sociales [5].

Un estudio realizado por la empresa administradora de contraseñas NordPass, reveló que desde el inicio de la pandemia un usuario promedio incrementó su cantidad de contraseñas en un 25%, obteniendo un promedio de 100 contraseñas por usuario [6] Considerando todas las cuentas por usuario, el 25% reutiliza los datos de usuario y contraseña [7].

La empresa de servicios de TI Xentic publicó un informe que destacaba vulnerabilidades para un grupo de dispositivos que utilizaban el nuevo estándar de autenticación y seguridad de Wi-Fi WPA3, donde los atacantes que estaban dentro del alcance de la red wifi obtenían información confidencial de los usuarios como contraseñas, correos y números de tarjetas de crédito [8]. Reportes publicados por Consumer Sentinel Data Book de la FTC en 2020 registraron 1.4 millones de informes de robo de identidad en internet representando un incremento del 46% en reportes de fraudes respecto al año 2019 [9].

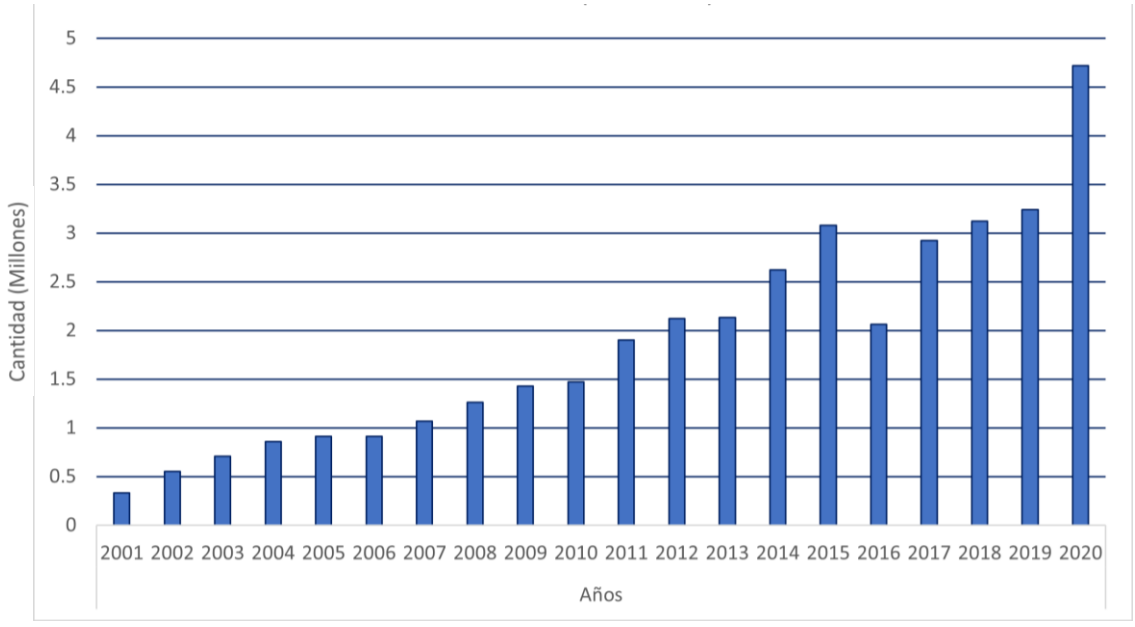


Fig. 1. Cantidad de reportes de fraudes, robo de identidad y otros por año.

Nota: Fuente Consumer Sentinel Data Book de la (FTC) Agencia encargada de promover los derechos de los consumidores.

Anteriores investigadores han propuesto alternativas de solución a casos similares, en 2020 un esquema para el intercambio de datos de usuarios u organizaciones con proveedores de servicios que utiliza la tecnología de cadena de bloques y consta de un protocolo de intercambio de información obteniendo un resultado del 100% de seguridad en las 150 pruebas realizadas con el método de emparejamiento bilineal [10].

La autenticación distribuida y la gestión de claves alcanza características de escalabilidad del sistema utilizando la plataforma de Ethereum utilizando el método de control FairAccess [11]. La optimización del transporte de datos utilizando cadena de bloques evita la sobrecarga de datos con una capacidad de 10Gbps y una baja latencia [12]. Las operaciones XOR en el modelo Real-or-Random (RoR) permite una autenticación triple para la seguridad de los datos en proceso de transporte [13]. El enfoque criptográfico basado en atributos permite un control de acceso detallado sin comprometer la privacidad de las políticas de acceso además de la ejecución en paralelo con otros protocolos [14]. EL algoritmo de cifrado AES-CBC obtuvo una ejecución más rápida en comparación al original utilizando blockchain un tiempo específico de 2,5941 segundos en compasión a 4.3240 del algoritmo original un incremento de velocidad de 40,2% en tiempo de ejecución [15].

Método Voice-CD obtiene una tasa de error es del 5,3% en el Intercambio de claves autenticadas por contraseña de dos factores [16]. WPA3 obtiene tasa de éxito del 99,5 % en las autenticaciones para solicitar las solicitudes por Mac address de dispositivo [17]. Alrededor del 90 % de las solicitudes de BACnet generan respuestas en ataques de denegación de servicio donde la tecnología Blockchain permitiría resolver la centralización de la nube en IoT en los hogares inteligentes [18]. La adopción de la tecnología blockchain en los gobiernos tiene un impacto significativo y positivo convirtiendo a los países principalmente en la transparencia de los datos [19].

La autenticación basada en tokens en los vehículos obtuvo una comunicación efectiva del 89,07 % con un tiempo de cálculo de 0,7 segundos [20]. En 2023 un esquema desarrollado para el intercambio de datos con blockchain logró una capacidad respuesta de 1000 transacciones cada 9 segundos [21]. Con un total de 85 295 datos de pruebas fraccionados en relación 70% y 30%, se logró obtener un resultado de 87,6% en precisión, 83.5% de recall, 85.5% de F1-score en clasificación de datos [22]. Modelos de aprendizaje automático utilizando blockchain obtienen una desviación estándar de 7,8 segundos en tiempo de ejecución [23].

Un esquema para el intercambio de datos financieros que utiliza la tecnología de cadena de bloques y consta de un protocolo de intercambio de información donde las bases de datos son cifradas para evitar la manipulación, a través de cifrados proxys con generación de claves distribuidas y el cifrado de datos confidenciales incrementado la seguridad en el proceso de intercambio de datos entre entidades financieras [24].

Similar es el trabajo que implementó una arquitectura para compartir información de forma segura entre los propietarios de los datos y la nube, utiliza el método AON para fragmentar y dispersar la información en diferentes servidores, está arquitectura permite reducir la amenaza del robo de información evitando que los datos se almacenan en un solo servidor en la nube [25].

En otra investigación se implementó el sistema SECUREDL, permite que las organizaciones proteger datos confidenciales y cierto tipo de información en procesos de entrenamiento para inteligencia artificial, el sistema permite validar cada petición de acceso con ciertas normas que previamente fueron establecidos por los propietarios originales del dataset, además de extraer la información sensible que puede afectar a los usuarios que generaron la data, el sistema SECURED fue diseñado principalmente para la construcción de modelos de inteligencia artificial,

utilizando en modelos de bases de datos estructurados y no estructurados [26]. Las bases de datos centralizadas que almacenan información de diferentes fuentes son susceptibles a sufrir alteraciones [27].

La investigación Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System, abarcando la problemática del transporte de datos desde los dispositivos P2P hasta los proveedores de servicio los cuales son los encargados de realizar la validación a partir de votos de los nodos de red, con una metodología de pruebas anónimas para la distribución de claves con emparejamientos bilineales y ECC, que admite la autenticación mutua entre un medidor inteligente y un proveedor de servicios, logrando como resultado el desarrollo del protocolo DBACP-IoTSG para el control de acceso basado en Blockchain en un sistema de red inteligente para los IoT en el proceso de envió de datos desde los dispositivos hasta los proveedores de servicios, donde concluyen que El modelo DBACP-IoTSG propuesto funciona sin involucrar a un tercero de confianza. Los bloques se verifican mediante un proceso de selección de líderes de forma segura en la red P2P [28].

Este problema recae en el proceso de autentificación, porque debido al exceso de contraseñas de cada usuario las credenciales de acceso pasan a ser fáciles de recordar o tienen que ser anotadas en texto plano, ocasionando una brecha de seguridad que es aprovechado por personas inescrupulosas, que utilizan esta información para falsificar la identidad digital de una persona en internet y ejecutar acciones sin autorización del usuario verdadero.

La contribución de la presente propuesta de investigación pretende desarrollar una nueva alternativa para la autenticación de credenciales de acceso implementando una estructura blockchain para la seguridad y autenticidad de los datos, el proceso consiste asociar las credenciales del usuario a sus dispositivos, formando un proceso de verificación doble que solo ciertos dispositivos tendrán acceso sin importar si el usuario y contraseña de la cuenta es filtrado por alguna modalidad de hacking.

1.2. Formulación del problema

¿De qué manera la tecnología Blockchain ayudará a mejorar la seguridad en la autenticación de credenciales de acceso en internet?

1.3. Hipótesis

Si se implementa la tecnología Blockchain para asociar usuario y dispositivo se logrará una autenticación de datos más segura en los accesos de cuentas de usuarios.

1.4. Objetivos.

Objetivo general

a) Implementar la tecnología Blockchain para mejorar la seguridad de autenticación asociando usuario y dispositivo.

Objetivos específicos

a) Analizar proyectos que utilizan tecnología blockchain para obtener características funcionales y esenciales de la tecnología Blockchain.
b) Diseñar una estructura blockchain considerando la compatibilidad de características según los proyectos evaluados.
c) Implementar la estructura que permita obtener resultados de efectividad en la autenticación de las credenciales de acceso.
d) Realizar pruebas del proyecto y corregir errores.

1.5. Teorías relacionadas al tema:

1.1.1. Internet: Internet funciona debido al estándar abierto de interconectividad entre redes donde cualquiera puede ofrecer servicios sin permisos de una autoridad central [29].

Es un conjunto de redes de alcance global descentralizadas e interconectadas, que permite el intercambio y comunicación de información a través de los protocolos TCP/IP.

1.1.1.1. Protocolos: El transporte de información por la red necesita de la interacción de ciertos procesos, el protocolo de internet (TCP/IP) está conformado por un conjunto de protocolos como: Capa de aplicación misma donde el usuario final interactúa, posteriormente a la capa de transporte de UDP y TCP, luego la capa de red la cual incluye la interfaz de red, mismas que son apoyadas por la red física [30].

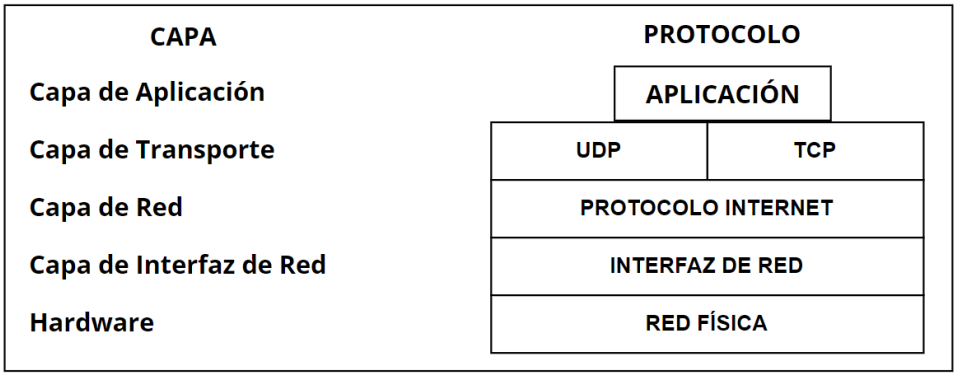


Fig. 2. Capas de aplicación del conjunto de protocolos en internet.

Nota: Fuente IBM empresa principal de desarrollo de redes para internet.

Los protocolos son un conjunto de reglas que permiten la conexión entre dispositivos a través de la red global. Los protocolos más importantes son TCP/IP [31]. El modelo OSI organiza la familia de protocolos en capas de red como las siguientes:

1.1.1.2. Protocolos de capa 1 - Capa Física:

A. **USB:** Siglas de Universal Serial Bus es un estándar de hardware para la transferencia de datos.

B. **Ethernet:** Siglas de Ethernet Physical Layer, utiliza señales eléctricas para la transmisión de datos y es un estándar de comunicación para redes de área local (LAN).

C. **DSL:** Siglas de Digital subscriber line, utiliza cobre característico que permite ser una alternativa a la fibra óptica para la transmisión de datos.

D. **Etherloop:** Refiere a la combinación de tecnologías de Ethernet y DSL.

E. **Infrared:** Utiliza la radiación infrarroja para la comunicación inalámbrica utilizados en dispositivos como televisores, etc.

F. **Frame Relay:** Utilizado para la conmutación de paquetes entre dos dispositivos en redes empresariales.

G. **SDH:** Utiliza la jerarquía digital síncrona combinando canales de baja velocidad a medios de alta velocidad.

H. **SONET:** Red óptica sincronizada es el estándar para la transmisión en alta velocidad a través de la fibra óptica.

1.1.1.3. Protocolos de capa 2 - Enlace de Datos:

A. **FDDI:** Utiliza la topología en anillo y una interfaz de distribución de datos en fibra para redes LAN.

B. **HDLC:** Utilizado para proporcionar un enlace de comunicación seguro entre dos dispositivos en redes locales y amplias.

C. **LAPD:** Utilizada por la red de telefonía celular GSM.

D. **PPP:** Soporta otros protocolos de red como TCP/IP, para conexiones punto a punto entre routers o dispositivos de red.

E. **STP:** Protocolo del árbol esparcido en cual previene la saturación y

garantiza la redundancia de la red permitiendo siempre el flujo de datos.

F. VTP VLAN: Permite que los switches de la red se comuniquen y sincronicen.

G. MPLS: Permite la fragmentación de paquetes para ser enviados a alta velocidad en la red de telecomunicaciones.

1.1.1.4. Protocolos de capa 3 - Red:

A. ARP: Resuelve de direcciones IP de internet en las direcciones físicas de las redes como las Mac Address.

B. **BGP:** Protocolo de frontera para conectar sistemas autónomos evitando la saturación de red.

C. **ICMP:** Proporcionada datos del estado de la red con acciones como ping, mensajes de entregas de paquetes, etc.

D. **IPv4:** Permite identificar direcciones IP de 32 bits, cada IP contiene cuatro octetos separados por puntos, gradualmente reemplazado por IPv6.

E. **IPv6:** Permite mayor seguridad y espacio para las direcciones IP de 128 bits, con cifrado de extremo a extremo.

F. **OSPF:** Utiliza un algoritmo para determinar la trayectoria más corta a partir de la topología de red compartida por los routers.

1.1.1.5. Protocolos de capa 4 - Transporte:

A. **SPX:** Permite la entrega de paquetes en orden utilizado para la transmisión de audio y video en tiempo real, gradualmente reemplazado por UDP.

B. **TCP:** Permite la transmisión de paquetes hasta que se complete correctamente, utilizado en transferencia de archivos, etc.

C. **UDP:** Permite enviar información sin conexión y sin garantía de entrega, utilizado en servicios donde la pérdida de datos no es de impacto.

D. **iSCSI:** Utilizado para la comunicación de dispositivos de almacenamiento.

E. **DCCP:** Proporciona control de congestión, se ajusta según la cantidad de paquetes, utilizado para videoconferencias.

1.1.1.6. Protocolos de capa 5 - Sesión:

A. **SMB:** Utiliza la capa de sesión para establecer conexión, utilizado por las impresoras.

B. **RPC:** Utilizado en sistemas distribuidos de cliente servidor como las bases de datos y aplicaciones web.

C. **SDP:** Utilizado para sesiones multimedia, con característica de resolución, tasa de bits y codificación.

D. **SMPP:** Utilizado para el envío de mensajes de texto (SMS) a través de aplicaciones en dispositivos móviles.

1.1.1.7. Protocolos de capa 6 - Presentación:

A. **TLS:** Garantiza un transporte de información protegido de manipulación donde solo las partes interesadas logren leer la información.

B. **SSL:** Es una capa adicional de seguridad para el protocolo HTTP.

C. **MIME:** En conjunto con el protocolo SMTP permite la transferencia de mensajes multimedia en los correos electrónicos.

1.1.1.8. Protocolos de capa 7 - Aplicación:

A. **FTP:** Permite la transferencia de archivos, utiliza comandos como “put” o “get” además de codificación de caracteres.

B. **DHCP:** Permite la asignación dinámica de direcciones IP, máscaras de subred, permitiendo una mejor administración de la red.

C. **DNS:** Traduce los nombres de los dominios en direcciones IP y viceversa, evitando que los usuarios ingresen direcciones IP numéricas para la conexión con los servidores.

D. **HTTP:** Protocolo de transferencia de hipertexto, utilizado por el proceso principal de la Word Wide Web para la transferencia de datos.

E. **HTTPS:** Utiliza SSL/TLS para cifrar los datos transmitidos entre cliente y servidor para protegerse de cualquier intercepción o manipulación por terceros en el proceso de transporte.

F. **POP3:** El usuario al proporcionar credenciales de sesión puede acceder y descargar mensajes del correo electrónico.

G. **SMTP:** Permite la transmisión de correo electrónico, que en conjunto con la capa POP permite el acceso a los correos desde cualquier parte del mundo.

1.1.2. Internet de las cosas: Es la red de objetos físicos que incorporan sensores, software y otras tecnologías para intercambiar información a través de internet, con una proyección de 22 mil millones de dispositivos interconectados para el 2025 desde objetos domésticos hasta herramientas industriales [32].

A. Dispositivos: Un dispositivo de IoT tiene características como sensores, software, etc. que les permite procesar y analizar datos de acuerdo con la programación. Para interactuar o transmitir datos a una plataforma central los dispositivos como cámaras, smartphones, computadoras, laptops, tablets, etc.

necesitan ser identificados con características individuales.

a. Características:

i. IP: Protocolo de internet que forman un conjunto de reglas que son utilizadas por los DNS para enrutar los paquetes de información y llegar al destino correcto de manera ordenada a través de los protocolos TCP/IP.

ii. Mac address (Media Access Control): Una serie de 12 caracteres que es único por cada dispositivo, también es conocida como dirección física de 48 bits porque se compone de 6 octetos en los cuales los primeros 3 identifican al fabricante y los últimos tres corresponde al modelo del dispositivo, la Mac address es inmutable y las maniobras para clonar, enmascarar o cambiar una dirección MAC en la actualidad es un proceso complejo que requiere de conocimiento profundo de redes de computadoras [33].

iii. IMEI: Corresponde al número de identificación que se utiliza para la identificación de dispositivos móviles, consta de 15 dígitos, utilizado por las empresas telefónicas para identificar un dispositivo en la red móvil, realizar seguimiento del uso e incluso localización en caso de pérdida o robo.

iv. Tarjeta SIM: Los números telefónicos se asocian con los dispositivos, de tal manera que se convierte en una característica para identificar los dispositivos telefónicos como los smartphones.

1.1.3. Datos e información:

A. Dato: La unidad básica de información, puede conformarse por un número, caracteres, una imagen, un sonido, etc. Son esenciales para los sistemas de información que pueden ser utilizados en una amplia gama de procesos, por tal razón es fundamental la protección, privacidad y seguridad de los datos para proteger contra amenazas de accesos no autorizados, modificación y divulgación no autorizada con herramientas de seguridad.

B. Información: Conformado por el contexto de los datos, lo que significa que es necesario el análisis y comprensión de los datos para un resultado significativo. A lo largo del tiempo va formando patrones de comportamiento, convirtiéndose de gran impacto para la toma de decisiones en negocios y otros procesos empresariales convirtiéndose en un aspecto crítico donde es necesario establecer un conjunto de normas para evitar el acceso no autorizado de agentes externos respetando propiedades como:

- **a. Confidencialidad:** Propiedad de la información que establece y garantiza que solo personal autorizado puede acceder a la información.
- **b. Privacidad:** Protección de información personal que no debería ser divulgada sin el permiso de los agentes involucrados. La privacidad de la información es un derecho fundamental de las personas y que debe ser protegido por los gobiernos y organizaciones.
- c. **Disponibilidad:** Propiedad que garantiza que las personas o dispositivos autorizados deben tener un acceso total el máximo tiempo posible en cualquier situación de emergencia.
- **d. Seguridad:** Protección de la información frente a amenazas, vulnerabilidades y riesgos, que puede afectar la disponibilidad, confidencialidad e integridad. Es necesario disponer de herramientas para mantener la seguridad de la información.

e. **Integridad:** Garantiza que la información no fue alterada, un aspecto fundamental para garantizar la confiabilidad y precisión de la información implementando medidas de control de acceso y auditoría constantes.

f. **Autenticidad:** Propiedad que garantiza que los datos son verdaderos y que provienen de una fuente confiable sin falsificación o manipulación.

g. **No repudio:** Capacidad de afirmar la autoría de la información, evitando que el autor niegue responsabilidad de haber recibido o enviado información con pruebas como firmas digitales, garantiza la autenticidad e integridad.

1.1.4. Métodos de autenticación: Proceso de verificación de que una pieza de información es genuina y que no fue alterada o manipulada de ninguna manera, utiliza propiedades de integridad y autenticidad con técnicas como la criptografía, que se podría utilizar en los métodos de autenticación como:

A. Autenticación basada en contraseñas: Proceso de autenticación más común, que requiere de un conjunto de caracteres que se asocian como usuario y contraseña y posteriormente permitirá acceder a una cuenta o información.

a. **Ventajas de la autenticación basada en contraseñas:**

- **Fácil implementación:** La autenticación basada en contraseñas es fácil de implementar en la mayoría de los sistemas y aplicaciones. No se necesitan dispositivos especiales ni software adicional para utilizarla.
- **Bajo costo:** La autenticación basada en contraseñas es un método económico en comparación con otras formas de autenticación, como la autenticación biométrica o la

autenticación basada en tokens.

- **Ampliamente conocida:** La autenticación basada en contraseñas es un método conocido y familiar para la mayoría de los usuarios de tecnología. La mayoría de las personas están acostumbradas a crear y utilizar contraseñas para acceder a sus cuentas.
- **Personalización:** Los usuarios pueden crear sus propias contraseñas, lo que les da cierto grado de control y personalización. Además, pueden cambiar sus contraseñas en cualquier momento.

b. Desventajas de la autenticación basada en contraseñas:

- **Vulnerabilidad a los ataques de fuerza bruta:** Los ataques de fuerza bruta son una técnica utilizada por los hackers para descubrir contraseñas al probar diferentes combinaciones hasta encontrar la correcta. Este tipo de ataque puede ser efectivo en contraseñas débiles o cortas.
- **Dificultad para recordar contraseñas complejas:** Para garantizar la seguridad de la cuenta, se recomienda utilizar contraseñas largas y complejas. Sin embargo, estas contraseñas pueden ser difíciles de recordar y llevar al usuario a escribirlas en un lugar no seguro o reutilizar la misma contraseña para varias cuentas, lo que aumenta el riesgo de ataques.
- **Vulnerabilidad a la ingeniería social:** La ingeniería social es una técnica utilizada por los hackers para engañar a los usuarios y obtener información confidencial, como contraseñas.

Los ataques de phishing son un ejemplo de ingeniería social que se enfoca en enviar correos electrónicos falsos que parecen provenir de una fuente confiable para engañar al usuario y obtener sus credenciales.

- **Falta de flexibilidad:** La autenticación basada en contraseñas puede ser limitada en términos de flexibilidad. Por ejemplo, si un usuario pierde su contraseña, puede tener dificultades para recuperar su cuenta o necesitar ayuda del proveedor del servicio.
- **Problemas de seguridad:** Si un atacante obtiene acceso a la base de datos de contraseñas, puede obtener acceso a las credenciales de los usuarios y comprometer su seguridad. Además, la autenticación basada en contraseñas no puede garantizar la identidad del usuario que está iniciando sesión en la cuenta, ya que alguien más puede conocer su contraseña.

B. Autenticación de dos factores (2FA): Además de un usuario y contraseña, se requiere de un código que es enviado al dispositivo móvil que previamente fue asociado en conjunto con el número de tarjeta SIM, con desventajas que puede representar algún costo adicional por las empresas, complejidad técnica por la correcta configuración que debe existir en los dispositivos causando incluso problemas de compatibilidad.

C. **Autenticación biométrica:** Método de autenticación que utiliza características físicas o de comportamiento únicas de un individuo para verificar su identidad. Algunos ejemplos de características biométricas incluyen huellas dactilares, reconocimiento facial, reconocimiento de voz, escaneo de retina, entre otros. Las ventajas de la autenticación biométrica incluyen:

a. **Alta precisión:** Las características biométricas son únicas para cada individuo, lo que hace que la autenticación biométrica sea muy precisa.
b. **Comodidad:** La autenticación biométrica es fácil de usar y conveniente para los usuarios, principalmente los procesos que requieren de huella dactilar.

D. Autenticación de clave pública: Método criptográfico utilizado para verificar la identidad de un usuario en una red. Funciona a través de un par de claves criptográficas: una clave pública y una clave privada. La clave pública se comparte con otros usuarios en la red, mientras que la clave privada se mantiene en secreto y solo es conocida por el propietario.

E. Autenticación de redes sociales: Método de autenticación que permite a los usuarios utilizar sus credenciales de redes sociales como Facebook, Twitter, Google, etc. para acceder a servicios y aplicaciones de terceros. Aunque es conveniente para los usuarios, ya que no necesitan recordar otra contraseña, también tiene sus ventajas de comodidad y la inclusión de 2FA con desventajas. Privacidad y fallos técnicos porque si la red social queda sin servicios el proceso de login para otras plataformas quedará deshabilitado.

F. Autenticación por correo electrónico: Método de autenticación que utiliza el correo electrónico del usuario para verificar su identidad. En este método, el usuario proporciona su dirección de correo electrónico y se le envía un enlace de autenticación a su correo electrónico registrado. El usuario debe hacer clic en el enlace para verificar su identidad y acceder al servicio o aplicación, representa simplicidad para el usuario con desventaja de suplantación de identidad que incluso le brindaría acceso a otros servicios o aplicaciones.

G. **Autenticación por SMS:** Método de autenticación en el que se utiliza un código enviado a través de un mensaje de texto (SMS) para verificar la identidad del usuario. En este método, el usuario proporciona su número de teléfono móvil registrado y se le envía un código de autenticación a través de un mensaje de texto. El usuario debe ingresar el código para verificar su identidad para acceder al servicio o aplicación, con ventaja de comodidad, simplicidad y desventajas de vulnerabilidad a los ataques de phishing, Dependencia del proveedor de servicios de telefonía móvil además de ataques de ingeniería social.

1.1.5. Métodos de vulnerabilidad de autenticación:

A. **Ingeniería social:** Técnica hacker que los atacantes utilizan para obtener credenciales de acceso aprovechándose de la manipulación psicológica, para que los usuarios realicen ciertas acciones obteniendo cómo consecuencia el envío de información confidencial, Las modalidades más comunes son el phishing y el spearfishing con mensajes personalizados suplantando la identidad de una fuente confiable.

B. **Fuerza bruta:** Proceso que implica probar todas las posibles combinaciones que podrían coincidir con los datos de autenticación de los sistemas en línea, principalmente cuando las credenciales contienen características débiles con datos o caracteres comunes en los usuarios similar al ataque de diccionario.

C. **Sniffing:** Ataque que analiza el tráfico de la red e intercepta paquetes que contengan credenciales de autenticación, sesiones de usuario, etc.

D. **keylogger:** Utiliza software malicioso que es instalado en el dispositivo para registrar pulsaciones del teclado y capturar datos que podrían estar relacionado a procesos de autenticación para posteriormente acceder a la información o cuenta vulnerada.

E. **Spoofing**: Técnica utilizada por los atacantes para hacerse pasar por otra persona o entidad en línea, Existen diferentes tipos de spoofing, algunos de los cuales son: Spoofing de correo electrónico: los atacantes envían correos electrónicos falsos haciéndose pasar por una entidad legítima misma modalidad para Spoofing de dirección IP de tal manera que el origen de un paquete de datos parezca que proviene de una fuente confiable, además los atacantes pueden falsificar direcciones MAC para ocultar su identidad.

1.1.6. La criptografía: Proceso para proteger la información mediante algoritmos codificados, firmas y hashes, con objetivos de confidencialidad, integridad, autenticación y no repudio en los datos [34].

Llave privada: Es la clave secreta para cifrar y descifrar en el caso de la criptografía simétrica y es necesario para descifrar información en la criptografía asimétrica.

Llave pública: Se comparte con otros usuarios que requieran enviar información cifrada al propietario de la llave, la clave pública se utiliza para cifrar y la clave privada se utiliza para descifrar.

Firmas digitales: Garantiza la autenticidad e integridad de un documento, utilizado en transacciones electrónicas, donde se utiliza una llave pública correspondiente a su llave privada para verificar si la información no fue alterada en el proceso.

ZKP (Prueba de Conocimiento Cero): Protocolo criptográfico que permite a un participante demostrar que tiene cierta información o conocimiento, sin revelar la información o el conocimiento en sí mismo. Es decir, se puede probar que se conoce algo sin tener que revelar lo que se conoce. Utilizado en los sistemas de votación electrónica, en las transacciones de criptomonedas y en la autenticación de identidad, Los protocolos de ZKP

se basan en la teoría de la complejidad computacional y utilizan algoritmos criptográficos para asegurar que la información se mantenga privada y segura durante todo el proceso.

Árbol de merkle: Estructura en árbol hash utilizado en criptografía para la verificación de la integridad de los datos, permite realizar las consultas a la información sin necesidad de acceder a todos los grupos de información previamente cifrados, esto es necesario para las transparencias de la red porque cualquier nodo puede verificar la veracidad de los datos.

Creado por Ralph Merkle un científico computacional de estados unidos, que permite resumir todas las transacciones ocurridas dentro de un bloque se simplifiquen a una sola línea, todas las transacciones son separadas en pares hasta ser considerada a todas en el hash general.

Por ejemplo, si en un bloque hay 512 transacciones realizadas por los usuarios, con la estructura del árbol propuesta por Merkle esto se van ordenando en 256 pares, posteriormente se reduce a 128, luego a 64 y así sucesivamente con 32,16,8,4,2 hasta considerar a cada una de las transacciones que han ocurrido por los usuarios, este proceso reduce de 16384 bytes a tan solo 32 bytes por cada bloque [35].

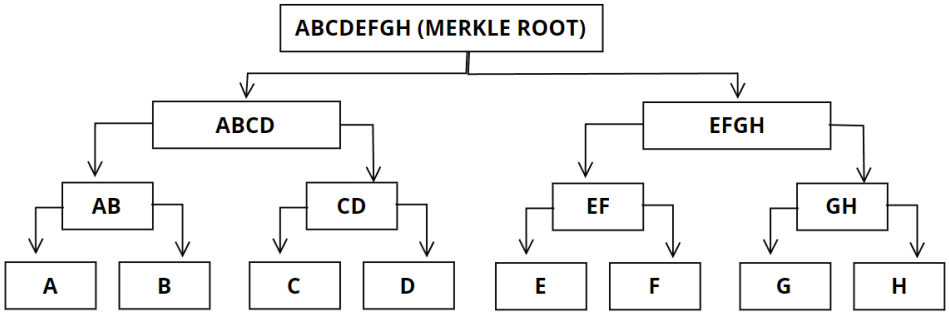


Fig. 3. Funcionamiento de árbol de merkle.

Nota: fuente bit2me academia de aprendizaje de conceptos blockchain, publicación de artículos de noticias y blogs [36].

1.1.6.1. Criptografía simétrica: La simetría se ubica en que el emisor y receptor necesitan de la misma llave para cifrar y descifrar el mensaje [37]. A nivel computacional es más rápido y eficiente en relación con la criptografía asimétrica, con la desventaja de que la clave debe ser compartida por el receptor, representando un riesgo de seguridad para ser interceptado por terceros no autorizados, Utiliza algoritmos como:

A. AES: Algoritmo estándar de cifrado para la Agencia de Seguridad Nacional de Estados Unidos (NSA) del gobierno de estado unidos desde el año 2001, genera un tamaño de bloque de 128 bits, con tamaños de claves de 128, 192 y 256 bits [38]. El algoritmo AES aparece con el nombre de Rijndael en un concurso posterior al anuncio de desfasar a DES como estándar de cifrado [39].

B. KECCAK HASH: Utiliza un enfoque denominado construcción de esponja y compresión, con un modelo de permutación también utilizado por las variantes del algoritmo SHA, pero ya no son incluidos en el estándar debido a que es un desarrollo posterior [40].

C. 3DES: Es uno de los más antiguos, una evolución del algoritmo DES debido a vulnerabilidades por fuerza bruta, desarrollado por IBM en 1970.

D. Blowfish: Algoritmo aplicado para redes de almacenamiento, no recomendable para aplicaciones de alta seguridad, es de dominio público y no patentado.

E. RC4: Utilizado para el flujo de información por las aplicaciones de seguridad web como HTTPS y SSL/TLS, con prohibición de utilidad y recomendado para ser reemplazado por algoritmos más seguros [41].

1.1.6.2. Criptografía asimétrica: La clave de cifrado es diferente a la clave de descifrado, también denominada criptografía de clave pública [42]. Proceso que utiliza dos claves relacionadas, una clave pública y otra clave de tipo privada y son utilizadas para cifrar y descifrar un mensaje. La clave pública puede ser utilizada de manera libre para cifrar un mensaje, posteriormente el receptor solo puede desencriptar con su clave privada. El principal beneficio de la criptografía asimétrica es el aumento de la seguridad de los datos y la información que se transporta dentro de cada una de estas transacciones. El proceso de cifrado es más seguro porque los usuarios no tienen que revelar o compartir sus claves privadas, lo que disminuye las posibilidades porque, aunque la clave pública sea interceptada por un tercero, es necesario la clave privada del receptor para conocer el mensaje. En el cifrado asimétrico solo quienes tienen la llave privada pueden acceder a la información y algunos algoritmos son unidireccionales donde los datos cifrados son imposibles volver a identificar la información original a menos que se cuente con la clave privada para descifrarlo, algunos de estos algoritmos son:

A. **SHA-256:** Es una de las funciones hash más comunes para el cifrado de información en las cadenas de bloques, pertenece al cifrado asimétrico, cuando se realiza el proceso de cifrado se genera un código de identificación el cual hace imposible visualizar la información que se haya registrado originalmente, fue creado por la agencia de seguridad nacional de estados unidos (NSA) y cuenta con cuatro variantes según el número de bits en el cifrado. SHA-256 pertenece al estándar actual de hash seguros conformado por SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 y SHA-512/256 [43].

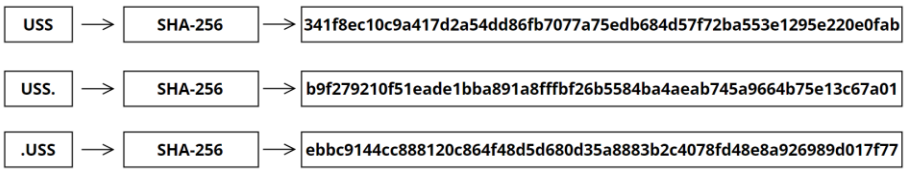


Fig. 4. Ejemplo de resultado producido aplicando hash.

Algoritmo unidireccional porque permite cifrar un mensaje de manera segura y eficiente, pero no pueden ser utilizados para descifrar el mensaje original. hasta conocer la clave de cifrado, lo que significa que es fácil de calcular la salida a partir de la entrada, pero es extremadamente difícil de calcular la entrada a partir de la salida. En el año 2012 el NIST actualizó el estándar a FIPS PUB 180-4 de hash seguro con la inclusión de algoritmos hash como: SHA-512/224 y SHA-512/256 [44].

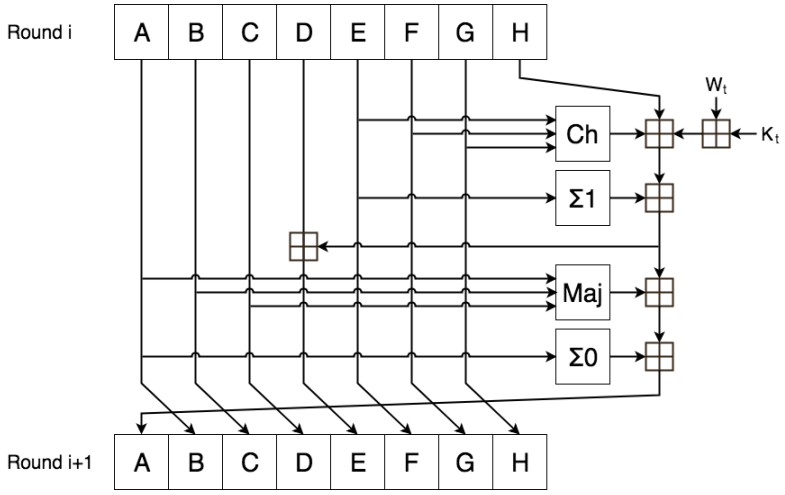


Fig. 5: Cifrado del algoritmo SHA-256

Nota: fuente FIPS institución de estándares de para la utilización en todas las agencias del gobierno no militares.

- Cada bloque de datos se procesa a través de una serie de rondas, y el resultado de cada ronda se utiliza como entrada para la siguiente ronda.
- Después de que todos los bloques hayan sido procesados, se

produce una salida de 256 bits que representa la huella digital única de la entrada. Estas operaciones incluyen rotaciones circulares de bits, sumas modulares, operaciones lógicas AND, OR y XOR, y transformaciones no lineales conocidas como funciones de ronda.

- Las funciones ronda utilizan operaciones aritméticas y lógicas para transformar los datos de entrada y producir una salida que se utiliza como entrada para la siguiente función de ronda.

Una iteración en la función de compresión de la familia SHA-2. Las funciones Ch, Σ1, Maj y Σ0 representan las siguientes operaciones:

$$Ch(E,F,G) = (E^F) \oplus (\neg E^G)$$

$$Ma\,(A,B,C) = (A^B) \oplus (A^C) \oplus (B^C)$$

$$\sum(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$

$$\sum\nolimits_1 (E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

- **A, B, C, D, E, F, G y H:** Variables de 32 bits que representan estados internos del algoritmo SHA-2.
- **Wt:** Variables de entrada de 32 bits que representan los datos de entrada a la función de compresión en la iteración t. En cada iteración, se utilizan 16 de estas variables de entrada, y las restantes se calculan a partir de ellas utilizando operaciones lógicas y aritméticas n.
- **Kt:** Constantes de 32 bits que se utilizan en cada iteración para aplicar transformaciones específicas a los estados internos de

SHA-2. En la iteración t, se utiliza la constante Kt correspondiente.

- **Ch:** Función lógica que se utiliza en la iteración para combinar los estados internos E, F y G mediante una operación XOR y una operación AND.
- **Ma**: Función lógica que se utiliza en la iteración para combinar los estados internos A, B y C mediante una operación XOR y tres operaciones AND.
- **Σ0 y Σ1:** Funciones de rotación de bits que se utilizan en la iteración para aplicar transformaciones específicas a los estados internos A y E.

B. RSA: Rivest-Shamir-Adleman permite el cifrado mediante operaciones matemáticas, para el proceso de cifrado utiliza la factorización de grandes cantidades de números primos y en cuanto más larga sea la clave, más complejo será el proceso de factorización que se debe seguir para desencriptar la información.

C. **DSA:** Digital Signature Algorithm permite las firmas digitales, en el proceso de firma el remitente genera una clave privada para crear una firma digital única en conjunto con los datos a enviar. DSA no proporciona cifrado a datos por tal razón el proceso debe realizarse de manera individual, es uno de los más lentos debido a la complejidad matemática para el cifrado.

D. Diffie-Hellman: La dificultad del cifrado se basa en el problema del logaritmo discreto, implica encontrar el valor de x de tal manera que “a” elevado a la “x” equivale a “b” módulo de “p”. Es decir, encontrar el exponente desconocido, el cual requiere de mayor tiempo

computacional incluso con la potencia de procesadores actuales.

$$A^{\mathrm{B}} mod C = (A mod C)^{B}\ mod C$$

$$(A^{B})^{C} = (C^{C})^{B}$$

Para A = $A^{b}\ mod C$, con a y C reconocidos, encontrar b a partir de A, cuando b y son dígitos extensos, es matemáticamente imposible o requiere de un gran poder computacional [45].

E. El Gamal: Utilizado para firmas digitales, complejidad de cifrado con el problema del logaritmo discreto, con característica de no repudio una vez firmada la información, es flexible para cifrar y firmar grandes cantidades de datos. La implementación en hardware requiere de detalles técnicos para el eficiente funcionamiento.

F. ECC: Elliptic Curve Cryptography para su complejidad reemplaza los números enteros por curvas elípticas, característica que le permite ser más eficiente porque solo utiliza 32 bits, utilizado en tecnologías de seguridad como TLS/SSL, tarjetas inteligentes, etc.

1.1.7. Tecnología Blockchain: Blockchain es un libro de contabilidad que registra transacciones realizadas en una red de manera visible para todos, pero es inalterable. es un concepto acuñado en el whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” [46].

Las características principales como inmutabilidad, transparencia y resistencia. cada bloque es interconectado con un bloque anterior que también contiene transacciones realizadas en la red, la seguridad de la información es mantenida a través de procesos criptográficos,

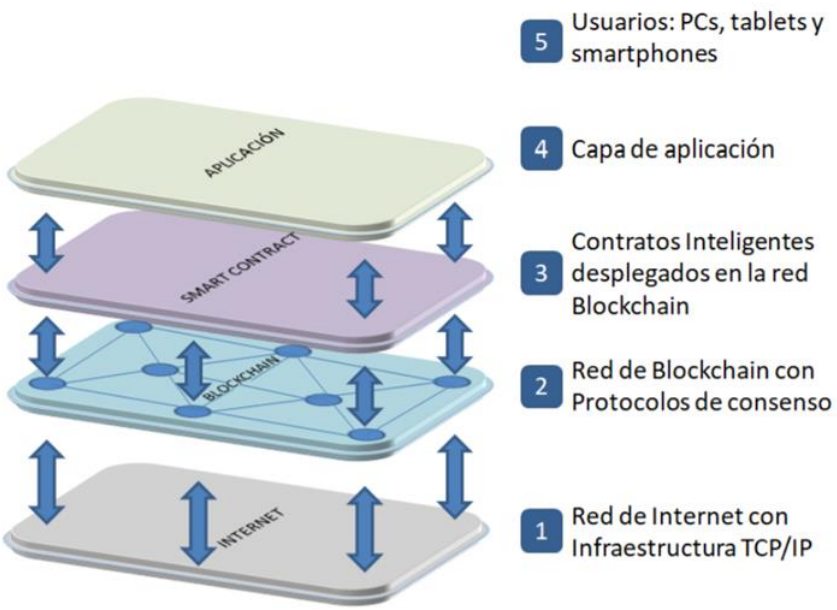


Fig. 6: integración blockchain a internet *[47]*

El término se popularizó con la publicación del paper de Bitcoin (Nakamoto, 2008), la primera moneda digital con la visión de descentralización de los bancos financieros, a partir de la presentación del whitepaper, la tecnología Blockchain se ha utilizado para diferentes áreas investigativas. Algunas de las características de la cadena de bloques es que los registros son encerrados en un bloque, posteriormente realizada la validación de la información se convierte en inmutable porque los datos son agrupados en un nuevo bloque para integrarse al conjunto de bloques anteriores y quedando grabado en el registro general de la Blockchain [28].

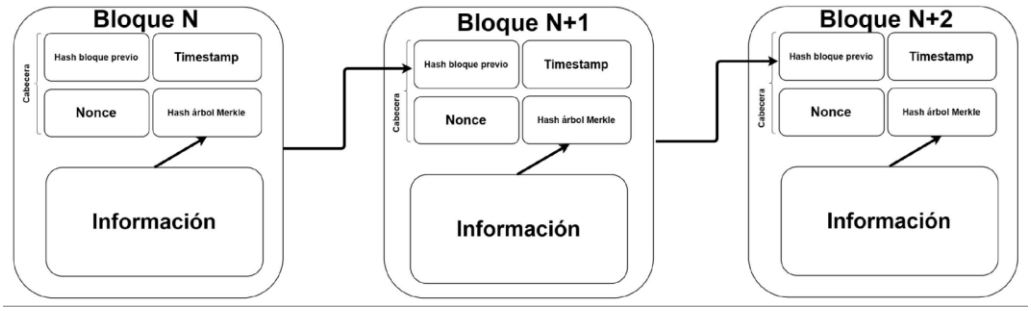


Fig. 7. Registro de información en la cadena de bloques

Nota: Metadato de datos que registran la mayoría de cadenas de bloques [48]

Bloque Génesis: El bloque génesis también denominado bloque cero es el primer bloque de un Blockchain o cadena, Satoshi Nakamoto, el autor de Bitcoin, es el primero en utilizar dicha designación para dialogar del primer bloque de la cadena de Bitcoin. Sin embargo, cualquier cadena de bloques va a tener un bloque de semejantes propiedades cuando inicia su Blockchain [47].

Mempool: Las cadenas de bloques actuales que su funcionamiento principal de encuentra bajo los procesos de transacciones, contiene un concepto denominado mempool, la cual es una memoria temporal de las transacciones de los usuarios previo a la validación, esto permite completar la capacidad de cada bloque de manera rápida, donde los validadores pueden tomar estas transacciones, realizar el proceso de verificación para finalmente crear el nuevo bloque que se agregara a la cadena de bloques, conlleva un cierto grado de inseguridad porque usuarios maliciosos pueden aprovecharse con la vulnerabilidad de doble gasto si la red no aún no ha solucionado dichos inconvenientes. Es por ello por lo que las cadenas de bloques agregan al proceso de un rango de confirmaciones previo a que la transacción sea irreversible, previo al proceso las transacciones son almacenadas en una memoria temporal [28].

Testnet: Las actualizaciones de las cadenas de bloques no ocurren directamente en la red principal, es por ello que se crea una red alterna para las pruebas, hasta verificar que los nuevos Incorporaciones cumple con los requisitos principales de la red, estas redes de pruebas permiten mantener a salvo de vulnerabilidades a la mainnet, característica de seguridad y una alternativa para los nuevos proyectos que se logren desarrollar en la cadena de bloques.

Blockchain 1.0: Cadena de bloques de primera generación, esto se refiere a la cadena de bloques nativa original, utilizada para transferir y almacenar valores. La cadena de bloques de primera generación se centra en desarrollar criptomonedas y creación de base sólida para la tecnología blockchain, Algunos ejemplos de proyectos de primera generación incluyen: Bitcoin la cual fue la primera criptomoneda y la blockchain original creada en el año 2009 y el objetivo principal era permitir transacciones P2P seguras y dispersas.

Blockchain 2.0: Enfocado principalmente en crear contratos inteligentes y aplicaciones descentralizadas (DAPPS) además permite la creación de tokens y otras formas de activos digitales. Ethereum (ETH) es la cadena de bloques más conocida de esta generación.

Blockchain 3.0: Tercera generación de cadena de bloques se centra en mejorar la escalabilidad, la interoperabilidad, la velocidad y la privacidad. Las cadenas de bloques de tercera generación, como Cardano y Polkadot, intentan resolver los desafíos técnicos de las generaciones anteriores y permitir una adopción más amplia de la tecnología blockchain.

1.1.7.1. Mecanismos de consenso:

Proof of work (POW): Prueba de Trabajo (POW), es el algoritmo de consenso original en una red de Blockchain. En la Blockchain, este algoritmo se utiliza para confirmar transacciones y generar nuevos bloques en la cadena. Con PoW, los mineros compiten entre ellos para terminar transacciones en la red y obtener recompensas. No obstante, se debería tener cuidado para confirmar las transacciones y ordenar bloques [47].

Proof of Stake (POS): El propósito de este algoritmo es producir un consenso entre cada uno de los nodos que conforman la red. A los nodos que cumplían

la función de mineros en PoW, en PoS se les denomina validadores. La elección sobre qué nodo ha de validar un bloque se hace de manera aleatoria sin embargo brinda mayor posibilidad a quienes cumplan una secuencia de criterios. Una vez establecidos, se inicia el proceso de selección de nodos de manera aleatoria. En PoS el proceso es muchísimo más sencillo y energéticamente amistoso con el medio ambiente [47].

La seguridad de la red es mantenida por quienes participan en ella, es necesario considerara que para estos procesos ya no es tan necesario el poder computacional que se utilizada para las validaciones por prueba de trabajo, en la mayoría de los casos la red contiene una forma de generar los consensos a través de los votos, y según la relevancia que tiene cada nodo en la red este será su poder de voto en la red [49].

Proof-of-History (POH): Proceso de validación donde los nodos incorporan marcas tiempo en la blockchain, que garantiza que cierta transacción ocurrió realmente en un momento exacto de tiempo, es un algoritmo con características viables para ser integrado a los procesos de validación de POS o POW además de permitir la escalabilidad de la red con un menor costo de comisiones, pero lo convierte en una red centralizada. Debido a estos procesos de validación hay un problema conocido como el trilema de las blackchains.

1.1.7.2. Problema del Trilema Blockchain:

Teoría propuesta por Vitalik Buterin que plantea que las redes blockchain no pueden tener simultáneamente sus 3 características principales como: Escalabilidad, seguridad y descentralización, sólo es posible obtener 2 / 3 características fundamentales [50].

Fig. 8: Trilema de la Blockchain

Nota: Fuente Ethereum org plataforma blockchain de contratos inteligentes *[50]* .

A. **Escalabilidad:** La escalabilidad permite lograr la capacidad para procesar una gran cantidad de transacciones en el menor tiempo posible y de manera eficiente. A medida que la red tiene mayor alcance y se utilizan más transacciones, es necesario una mayor capacidad de procesamiento para mantener un rendimiento óptimo.

B. **Seguridad:** Cadena de bloques segura es la que garantiza la integridad y la inmutabilidad de los datos almacenados, principalmente mediante el uso de algoritmos criptográficos y nodos validadores de la red.

C. **Descentralización:** La descentralización de la red se refiere a la capacidad de una cadena de bloques para operar de manera distribuida sin la necesidad de una autoridad central que verifique la veracidad de los datos, sino que sean los mismos nodos participantes que a partir de reglas bien establecidas logren mantener la seguridad. En una blockchain descentralizada los nodos en la red tienen el mismo rendimiento y pueden participar en el proceso de validación.

Adicional a los tres pilares fundamentales de la blockchain también es posible considerar a:

D. **Inmutabilidad:** Garantiza que la información es la originalmente fue verificada y aceptada, porque cada nodo de la red tiene una copia completa de la red, donde actividades de manipulación de datos por un nodo no sea reflejado en la blockchain sin antes recibir la validación de la mayoría de los nodos.

E. **Transparencia:** Característica que permite que todas las transacciones sean visibles para todos los participantes de la red, solo requiere solicitar una copia de la blockchain.

1.1.7.3. Blockchain Pública:

Base de datos distribuida que permite a cualquier persona unirse a la red, realizar transacciones y validarlas sin necesidad de permisos o autorización previa. En una blockchain pública, todos los datos son transparentes y están disponibles públicamente para cualquier persona que tenga acceso a internet, lo que significa que no hay una única entidad o autoridad central que controle la red. En lugar de eso, los nodos trabajan juntos para validar las transacciones y asegurar la integridad del libro mayor.

1.1.7.4. Blockchain Privada:

Red que está diseñada para ser utilizada por un grupo específico de participantes, en lugar de ser accesible para cualquier persona en Internet. A diferencia de la blockchain pública, en la que cualquier nodo puede unirse a la red y participar en la validación de transacciones y la creación de bloques, una blockchain privada está controlada por un conjunto predefinido

de nodos de la red y tienen un mayor control sobre el acceso a la red, la validación de transacciones y la configuración de la estructura de datos de la blockchain. Las blockchains privadas son particularmente útiles para aplicaciones empresariales y gubernamentales en las que la privacidad y la confidencialidad son importantes para la organización, porque les permite a las compañías y organizaciones crear redes blockchain personalizadas que se adapten a sus necesidades específicas incorporando características individuales.

1.1.7.5. Blockchain Híbrida:

Blockchain que combina las características de una red pública y una red privada, utiliza características de ambas para crear una solución híbrida adaptada a las necesidades específicas de una organización o aplicación además los nodos de la red pueden ser tanto públicos como privados. Esto permite a la empresa tener un mayor control sobre la privacidad y la confidencialidad de sus datos, al mismo tiempo que se beneficia con características de transparencia y seguridad de una blockchain pública.

1.1.7.6. Nodos De Red: Es la base importante de la tecnología Blockchain, porque permite tener la posibilidad de generar una gigantesca red de computadores interconectadas que comparten información de manera segura, instantánea y descentralizada, además de permitirnos gozar de cada una de las bondades que la tecnología Blockchain puede ofrecernos. De esta forma, a partir de la perspectiva de la tecnología Blockchain (cadena de bloques) y las criptomonedas, los nodos se conforman por todos esos pc que permanecen interconectados a la red de una criptomoneda, ejecutando el programa que se ocupa de todo su manejo. Lo cual supone que todos los nodos operan de manera igual y equivalente entre sí. Además, los nodos tienen la posibilidad de comunicarse entre ellos para transmitir y compartir datos e información por medio de esa red, sin embargo, los nodos son muchísimo más que un programa que hace funcionar a la red Blockchain [51].

A. **Nodos red P2P:** Son un tipo de red descentralizada que se conforman por cientos de ordenadores (nodos) ubicados en diferentes lugares del mundo, permite compartir información de diferentes tipos, proceso para el cual no es necesario de la confianza en un tercero que permita validar la veracidad de los hechos, entonces este tipo de red permite el intercambio de información o recursos con la verificación de los participantes de la red que actúan como testigos de los hechos pasados y que se hayan registrado en la cadena de bloques, para acceder a ciertos requerimientos es posible encontrar dos tipo de redes, la primera es de forma estructurada donde existen una serie de nodos que reciben las peticiones y facilitan la información y la no estructurada donde cada nodo tiene las mismas funciones y mismo nivel de autoridad que el resto [35]

Fig. 9. Transporte de información con nodos descentralizados.

Nota: Puentes de comunicación generado por red descentralizada. [36].

B. **Nodo semilla:** Permite la incorporación de nuevos bloques, permitiendo una sincronización, para replicar los datos que se han registrado en la cadena de bloques, un comportamiento similar a un rastreador porque registran las ip de los dispositivos que operan dentro de la red, y se utilizan como puentes para seguir manteniendo los registros en la cadena de bloques, mismo concepto que es arraigado para los DNS cuando se agregan como nuevos validadores [52].

C. **Pruned node:** Mantiene requisitos similares a un nodo normal, la diferencia principal radica en que estos tipos de nodos tienen una copia completa de la cadena de bloques, esto permite mantener actualizada la red para los procesos de edificación de datos, estos nodos permiten recortar el espacio de almacenamiento pero manteniendo todos los registros de la cadena de bloques, estos nodos facilitan que muchos más usuarios logren convertirse en validadores además de obtener una copia optimizada de la cadena de bloques, tecnología que es

complementada con los árboles de merkle.

D. **Nodos completos:** Estos son nodos que guardan una copia completa de la cadena de bloques además verifican todas las transacciones y bloques agregados a la red. Estos nodos pueden detectar estafas o gastos duales, que ayudan a garantizar la seguridad y la integridad de la red [52]

E. **Nodos mineros:** Son nodos competidores para resolver problemas matemáticos complejos y agregar nuevos bloques a blockchain. A cambio de su trabajo, reciben recompensas con la criptomoneda nativa de la red. Este tipo de nodos son esenciales para la blockchain pública.

F. **Nodos de validación:** Estos son nodos que verifican transacciones y bloques, pero no necesariamente guardan una copia completa de la cadena de bloques. Estos nodos generalmente son utilizados por empresas y desarrolladores que desean interactuar con blockchain sin generar altos costos de almacenamiento relacionados con los nodos completos.

G. **Nodos de puente:** Estos son nodos que conectan diferentes blockchains y habilitan la transferencia de activos digitales entre ellos. Estos nodos son esenciales para la interoperabilidad entre blockchains y pueden facilitar la adopción masiva de la tecnología blockchain [52].

H. **Hard fork:** Actualización o cambio en el protocolo de la cadena de bloques que requiere que los nodos de la red actualicen su software para seguir siendo compatibles con la cadena de bloques actualizada. En un hard fork, se crea una nueva cadena de bloques separada de la cadena original y las dos cadenas divergen a partir de ese momento. Puede ocurrir por varias razones, como la corrección de errores críticos en el protocolo, la implementación de nuevas características, etc.

Cuando se produce un hard fork, los usuarios pueden elegir seguir utilizando la cadena original o cambiar a la nueva cadena. Si bien los saldos de activos se reflejan en ambas cadenas, la comunidad y los desarrolladores de la cadena original pueden decidir no admitir la nueva cadena, todo depende de las características establecidas para el nuevo protocolo, cualquier nodo que no actualice su software dejará de ser compatible con la nueva cadena.

1.1.7.7. Metadatos de la blockchain:

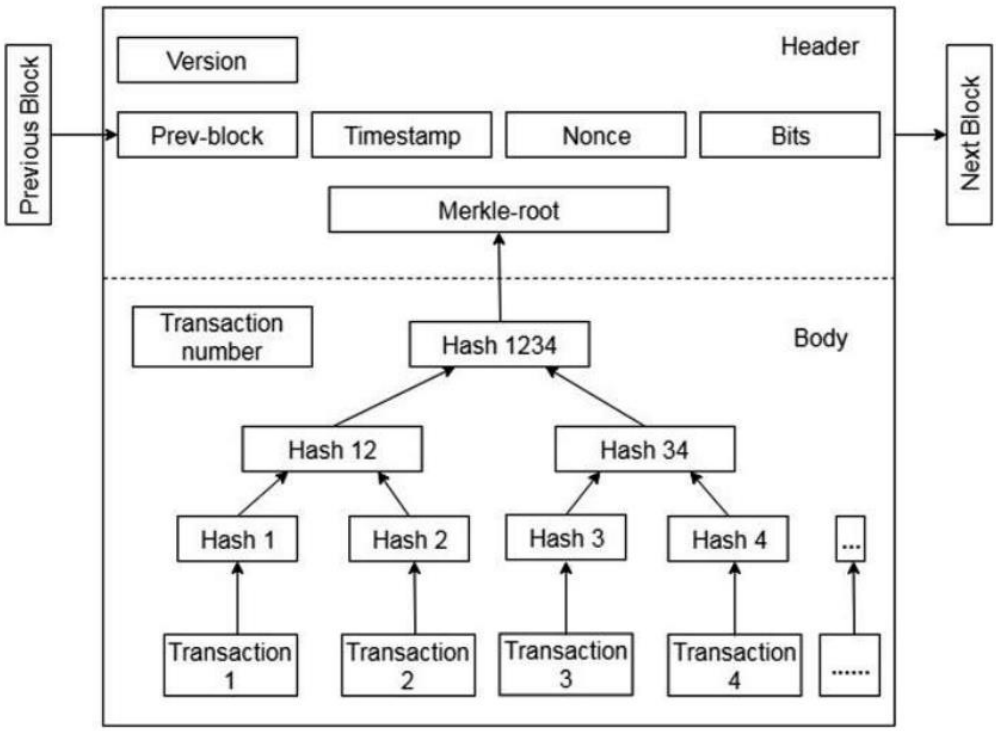


Fig. 10. Estructura de un bloque en la red de bitcoin

Nota: Estructura interna por bloque con la información de transacciones [53]

A. **Hash:** Es una de las principales tecnologías que utiliza la Blockchain para procesar y mantener seguridad la información, entre los más conocidos se encuentra SHA-256 y el RSA, algoritmos que permiten incorporar un grado de cifrado simétrica en los datos, donde la información original no es posible obtenerse si se tiene el hash, y es necesario de una clave privada para visualizar la información.

B. **Nonce:** Es un contador que permite la validación por parte de la prueba de trabajo, procesos donde los nodos mineros buscan un valor único hasta cumplir con las normas establecidas para el nuevo hash.

C. **Timestamp:** Referencia al tiempo en el que se crea el bloque, esto permite llevar un orden en cada uno de los bloques que se van agregando a la red.

D. **Transacción:** Transferencia de valor entre dos participantes de la red, que se registra en la cadena de bloques de manera inmutable y transparente. En una transacción, se especifica la cantidad de activos que se están transfiriendo, así como las direcciones de las billeteras de origen y destino, donde la persona que desea enviar los activos debe tener acceso a una billetera que contenga los activos que desea enviar. En segundo lugar, la billetera debe estar conectada a la red blockchain, ya sea directamente o a través de un servicio de terceros. La validación de una transacción en blockchain implica la verificación de que el remitente tiene los activos necesarios para la transacción y que la transacción cumple con las reglas y protocolos establecidos por la red. Si la transacción es válida, se agrega a un bloque en la cadena de bloques y se transmite a otros nodos de la red para su confirmación y validación. Los detalles de la transacción, como la cantidad transferida y las direcciones de las billeteras de origen y destino, se almacenan en la cadena de bloques de manera permanente

E. **Hash Rate:** Concepto que es utilizado para las redes que mantienen la seguridad de la información a través de la prueba de trabajo, hace referencia a la cantidad de operaciones en cómputo que general todos los nodos validadores en conjunto, mientras más alto más nivel se seguridad en los datos, en algunas redes Blockchain esta potencia es utilizada para resolver los hashes de validación de tipo SHA-256, esto se debe a que con un alto nivel de hashrate es muy poco probable que la red sufre del ataque del 51% porque será necesario de mucha inversión económica para lograr superar el poder de validación [54].

F. **Gas Fee:** Tarifa que se cobra por la ejecución de una transacción en la red blockchain porque cada transacción en la red consume recursos computacionales y energía, por lo que los nodos validadores deben ser incentivados para procesarlas, el gas fee se calcula en función de la complejidad de la transacción, el tamaño de los datos que se deben procesar y la congestión de la red en ese momento.

G. **Hash previo del bloque:** permite enlazar a incluirse en la cadena de bloques, un proceso que una vez registrado ya no es posible volver a modificar la información, debido a que los bloques al estar enlazados no deberían ser alterados por ningún motivo.

1.1.7.8. Métodos de vulnerabilidad:

A. Practical Byzantine Fault Tolerance: Tecnología que permite evitar los nodos que brindan información errónea, esto es para evitar que la red entre en conflicto solo porque algunos nodos no están de acuerdo con la información que se está registrando, es por ello que se tiene que evitar a aquellos datos anómalos que pueden ocurrir dentro de la red [55].

B. **Ataque replay:** Ataques que en la mayoría de veces se producen en los procesos de Hartford de la cadena de bloques, se produce cuando un actor externo intercepta para posteriormente repetir un proceso de transmisión de datos, las cadenas de bloques que no contemplan estas brechas de seguridad los atacantes pueden realizar sus ataques sin problemas, esta vulnerabilidad se encuentra principalmente en los registros que son divididos en el proceso de Hartford debido a que los usuarios que previamente realizaron transacciones en la cadena de bloques pueden volver a realizar movimientos para recuperar los

fondos enviados previo al hardford de la blockchain principal esto se debe a que existen nuevos validadores que no tienen referencia de las transacciones realizadas [56].

C. **Ataque Eclipse:** Ataque a la red blockchain en la que se los nodos de las víctimas son inundados con datos falsos, para poder manipular los datos que recibe el nodo fraudulento y de esta manera manipular la información en contra de la víctima, donde se desconecta del flujo de datos válidos de la red, esto es más comunicación para comunicación peer-to-peer debido a que se cuenta con una limitación en la cantidad de conexiones de cada nodo [57].

D. **Ataque de "51%":** Amenaza para la seguridad de cualquier blockchain que utiliza un algoritmo de consenso basado en prueba de trabajo (PoW), como Bitcoin. Este tipo de ataque se produce cuando un solo minero o un grupo de mineros controlan más del 51% de la potencia de procesamiento total de la red, lo que les permite controlar y manipular las transacciones y los registros en la cadena de bloques, mientras más nodos conformen la red más difícil se convierten ataques de 51% porque el atacante debe mantener constante el poder computacional que requiere la red.

E. **Quantum resistance:** Capacidad de una blockchain para resistir los ataques de los ordenadores cuánticos, que son mucho más poderosos que los ordenadores convencionales para la resolución de problemas matemáticos, este problema que aún no se ha resuelto afecta a las blockchains de PoW. Por lo tanto, es importante que los desarrolladores de blockchain continúen trabajando en soluciones para garantizar la resistencia cuántica en el futuro.

F. **Orphan block:** Bloque que se ha minado pero que finalmente no se ha incluido en la cadena de bloques principal. Esto puede ocurrir cuando se producen dos bloques válidos al mismo tiempo y la red de blockchain tiene que elegir uno de ellos para incluirlo en la cadena principal. Los bloques huérfanos pueden ocurrir en cualquier blockchain que utilice un algoritmo de consenso que permita la creación de múltiples bloques al mismo tiempo en PoS, pero es más difícil de encontrar casos en blockchains que utilizan PoW para la validación de transacciones.

G. **Sybil attack:** Ataque malicioso en una red de blockchain, en el que un atacante crea múltiples identidades o nodos falsos para obtener una influencia desproporcionada en el sistema, es posible prevenir con procesos como la prueba de trabajo, la prueba de participación y la reputación de los nodos.

1.1.7.9. Métodos de Mejoras:

A. Bulletproofs: Protocolo tiene de base dos de los principales sistemas de privacidad: En primera instancia cuenta con el concepto de conocimiento cero conocida por las siglas ZKP y las transacciones confidenciales conocido como confidential transactions – CT, en el primer concepto el nodo probador necesita convencer a un verificador de que cuenta con la información secreta verificable, esto brinda la ventaja de una máxima seguridad, privacidad y anonimato en la información de las transacciones, y el protocolo CT permite que las transacciones de la red sean cifradas y codificadas evitando que la información interna sea expuesta y visible [10].

B. **ZK-STARK:** Es una prueba criptográfica altamente seguras que basan en los principios de conocimiento cero, en la que los datos pueden ser fácilmente verificados la información privada de las transacciones que ocurren dentro de la red sin exponer la información, el significado deriva de preservación de privacidad, donde es posible realizar validaciones con un mínimo de pruebas, lo que convierte en un esquema con bastante integridad y solidez para la seguridad de información de la cadena de bloques [36].

C. **DAG (grafo acíclico dirigido):** Tipo de estructura de datos que se utiliza en ciertos tipos de tecnologías de registro distribuido, un DAG es un grafo dirigido en el que las aristas o enlaces van de un nodo a otro en una sola dirección y no hay ciclos en el grafo. Esto significa que no se puede seguir una secuencia de enlaces para volver a un nodo que ya se haya visitado, lo que evita cualquier tipo de bucle o retroceso en la estructura. Los DAG se utilizan como alternativa al proceso de minería en bloques en la cadena de bloques tradicional. En lugar de agregar transacciones a bloques y luego validar y confirmar esos bloques, los DAG permiten que las transacciones se confirmen y validan mientras se realizan.

D. **Sharding:** Técnica de escalabilidad que consiste en dividir la base de datos global en fragmentos más pequeños, llamados "shards" o fragmentos. Cada shard funciona como una cadena de bloques independiente, con su propio conjunto de validadores y su propio historial de transacciones, esto permite que no todas las transacciones lleguen directamente a la blockchain principal, sino que permita escalabilidad porque permite a la red soportar más transacciones y a mayor velocidad, la incorporación de los sharding en una blockchain

se realiza solo si es permitido por la red principal porque requiere de ciertos cambios en el protocolo principal.

E. **Master public key:** Tiene una propiedad de generar múltiples claves públicas sin la necesidad de acceder a las claves privadas, por tal razón estas direcciones públicas pueden ser compartidas sin arriesgar la información que debería ser privada por seguridad, estas llaves públicas permiten la transparencia en la información porque es posible verificar cierta información que contiene, pero no es posible acceder para una posterior modificación de los datos. Las claves semillas son generadas por el algoritmo HMAC-SHA512 y un número de 32 bits de aleatoriedad [36].

   Aleatoriedad en las Blockchain le permite obtener el grado de seguridad con el que actualmente cuentan, la criptografía asimétrica permite que la información solo es accedida por quien posee la clave privada, además para las máquinas es un proceso pueden realizar sin dificultades en la elección de número aleatorio para la clave public y la clave privada.

   Las áreas jurídicas y en las que se interactúa con información sensible son características únicas para aplicar los conceptos de Blockchain, para simplificar y acelerar los procesos de seguridad de información porque en cada uno de estos procesos la información es encriptada y solo es visible por personas autorizadas para el acceso a la información, esto es viable porque genera un cierto grado de confianza en cada uno de los actores que interactúan en los diferentes procesos de tratamiento de la información, esto permite una mejor gestión de documentos con veracidad en los datos convirtiéndose en un servicio seguro en el tratamiento y cuidado de la información [58].

La importancia y oportunidad que presenta para la democracia, los sistemas que permiten descentralizar la información con un grado de seguridad que no permita ser modificada, principalmente de los gobiernos y las aplicaciones de voto electrónico [59].

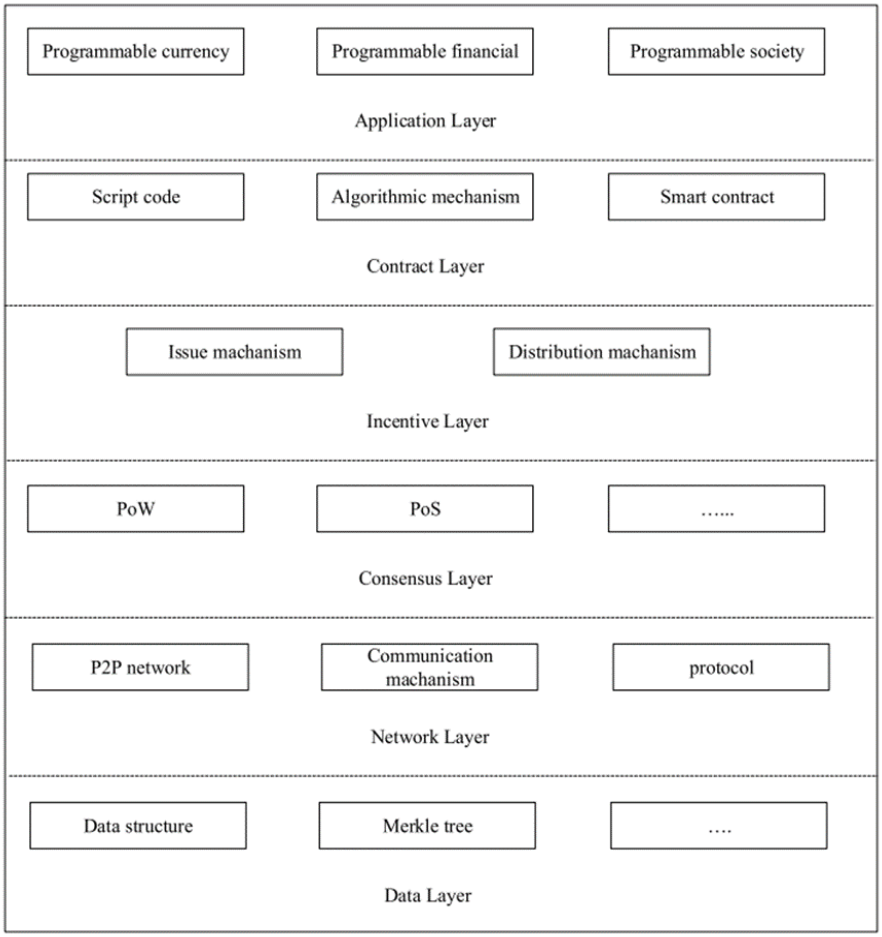


Fig. 11. Infraestructura de Blockchain sobre la capa de internet.

Nota: fuente IEEE explore, biblioteca digital de bases de datos, revistas y artículos de investigación [60].

1.1.7.10. Proyectos Blockchain:

A. Bitcoin: Presentado en 2008 por Satoshi Nakamoto [46]. Acuñó el concepto de blockchain con la incorporación de la moneda digital bitcoin. La blockchain es una base de datos descentralizada y pública

que registra todas las transacciones en la red de Bitcoin. Todos los usuarios de Bitcoin pueden ver todas las transacciones que ocurren en la red, pero no pueden acceder a la información personal de los usuarios, cada nueva moneda BTC se crea mediante un proceso llamado minería, que implica la resolución de complejos problemas matemáticos por parte de los nodos de la red. A medida que los nodos resuelven estos problemas, se crean nuevos bloques de transacciones y se agregan a la blockchain. La cantidad total de monedas que pueden existir solo será 21 millones, misma que está predefinida en el protocolo de la blockchain y se espera que el último Bitcoin sea minado en el año 2140.

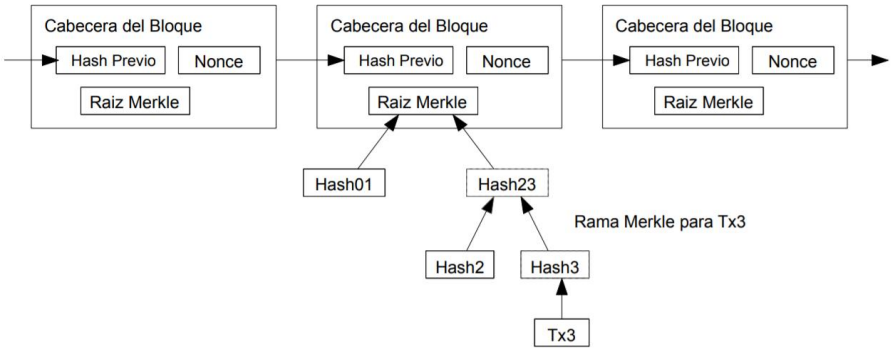


Fig. 12. Estructura para enlazar los bloques en la blockchain de bitcoin.

Nota: Los bloques consideran el hash del bloque previo para considerar la continuidad de la cadena [61].

B. **Ethereum:** Plataforma blockchain descentralizada que permite la creación de aplicaciones descentralizadas (dApps) y contratos inteligentes. Fue creada en 2015 por el programador Vitalik Buterin, algunas de sus características que ha logrado desarrollar son, soporte para contratos inteligentes los cuales son programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones y son los nodos de la red los encargados de que los contratos se cumplan según

lo acordado, la mayoría de las criptomonedas en Ethereum son tokens ERC-20. Estos tokens son creados utilizando un conjunto de reglas específicas y permiten a los desarrolladores crear sus propias criptomonedas, pero necesita de ciertos complementos como EVM para su correcto funcionamiento:

EVM (Ethereum Virtual Machine): Máquina virtual que se utiliza en la red de Ethereum para ejecutar contratos inteligentes escritos en lenguaje de programación Solidity. La EVM es una parte fundamental de la arquitectura de Ethereum y es responsable de procesar y ejecutar todas las transacciones y operaciones en la red. La incorporación de una máquina virtual se incorporó porque permite crear un ambiente seguro y confiable para la ejecución de contratos inteligentes, porque la EVM proporciona un ambiente de ejecución de programas aislado, en el que los contratos se ejecutan sin interferencia externa, lo que garantiza la seguridad y la confidencialidad de los datos y operaciones en la red, además permite que los desarrolladores pueden escribir contratos en cualquier lenguaje que pueda compilar a bytecode de la EVM, lo que brinda flexibilidad y facilidad de desarrollo en la red de Ethereum.

Ethereum utiliza un sistema de gobernanza descentralizada en el que los titulares de tokens pueden votar en propuestas para mejorar la plataforma además permite la interoperabilidad con otras cadenas de bloques, Algunos ejemplos de dApps en ETH son:

Uniswap: Exchange descentralizado. que permite el intercambio de compra o venta de criptoactivos.

MakerDAO: Proyecto que utiliza contratos inteligentes para crear una moneda estable respaldada por activos.

Chainlink: Proyecto que conecta los datos del mundo real con los contratos inteligentes en la blockchain de Ethereum.

C. **Polkadot:** Blockchain de código abierto que fue desarrollada por la fundación Web3 en 2016 y lanzada en mayo de 2020. Su objetivo es permitir la interoperabilidad y la conexión entre diferentes cadenas de bloques es decir un ecosistema de blockchain interconectado y descentralizado, diseñada para permitir la creación de cadenas de bloques independientes y especializadas que se conectan a través de la cadena de bloques principal, llamada Polkadot Relay Chain, el proceso de validación se produce mediante consenso PoS, cuenta con su propio token nativo (DOT), que se utiliza como medio de intercambio en la red y se puede utilizar para participar en el gobierno y la toma de decisiones de la red.

D. **Cardano:** Blockchain de código abierto lanzado en 2017, está diseñado para ser más medible, interoperable y sostenible que otras plataformas blockchain. Fundada por Charles Hoskinson, y desarrollada por la Compañía IOHK, Cardano se enfoca en la gobernanza descentralizada y la interoperabilidad, permitiendo a los desarrolladores crear aplicaciones descentralizadas (dApps) y contratos inteligentes. Utiliza un algoritmo de consenso llamado Ouroboros basado en PoS, que es energéticamente eficiente y seguro contra ataques del 51%. Cardano ha implementado un modelo de financiamiento descentralizado para proyectos y mejoras en la plataforma llamado "Cardano Improvement Proposals" (CIP), que permite a los miembros de la comunidad proponer ideas y mejoras, y votar sobre su implementación, La criptomoneda ADA se utiliza para pagar las tarifas de transacción en la plataforma.

1.1.7.11. Aplicaciones sobre una blockchain: Una blockchain puede tener diferentes utilidades, depende de los creadores las características que deseen incorporar, según su estructura y sus protocolos son diseñadas para pagos, finanzas descentralizadas, contratos inteligentes, etc.

A. **Smart Contracts** (Contratos inteligentes): Es comúnmente utilizado en las aplicaciones descentralizadas, donde lo que se haya establecido en las condiciones de un contrato este sea inmutable, un contrato inteligente hace referencia a un convenio entre dos personas o dos entidades como instituciones o empresas por ejemplo a modo de código informático programado el cual tiene la posibilidad de ejecutarse automáticamente cuando algunas de las partes no cumplen con lo acordado. La iniciativa ha sido iniciada en los años 90 por Nick Szabo, un pionero de la informática actualizada, que los definió como un grupo de promesas virtuales con unos protocolos asociados para hacer que se cumplan. Los contratos capaces se ejecutan en Blockchain, lo cual involucra que los términos se almacenan en una base de datos distribuida y no tienen la posibilidad de modificarse. Desde la aparición de la moneda digital Ethereum, se simplificó la construcción y ejecución de Smart contracts, debido a que en su protocolo tienen la posibilidad de desarrollar transacciones complicadas. Los contratos inteligentes son líneas de código que son ejecutadas automáticamente por las máquinas de acuerdo con las circunstancias, en estos procesos no existe un ente mediador, este último es reemplazado por un conjunto de máquinas que deben validar que se cumplan las condiciones que ambas partes firmaron como un acuerdo inicial.

B. **DAO (Organizaciones Autónomas Descentralizadas):** Las decisiones se toman a través de un sistema de votación descentralizado y las operaciones de la organización se ejecutan automáticamente a través de contratos inteligentes en una blockchain. Los miembros de la organización pueden proponer y votar sobre decisiones, y los resultados de las votaciones se implementan automáticamente a través de contratos inteligentes,

C. **Web 3:** Arquitectura descentralizada que utiliza tecnologías blockchain, los usuarios tienen un mayor control sobre sus datos y transacciones, debido a que no dependen de un tercero centralizado para procesar y almacenar la información. En su lugar, los usuarios interactúan directamente entre sí a través de la red blockchain, algunos de los proyectos en web3 pueden involucrar contratos inteligentes y utilizar criptomonedas y tokens digitales como medio de intercambio y almacenamiento de valor en la red. Web3 funciona como una red descentralizada que integra tecnologías blockchain, criptomonedas y contratos inteligentes, etc. para permitir la creación y operación de aplicaciones descentralizadas en una red P2P.

1.1.8. Lenguajes de programación blockchain:

A. Rust: Lenguajes más eficientes para el desarrollo de contratos inteligentes, principalmente por el manejo de memoria, además de una rápida integración con otros lenguajes de programación, la fiabilidad la productividad también caracterizan a este lenguaje, permite la ejecución de diferentes códigos en funcionalidades simultáneas, cuenta con sus propios pila Compiladores y una documentación definida para los desarrolladores. Se comenzó a integrar

desde el año 2018, Rust cuenta con su propia herramienta de línea de comandos para su ecosistema, permite la integración web Assembly con javascript y en lo relacionado a redes se caracteriza por un consumo mínimo de recursos. Entre los proyectos más resaltantes de este lenguaje encontramos a Solana la cual es una cadena de bloques dedicada a los pagos digitales a una alta velocidad.

B. **Solidity:** Es un lenguaje de alto nivel orientado a objetos, fue creado para implementar los contratos inteligentes en la red de Ethereum, adaptado para la máquina virtual de Ethereum y está estrechado interrelacionada con lenguajes como C++ más Python y JavaScript- la última versión estable de lenguaje es la Versión v0.8.17 según la información pública de su sitio web. Proyectos como Ethereum se han desarrollado en este lenguaje para la incorporación de contratos inteligentes.

C. **Haskell:** Es un lenguaje de programación funcional Las primeras versiones se registran desde 1990 Está dirigido principalmente para la Integración a partir de funciones, Agrégame mejoras de productividad para los desarrolladores Además de mantener un código limpio y fácil de mantener Contiene una documentación para el manejo de errores Y ofrece una gran estabilidad y viabilidad porque es poco frecuente encontrar errores de compilación según se detalla en sus medios sitios oficiales. Proyectos como la cadena de bloques de cardano de las finanzas descentralizadas fue desarrollada en este en este lenguaje.

D. **Lenguaje C++:** Debido a la cercanía que cuenta con el lenguaje máquina, permite agregar optimización en cada uno de los proyectos que son

desarrollados en dicho lenguaje de programación, aquí podemos encontrar a bitcoin el cual fue desarrollado en lenguaje C++ debido a que debe implementarse lo más cercano al lenguaje máquina y los protocolos bases de internet.

Para el cifrado de la información referente a las direcciones MAC las normas ISO han establecido un conjunto de normas que se han establecido como un estándar a cumplir en los procesos que involucra la dirección MAC, mismo es necesario utilizar el algoritmo de cifrado Keccak, debido a que permite utilizarse en procesos para verificar la integridad de los datos. [62]

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación:

Tipo de Investigación: Investigación tecnológica aplicada de tipo cuantitativa por el análisis de los datos recopilados en los procesos de inicios de sesión para determinar el porcentaje de efectividad en la autenticación y respaldar la hipótesis establecida fundamentado en datos estadísticos de acuerdo con la información obtenida en el proceso. Además de tecnológica porque se implementará la tecnología blockchain en un sistema login de pruebas, que simulará los inicios de sesión con los datos registrados en la blockchain.

Diseño de investigación: La investigación corresponde a un diseño cuasi experimental porque será aplicada a un grupo de dispositivos bajo un ambiente controlado y supervisado.

donde se pretenda vulnerar la seguridad en el proceso de autenticación con datos registrados de los usuarios y los dispositivos asociados, con acciones como alteración de nombres de usuario, contraseñas y sobrecarga de datos, es decir manipulando deliberadamente la variable Independiente para determinar el efecto en las variables dependientes [63].

2.2. Variables, Operacionalización

Variable Independiente:

implementación de tecnología blockchain asociando usuario y dispositivo

Variable Dependiente:

seguridad de autenticación.

TABLA 1: OPERACIONALIZACIÓN DE VARIABLES INDEPENDIENTE Y DEPENDIENTE.

Variable de estudio	**Definición conceptual**	**Definición operacional**	**Dimensiones**	**Indicadores**	**Ítems**	**Instrumento**	**Valores finales**	**Tipo de variable**	**Escala de medición**
Implementación de tecnología blockchain asociando usuario y dispositivo	Blockchain registrará los datos de los usuarios y dispositivos para los inicios de sesión.	La dificultad para los usuarios utilizar la tecnología implementada.	Accesibilidad	Usabilidad	Facilidad de uso Eficiencia Satisfacción	Ficha de Observación	Escala de 0/10 según promedio de los valores	Variable independiente	$\boldsymbol{U = \frac{(F + E + S)}{3}}$

Seguridad de autenticación	Proceso que permite verificar los permisos y la identidad del usuario mediante la presentación de credenciales	Medidas de seguridad con características de la tecnología blockchain	Seguridad de acceso	Eficacia	Intentos exitosos / total de intentos	Registro electrónico	Valor porcentual	Variable dependiente	$\boldsymbol{TS} = \left(\frac{\boldsymbol{T}}{\boldsymbol{N}}\right)\mathbf{100}$
				Efectividad	Accesos vulnerados / Total de intentos				$\boldsymbol{A} = \left(\frac{\boldsymbol{CN}}{\boldsymbol{T}}\right)\mathbf{100}$

2.3. Población y muestra de estudio:

Población:

La población en esta investigación considera la totalidad del problema a estudiar, donde las entidades que se están estudiando tienen una característica en común y da origen a los datos a la investigación con base en los objetivos del estudio [63].

La población para la presente investigación será representada por 7 métodos de autenticación más utilizados que existen hasta el año 2023 que son utilizados por los diferentes sistemas que están activos en el mercado, para los procesos de autentificación de los usuarios [64] las cuales se evaluarán mediante las ventajas y desventajas de cada método. La evaluación se detalla en el Anexo 07.

Muestra:

La muestra para la investigación es un subgrupo de la población, y será no probabilística, debido a que la selección de los elementos de estudio no depende de una probabilidad, sino a características planteadas por el investigador [63]

La muestra no probabilística para la presente investigación está representada por un (01) método de autenticación, se determinó según la percepción de seguridad por los usuarios explicada en la matriz de evaluación de los métodos de autenticación que se muestra en el anexo 08.

2.4. Técnicas e instrumentos de recolección de datos:

Observación: Técnica de investigación que implica observar y registrar sistemáticamente el comportamiento y los eventos de interés en un contexto determinado. El propósito es obtener información detallada y específica sobre el comportamiento humano en situaciones reales.

Con respecto a esta investigación, la observación es directa al comportamiento humano al momento de utilizar el prototipo de inicio de sesión que utiliza tecnología blockchain porque se pretender obtener datos como: Facilidad de uso, eficiencia y satisfacción del usuario, por lo tanto, es necesario el uso de técnicas de observación para evitar condicionar al usuario como es el caso de las encuestas para datos como satisfacción de usuario, el instrumento se detalla en el anexo 04:

Registro electrónico: Instrumento que registrará digitalmente los resultados de las diferentes pruebas que se realicen a la cadena de bloques para posteriormente determinar qué acciones lograron crear datos atípicos y analizarlos su influencia en los resultados. Permitirá el registro de cantidad de intentos de sesión, cantidad de sesiones con éxito y cantidad de accesos con datos aleatorios no registrados. el instrumento se detalla en el anexo 04:

2.5. Procedimiento de análisis de datos:

- **Usabilidad:** Facilidad con la que los usuarios pueden interactuar con él sistema. La facilidad permite a los usuarios realizar tareas específicas dentro del sistema sin dificultades, la eficiencia se refiere a la rapidez y precisión y la satisfacción se refiere a la percepción general de los usuarios sobre la experiencia al utilizar el sistema.

  En el año 2000 Jakob Nielsen y Tom Landauer demostraron que un test de usabilidad solo requiere de 5 test para obtener resultados representativos equivalentes a gran escala [65].

$$U = \frac{(F\ +\ E + S)}{3}$$

  Usabilidad = (Facilidad de uso + Eficiencia + Satisfacción del usuario) / 3

  Por ejemplo:

  F = 8/10 Facilidad de uso

  E = 7/10 Eficiencia

  S = 9/10 Satisfacción del usuario

  Usabilidad = (8 + 7 + 9) / 3 = 8

- **Eficacia:** Proporción de intentos de inicio de sesión exitosos en relación con el número total de intentos de inicio de sesión realizados, una alta tasa de éxito de sesión es deseable ya que indica que el sistema de autenticación es efectivo en la verificación de la identidad de los usuarios y permite un acceso seguro al sistema.

$$\boldsymbol{TS = \left(\frac{T}{N}\right)100}$$

  Un sistema de autenticación depende de la eficacia para lograr identificar al usuario verídico en un tiempo óptimo que no retrase los procesos posteriores [66].

  Eficacia = (Número de intentos de inicio de sesión exitosos / Total de intentos de inicio de sesión) x 100

  Por ejemplo:

  N = 100 intentos de inicio de sesión

T = 85 se completaron correctamente
TS = (85 / 100) x 100 = 85%

- **Efectividad:** Práctica de introducir información falsa o inventada en los campos de autenticación para intentar acceder al sistema de forma fraudulenta. Práctica conocida como "diccionario de datos" y es una técnica común utilizada por los hackers para acceder a los sistemas.

$$\boldsymbol{A = \left(\frac{CN}{T}\right) 100}$$

Seguridad informática son medidas que impiden operaciones no autorizadas en un sistema evitando daños de confidencialidad o integridad de la información [67].

Efectividad = (Cantidad de autenticaciones vulneradas / Total de intentos de acceso) x 100
Por ejemplo:
CN = 10 Accesos con datos aleatorios no registrados.
T = 100 intentos totales
A = (10 / 100) x 100 = 10%

2.6. Criterios éticos:

A. **Confidencialidad**: Principios relacionados con la privacidad de la información, garantizando de que la información obtenida en la investigación será protegida y no divulgada sin previo consentimiento del sujeto, garantía que se llevará a cabo mediante un conjunto de normas que limitan el acceso a la información.

Criterios de Rigor Científico:

A. **Credibilidad:** La investigación sigue los pasos estándares para la seguridad de información y el acceso a los resultados verídicos, con aspectos de confianza y fiabilidad en los resultados y conclusiones obtenidos a través de la investigación.
B. **Neutralidad:** El investigador no debe tener prejuicios o preferencias personales que puedan influir en los resultados de la investigación, evitando cualquier tipo de conflicto de interés que pueda sesgar la investigación además de utilizar técnicas de análisis y estadísticas apropiadas para asegurar la objetividad en la interpretación de los resultados.
C. **Validez:** Evaluar los diferentes resultados obtenidos en la investigación con precisión y confiabilidad para ser utilizados de manera efectiva en la toma de decisiones, estableciendo una validez externa para generalizar los resultados de la investigación a otros contextos o sistemas.

2.7. Controles ISO 27001 Blockchain y ciberseguridad:

ISO 27001 Desarrollado por la Organización internacional de normalización la cual tiene el propósito de gestionar la seguridad de información en las empresas, en la cual sin importar tamaño o actividad el eje más importante radica en los activos de información además de la teoría de gestión de calidad de PDCA (Planificar, hacer, verificar y actuar) generando una mejora continua en los sistemas de información de las empresas. [68]

5.1.1 Políticas Para La Seguridad De La Información: Se definen las políticas de la seguridad de la información, deben ser aprobadas por la dirección además de publicarse y comunicarse a las partes pertinentes ya sea usuarios o colaboradores que interactuarán con el sistema implementado, Las políticas deben actualizarse constantemente.

8.1.1 Inventario De Activos: La identificación de los activos de información que interactúan en todo el proceso del sistema es necesario identificarlo para definir los objetivos como mayor relevancia e importancia, de esta manera las brechas de seguridad deben ser minimizadas según el proceso de mejora continua que plantea la ISO 27001.

9.1.1 Política De Control De Acceso: Sólo personas autorizadas deben tener permisos de acceso limitado a cierta información confidencial o módulos del sistema, minimizando el riesgo de una vulnerabilidad total, Los privilegios de acceso deben realizarse de manera individual Además de que la organización debe contar con un plan de autenticación secreta para evitar brechas de seguridad a hackers en módulos confidenciales.

10.1.1 Política Sobre El Empleo De Controles Criptográficos: Establecer un sistema de cifrado de información Para mantener la confidencialidad e integridad de la información que mantiene internamente la empresa, quedando a cargo un área específica de la administración e implementación para mantener seguras las claves de cifrado de datos, además de establecer fechas de activación y desactivación de claves sobre todo cuando se emitan nuevas claves públicas desde un proveedor externo.

13.1.1 Controles De Red: Determinar procedimientos de comunicación e intercambio de información dentro de la organización, además de establecer acuerdos con los proveedores de telecomunicaciones y red para mantener la disponibilidad confidencialidad e integridad de los datos con la información que se utiliza en la organización, es necesario de un monitoreo y registro constante para identificar pruebas de sniffing u otras técnicas que se utilicen para el robo de información en red.

PDCA en ISO 27001: La Mejora continua en los sistemas de información, en conjunto con los activos de información se logra que los datos de una empresa resulten tratados y almacenados de manera segura. [68] Los resultados de la implementación ISO 27001 abarcan desde la minimización de riesgos, un incremento de confianza con la información los clientes y disminución de costos por multas de leyes de tratado de información personal.

SGSI en ISO 27001: Los sistemas de gestión de seguridad de la información es una implementación interna dentro de una empresa según sus requerimientos por organización, aplicado en proyectos de implementación blockchain se adaptará a la misión visión y objetivos de la empresa que implementa el proyecto.

Términos y condiciones:

El uso de datos confidenciales como la dirección MAC de un dispositivo debe ser aceptado bajo pleno conocimiento del usuario, evitando de esta manera multas por recopilación y tratado de información personal, la propuesta blockchain como servicio será realizado por una empresa externa de manera tercerizada debido a que los formularios de acceso a las plataformas actuales ya cuentan con un proceso establecido y para la incorporación de nuevas características es necesario que se muestre como un servicio adicional a los ya existentes, de esta manera será el mismo usuario quien acepte los términos y condiciones antes de utilizar el servicio blockchain.

IEC (Comisión Electrotécnica Internacional): Organización que mantiene más de 10000 estándares en 170 países y en conjunto con la ISO generan normas internacionales qué son un estándar para el tratamiento de información a nivel de usuario y empresarial. [69]

NIST (Instituto Nacional de Normas y Tecnología): Organización con sede en Estados Unidos Que promueve y desarrolla estándares en tecnologías Emergentes como blockchain. [70]

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados:

Los inicios de sesión se realizaron considerando tecnologías web con lenguajes de programación como JavaScript, css, HTML, php, electrón, power Shell y conexiones a bases de datos remota para la comunicación e intercambio de datos con la blockchain.

Usabilidad: Esta prueba se realizó mediante el método de recolección de datos por observación, los cuales fueron obtenidos durante el proceso de pruebas de la plataforma de pruebas con tecnología blockchain y la plataforma de login tradicional, son datos por observación ya que fue necesario obtener datos como:

a) **Facilidad de uso:** Considera las dificultades que tuvieron los usuarios en la fase de pruebas, esto permitirá considerar si la implementación de la tecnología blockchain representa un cambio radical para el usuario final.

b) **Eficiencia:** El sistema permite realizar las autenticaciones en un tiempo y similar a los procesos tradicionales.

c) **Satisfacción:** Considera la reacción que tuvieron los usuarios en el proceso de pruebas, es un valor determinado por el investigador a partir de visualizar la actividad.

TABLA 2: RESULTADOS DE USABILIDAD DE LA TECNOLOGÍA BLOCKCHAIN.

N° Prueba	Usabilidad	Usabilidad Promedio General
1	9.67	9.67
2	10.00	
3	9.33	
4	9.67	
5	10.00	
6	10.00	
7	9.33	
8	10.00	
9	9.67	
10	9.67	
11	9.67	

12	10.00	
13	9.67	
14	9.67	
15	9.67	
16	9.33	
17	9.00	
18	10.00	
19	9.67	
20	9.67	
21	10.00	
22	9.67	
23	9.33	
24	9.66	
25	9.33	

Nota: Resultado de datos obtenidos por observación, en una escala de 0-10 se logró obtener un promedio de 9.67, el cual representa un alto nivel de los ítems que conforman la usabilidad de una tecnología en la incorporación a los sistemas tradicionales, la usabilidad es el resultado promedio de 3 indicadores como: Facilidad de uso, eficiencia y satisfacción de usuario.

Efectividad: Representa el porcentaje de eficacia para autentificar al usuario con sus datos correspondientes, considera los intentos totales de inicio de sesión y el total de autenticaciones realizadas con datos verdaderos que corresponde a la cuenta.

$$\boldsymbol{A = \left(\frac{CN}{T}\right)100}$$

$$\boldsymbol{A = \left(\frac{25}{27}\right)100}$$

$$\boldsymbol{A = (0.92)100}$$

$$\boldsymbol{A = 92\%}$$

Fig. 13: Tasa de éxito de sesión.

Nota: El 92% de tasa de éxito de inicio de sesión significa que el sistema fue capaz de reconocer los datos a los que fue asociado la cuenta, para obtener este dato cada usuario en la fase de pruebas realizó su respectivo inicio de sesión con sus datos verdaderos. En el

proceso se agregó dos intentos de inicio de sesión porque esos usuarios tuvieron inconvenientes con el manejo del teclado al digitalizar sus datos verdaderos de acceso.

Eficacia: Datos obtenidos en el proceso de simulación de hackeo, donde el atacante recibe una serie de datos que corresponden a contraseñas de la cuenta real e intentará realizar combinaciones para lograr hackear la cuenta.

$$\boldsymbol{TS = \left(\frac{T}{N}\right)100}$$

$$\boldsymbol{TS = \left(\frac{1}{75}\right)100}$$

$$\boldsymbol{TS = (0.013)100}$$

$$\boldsymbol{TS = 1.33\%}$$

$$\boldsymbol{Efectividad = 100\% - 1.33\% = 98.67\%}$$

Fig. 14: Autenticaciones con datos aleatorios.

Nota: En la fase de pruebas de hackeo de cuentas con datos aleatorios no registrados solo El 1.33% de solicitudes fueron permitidas el acceso con datos que no correspondían a la cuenta y dispositivo del usuario verdadero, esto significa que la eficacia es de 98.67%, el caso del 1.33% fue un escenario atípico en el que el hacker obtuvo el usuario, la contraseña además logró obtener la dirección Mac del otro dispositivo y cambió la dirección MAC en su dispositivo de hackeo logrando que el sistema de autenticación lo reconociera como el usuario verdadero.

Código fuente: El código fuente desarrollado se detalla en el anexo 11, utiliza tecnologías web debido a que están ya integran librerías con que permiten el cifrado y la conexión a una arquitectura de base de datos que es utilizada para la blockchain.

```php
$databloques = [];
    $dataultimo =[];
    while($item = $res->fetch(PDO::FETCH_OBJ)) {
        $databloques[] = [
            'id' => $item->id,
            'correo' => $item->correo,
            'mcd' => $item->mcd,
            'password' => $item->password
        ];
    }
    echo json_encode($databloques);
```

Fig. 15: Listado de bloques registrad

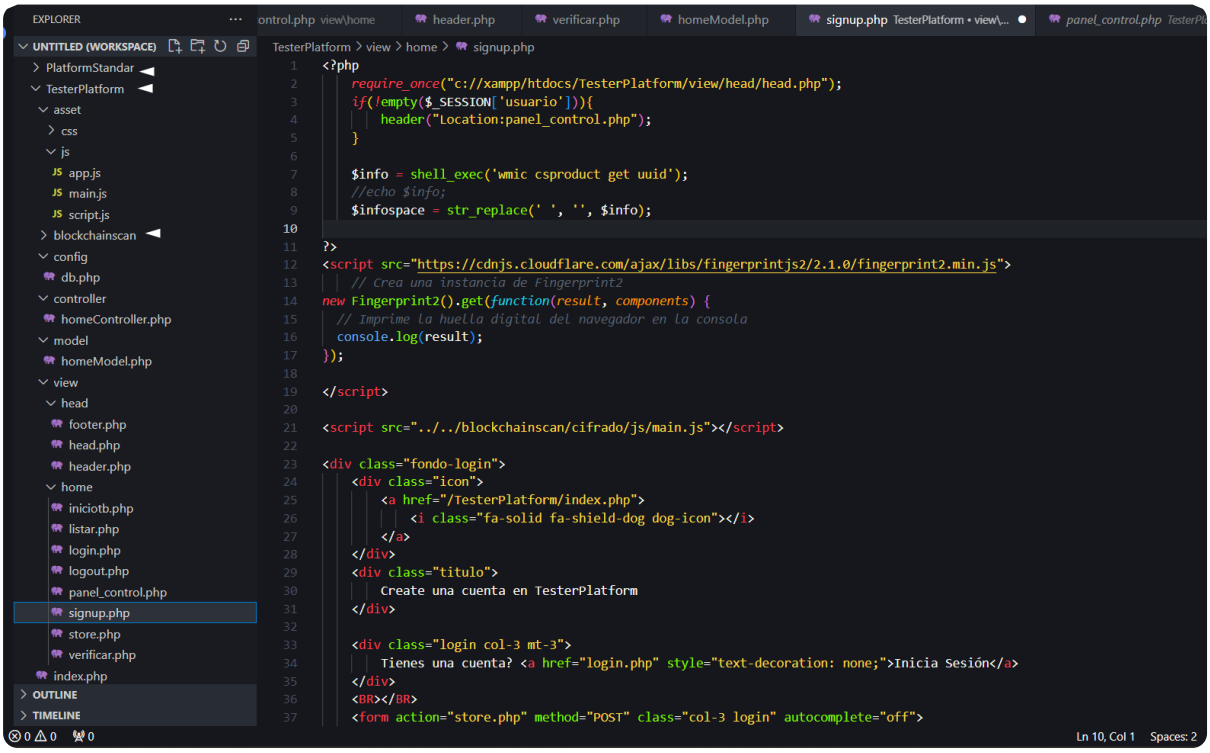


Fig. 16: Directorio de archivos de plataformas de investigación y pruebas

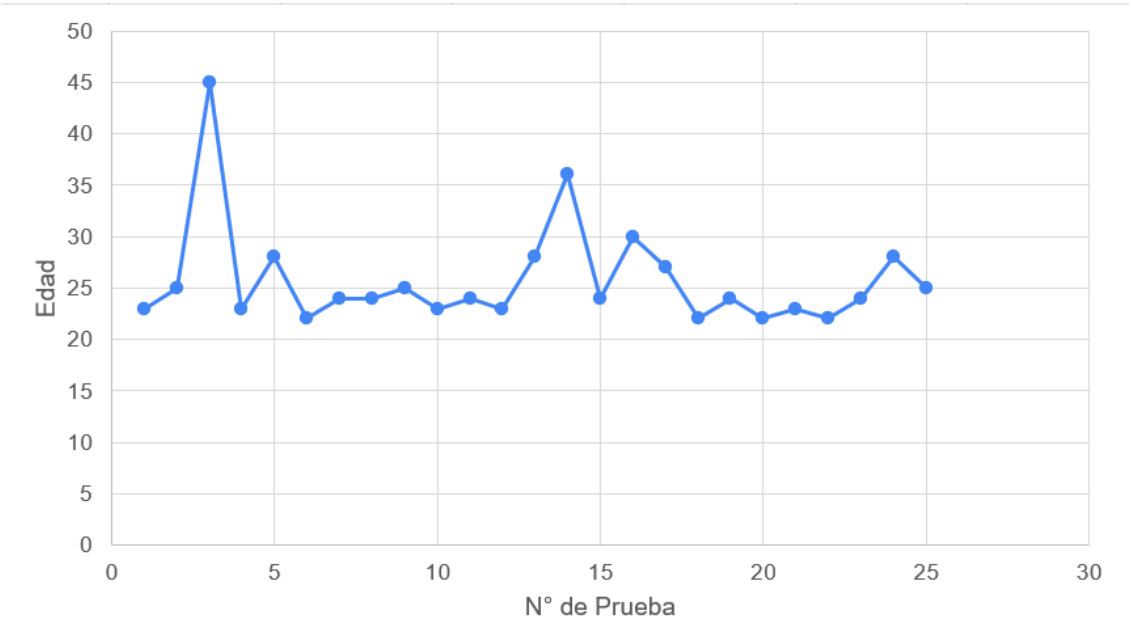


Fig. 17: Edad de personas participantes en la fase de pruebas

Nota: El rango de edades de usuarios que participaron en la fase de pruebas del sistema de autenticación se encuentra entre 20 a 50 años.

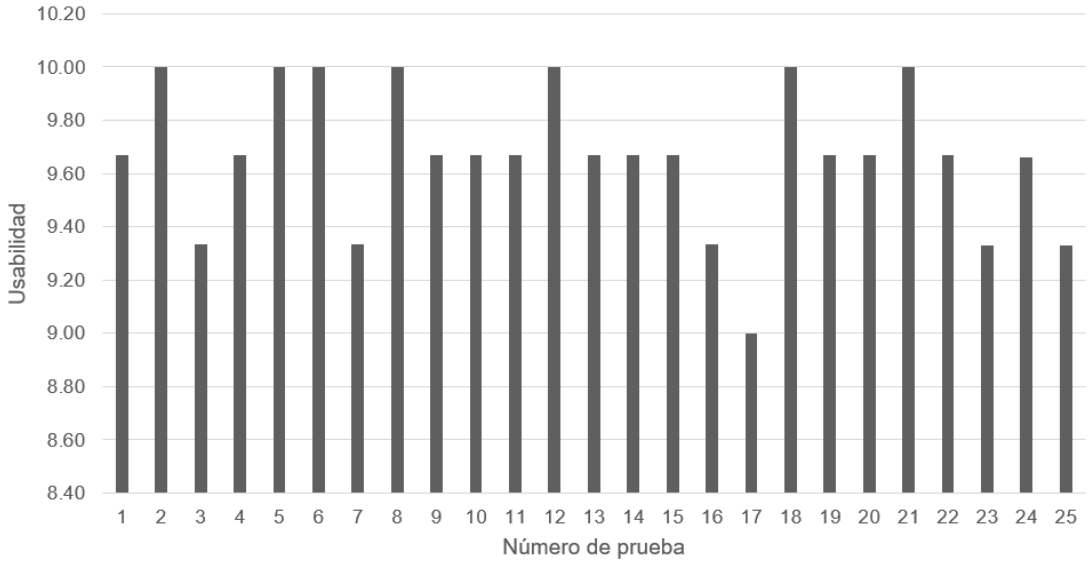


Fig. 18: Usabilidad individual por cada prueba.

Nota: Datos de usabilidad de la tecnología obtenidos por método de observación en cada prueba individual.

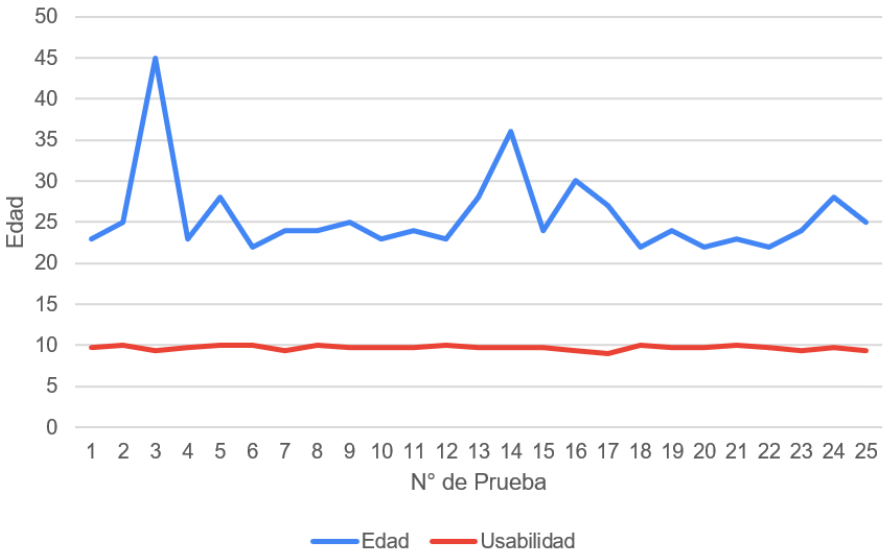


Fig. 19: Correlación entre edad de usuarios y usabilidad.

Nota*:* Las variaciones de las edades no representa un obstáculo para la usabilidad de la tecnología en el nuevo método de autenticación, porque jóvenes y adultos conocen el proceso de creaciones de cuentas y login de acceso, esto tambien significa que la incorporación de la dirección MAC de los dispositivos para asociar y verificar una cuenta, no representa un cambio radical en el estándar de autenticaciones tradicional porque en el formulario de registro o login de acceso lo correspondiente a la dirección Mac del dispositivo es autocompletada por el sistema de manera automática.

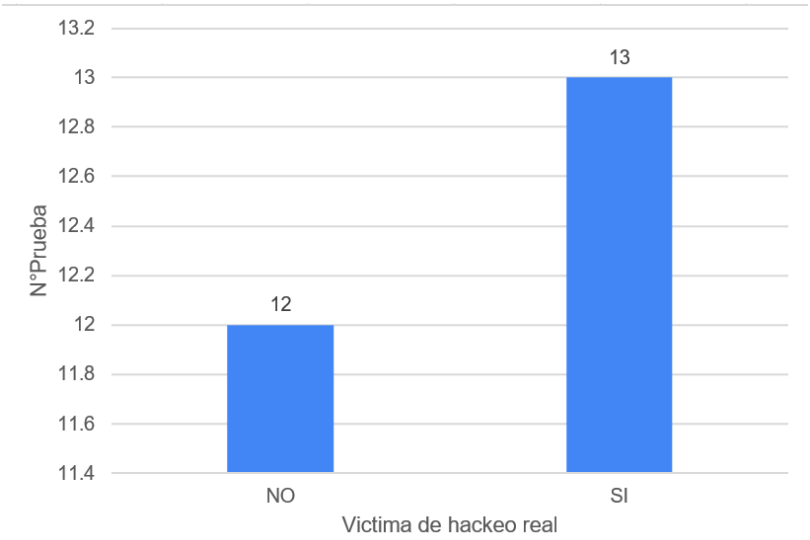


Fig. 20: Víctimas de hackeo de cuentas.

Nota: El 52% de los usuarios consultados respondió que fueron víctimas de hackeo donde sus cuentas fueron accedidas desde otro dispositivo.

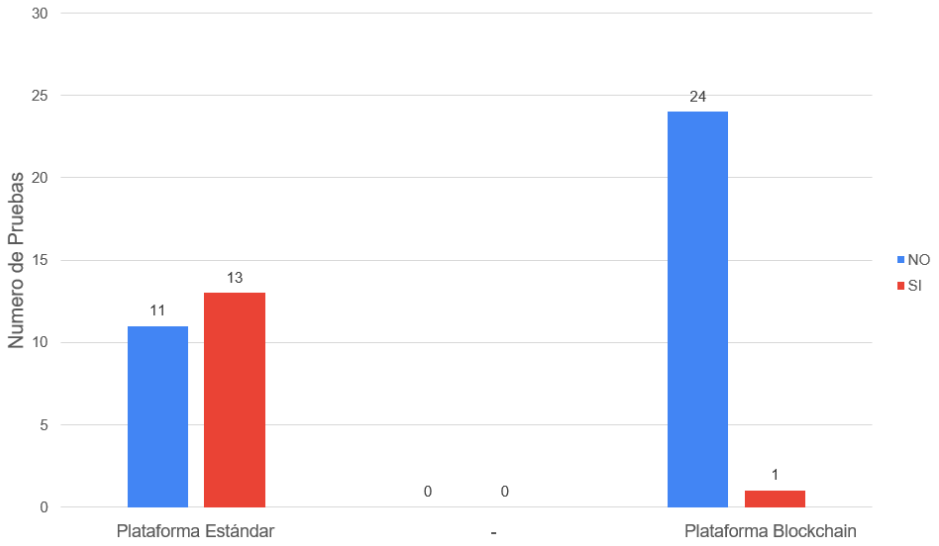


Fig. 21: Vulneración de cuentas desde otro dispositivo.

Nota: La plataforma con autenticación tradicional obtuvo un resultado de 44% para detectar al usuario verdadero, mientras que la plataforma que integra la Mac address para asociar los dispositivos y usuario logró un resultado de 96% para detectar el usuario y la cuenta asociada en los procesos de registro y autenticación con vulneración de cuenta desde otro dispositivo.

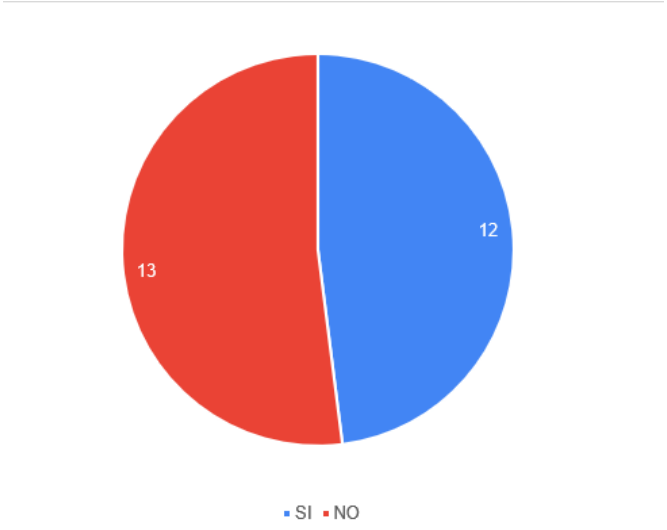


Fig. 22: Usuarios que utilizaron características de contraseñas seguras.

Nota: Las contraseñas creadas por los usuarios en la fase de prueba, el 52% no incorporó características de contraseñas seguras para crear una cuenta en la fase de pruebas, brecha de seguridad facilita el hackeo de cuentas por diccionario de datos de contraseñas comunes.

La figura 20 en relación con la figura 18 se puede obtener que el uso de contraseñas con características seguras no es un indicio de seguridad, porque los hackers igualmente vulneran las cuentas desde otro dispositivo cuando las contraseñas de los usuarios son expuestas u obtenidas a través de métodos por ingeniería social, fishing o incluso las mismas empresas de los sistemas filtran bases de datos debido a brechas de seguridad no controladas.

En la plataforma de pruebas de un total de 25 usuarios que participaron solamente uno conocía sobre el proceso de cambio de Dirección Mac de un dispositivo, en la que propuso el escenario para vulnerar una cuenta con el sistema planteado en la investigación cambiando la dirección Mac con la que pertenecía al usuario real de la cuenta, es el caso atípico que causó el hackeo de 1/25 de cuentas que fueron puestos a prueba en toda la fase.

3.2. Discusión:

Investigaciones previas lograron resultados similares, el caso del Método Voice-CD obtiene una tasa de error es del 5,3% en el Intercambio de claves autenticadas por contraseña de dos factores [16] lo que representa un 94.7% de efectividad en la autenticación para procesos de doble factor en un total de 30 participantes en la fase de pruebas.

En esta investigación se obtuvo un resultado de 98.67% de efectividad para autentificar a un usuario verídico y el dispositivo asociado a la cuenta con un total de 25 pruebas realizadas.

La investigación propuesta por [16] obtuvo un 5% de tasa de error mientras que según los resultados obtenidos en esta investigación esto se reduce al 1.33%, este porcentaje representa las cuentas que fueron hackeadas con datos falsos en las plataformas de pruebas.

La autenticación basada en tokens en los vehículos obtuvo una comunicación efectiva del 89,07 % con un tiempo de cálculo de 0,7 segundos [20]. En esta investigación se obtuvo un resultado de 98.67% en autenticación de cuentas de acceso, con la diferencia de que los tokens son reemplazados por un hash de información los cuales se registran en la blockchain

para que los participantes de la red solo puedan verificar, pero no conocer el contenido legible de la información original debido a que previamente es cifrado.

El método de autenticación propuesto en la investigación [71] consta de tres entes participantes como: usuario, autoridad y tercero en el cual el usuario permite que terceros accedan a los datos y visualicen las solicitudes y la autoridad es la encargada de agregar los datos a la blockchain.

En esta investigación se consideraron características como: Usuario, Dispositivo y la cuenta estos tres datos son asociados entre si para el proceso de autenticación, el usuario agregar los datos tradicionales de usuario y contraseña, el dispositivo agrega la dirección mac y esta información se considera para enlazar a la cuenta que pertenece al usuario verídico, si en el proceso de autenticación se detecta que la dirección mac es diferente a la que fue registrado entonces no se permite el acceso, esta información es almacenada en la blockchain por transparencia para verificar la autenticidad de los datos, porque si brinda los mismos hash por cada dato entonces corresponde al usuario verídico.

Procesar 1000 transacciones para intercambiar información se requirió un tiempo de respuesta estimado de 9 segundos [21] En esta investigación según la arquitectura propuesta cada nuevo usuario genera un bloque que se agregará a la blockchain conteniendo los datos que registró el usuario, es decir el tiempo por bloque no está preestablecido debido a que depende a la frecuencia de nuevos usuarios que requieran utilizar los servicios de autenticación.

Blockchain para brindar la solución de privacidad y seguridad para bases de datos utilizadas para inteligencia artificial, principalmente a información sensible y/o confidencial en bases de datos SQL y NoSQL [26] En esta investigación se utilizó la privacidad que brinda un hash de cifrado para evitar guardar en la blockchain la información en un formato legible para los seres humanos. El cifrado permitirá a los nodos participantes únicamente verificar una solicitud de autenticación porque si la información es verídica a la originalmente registrada entonces se generará el mismo hash.

3.3. Aportes de la investigación:

3.3.1. En esta investigación para el primer objetivo fueron seleccionados tres proyectos de finanzas descentralizadas, con el propósito de identificar las características funcionales y esenciales de la tecnología blockchain, a continuación, se muestran los resultados del análisis.

1. Proyecto Bitcoin:

Bitcoin es el primer proyecto que utilizó la cadena de bloques para respaldar la seguridad de las transacciones de pagos realizadas en la red. Utiliza blockchain pública, permite la descentralización y seguridad, debido al trilema de las blockchains no permite escalabilidad debido a que solo soporta entre 7 y 10 transacciones por segundo, entre sus características es posible resaltar:

A. Utiliza blockchain pública para el registro de las transacciones previamente cifrada con el algoritmo SHA-256 y posteriormente validada por los respectivos nodos.

B. Las transacciones son inmutables y visibles para todos los participantes de la red, pero anónimas porque se conforman de caracteres alfanuméricos no legibles para el humano que evita asociar una dirección wallet a una persona natural.

C. La validación de transacciones se realiza por nodos mineros que cuentan con hardware computacional.

D. Utiliza el método de consenso de prueba de trabajo (PoW) en cuál requiere de procesamiento computacional para encontrar el nonce, el cual es un número que confirma la validación de un bloque nuevo.

E. Un nuevo bloque de la blockchain es agregado cada 10 minutos, la dificultad de minado se adapta para lograr cumplir con la norma

previamente establecida en el protocolo de la red.

F. Las transacciones requieren de un pago con la moneda de la res (BTC) utilizado para recompensar a los nodos mineros de la red.

G. Permite la integración de blockchain de capa dos para permitir mayor escalabilidad en la red principal.

Considerando el white paper de bitcoin del 2008 [46] además del portal de transparencia de la red [72] que permite visualizar detalles de:

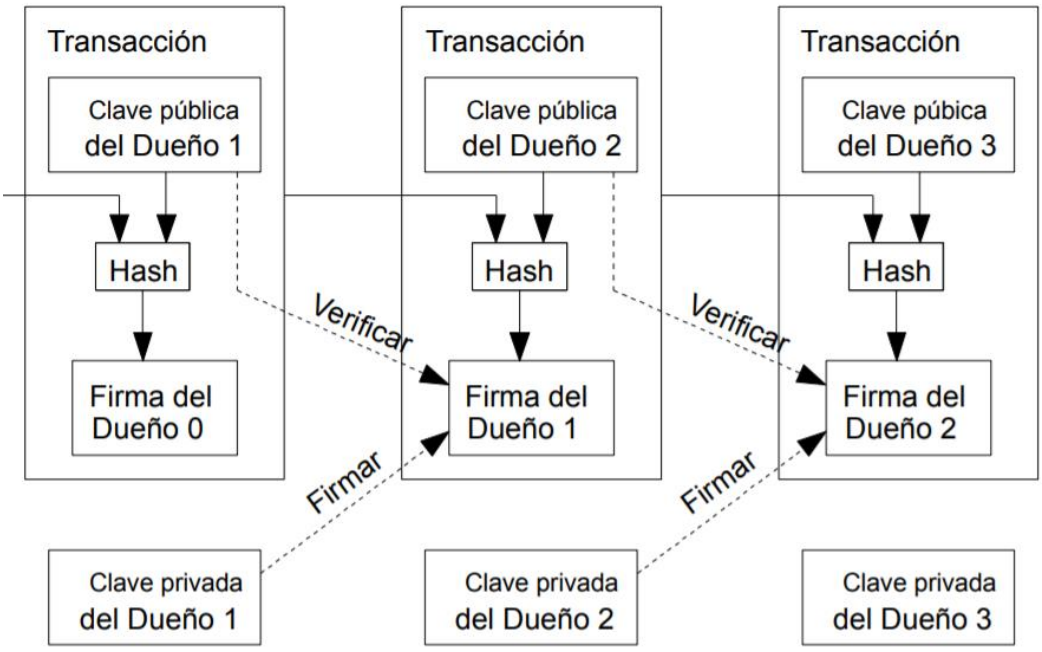


Fig. 23: Validación de transacciones

Nota: Fuente bitcoin org *[46]* proyecto de moneda descentralizada para pagos online a través de internet.

Estadísticamente es la primera red que actualmente tiene menos ataques originados dentro de la blockchain principal permitiendo que el alto hashrate lo convierte en uno de los activos más seguros [73], los ataques de “51%” en la red requieren de un gran poder computacional para poder mantener constante la minería de bloques a la misma cantidad de la red honesta.

La probabilidad de éxito del nodo hacker cae de manera exponencial según los valores de Z mientras el número de bloques en los que deberá encontrar el nonce

sigue incrementándose [46], representado por la fórmula.

$$1 - \sum_{k=0}^{z} \frac{\gamma^k \, e^{-y}}{k!} \, (1 - \, (^{q}/_{p})^{(z-k)})$$

Donde:

La fórmula permite calcular la probabilidad de éxito de un atacante en un escenario específico. En primera instancia se representa la sumatoria de los valores del rango específico desde 0 hasta el nuevo valor que obtiene K. El valor “q” representa la probabilidad de que un evento de ataque tenga éxito en un intento individual, mientras que “z” indica el número máximo de intentos que el atacante realizará y mientras más intentos por agregar bloques a la cadena la probabilidad disminuye exponencialmente porque los nodos honestos siguieron incluyendo bloques.

2. Proyecto Ethereum:

Plataforma que utiliza la tecnología de la cadena de bloques con capacidad para la ejecución de Smart Contracts, además permite la ejecución de aplicaciones descentralizadas desarrolladas en solidity el cual es su lenguaje de programación principal para los proyectos de la red.

- **A.** Ethereum utiliza el método de validación de transacciones Proof of Stake (PoS)
- **B.** Permite la incorporación de blockchains de segunda capa que brinda características de escalabilidad, ya que la red principal solo puede validar en promedio 13 transacciones por segundo.
- **C.** El cifrado de la información de las transacciones se realiza a través de los algoritmos como Keccak-256 o SHA-3 además de Elliptic Curve Digital Signature Algorithm (ECDSA) para la verificación y autenticación de

transacciones.

D. Permite la interoperabilidad con otras cadenas de bloques, utilizando el estándar único de la red como los ERC-20 y ERC-721, el estándar ERC-20 permite la creación de token fungibles que permite la transferencia y gasto entre cuentas (criptomonedas) en cambio el estándar ERC-721 permite la creación de token no fungibles (NFT) los cuales cuentan con un identificador único en la red.

La blockchain de Ethereum cuenta con su respectiva plataforma de transparencia denominada Etherscan, la cual permite verificar el estado de la red, actualmente mantiene un registro de 1961.91 Millones de transacciones, con un total de 17225751 bloques. La estructura de la red brinda seguridad a los contratos inteligentes y a los procesos de pagos, permite la tokenización de activos para realizar seguimiento seguro dentro de la cadena de bloques.

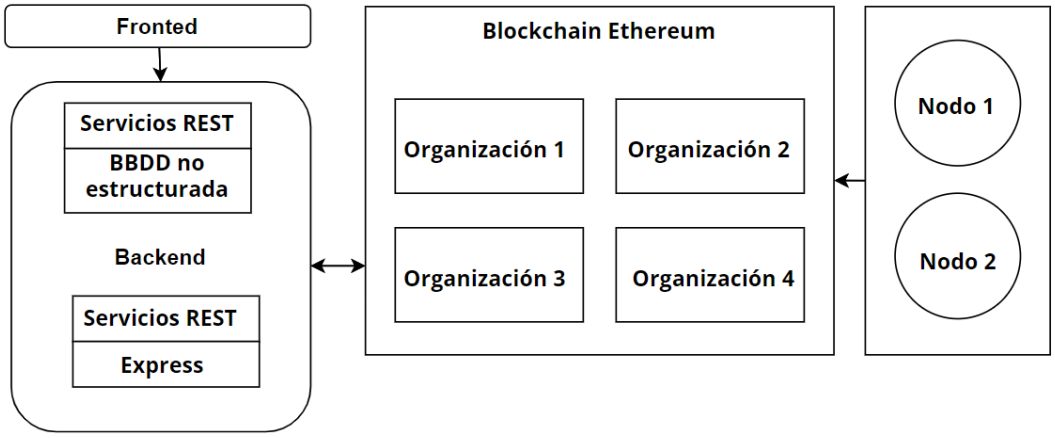


Fig. 24: Arquitectura de proyecto Ethereum

Nota: fuente Ethereum org proyecto blockchain para contratos inteligentes.

3. Proyecto Solana:

La cadena de bloques más rápida hasta la actualidad utiliza el método de consenso de PoH (Proof of history), posee una capacidad para procesar 60.000 transacciones por segundo, la blockchain principal contiene 175.918.268 bloques, con un total de 173.983.415.644 hasta mayo 2023, sus características principales son:

A. Utiliza el método de consenso de Proof of Stake y Proof of history que permite la validación por votos con sus respectivas marcas de tiempo.

B. Permite procesar 60 000 transacciones por segundo, lo convierte en la cadena de bloques más escalable para procesos que requieren gran cantidad de transacciones en la mínima cantidad de tiempo.

C. Bajos coste por transacción para los pagos a los nodos validadores, permite la incorporación de contratos inteligentes con interoperabilidad para intercambiar información con otras cadenas de bloques.

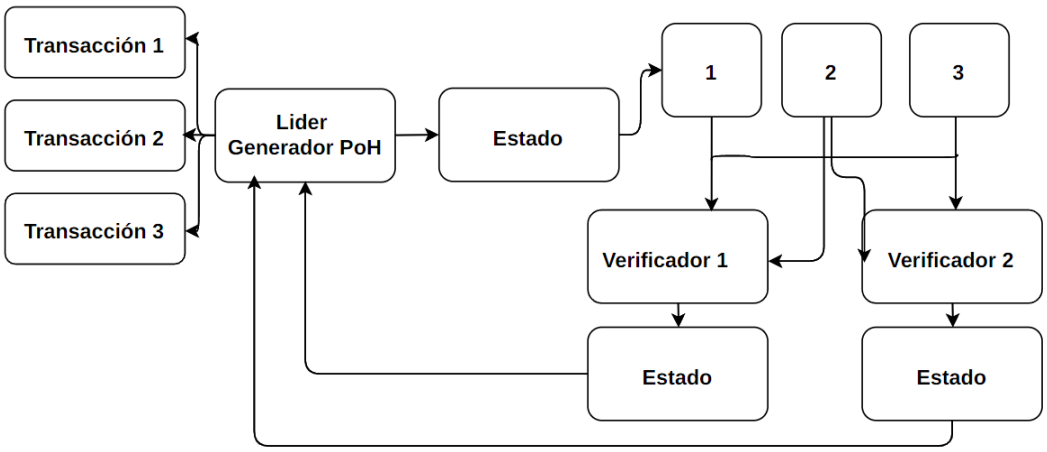


Fig. 25: Arquitectura de blockchain de solana networks

Nota: fuente solana org proyecto de blockchain para dapps de alta escalabilidad.

Integra un sistema de paralelización de transacciones llamado Pipeline, características que le permite obtener altas velocidades de en las transacciones, la escalabilidad expone la seguridad de la red porque los datos tienen que ser validados sin demasiadas confirmaciones, una característica que podría saturar a un nodo y pausar la red de manera indeterminada. El mecanismo de consenso Proof of History (PoH) permite que los nodos se sincronicen rápidamente y de manera precisa, lo que reduce el tiempo de procesamiento y aumenta la velocidad de la red. Además de utilizar una arquitectura orientada a eventos que permite la

ejecución simultánea de múltiples transacciones en paralelo.

TABLA 3: RESULTADOS DE ANÁLISIS DE PROYECTOS DEFI.

	Método de consenso	Transacciones / segundos	Metadatos de bloque
Bitcoin	Prueba de Trabajo (PoW)	7 – 10	Marca de tiempo, direcciones de billeteras, nonce, dificultad, monto de transacciones, número de bloque, hash de la transacción y del bloque y firma de la transacción.
Ethereum	Prueba de participación (PoS)	13	Marca de tiempo, direcciones de billeteras, monto de transacciones, número y hash del bloque anterior, códigos y estados de contratos inteligentes.
Solana	Prueba de participación (PoS) y Prueba de historial (PoH)	60 000	Marca de tiempo, direcciones de billeteras, monto de transacción, número de bloque, firma digital.

Nota: Elaboración propia

3.3.2. El diseño de la estructura blockchain para el segundo objetivo requirió la definición de un conjunto de características de compatibilidad con base a los rasgos de los proyectos previamente examinados, a continuación, se muestra la descripción de estas características:

A. Las cadenas de bloques privada permiten mayor rapidez en validación de las transacciones, limita la descentralización, pero es una característica necesaria porque según el análisis de proyectos, solana obtiene escalabilidad que puede llegar a las 66000 transacciones por segundo y considerando que se aplicará para procesos de accesos a los sistemas se espera un gran flujo de usuarios.

Los usuarios de un sitio web solo tienen un margen de espera de 3 a 4 segundos para posteriormente buscar otra alternativa [74].

B. La criptografía de la información requiere de eficiencia en seguridad, tiempo y procesamiento computacional, SHA-256 o AES son algoritmos que consideran estas características, el proyecto bitcoin incluye estos algoritmos para el cifrado de las transacciones y las firmas digitales.

C. Metadatos de marcas de tiempo (timestamp) permite en los registros de la blockchain una mayor eficiencia en la red para organizar las transacciones según orden cronológico de ejecución, el proyecto de solana considera esta característica para otorgar prioridad de validación a las transacciones que llevan mayor tiempo en espera.

D. Las validaciones de campos completos es un proceso que realizan todas las cadenas de bloques porque son datos obligatorios para completan la estructura de una transacción y antes de ser enviada para la respectiva validación se verifica que se incluyan los datos completos.

E. La validación de una transacción en los proyectos analizados se produce después de que los nodos participantes de la red confirman que la dirección wallet de envío y recepción son válidas y cuentan con los activos suficientes según los registros de los bloques previos que ya pertenecen a la blockchain.

F. Los bloques de la red contienen registros que previamente fueron aceptados y distribuidos a todos los nodos de la red, la información de un bloque es inalterable, esta solo puede ser consultada para verificar futuras transacciones.

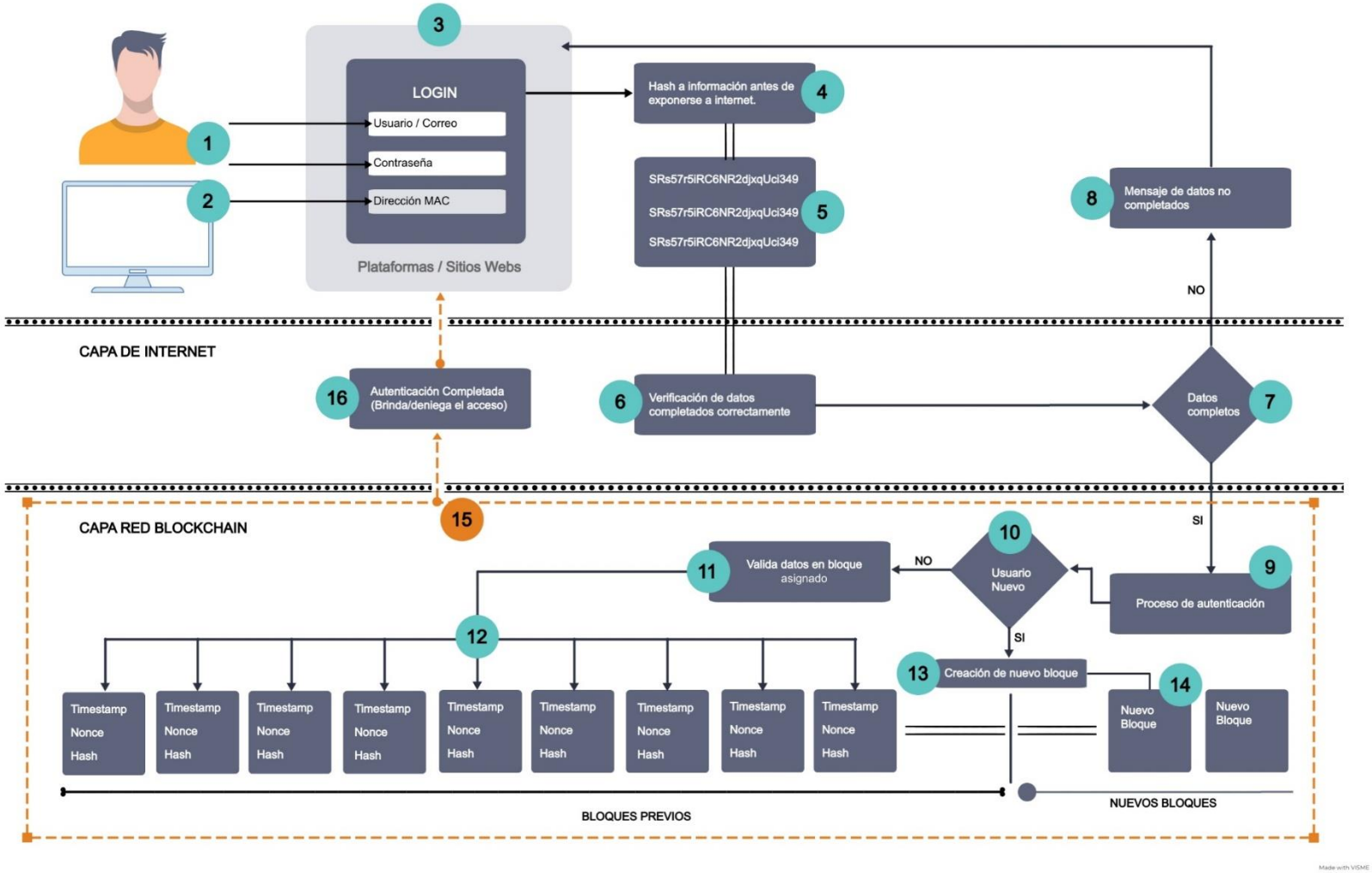


Fig. 26: Propuesta de arquitectura blockchain.

N° de proceso	Descripción
1	El usuario utilizará sus datos de usuario y contraseña de la misma manera tradicional para acceder a sus cuentas en sitios web y plataformas en internet.
2	El campo correspondiente a la dirección Mac del dispositivo será no editable y se auto completará por el sistema, es la información principal que utilizará la blockchain para brindar la seguridad a la cuenta.
3	Interfaz gráfica de login para la arquitectura propuesta, incluye los campos de datos que corresponde al usuario y al dispositivo, los sitios web o plataformas que utilicen esta tecnología implementará el nuevo modelo de formulario.
4	Los datos del usuario y dispositivo se encriptarán antes de interactuar con la capa de internet evitando que la información del usuario sea expuesta y que posteriormente se utilice para la suplantación de identidad.
5	Los datos correspondientes son cifrados y no legible para el ser humano, datos que se enviarán para la primera validación.
6	La validación en primera instancia se realiza verificando que los tres campos correspondientes contengan información, es necesario para evitar la sobrecarga de transacciones en la mempool de la blockchain de transacciones con datos incompletos.
7	Si un dispositivo contiene algún tipo de restricción a la dirección Mac el formulario no auto completará, por tal razón no será posible continuar con el proceso y se le informará al usuario antes de continuar con el proceso de autenticación.

8	El usuario será informado a través de la interfaz gráfica del proceso N°3, mostrando un mensaje que ciertos campos de entrada no fueron completados.
9	El proceso de autenticación se realiza en la blockchain según la autenticidad de los datos recibidos, porque la primera validación solo se comprueba que la solicitud de autenticación posea los datos completos.
10	Proceso condicional donde si es un usuario ya registrado se procede a verificar su información en los bloques previos, pero si es un nuevo usuario de la red entonces se asignará un nuevo bloque que registrará su información para los próximos inicios de sesión.
11	Proceso que prepara a los nodos participantes para verificar que la información proporcionada desde el formulario es verídica antes de autorizar el ingreso.
12	Los usuarios registrados únicamente consultan la veracidad de los datos en los bloques previos de la blockchain, si los datos proporcionados corresponden a la información registrada en un bloque entonces se autorizará en proceso de autenticación.
13	La creación de un bloque significa un nuevo usuario y que recién está creando su cuenta en la plataforma o sitio web. Porque posterior a la implementación de esta arquitectura de autenticación en una plataforma, todos los usuarios empezarán por defecto con la condición de “nueva cuenta” para evitar que personas externas que cuenten con la información de acceso de la cuenta normal logren registrar dispositivos no autorizados por el usuario verídico.
14	Un nuevo bloque registra una marca de tiempo (timestamp) un nonce y un hash que corresponden a la información verídica que se consultará para autorizar futuros inicios de sesión en la plataforma.

15	Proceso que engloba la autenticación del usuario, la creación de un bloque permite la autorización automática porque es un nuevo usuario, pero si es un usuario ya registrado dependerá de la autenticidad de los datos proporcionados en el formulario para obtener una autorización o denegación de acceso a la cuenta.
16	El resultado del proceso de autenticación es informado al usuario a través de la interfaz del proceso N°3 después de validarse en la capa de red blockchain y comunicarse por intermedio de la capa de internet.

Tabla 4: Descripción de procesos de propuesta de arquitectura blockchain

Para el usuario final la implementación de la tecnología blockchain bajo la arquitectura propuesta en esta investigación no representa una disrupción total en el estándar de accesos a las cuentas, porque el nuevo campo no editable del formulario para la dirección MAC se auto completará por el sistema.

3.3.3. En esta investigación para el tercer objetivo se utilizaron tecnologías web para implementar la estructura planteada y obtener los respectivos resultados, se conforma de un sistema que representa los accesos y el sistema descentralizado que será con el cual interactúan los nodos participantes de la red para validar las transacciones o solicitudes de acceso. La plataforma de pruebas se construyó bajo la arquitectura modelo-vista-controlador (MVC), utilizando tecnologías como JavaScript, php, HTML, css, etc. que permiten una simulación general de los sistemas que actualmente se utilizan para asignar credenciales para identificar a un usuario dentro de su plataforma.

ARQUITECTURA DE SOFTWARE CLIENTE - SERVIDOR:

La arquitectura cliente servidor ha logrado una popularidad debido a las ventajas que ofrece como la bajo costes en hardware, diferentes herramientas como Oracle incorporan formas de integración para lograr el desarrollo de aplicaciones de cliente servidor de manera eficiente al igual que aplicaciones que se ejecutan a nivel local. [75]

La plataforma de la investigación presenta la arquitectura de software cliente – servidor, porque permite la separación de la lógica de la aplicación y la gestión de la base de datos que en esta investigación es representada por la Blockchain, a continuación, se detalla la arquitectura de software cliente – servidor en conjunto con la arquitectura lógica y física de los componentes de la plataforma implementada en la investigación.

CLIENTE: Engloba todo el proceso relacionado con interfaces visuales (front-end) que el usuario visualiza e interactúa al utilizar la plataforma de prueba, considerando que las aplicaciones web y nativas requieren de un proceso de autenticación de usuarios, es por ello por lo que cuentan con un proceso en el cual se encargan de enviar información a los servidores para verificar la veracidad de los usuarios.

SERVIDOR: Abarca todos los procesos relacionados con el backend del sistema, permitiendo la integración de la función principal la cual consiste en manejar las solicitudes de autenticación ingresadas como peticiones a los usuarios y la blockchain se encargará de verificar entre la información registrada y los datos brindados por el usuario pertenecen al usuario verídico, esto se realiza a través de tokens por usuario y en las credenciales registradas inicialmente, la información es transportada por protocolo de TCP/IP a través de sockets.

La arquitectura cliente servidor su característica principal es la segmentación de responsabilidades, según las actividades llevadas a cabo por parte del cliente y el servidor, logrando una mayor escalabilidad del proyecto, además de brindar mantenibilidad Y seguridad en todo el proyecto de software.

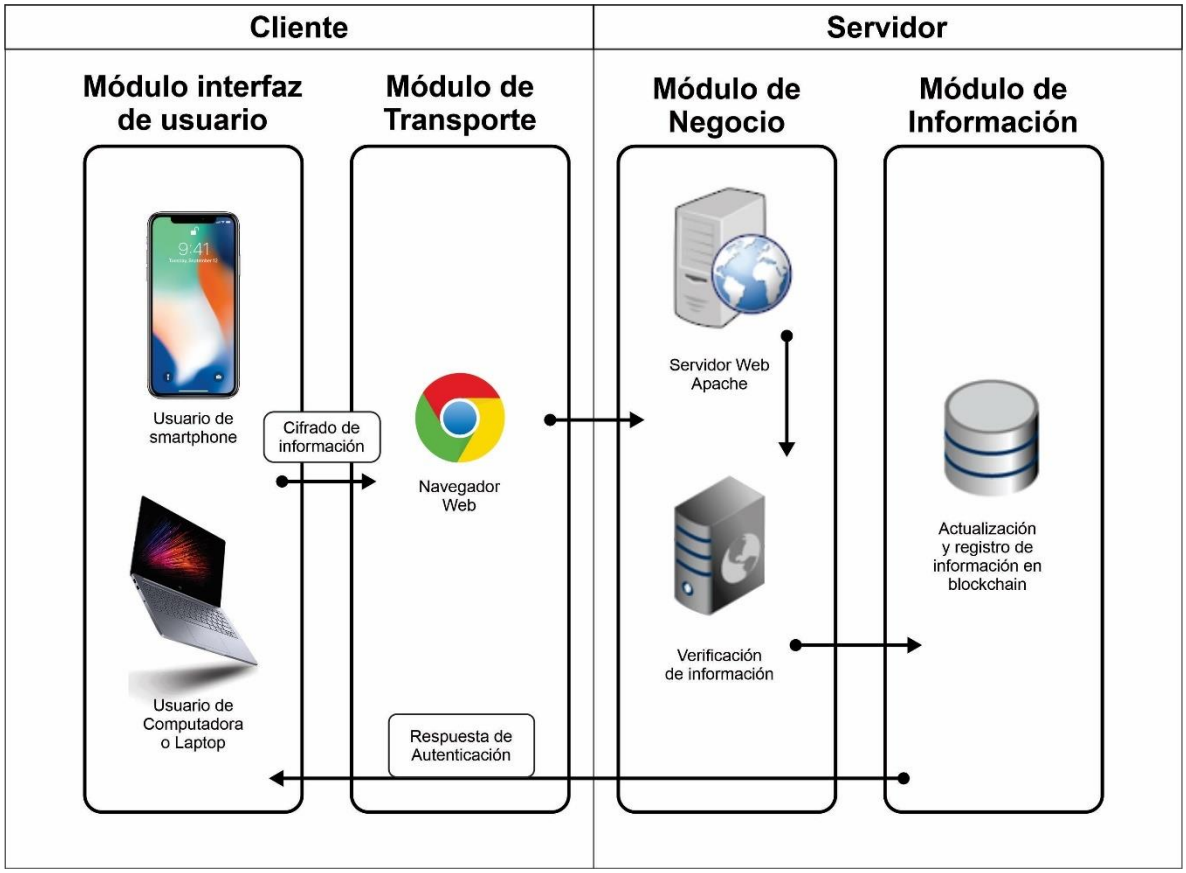


Fig. 42: Arquitectura física del software implementado

Fuente: Elaboración Propia

Descripción de componentes: A continuación, se explican los componentes físicos que interactúan para permitir el correcto funcionamiento de la plataforma de pruebas desarrollado para la investigación.

- **Componente de usuario de Smartphone o computadora:** El primer componente con el que se interactúa para utilizar el sistema es aquel donde se encuentran los dispositivos de los usuarios. A través de este componente, los usuarios pueden iniciar sesión o registrarse para obtener una cuenta en las plataformas que implementen el método de autenticación presentado en esta investigación.
- **Componente cifrado de información:** Componente responsable de recibir y procesar la información del usuario, la cual se asociará con la cuenta al momento de su registro en la plataforma. Este proceso de cifrado se lleva a cabo de manera local en el dispositivo del usuario, garantizando que la información confidencial no sea

expuesta a riesgos que se encuentran en la capa de internet.

- **Componente de navegador web:** Este componente se encarga de verificar que los formularios de registro o inicio de sesión estén completos con la información correspondiente en cada campo, garantizando así que la blockchain no realice validaciones con datos incompletos. Posteriormente, esta información es transportada de manera cifrada a los servidores que alojan la blockchain para su validación respectiva.
- **Componente de servidor web:** El componente encargado de recibir y procesar la información según la lógica de negocio implementada internamente, utiliza diversas tecnologías relacionadas con el tratamiento de datos y el backend correspondiente. Este proceso incluye las reglas de almacenamiento estructurado conforme a las directrices de la programación de la cadena de bloques.
- **Componente de verificación de información:** Este componente se encarga de realizar la verificación de datos para determinar si el usuario ha sido registrado previamente, esto permite comprobar si la información recibida corresponde verdaderamente al usuario que está intentando iniciar sesión.
- **Componente de actualización y registro de información:** Componente que se encarga de integrar un nuevo bloque en la blockchain, lo que implica actualizar la cadena de bloques para que sea visible en los nodos servidores responsables de validar la información para futuros procesos de inicio de sesión.
- **Componente de respuesta de autenticación:** Componente responsable de generar la respuesta al cliente según los resultados de la validación de información en la blockchain. Basado en dichos resultados, se actualizará la interfaz de usuario para permitirle visualizar el mensaje final del proceso.

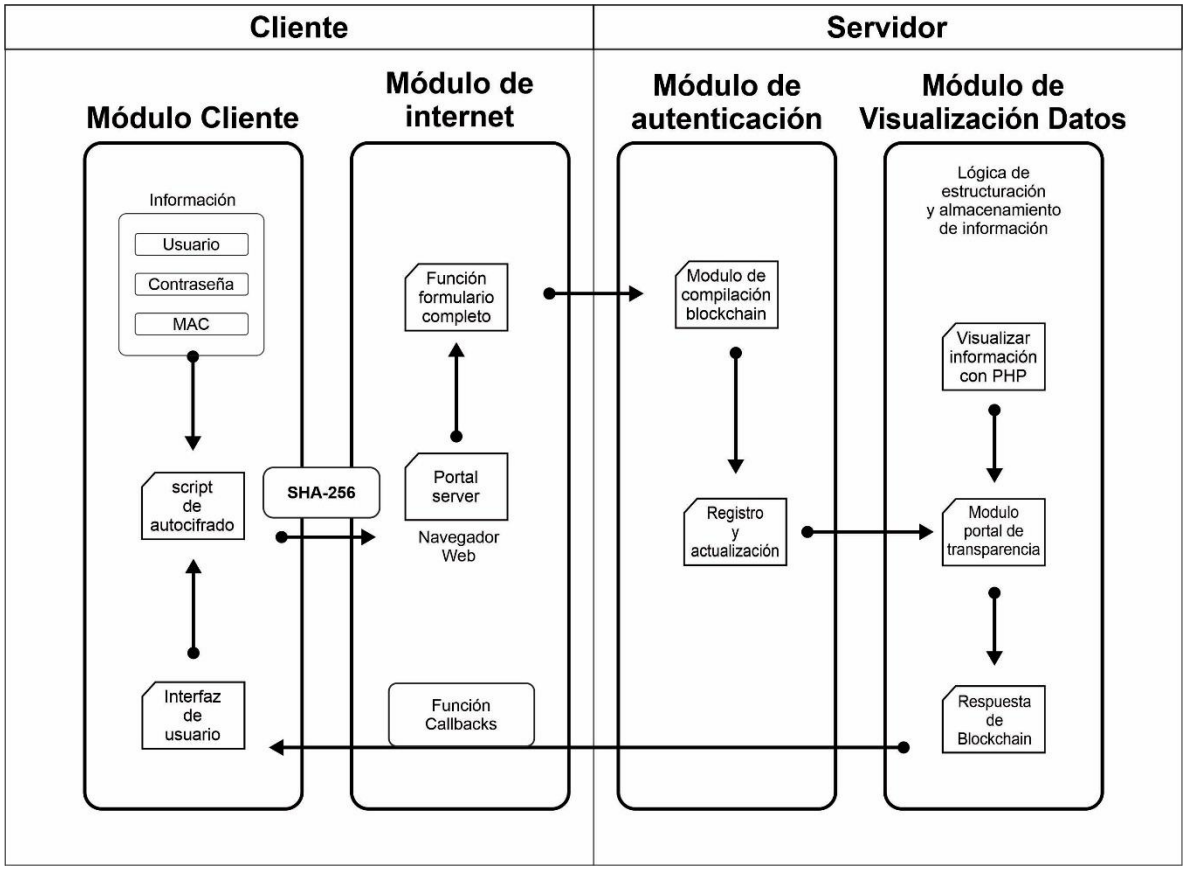


Fig. 43: Arquitectura lógica del software implementado

Fuente: elaboración propia

Descripción de componentes: A continuación, se detallan los componentes lógicos que interactúan con para lograr el funcionamiento de la plataforma implementada en la investigación.

- **Componente de interfaz de usuario:** Componente que se encarga de la lógica que permite crear los elementos visuales con los cuales los usuarios interactúan, incluye formularios de inicio de sesión, registro y mensajes de error, realizado con tecnologías como HTML, CSS y JavaScript.
- **Componente de información:** este componente se encarga de recopilar la información a la que se asociaras la cuenta al momento del registro, toda la información recopilada en este proceso es enviada al componente de cifrado, mantiene una actualización constante mientras el usuario digita su información de usuario y contraseña, al igual que la dirección MAC del dispositivo.

- **Componente de script de auto cifrado:** Componente que integra algoritmos descifrador necesario que permiten mantener la seguridad y la privacidad de la información recopilada, este script de auto cifrado permite exponer datos sensibles a la capa de Internet, esto se realiza a través de bibliotecas de cifrado que actualmente ya están disponibles para implementación en proyectos.

- **Componente de SHA-256:** Componente que se encarga de generar hash de cifrado de 256 bits para cada grupo de información de un usuario, La misma información siempre producirá el mismo hash, Este componente es crucial para cifrar la información de los usuarios y enviarse a los servidores de validación para la respectiva respuesta de la solicitud autenticación.

- **Componente de portal server:** Componente que actúa como un servidor principal para gestionar las solicitudes de los usuarios, validación de tokens y comunicación con la blockchain, además de contener la lógica para interactuar con la blockchain, frameworks y tecnologías como los servidores webs de apache son utilizados en este componente.

- **Componente de formulario completo**: Se encarga de verificar la validez y exactitud de la información ingresada por los usuarios en el proceso de formularios esto permite asegurarse que los campos están completos correctamente y que cumplen un formato requerido ya sea en los correos y que las contraseñas de confirmación sean las mismas, Esto también nos permite evitar ataques con inyección de código scripting Se utilizaron tecnologías como JavaScript Para una rápida válida validación antes de enviarse a los servidores**.**

- **Componente de compilación:** Componente fundamental porque encapsulan toda la lógica necesaria para la creación y validación de nuevos bloques además integra funciones que aseguran la integridad y seguridad de la blockchain dentro del sistema. utiliza algoritmos de consenso para validar las solicitudes, se administra que todos los

nuevos participantes de la red tengan una copia exacta de la blockchain.

- **Componente de registro y actualización:** Gestiona las funciones de creación modificación de la información de los usuarios que utilizan la plataforma como método de autenticación, Este componente asegura que los datos de los usuarios se almacenen de maneras precisa y segura, la actualización permite redistribuir la cadena de bloques actualizada a los nodos encargados de la verificación.
- **Componente de portal de transparencia:** Componente que proporciona una interfaz donde los usuarios puedan verificar, auditar los registros y transacciones de la cadena de bloques toda la información de este portal es completamente cifrada sólo se permite verificar la información a través de las hashes de información, Este componente facilita la auditoría de seguridad por parte de los usuarios o empresas terceras para verificar que la plataforma cumple con el estándar de seguridad y privacidad requeridos, para el apartado front-end utiliza tecnologías como css y JavaScript y tecnologías de Backend para visualización de bases de datos.
- **Componente de visualización con PHP:** Componente de visualización que permite los usuarios ver de manera estructurada la información de la blockchain esto se realiza a través de scripts PHP que estructuran la información de la cadena de bloques utilizando tecnologías como HTML CSS y PHP para generar páginas dinámicas que se actualizan con la integración de nuevos bloques.

Componente de respuesta blockchain: Componente de respuesta blockchain fundamental para la gestión de accesos en el sistema de autenticación debido a que se encarga de generar La decisión final que permitirá al usuario acceder o denegar el acceso a la plataforma basándose en la información y transacciones registradas en la cadena de bloques en ambos casos esta respuesta es notificada al usuario a través de su interfaz.

- **Componente de funciones callbacks:** Componente que se encarga de transportar la respuesta de la blockchain hacia la interfaz de luz usuarios es realizado de manera asíncrona según el tiempo de respuesta de la validación de la calidad de bloques, Además transporta notificaciones o alertas al administrador en caso de intentos de acceso fallidos o actividades sospechosas, las funciones callbacks actualizan la interfaz del usuario para visualizar la respuesta en tiempo real.

En el apartado de cliente se encuentran los formularios de inicio de sesión, un proceso en el que muchas plataformas actuales llevan a cabo la identificación de usuarios, esta información es transportada hacia los servidores para la respectiva validación y autorización de acceso, y por parte del servidor es quien se encarga de recibir las solicitudes de autenticación, a través de tokens cifrados, y según la programación de los módulos de verificación dentro de la blockchain los nodos se encargarán de autorizar o denegar el acceso al cliente, esta arquitectura de software es llevada a cabo bajo la arquitectura de diseño de modelo vista controlador.

A. **Modelo:** Representa y gestiona los datos y la lógica de negocio de la aplicación. Es responsable de la manipulación de los datos, la validación, el acceso a la base de datos que se representa por la blockchain además permitió definir los algoritmos que procesan la información un proceso previo a la exposición de la capa de internet, también permite la abstracción de datos para la interacción con la capa vista y los respectivos controladores.

B. **Vista:** Permite mostrar datos que sean más accesibles para el usuario final, para el desarrollo de la plataforma se utilizó HTML, css y javascript para los formularios que simulan el acceso de un usuario en las plataformas online a través de un login de verificación.

La implementación de la tecnología blockchain en los métodos de autenticación de usuarios, requiere de la inclusión de nuevas características de información para lograr enlazar a usuario y dispositivo, las cuales abarcan como la dirección MAC del dispositivo, ya que es una de las características únicas que identifica a cada dispositivo además de que el cambio de información de una dirección MAC requiere de altos conocimientos de redes de computadoras.

C. **Controlador:** Interactúa con la capa vista, se encarga de recibir los eventos generados en la interfaz gráfica, en la plataforma de pruebas cuando el usuario digita su información en el formulario, automáticamente la información es cifrada creando un hash único para cada campo de información del formulario.

   El cifrado de la información antes de interactuar con la capa de internet permite evitar brechas de seguridad que pueden capturar la información en el proceso de transporte por la capa TCP/IP de internet.

   Para mayor detalle revisar el anexo 11 en conjunto con la ilustración 34 que se encuentra en la parte de anexos.

Interfaz Del Software:

A. **Interfaz de Registro:** El proceso de registro es un módulo que se ejecuta de manera offline, este registro permite asociar los datos de usuario y su dispositivo para ser almacenados en la blockchain para los posteriores inicios de sesión.

Los detalles de la implementación y código fuente se detallan a partir del anexo 11.

Fig. 27: Nuevo modelo de registro propuesto

B. Interfaz de Login: El usuario ingresa sus datos de identificación de la cuenta, el sistema desarrollado requiere de un campo adicional al método tradicional que considera la dirección Mac del dispositivo, este nuevo campo en el formulario de registro será no editable para el usuario y es autocompletado por el dispositivo de manera automática a través de un script.

Fig. 28: Modelo de login propuesto

Componentes Blockchain:

A. **Bcrypt:** Agrega un cifrado extra a la contraseña del usuario, bcrypt permite obtener un hash diferente incluso si los datos de ingreso son los mismos, esto se debe porque en el proceso de cifrado se agrega un número aleatorio que se conoce con el seudónimo de “sal”. La sal se enlaza con la contraseña para ser almacenados en la base de datos para posteriormente nuevamente se utilizado cuando se intente verificar la contraseña.

B. **Cifrado de información:** El cifrado de la información previo a la exposición por la capa de internet permitirá agregar privacidad y seguridad al proceso de autenticación, porque a partir de que el usuario ingresa sus datos de identificación estos son cifrados para evitar vulnerabilidades en la red que puedan capturar los datos de los usuarios. En la arquitectura propuesta toda la información del usuario se convertirá en hashes de información cifrada, la asignación de información de una cuenta ya estará enlazada con una dirección de correo legible sino a un hash de caracteres que representa la veracidad del correo o nombre de usuario.

C. **Nodos Validadores:** Los nodos de verificación de los datos se encuentran bajo un sistema de transparencia conocido como blockchain scanner, el cual permite obtener transparencia de la blockchain porque cualquier persona puede verificar que la información realmente pertenece a un usuario con una singularidad de que verifican solamente los hashes de información debido a que estos representan a los datos originales del usuario.

Componentes Offline: La arquitectura propuesta requiere del uso de un módulo para ejecución offline, por motivos de seguridad los navegadores no permiten acceder a características como la Mac address de un dispositivo porque para esta investigación se utilizó un script que permite acceder a características.

```
$mcd = shell_exec('wmic csproduct get uuid');
$mcdspace = str_replace(' ', '', $info);
```

Fig. 29: Código para obtener dirección MAC

A. **SHA-256:** Algoritmo de cifrado de una sola vía porque es eficiente de calcular el valor del hash a partir de los datos de entrada, pero es computacionalmente imposible saber los datos originales a partir de un hash generado previamente, para lograrlo se requiere de técnicas avanzadas de cifrado. Para el sistema de pruebas propuesto se utiliza en el proceso de cifrado previo a la exposición a la capa de internet, donde los campos del formulario correspondiente a usuario, correo, contraseña, repetición de contraseña y dirección de MAC del dispositivo son convertidos en hashes independientes que los identifica de manera única.

ARQUITECTURA DE PRUEBAS:

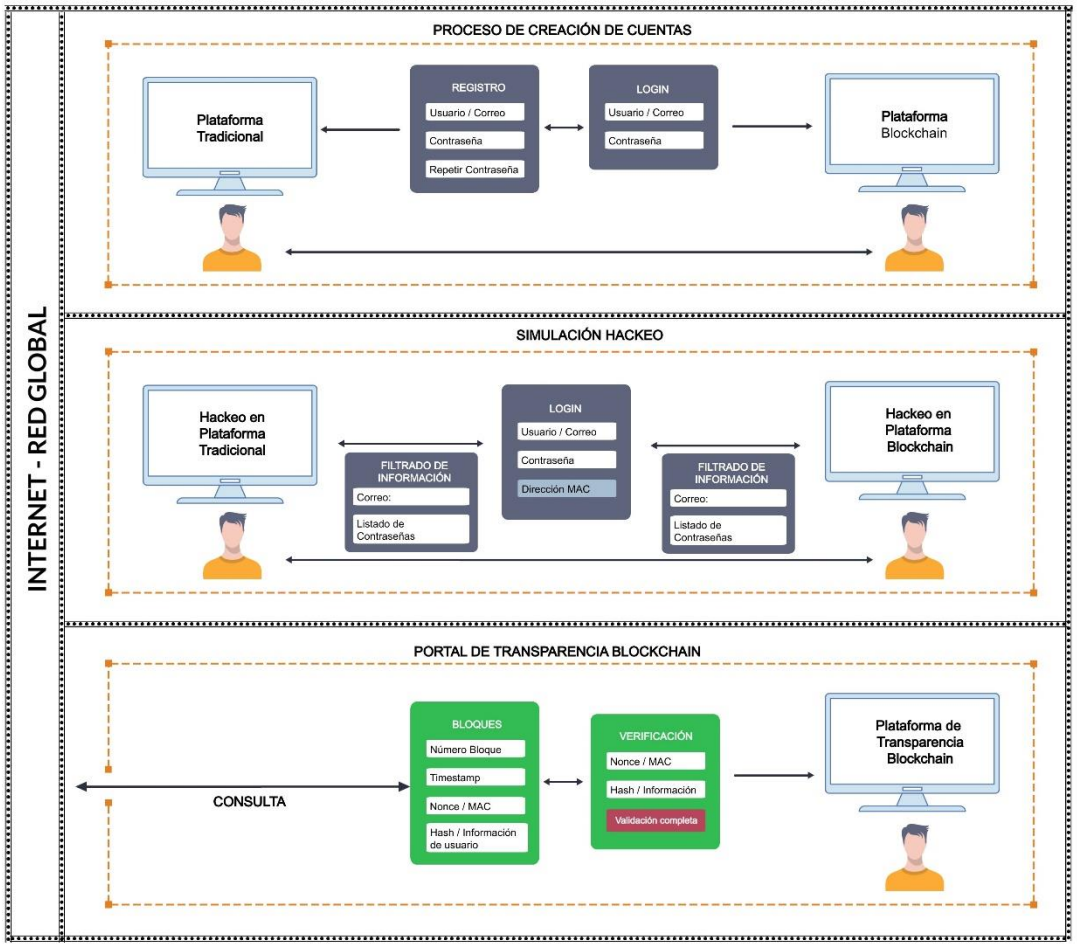


Fig. 30: Arquitectura de pruebas para validar hipótesis de investigación

Para el proceso de pruebas se generó una estructura que se conforma de un total de cinco (5) computadoras, estos activos se utilizarán para simular los diferentes componentes de la red y los diferentes escenarios que las plataformas actuales tienen prevenir para evitar el acceso a cuentas sin la autorización o verificación del usuario verdadero, los escenarios de plataforma tradicional y plataforma blockchain permitirá obtener resultados bajo las mismas condiciones, previo a todo el proceso de pruebas el usuario es informado para no exponer información privada que sea verdadera.

a) **Usuario de plataforma estándar:** Proceso que simulará el registro y login de usuario bajo la arquitectura tradicional mientras que en el otro dispositivo se realizará considerando la arquitectura propuesta en esta investigación, en el cual para el proceso de registro se necesita de un campo de información adicional que corresponde a la dirección Mac del dispositivo misma que se asocia con los datos del usuario original que realizó la creación de cuenta, los datos correspondientes a usuario y contraseña son creados para el proceso de pruebas no deberán exponer información real y privada porque en el proceso de simulación de hackeo el usuario real deberá proporcionar sus datos sus datos registrados.

b) **Simulación de hackeo a cuentas de prueba:** Proceso donde se solicita al usuario facilitar un conjunto de palabras en el cual esté incluido la contraseña y el hacker solo cuenta con un tiempo estimado de 2 minutos para intentar vulnerar la seguridad autenticación y acceder a la cuenta de otro usuario, los datos que el usuario real filtró para el proceso de hackeo corresponde a la dirección de correo que utilizó para crear la cuenta y además agrega un grupo de 4 palabras para representar un diccionario de datos que los hacker utilizará para vulnerar la cuenta, este proceso es realizado en ambas plataformas considerando las mismas condiciones.

c) **Portal de Transparencia Blockchain:** Proceso que representa el portal de transparencia que todos los proyectos de cadena de bloques tienen por requerimiento mínimo, debido a que permite agregar transparencia a red porque facilita la verificación de que las transacciones que se hayan realizado previamente son verídicas, en el modelo de investigación propuesto el portal de transparencia se utilizará para visualizar la lista de bloques además de mantener accesible la información de cuáles son los usuarios que tienen registrado sus datos de inicio de sesión, todos los datos de la blockchain son cifrados por lo tanto solo se verifica que la información brindada genera el hash registrado, el portal no permite la modificación de datos, es un sistema que tiene únicamente la funcionalidad de visualizar el contenido de la blockchain.

3.3.4. En esta investigación para el cumplimiento del cuarto objetivo se realizaron las correcciones de código para algunos módulos del sistema, con la finalidad de que el usuario no visualice ciertos procesos que se deberán realizar internamente, por ejemplo, en el proceso de cifrado previo a la exposición a la capa de internet, este proceso será oculto para el usuario final. Los procesos de verificación de información que se realiza en la blockchain se realizarán de manera automática sin depender de que el usuario realice acciones para validar su información, de manera similar se actualizaron los colores que corresponderá a la plataforma tradicional para diferenciarse a simple vista y evitar confusiones al momento de registrar los datos, el proceso de implementación y código fuente se detalla en el anexo 11.

FUNCIONALIDADES EN SEGURIDAD		
Criterio	**Plataforma Estándar**	**Plataforma Blockchain**
Riesgo de hacking	Vulnerabilidad de seguridad cuando datos confidenciales como usuario y contraseña son expuestos por diversos métodos como: Falta de medidas de seguridad para mantener la información privada o vulnerabilidades en el desarrollo del software.	Riesgo minimizado debido a que, al nuevo modelo de autenticación propuesto en la investigación, requiere tener la dirección MAC del dispositivo para verificar la autenticidad del usuario, restringiendo los accesos no autorizados porque los hackers necesitarían del dispositivo en físico para lograr comprometer la cuenta.
Alta afluencia de usuarios	Limitado a la arquitectura de base de datos implementado en los servidores, además de la optimización de consultas para manejar grandes volúmenes de datos.	Los usuarios registrados bajo la nueva arquitectura únicamente necesitan verificar que su información este anexada al dispositivo, proceso optimizado para facilitar la autorización de accesos por diversos nodos que conforman de la red blockchain.
Multidispositivo	Es posible vincular múltiples dispositivos sin restricciones, ya que la verificación de la identidad del usuario se realiza únicamente a través del nombre de usuario y contraseña al acceder a la cuenta	Restringido a dispositivos autorizados según las preferencias del usuario autenticado determinando a que dispositivos desea vincular la cuenta. .
Accesibilidad	Es la manera estándar, fácil y común que utilizan la gran mayoría de usuarios actualmente para acceder a una cuenta.	No representa un cambio de paradigma a la seguridad actual, debido a que la asociación de la cuenta con el dispositivo se realiza de manera automática.
Cifrado de datos	Las alteraciones en el cifrado de la información pueden ocasionar la pérdida de acceso a la cuenta, debido a que no se dispone de un registro que permita restaurar la información de la cuenta a un estado inicial.	En caso se comprometa la integridad de la información cifrada, cualquier modificación se detecta inmediatamente por la red, generando en una restricción automática de los accesos a la cuenta afectada sea restaurada a su estado original.

Tabla 5: Cuadro comparativo de funcionalidades en seguridad

Fuente: Elaboración Propia.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones:

Se utilizó las características de usuario, contraseña, dirección Mac para una sola cuenta en un dispositivo y logró una seguridad del 98.67% frente a ataques cibernéticos donde los hackers tienen acceso a las contraseñas por intermedio de ingeniería social o fishing.

Se implementó la tecnología blockchain en conjunto con la característica de la dirección Mac para asociar cada cuenta obteniendo una usabilidad de 9.67 de una escala de 0/10, lo que significa que la incorporación de dichas características, para el usuario final no representó un cambio radical en el proceso estándar de login de una cuenta.

La incorporación de las características permitió a asociar de manera precisa al usuario y dispositivo demostró ser altamente efectiva. Los resultados obtenidos indican que solo el 1.33% de las cuentas analizadas fueron accedidas utilizando datos que no correspondían al usuario verídico, este dato resaltó la eficacia de seguridad de asociar una cuenta a un dispositivo

Se determinó según las pruebas que la seguridad de la blockchain es escalable según la cantidad de nodos que participen en la red, porque cada solicitud de acceso será verificada por más usuarios que pueden comprobar que la información es verídica antes de permitir el acceso a la respectiva cuenta.

4.2. Recomendaciones:

Se recomienda que para la vinculación de una cuenta con otros dispositivos utilizando la arquitectura propuesta en esta investigación requiere de la incorporación de un proceso adicional con hardware en los dispositivos que permita obtener la huella digital del usuario verdadero. Capturar y verificar la huella digital permitirá crear una capa adicional de autenticación biométrica que agrega mayor seguridad al proceso de vinculación porque de esta manera se otorgarán permisos de acceso a otro dispositivo solo con la autorización del usuario legítimo debido a que es verificado a través del lector de huella dactilar.

Para el proceso de replicación del método planteado en esta investigación referente a la blockchain es necesario conocer de algoritmos de cifrado, tecnologías web para la simulación de plataformas con registro tradicional y la plataforma que incorpora las características de la Blockchain para los procesos de autenticación.

La cadena de bloques planteada en esta investigación pertenece a blockchain privada porque no requiere de una gran cantidad de nodos conectados para validar las transacciones, esto fue necesario para evitar grandes costes económicos en la contratación de servidores.

Se aconseja crear una cadena de bloques privada porque utilizar una blockchain existente requiere de un pago económico por cada transacción de registro, razón que no permite la escalabilidad para utilizarse en sistemas reales a gran escala con alta concurrencia de usuarios, crear una propia cadena de bloques permitirá definir normas y condiciones propias de la blockchain logrando viabilidad, utilidad y escalabilidad de la arquitectura de autenticación de credenciales planteada en esta investigación.

REFERENCIAS

[1] INCIBE, «www.incibe.es,» 2021. [En línea]. Available: https://www.incibe.es/ciudadania/blog/por-que-un-ciberdelincuente-le-interesa-duplicar-tu-tarjeta-sim. [Último acceso: 03 04 2023].

[2] M. Hillyard, «Can Blockchain End the Need for Passwords in Identity Management?,» Disponible en: https://www.beyond20.com/blog/can-blockchain-eliminate-need-for-passwords-identity-management/, 2020.

[3] D. Granados, «El robo de cuentas bancarias aumentó un 20% en 2020,» Disponible en: https://latam.kaspersky.com/blog/el-robo-de-cuentas-bancarias-aumento-un-20-en-2020/21357/, 2021.

[4] D. Whitworth, «Having my identity stolen cost me £10,000,» Disponible en: https://www.bbc.com/news/business-53106532, 2020.

[5] Álvarez, «Digital Report - El Informe Sobre Las Tendencias Digitales, Redes Sociales Y Mobile,» Disponible en: https://wearesocial.com/es/blog/2021/01/digital-report-2021-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/, 2021.

[6] A. Spadafora, «Struggling with password overload? You're not alone,» Disponible en: https://www.techradar.com/uk/news/most-people-have-25-more-passwords-than-at-the-start-of-the-pandemic., 2020.

[7] J. Desirée, «Robo de credenciales: Cómo suceden y qué medidas de seguridad hay que tomar.,» Disponible en: https://www.infobae.com/america/tecno/2021/07/28/robo-de-credenciales-como-suceden-y-que-medidas-de-seguridad-hay-que-tomar/, 2021.

[8] A. Sánchez, «Dragonblood - Sepa más de las vulnerabilidades de WPA3. Xentic SAC,» [En línea]. Available: https://xentic.com.pe/dragonblood-vulnerabilidades-wpa3-wifi/.

[9] FTC, «Consumer sentinel Network,» 2019. [En línea]. Available: https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf. [Último acceso: 04 05 2023].

[10] B. Basudeb y S. Sourav, «Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System,» *IEEE. DOI 10.1109/JIOT.2020.3030308,* p. 18, 2020.

[11] P. Soumyashree, J. Debasish y et al., «Authentication and Key Management in Distributed IoT using Blockchain Technology,» *DOI 10.1109/JIOT.2021.3063806,* 2021.

[12] H. Zaher, F. Mostafa y et al., «Blockchain-based Authentication for 5G Networks,» *https://doi.org/10.1109/ICIoT48696.2020.9089507,* 2020.

[13] Xiangwei, Jianbo y et al., «A Secure Mutual Authentication Scheme of Blockchain-Based in WBANs,» *http://dx.doi.org/10.23919/JCC.2020.09.004,* 2020.

[14] «HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes,» *IEEE. DOI 10.1109/JIOT.2019.2944400,* 2019.

[15] A. Hashim y A. Rawaa, «A security services for internet of thing smart health care solutions based blockchain technology,» *DOI: 10.12928/TELKOMNIKA.v20i4.23765,* 2022.

[16] J. Stanislaw, J. Mohammed y et al., «Two-factor Password-authenticated Key Exchange with End-to-end Security,» *ACM: https://doi.org/10.1145/3446807,* nº 17, p. 37, 2021.

[17] M. Vanhoef y E. Ronen, «Dragonblood: Analyzing the Dragonfly Dragonblood: Analyzing the Dragonfly,» *https://papers.mathyvanhoef.com/dragonblood.pdf,* p. 17, s.f..

[18] G. Vitor, T. Cruz y P. Simöes, «Security of Building Automation and Control

Systems: Survey and future research directions,» *https://doi.org/10.1016/j.cose.2021.102527,* p. 24, 2021.

[19] G. Osariemen y M. Osei, «The Effects of Blockchain Technology on Corporate Governance: Evidence from Emerging Economy,» *Sciendo. DOI 10.2478/mdke-2022-0016,* 2022.

[20] M. Gunasekaran, «Token-based Authorization and Authentication for Secure Internet of Vehicles Communication,» *ACM. http://dx.doi.org/10.1145/3491202,* 2022.

[21] X. Shujiang, Z. Jinrong y et al., «A privacy-preserving and efficient data sharing scheme with trust authentication based on blockchain for mHealth,» *https://doi.org/10.1080/09540091.2023.2186316,* p. 24, 2023.

[22] R. Yong , T. Hongwei y et al., «Improving transaction safety via anti-fraud protection based on blockchain,» *https://doi.org/10.1080/09540091.2022.2163983,* p. 19, 2023.

[23] T. Tsung, J. Kim y G. Rodney, «Privacy-preserving model learning on a blockchain network-of-networks,» *doi: 10.1093/jamia/ocz214,* p. 12, 2019.

[24] S. Zhan , W. Hejian y W. Huanjuan, «A Financial data security sharing solution based on blockchain technology and proxy re-encryption on technology,» *https://ieeexplore.ieee.org/document/9332363,* 2021.

[25] Meikang , Qiu, Bhavani y Meiqin Liu, «Secure Data Sharing Through Untrusted Clouds with Blockchain-enhanced Key Management,» *IEEE. https://ieeexplore.ieee.org/document/9415702,* 2020.

[26] &. F. S. Murat Kantarcioglu, «Securing Big Data in the Age of AI,» *https://ieeexplore.ieee.org/document/9014354,* 2019.

[27] D. Lopez, «Blockchain: la revolución industrial de Internet,» 2017. [En línea]. Available: https://doi.org/10.22235/rd.v0i19.1721. [Último acceso: 2023].

[28] A. Guardeño, V. Días y E. Hernández , Que sabemos de Blockchain, Madrid: https://elibro.net/es/ereader/bibsipan/111431, 2019.

[29] I. Society, «www.internetsociety.org,» 2017. [En línea]. Available: https://www.internetsociety.org/es/about-the-internet/how-it-works/. [Último acceso: 02 05 2023].

[30] I. Documentation, «Protocolos a nivel de aplicación de Internet.,» 2022. [En línea]. Available: https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/es/aix/7.2?topic=protocols-internet-application-level.

[31] Kionetworks, «¿Qué son y para qué sirven los protocolos de comunicación de redes?,» 2021. [En línea]. Available: https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes.

[32] Oracle, «¿Qué es el Internet de las cosas (IoT)?,» https://www.oracle.com/mx/internet-of-things/what-is-iot/, 2014.

[33] Z. Dévora, «Identificación de computadoras, utilizadas para la concreción de delitos informáticos, a partir de su dirección física, en redes de Área Local,» 2017. [En línea]. Available: http://bibliotecas.ucasal.edu.ar/opac_css/doc_num.php?explnum_id=1092. [Último acceso: 2023].

[34] Amazon, «¿Qué es la criptografía? - Explicación sobre la criptografía,» Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cryptography/, 2023.

[35] Bit2me, «Conceptos blockchain en el primer Máster Online Descentralizado y Tokenizado sobre Web 3.0 e Innovación.,» 2020. [En línea]. Available: https://academy.bit2me.com/en/what-is-a-merkle-tree/. [Último acceso: 2023].

[36] Academy-bit2me, «Diccionario Bitcoin & Blockchain,» 2018. [En línea]. Available:

https://academy.bit2me.com/diccionario-crypto/. [Último acceso: 2023].

[37] EcuRed, «Criptografía simétrica,» 2023. [En línea]. Available: https://www.ecured.cu/Criptograf%C3%ADa_sim%C3%A9trica. [Último acceso: 01 04 2023].

[38] M. Plaza , Manual De Criptografía: Fundamentos Matemáticos De La Criptografía Para Un Estudiante De Grado, España: https://doi.org/10.14201/0DD0169, 2021.

[39] . J. Daemen y . V. Rijmen, The Design of Rijndael AES — The Advanced Encryption Standard, Recuperado de: https://cs.ru.nl/~joan/papers/JDA_VRI_Rijndael_2002.pdf, 2001.

[40] A. Andrade, Características y aplicaciones de las funciones resumen criptográficas en la gestión de contraseñas, Universidad de alicante: https://rua.ua.es/dspace/bitstream/10045/96849/1/tesis_alicia_andrade.pdf, 2019.

[41] A. Popov, «RFC 7465: Prohibiting RC4 Cipher Suites,» IETF Datatracker, 2015. [En línea]. Available: https://datatracker.ietf.org/doc/rfc7465/.

[42] FIPS, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Secure Hash Standard (SHS), http://dx.doi.org/10.6028/NIST.FIPS.180-4, 2015.

[43] FIPS, Announcing Approval of Federal Information Processing Standard, Secure Hash Standard (SHS); a Revision of FIPS 180-3, 2012.

[44] KeepCoding, «¿Qué es el algoritmo AES?,» grokkeepcoding, 2014. [En línea]. Available: https://keepcoding.io/blog/que-es-el-algoritmo-aes/.

[45] Nakamoto, «Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario,» *https://bitcoin.org/bitcoin.pdf,* p. 9, 2008.

[46] I. Rojo, «Blockchain fundamentos de la cadena de bloques,» *Bogotá: Ra-Ma. https://elibro.net/es/ereader/bibsipan/127086,* 2019.

[47] R. Dolader , R. Bel y et al., «La Blockchain: Fundamentos aplicaciones y relacion

con otras tecnologías,» 2018. [En línea]. Available: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf. [Último acceso: 03 04 2023].

[48] J. Benson, «¿Qué Es El Proof of Stake o Prueba De Participación? En Qué Se Diferencia De La Prueba De Trabajo,» 2021. [En línea]. Available: https://decrypt.co/es/resources/que-es-el-proof-of-stake-o-prueba-de-participacion-en-que-se-diferencia-de-la-prueba-de-trabajo. [Último acceso: 01 05 2023].

[49] Vilatik, «ethereum.org,» 2015. [En línea]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains. [Último acceso: 19 04 2023].

[50] A. Rojas y L. Rodigo, «Análisis De La Tecnología Blockchain, Su Entorno Y Su Impacto En Modelos De Negocios,» 2018. [En línea]. Available: https://doi.org/https://hdl.handle.net/11673/47346.

[51] A. Preukschat, Blockchain: La revolución industrial de internet., Planetadelibros, 2017.

[52] W. Bozhi y Z. Liming, A Simulation Approach for Studying Behavior and Quality of Blockchain Networks, Australia: https://doi.org/10.1007/978-3-319-94478-4_2, 2018.

[53] O. Leech, «¿Qué es el hashrate y por qué importa?,» 2021. [En línea]. Available: https://www.coindesk.com/markets/2021/07/08/que-es-el-hashrate-y-por-que-importa/. [Último acceso: 2023].

[54] M. Castro, «Practical Byzantine Fault Tolerance,» 2001. [En línea]. Available: https://www.researchgate.net/publication/2516268_Practical_Byzantine_Fault_Toleranc.

[55] K. Mazara, «Ataque de repetición o Replay Attack - Ataques, amenazas y vulnerabilidades de ciberseguridad (CompTIA Security+ SY0-601),» 2021. [En línea]. Available: https://es.linkedin.com/learning/ataques-amenazas-y-vulnerabilidades-de-ciberseguridad-comptia-security-plus-sy0-601/ataque-de-repeticion-o-replay-attack.

[56] E. Heilman, A. Kendler y A. Zohar, «Boston University,» 2015. [En línea]. Available: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf.

[57] Zamorano, «Reclutamiento fiable y barato con blockchain y Fiduxa,» 2018. [En línea]. Available: http://www.blockchainservices.es/casos-exitoblockchain/reclutamiento-fiable-y-barato-con-blockchain-y-fiduxa/. [Último acceso: 2023].

[58] J. Plasencia, «Sistema de votación electrónica basado en blockchain,» 2018. [En línea]. Available: https://riull.ull.es/xmlui/handle/915/9462. [Último acceso: 2023].

[59] G. Chunpeng y F. Liming, «A blockchain based decentralized data security mechanism for the Internet of Things,» 2020. [En línea]. Available: https://doi.org/10.1016/j.jpdc.2020.03.005.

[60] C. Shiping, W. Harry y Z. Liang, Blockchain – ICBC. Held as Part of the Services Conference Federation, https://springer.com/book/10.1007/978-3-319-94478-4, 2018.

[61] Sampieri y et al, Metodología de la investigación., Mexico: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf, 2014.

[62] Evidian, Los 7 métodos de Autentificación más utilizados, https://www.evidian.com/pdf/wp-strongauth-es.pdf, s. f..

[63] A. Jamal, A. Nurin y R. Abbas, «Blockchain-Based Identity Verification System,»

IEEE, p. 5, 2019.

[64] B. Explorer, «Bitcoin Tracker & More,» Blockchain.com, 2023. [En línea]. Available: https://www.blockchain.com/es/explorer. [Último acceso: 2023].

[65] Investing, «Analista de Bloomberg: hashrate de BTC crece 25% en 2023, “es el activo más seguro”,» 2023. [En línea]. Available: https://es.investing.com/news/cryptocurrency-news/analista-de-bloomberg-hashrate-de-btc-crece-25-en-2023-es-el-activo-mas-seguro-2381515#addAComment. [Último acceso: 2023].

[66] C. Moncayo, «La importancia del tiempo de carga de una página web para una empresa,» 2018. [En línea]. Available: https://incp.org.co/la-importancia-del-tiempo-de-carga-de-una-pagina-web-para-una-empresa/. [Último acceso: 2023].

[67] Santiago, Nuevos métodos de autenticación digital mejoran seguridad y conveniencia, https://www.computerweekly.com/es/opinion/Nuevos-metodos-de-autenticacion-digital-mejoran-seguridad-y-conveniencia, 2019.

[68] N. I. 27001, «normaiso27001,» 06 2024. Disponible en: https://normaiso27001.es/.

[69] C. I. E. IEC, «IEC,» 09 06 2024. Disponible en: https://www.iec.ch/homepage.

[70] T. N. I. o. S. a. NIST, «NIST,» 09 06 2024. Disponible en: https://www.nist.gov/.

[71] A. Jamal, A. Nurin y R. Abbas, «Blockchain-Based Identity Verification System,» IEEE, p. 5, 2019

[72] B. Explorer, «Bitcoin Tracker & More,» Blockchain.com, 2023. [En línea]. Available: https://www.blockchain.com/es/explorer

[73] Investing, «Analista de Bloomberg: hashrate de BTC crece 25% en 2023, “es el activo más seguro”,» 2023. [En línea]. Available: https://es.investing.com/news/cryptocurrency-news/analista-de-bloomberg-hashrate-de-btc-crece-25-en-2023-es-el-activo-mas-seguro-2381515#addAComment.

[74] INCP, «incp org,» 2018. Available: https://incp.org.co/la-importancia-del-tiempo-de-carga-de-una-pagina-web-para-una-empresa/.

[75] N. Brisaboa, Un método para establecer una comunicación en entorno cliente-servidor, Granada: II Jornadas de informática, 1996.

ANEXOS:

ANEXO 01: DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la DECLARACIÓN JURADA, soy Rober Yubelder López Vallejos**.** Del Programa de Estudios de Ingeniería de sistemas de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autor del trabajo titulado:

IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN ASOCIANDO USUARIO Y DISPOSITIVO PARA MEJORAR LA SEGURIDAD EN LAAUTENTICACIÓN DE CREDENCIALES DE ACCESO

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

Rober Yubelder López Vallejos	DNI: 75860716	

Pimentel, 19 de julio de 2023.

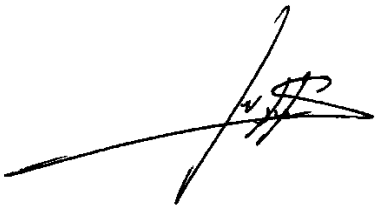
ANEXO 02: ACTA DE REVISIÓN DE SIMILITUD DE LA INVESTIGACIÓN

Yo **Heber Ivan Mejia Cabrera** docente del curso de **Investigación II** del Programa de Estudios de **Ingeniería de Sistemas** y revisor de la investigación del estudiante, **Lopez Vallejos Rober Yubelder**, titulada:

IMPLEMENTACIÓN DE TECNOLOGÍA BLOCKCHAIN ASOCIANDO USUARIO Y DISPOSITIVOS PARA MEJORAR LA SEGURIDAD EN LA AUTENTICACIÓN DE CREDENCIALES DE ACCESO

Se deja constancia que la investigación antes indicada tiene un índice de similitud del **13%,** verificable en el reporte final del análisis de originalidad mediante el software de similitud TURNITIN. Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos y de investigación en la Universidad Señor de Sipán S.A.C., aprobada mediante Resolución de Directorio N° 0758-2022/FIAU-USS.

Pimentel, 21 de Julio del 2022



Mg. Heber Ivan Mejia Cabrera

DNI N° 41639565

ANEXO 03: Acta de aprobación de asesor:

Universidad Señor de Sipán

ANEXO 03: ACTA DE APROBACIÓN DEL ASESOR

Yo **Víctor Alexci Tuesta Monteza** quien suscribe como asesor designado mediante Resolución de Facultad N° 760-2022/FIAU-USS, del proyecto de investigación titulado **Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso**., desarrollado por el(los) estudiante(s): **Rober Yubelder López Vallejos**., del programa de estudios de **ingeniería de sistemas**, acredito haber revisado, realizado observaciones y recomendaciones pertinentes, encontrándose expedito para su revisión por parte del docente del curso.

En virtud de lo antes mencionado, firman:

Víctor Alexci Tuesta Monteza	DNI: 42722929.	
Rober Yubelder López Vallejos	DNI: 75860716	

Pimentel, 20 de 07 de 2023

ANEXO 04: Instrumentos de recolección de datos:

Proyecto	**Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso**		
Documento	**Instrumento de recolección de datos por observación.**		
Autor	**López Vallejos Rober Yubelder**		
Número de sesión de pruebas		**Fecha ejecución de pruebas**	**DD/MM/AAAA** **_____/_____/_____**

N° Prueba	**Item**	**Puntaje 0/10**	**Descripción**
1	**Facilidad de uso**		
	Eficiencia		
	Satisfacción del usuario		
N° Prueba	**Item**	**Puntaje 0/10**	**Descripción**
2	**Facilidad de uso**		
	Eficiencia		
	Satisfacción del usuario		
N° Prueba	**Item**	**Puntaje 0/10**	**Descripción**
3	**Facilidad de uso**		
	Eficiencia		
	Satisfacción del usuario		

Proyecto	**Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso.**
Documento	**Instrumento de recolección de datos del registro electrónico de ingreso a cuenta de usuario con datos aleatorios.**
Autores	**López Vallejos Rober Yubelder**
Fecha de ejecución de pruebas	**DD/MM/AAAA: _____/_____/_____**

N° De Prueba **_____1_____**	**Estado de Acceso Login**	**Fecha - Timestamp**	**Tiempo (0 – 2 minutos)**	**Firma de usuario**
Plataforma Estándar	**Acceso Permitido ( )** **Acceso denegado ( )**			
Plataforma Blockchain	**Acceso Permitido ( )** **Acceso denegado ( )**			

ANEXO 05: Ficha técnica del instrumento:

Universidad Señor de Sipán

1. VALIDACIÓN DEL INSTRUMENTO

1.1. Instrumento de Validación No Experimental por Juicio de expertos

1. NOMBRE DEL JUEZ		Dr. Victor Alexci Tuesta Monteza
2.	**PROFESIÓN**	Doctorado en Ciencias de la Educación, Ingeniero de Sistemas, maestría en Administración de Negocios.
	ESPECIALIDAD	Ingeniero de Sistemas.
	GRADO ACADÉMICO	Doctorado y Maestría
	EXPERIENCIA PROFESIONAL (AÑOS)	10 años
	CARGO	Decano de la Facultad de Ingeniería, Arquitectura y Urbanismo
TÍTULO DE LA INVESTIGACIÓN: Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso.		
3. DATOS DEL TESISTA		
3.1 3.2	**NOMBRES Y APELLIDOS**	López Vallejos Rober Yubelder
	PROGRAMA DE POSGRADO	Ingeniería de sistemas.
4. INSTRUMENTO EVALUADO		Entrevista ( ) Cuestionario ( ) Lista de Cotejo (x) Encuesta ( )
5. OBJETIVOS DEL INSTRUMENTO		**GENERAL** Evaluar tasa de éxito de sesión con capacidad de autenticación para datos aleatorios.
		ESPECÍFICOS • Monitorear el número de intento de inicio de sesión en las plataformas de prueba. • Verificar la integridad y validez de los datos ingresados durante el proceso de inicio de sesión. • Prevenir accesos no autorizados en los sistemas utilizando datos aleatorios no registrados
A continuación, se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS.		

No	DETALLE DE LOS ÍTEMS DEL INSTRUMENTO

Proceso	Descripción
Escenario de prueba	Detalle de situación de prueba a evaluar, se deben considerar diversos escenarios que pueden llevarse suceder en contextos reales.
Simulación Hackeo plataforma estándar	Considera los tiempos establecidos e indicaciones para generar 3 contraseñas distintas, las cuales el hacker utilizará como diccionario de datos y deberá utilizar para vulnerar la cuenta.
Simulación hackeo plataforma blockchain	Considera los tiempos establecidos e indicaciones para generar 3 contraseñas distintas, las cuales el hacker utilizará como diccionario de datos y deberá utilizar para vulnerar la cuenta.

N° De Prueba _____	Estado de Acceso Login (Acceso Permitido y Acceso denegado)	Fecha - Timestamp	Tiempo (0 – 2 minutos)
Plataforma Estándar	A (X) D( )	A (X) D( )	A (X) D( )
Plataforma Blockchain	A (X) D( )	A (X) D( )	A (X) D( )
PROMEDIO OBTENIDO:		A (X) 100 %	D ( )

6. COMENTARIOS GENERALES

7. OBSERVACIONES

Juez Experto:
Victor ~~Alexci~~ Tuesta Monteza

Universidad Señor de Sipán

1. VALIDACIÓN DEL INSTRUMENTO

1.1. Instrumento de Validación No Experimental por Juicio de expertos

1. NOMBRE DEL JUEZ		Dr. Victor Alexci Tuesta Monteza
2.	**PROFESIÓN**	Doctorado en Ciencias de la Educación, Ingeniero de Sistemas, maestría en Administración de Negocios.
	ESPECIALIDAD	Ingeniero de Sistemas.
	GRADO ACADÉMICO	Doctorado y Maestría
	EXPERIENCIA PROFESIONAL (AÑOS)	10 años
	CARGO	Decano de la Facultad de Ingeniería, Arquitectura y Urbanismo
TÍTULO DE LA INVESTIGACIÓN: Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso.		
3. DATOS DEL TESISTA		
3.1 3.2	**NOMBRES Y APELLIDOS**	López Vallejos Rober Yubelder
	PROGRAMA DE POSGRADO	Ingeniería de sistemas.
4. INSTRUMENTO EVALUADO		Entrevista ( ) Cuestionario ( ) Lista de Cotejo (x) Encuesta ( )
5. OBJETIVOS DEL INSTRUMENTO		**GENERAL** Obtener resultados de Usabilidad de la tecnología blockchain en implementación para software tradicional.
		ESPECÍFICOS • Evaluar la tecnología para utilizarse de manera intuitiva en los sistemas. • Evaluar la reacción de los usuarios de la eficiencia de la tecnología para autenticar accesos en sistemas tradicionales. • Evaluar la percepción del usuario utilizando la tecnología.
A continuación, se le presentan los indicadores en forma de preguntas o propuestas para que Ud. los evalúe marcando con un aspa (x) en "A" si está de ACUERDO o en "D" si está en DESACUERDO, SI ESTÁ EN DESACUERDO POR FAVOR ESPECIFIQUE SUS SUGERENCIAS.		

N°	DETALLE DE LOS ÍTEMS DEL INSTRUMENTO

Facilidad de uso: El usuario identifica correctamente los botones y formularios de registro de manera intuitiva sin necesidad de instrucciones adicionales.

Eficiencia: El sistema permite la autenticación sin demoras significativas, además no presenta intentos fallidos de inicio de sesión con datos verídicos.

Satisfacción del usuario: Evaluación realizada al usuario para obtener feedback de la experiencia del sistema en prueba.

Escala Medición: Se representa según el resultado del promedio de: facilidad de uso, eficiencia y satisfacción de usuario, se distribuye según la siguiente table:

Escala	descripción
1	Sistema totalmente inaccesible e ineficiente
2	Sistema muy difícil de usar, con muchos errores y fallas
3	Sistema difícil de usar, con problemas frecuentes y lento
4	Sistema con accesibilidad limitada, con algunos errores y demoras
5	Sistema con accesibilidad aceptable, pero con dificultades y lentitud
6	Sistema razonablemente accesible, con algunos problemas
7	Sistema bastante accesible, aunque con algunas áreas de mejora
8	Sistema muy accesible, con pequeños inconvenientes ocasionales
9	Sistema casi totalmente accesible, con mínimos problemas
10	Sistema totalmente accesible

Tabla 6: Escala de accesibilidad de un sistema

N° Prueba	Item	Puntaje 0/10	Descripción
01	Facilidad de uso	A (X) D( )	A (X) D( )
	Eficiencia	A (X) D( )	A (X) D( )
	Satisfacción del usuario	A (X) D( )	A (X) D( )
PROMEDIO OBTENIDO:		A (X) 100% D( )	
6. COMENTARIOS GENERALES			
7. OBSERVACIONES			

Juez Experto:
Victor Alexei Tuesta Monteza

ANEXO 06: Evidencia de ejecución de plataformas

Fig. 31: Preparación de computadoras para fase de pruebas.

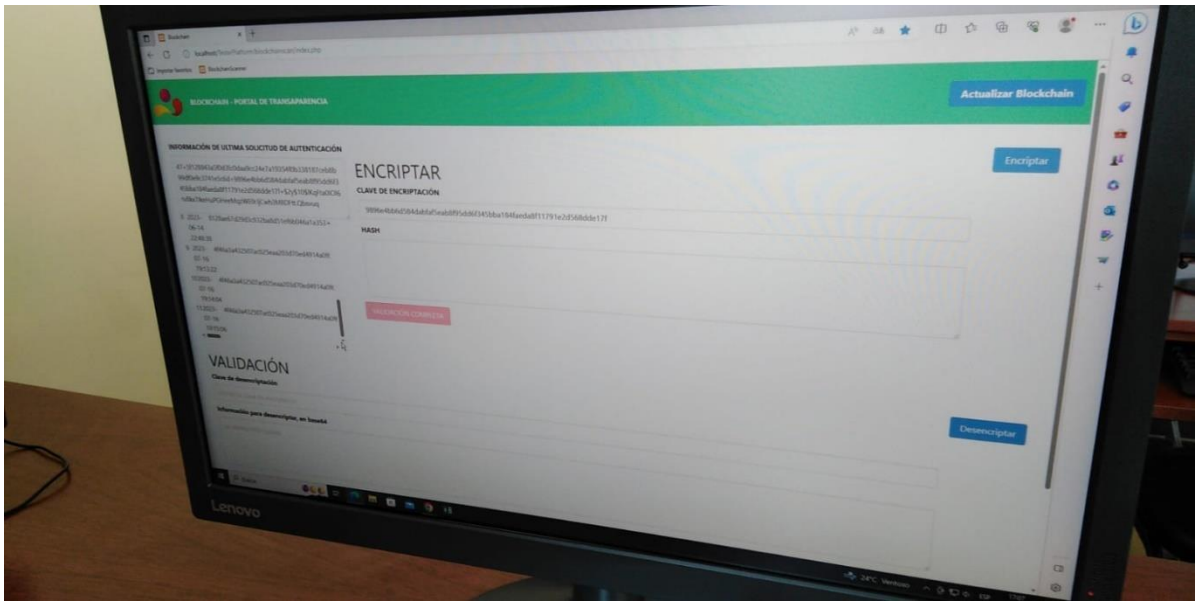


Fig. 32: Plataforma de blockchain scan

Nota: La plataforma de blockchain scan se utiliza para visualizar la información que se registra en la cadena de bloques.

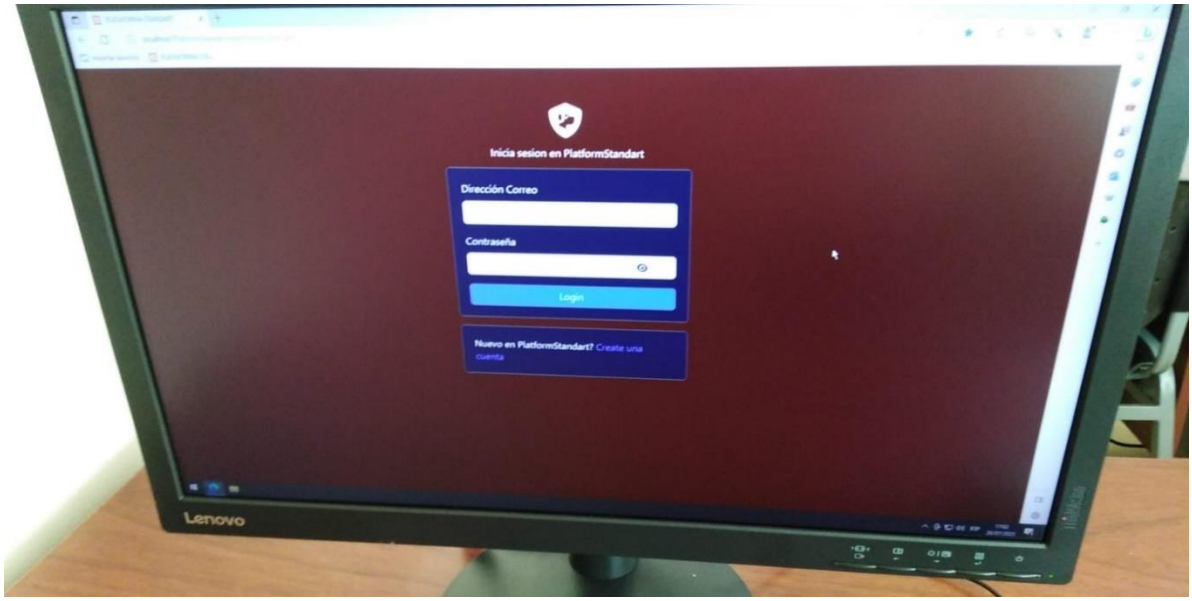


Fig. 33: Proceso de pruebas en plataforma tradicional

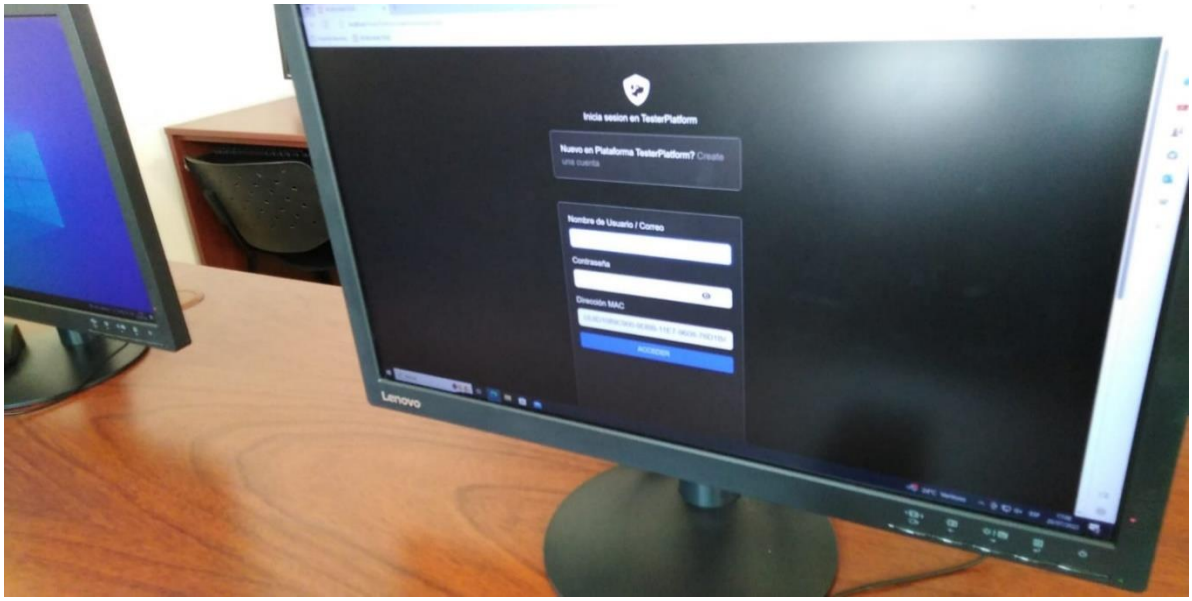


Fig. 34: Proceso de pruebas de autenticación con dirección MAC

Universidad Señor de Sipán

Proyecto	**Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso**		
Documento	**Instrumento de recolección de datos por observación.**		
Autor	**López Vallejos Rober Yubelder**		
Número de sesión de pruebas	01	**Fecha ejecución de pruebas**	**DD/MM/AAAA** 13 / 06 / 2023

N° Prueba	Item	Puntaje 0/10	Descripción
1	Facilidad de uso	10	identicación de opcion para Crear Cuenta. y no notó cumbios al crear la Cuenta.
	Eficiencia	9	
	Satisfacción del usuario	10	
N° Prueba	**Item**	**Puntaje 0/10**	**Descripción**
2	Facilidad de uso	10	logro Realizar todo de maner normal user edad. 25
	Eficiencia	10	
	Satisfacción del usuario	10	
N° Prueba	**Item**	**Puntaje 0/10**	**Descripción**
3	Facilidad de uso	8	inconvenientes para Repetir Contraña edad: 50
	Eficiencia	10	
	Satisfacción del usuario	10	

Fig. 35: Registro de información por método de observación

N° Prueba	Item	Puntaje 0/10	Descripción
19	Facilidad de uso	10	Nosotros haciendo. manejo de Programas y sistemas. no notó cambios.
	Eficiencia	9	
	Satisfacción del usuario	10	
N° Prueba	Item	Puntaje 0/10	Descripción
20	Facilidad de uso	10	No sufrió contratiempos edad 26.
	Eficiencia	9	
	Satisfacción del usuario	10	
N° Prueba	Item	Puntaje 0/10	Descripción
21	Facilidad de uso	10	Noto que el usuario es hasta de no logible edad 23. No sufrio de hacckeo.
	Eficiencia	10	
	Satisfacción del usuario	10	
N° Prueba	Item	Puntaje 0/10	Descripción
22	Facilidad de uso	10	sufrió hackeos. edad: 22 dificultad con Mouse. est. medicina.
	Eficiencia	9	
	Satisfacción del usuario	10	
N° Prueba	Item	Puntaje 0/10	Descripción
23	Facilidad de uso	9	no presento dificultad del Registro y fue victima de hackeo.
	Eficiencia	10	
	Satisfacción del usuario	9	

Número de sesión de pruebas	02	Fecha ejecución de pruebas	DD/MM/AAAA 17/06/2023

Universidad Señor de Sipán

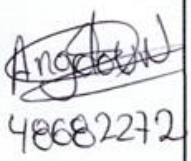
Proyecto	**Implementación de Tecnología Blockchain Asociando Usuario y Dispositivo Para Mejorar la Seguridad en la Autenticación de Credenciales de Acceso.**
Documento	**Instrumento de recolección de datos del registro electrónico de ingreso a cuenta de usuario con datos aleatorios.**
Autores	**López Vallejos Rober Yubelder**
Fecha de ejecución de pruebas	**DD/MM/AAAA: 13 / 06 / 2023**

N° De Prueba 1	Estado de Acceso Login	Fecha - Timestamp	Tiempo (0 – 2 minutos)	Firma de usuario
Plataforma Estándar	Acceso Permitido ( ) Acceso denegado (•)	1686782440	2 min	
Plataforma Blockchain	Acceso Permitido ( ) Acceso denegado (•)	1686782453	2 min	

Fig. 36: Registro de resultados de autenticación según plataforma.

Nota: En el anexo 09 se detalla todos los resultados obtenidos por método de observación.

N° De Prueba _____8_____	Estado de Acceso Login	Fecha - Timestamp	Tiempo (0 – 2 minutos)	Firma de usuario
Plataforma Estándar	Acceso Permitido ( ) Acceso denegado (•)	1686791874	2 min	
Plataforma Blockchain	Acceso Permitido ( ) Acceso denegado (•)	1686791975	2 min	

N° De Prueba _____9_____	Estado de Acceso Login	Fecha - Timestamp	Tiempo (0 – 2 minutos)	Firma de usuario
Plataforma Estándar	Acceso Permitido (•) Acceso denegado ( )	1686794384	0.50 min-	
Plataforma Blockchain	Acceso Permitido ( ) Acceso denegado (•)	1686794768	2 min	48682272

N° De Prueba _____10_____	Estado de Acceso Login	Fecha - Timestamp	Tiempo (0 – 2 minutos)	Firma de usuario
Plataforma Estándar	Acceso Permitido (•) Acceso denegado ( )	1687022405	1.06 m.n.	
Plataforma Blockchain	Acceso Permitido ( ) Acceso denegado (•)	1687022465.	2 min.	

Nota: En el anexo 10 se detalla todos los resultados obtenidos por registro electrónico en la plataforma estándar y la plataforma propuesta en la investigación.

ANEXO 07:

Matriz de evaluación de ventajas y desventajas de los métodos de autenticación:

Método de autenticación	Características	Ventajas	Desventajas	Referencia
Autenticación basada en contraseñas	Usuario ingresa una contraseña única	Fácil de implementar, familiar para los usuarios	Contraseñas pueden ser fácilmente adivinadas o robadas	Evidian IAM [64]
OTP	Método de autenticación de dos factores	No requiere hardware especializado	Los usuarios pueden perder sus teléfonos móviles o tener problemas de conectividad	Evidian IAM [64]
Token USB	Usuario ingresa un código generado por un dispositivo de token	Altamente segura, difícil de hackear	Costoso de implementar, los usuarios pueden perder o dañar el dispositivo	Evidian IAM [64]
Tecla confidencial	Utiliza recursos criptográficos para autenticar a los usuarios	Alta seguridad, difícil de hackear	Requiere habilidades técnicas para generar y usar los certificados	Evidian IAM [64]
Tarjeta inteligente	Usuario inserta una tarjeta inteligente en un lector	Alta seguridad, difícil de hackear	Costoso de implementar, los usuarios pueden perder o dañar la tarjeta	Evidian IAM [64]

Biometría	Utilizado en sistemas automatizados	No requiere la memorización de contraseñas	Condiciones de iluminación y preocupaciones de privacidad.	Evidian IAM [64]
RFID	Tecnología de identificación por radiofrecuencia	Identificación y seguimiento de objetos o personas en tiempo real sin necesidad de contacto físico	Interferencia de radiofrecuencias externas o a la interceptación de datos.	Evidian IAM [64]

ANEXO 08: Métodos de autenticación mejor evaluados:

Método de autenticación	Características	Porcentaje de percepción de seguridad	Ventajas	Desventajas	Referencia
Autenticación basada en contraseñas	Usuario ingresa una contraseña única	51%	Fácil de implementar, familiar para los usuarios	Contraseñas pueden ser fácilmente adivinadas o robadas	Santiago, R. [76]
Huellas dactilares	La autenticación se realiza mediante la comparación de la huella dactilar	48%	Únicas y no se pueden falsificar fácilmente.	Difíciles de leer en ciertas situaciones	Santiago, R. [76]
Reconocimiento facial	Tecnología de reconocimiento facial	11%	Conveniente por el uso de la cámara.	Condiciones de iluminación y preocupaciones de privacidad.	Santiago, R. [76]
reconocimiento de voz	Utilizado en sistemas automatizados	16%	No requiere la memorización de contraseñas	Afectada por el ruido ambiental o una afección de voz	Santiago, R. [76]

ANEXO 09: Datos obtenidos en fase de pruebas con método por observación.

N°Prueba	Facilidad de uso	10	Descripción	Rápida identificación de opción para crear cuenta y no noto cambios al crear la cuenta, edad aproximada 23, hackeo vida real no.
1	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Logró realizar todo de manera manual normal, con edad aproximada 25 años. Si fue víctima de hackeo en vida real.
2	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	8	Descripción	Inconvenientes para repetir la contraseña edad aproximada de 45 años, fue víctima de hackeo en vida real si
3	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Logró acceder sin representar ningún problema edad aproximada 23 años, fue víctima de hackeo en vida real no
4	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Logró identificar todos los ítems, edad aproximada de 28 años, fue víctima de hackeo en vida real si
5	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Logró identificar que al usar la dirección Mac será más segura, edad aproximada de 22 años, fue víctima de hackeo en vida real no
6	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	9	Descripción	Poco manejo del teclado error al recordar la contraseña, edad aproximada 24 años, fue víctima de hackeo en vida real no
7	Eficiencia	10		
	Satisfacción del usuario	9		
N°Prueba	Facilidad de uso	10	Descripción	Conoce los temas de login y consulta sobre vincular en otros dispositivos, edad aproximada 24, fue víctima de hackeo en vida real no
8	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	

9	Eficiencia	9		Comenta que es el mismo proceso y que no noto los cambios para acceder a la aproximada 25 años, fue víctima de hackeo en vida real si
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Conoce los registros en línea. edad 23, fue víctima de hackeo en vida real no.
10	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	No sufrió robo de cuentas o contraseñas y no notó los cambios en los registros, edad aproximada 24 años
11	Eficiencia	10		
	Satisfacción del usuario	9		
N°Prueba	Facilidad de uso	10	Descripción	Anteriormente si ha tenido casos de contraseña filtrada en hackeo de su cuenta, edad aproximada 23 años
12	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	9	Descripción	Conoce de Login y accesos si ha tenido hackeo de cuentas y presentó problemas de recordar contraseña por mal ingreso de teclado al momento del registro, edad 28.
13	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	9	Descripción	Tiempo de registro prolongado, dificultad para registrarse, no ha sufrido robo de contraseñas y usa contraseñas robustas, edad 36 años.
14	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Facilidad de uso de logins y no sufrió hackeo de contraseñas, edad 24 años.
15	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	9	Descripción	Dificultad para registrarse, sufrió ataques de robo de contraseñas por vinculación de correo a las contraseñas principales, edad 30 años.
16	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Facilidad de registro, sufrió hackeo de contraseñas y notó que el acceso de sus datos y su correo cambiaron a Hash, edad 27 años.
17	Eficiencia	9		
	Satisfacción del usuario	8		

N°Prueba	Facilidad de uso	10	Descripción	Conoces de autenticaciones, no sufrió hackeo en vida real, edad aproximadamente 22 años.
18	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	No sufrió hackeo de contraseñas además maneja programas y sistemas y no notó los cambios de registros, edad 24 años.
19	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	No sufrió hackeo de contraseñas y edad aproximada a 22 años
20	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Nota que el usuario es hash y no es legible para un humano edad aproximada a 23 años si sufrió hackeos de contraseñas en vida real.
21	Eficiencia	10		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	10	Descripción	Sufrió hackeo de contraseñas, edad aproximada 22 años y dificultad en el manejo del Mouse, es estudiante de medicina.
22	Eficiencia	9		
	Satisfacción del usuario	10		
N°Prueba	Facilidad de uso	9	Descripción	No presentó dificultad en el registro y fue víctima de hackeo en vida real, edad aproximada 24 años.
23	Eficiencia	10		
	Satisfacción del usuario	9		
N°Prueba	Facilidad de uso	10	Descripción	El usuario manifiesta poco manejo de tecnologías edad aproximadamente 28 años, no fue víctima de hackeo en vida real.
24	Eficiencia	10		
	Satisfacción del usuario	9		
N°Prueba	Facilidad de uso	9	Descripción	Usuario notó los cambios en el proceso de registro edad aproximada 25 años, si sufrió hackeo en vida real.
25	Eficiencia	10		
	Satisfacción del usuario	9		

ANEXO 10: Datos obtenidos en fase de pruebas con método de registro electrónico.

N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración en segundos (Max 2 min)	Firma de usuario
1	Estándar	Acceso Permitido		1686782440	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1686782550	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
2	Estándar	Acceso Permitido	1	1686782697	35	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1686782820	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
3	Estándar	Acceso Permitido	1	1686783820	53	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1686784471	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
4	Estándar	Acceso Permitido	1	1686784575	100	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1686784665	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
5	Estándar	Acceso Permitido	1	1686785607	58	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1686785790	120	
		Acceso Denegado	1			

N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
6	Estándar	Acceso Permitido	1	1686786787	25	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1686787085	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
7	Estándar	Acceso Permitido		1686788708	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		16867899999	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
8	Estándar	Acceso Permitido		1686791874	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1686791975	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
9	Estándar	Acceso Permitido	1	1686794384	50	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1686794768	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
10	Estándar	Acceso Permitido	1	1687022405	66	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1687022465	120	
		Acceso Denegado	1			

N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
11	Estándar	Acceso Permitido	1	1687022678	20	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1687022844	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
12	Estándar	Acceso Permitido		1687023392	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687023658	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
13	Estándar	Acceso Permitido		1687024675	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687025030	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
14	Estándar	Acceso Permitido		1687025861	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687026111	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
15	Estándar	Acceso Permitido		1687026775	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687026962	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario

16	Estándar	Acceso Permitido		1687026788	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687022328	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
17	Estándar	Acceso Permitido	1	1687027606	72	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1687022875	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
18	Estándar	Acceso Permitido		1687028418	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687029070	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
19	Estándar	Acceso Permitido		1687028940	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687029905	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
20	Estándar	Acceso Permitido	1	1687030365	74	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1687030855	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
21	Estándar	Acceso Permitido	1	1687030444	81	

		Acceso Denegado				
	Blockchain	Acceso Permitido		1687030840	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
22	Estándar	Acceso Permitido	1	1687031595	80	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1687031807	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
23	Estándar	Acceso Permitido	1	1687298880	58	
		Acceso Denegado				
	Blockchain	Acceso Permitido	1	1687298925	107	
		Acceso Denegado				
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
24	Estándar	Acceso Permitido	1	1687299045	80	
		Acceso Denegado				
	Blockchain	Acceso Permitido		1687299155	120	
		Acceso Denegado	1			
N°Prueba	Tipo Plataforma	Estado de Acceso Login	Estado	Fecha timestamp	Tiempo de Vulneración (0-2 min)	Firma de usuario
25	Estándar	Acceso Permitido		1687299053	120	
		Acceso Denegado	1			
	Blockchain	Acceso Permitido		1687299154	120	
		Acceso Denegado	1			

ANEXO 11: Código fuente de la arquitectura blockchain propuesta:

```php
public function agregarNuevoUsuario
($correo,$mcd,$password){
            $statement = $this->PDO->prepare("INSERT INTO
 bloques values(null,:correo,:mcd, :password)");
            $statement->bindParam(":correo",$correo);

            $statement->bindParam(":mcd",$mcd);

            $statement->bindParam(":password",$password);
            try {
                $statement->execute();
                return true;
            } catch (PDOException $e) {
                return false;
            }
        }
```

Fig. 37. Proceso de registro de un nuevo usuario en la blockchain

Nota: Código fuente adaptado en la implementación del blog de Parzibyte's.

```javascript
const bufferABase64 = buffer => btoa(String.fromCharCode(...new
Uint8Array(buffer)));
        const base64ABuffer = buffer => Uint8Array.from(atob(buffer), c
=> c.charCodeAt(0));
        //sal permite agregr una capa de seguridad al hash.
        const LONGITUD_SAL = 16;
        const LONGITUD_VECTOR_INICIALIZACION = LONGITUD_SAL;
        //función asincrona,
        const derivacionDeClaveBasadaEnContraseña = async (contraseña,
sal, iteraciones, longitud, hash, algoritmo = 'AES-CBC') => {
            const encoder = new TextEncoder();
            let keyMaterial = await window.crypto.subtle.importKey(
                'raw',

//se crea una una clave privada considerando la contraseña de texto plano

                encoder.encode(contraseña),
                { name: 'PBKDF2' },
                false,
                ['deriveKey']
            );
            return await window.crypto.subtle.deriveKey(
                {
                    name: 'PBKDF2',
                    salt: encoder.encode(sal),
                    iterations: iteraciones,
                    hash
                },
                keyMaterial,
                { name: algoritmo, length: longitud },
                false,
                ['encrypt', 'decrypt']
            );
        }
```

Fig. 38: Modulo de encriptación con algoritmo AES-CDC

```
let str = '';
    let databloques = '';
    data.map(item => {
        str += `
            <tr>
                <td>${item.id}</td>
                <td>${item.correo}</td>
                <td>${item.mcd}</td>
                <td>${item.password}</td>

            </tr>
        `

        databloques +=`${item.id}+${item
.correo}+${item.mcd}+${item.password}`
    });
```

Fig. 39: Listado de bloques registrados en la plataforma Blokchain scan.

```
const encriptar = async (contraseña, textoPlano) => {
            const encoder = new TextEncoder();
            const sal = window.crypto.getRandomValues(new Uint8Array(16));
            const vectorInicializacion = window.crypto.getRandomValues(new Uint8Array(16));
            const bufferTextoPlano = encoder.encode(textoPlano);
            const clave = await derivacionDeClaveBasadaEnContraseña(contraseña, sal, 100000
, 256, 'SHA-256');
            const encrypted = await window.crypto.subtle.encrypt(
                { name: "AES-CBC", iv: vectorInicializacion },
                clave,
                bufferTextoPlano
            );
            return bufferABase64([
                ...sal,
                ...vectorInicializacion,
                ...new Uint8Array(encrypted)
            ]);
        };
```

Fig. 40: Módulo de encriptación utilizando SHA-256.

Nota: Código fuente inspirado en Lindbergh Morales, para el cifrado de la contraseña como proceso agregado al cifrado del módulo principal, proceso realizado previo a la exposición de la capa de internet.

```
$(document).ready(function() {
    var input = $('#exampleInputEmail1');
    var output = $('#output');

    var input2 = $('#password');
    var output2 = $('#output2');

    var input3 = $('#exampleInputmcd1');
    var output3 = $('#output3');

    var checkbox = $('#auto-update');
    var dropzone = $('#droppable-zone');
    var option = $('[data-option]');
    var inputType = $('#input-type');

    var execute = function() {
      try {
        var type = 'text';
        var val = input.val();
        var val2 = input2.val();
        var val3 = input3.val();
        if (inputType.length) {
          type = inputType.val();
        }
        if (type === 'hex') {
          val2 = hexToString(val2);
          val3 = hexToString(val3);
        }
        output.val(method(val, option.val()));
        output2.val(method(val2, option.val()));
        output3.val(method(val3, option.val()));


      } catch(e) {
        output.val(e);
        output2.val(e);
        output3.val(e);
      }
    }
```

Fig. 41: Proceso de cifrado principal en el módulo offline.

Reporte de similitud

NOMBRE DEL TRABAJO

LOPEZ_VALLEJOS_ROBER_YUBELDER_INFORMECOMPLETO para turnitin.docx

AUTOR

LOPEZ_VALLEJOS_ ROBER_YUBELDER

RECUENTO DE PALABRAS

21385 Words

RECUENTO DE CARACTERES

116390 Characters

RECUENTO DE PÁGINAS

100 Pages

TAMAÑO DEL ARCHIVO

2.9MB

FECHA DE ENTREGA

Jul 4, 2024 12:24 PM GMT-5

FECHA DEL INFORME

Jul 4, 2024 12:26 PM GMT-5

12% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 8% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 8% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)