UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Comparación de las Blockchains Aplicadas al IoT en Relación al Rendimiento y Seguridad en la Empresa Guimartbot SAC Lima 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTOR(ES):

Farfan Rosales, Handerson Joel (orcid.org/0000-0002-4526-1699)

Lopez Cordova, Rafael (orcid.org/0000-0001-6114-7821)

ASESOR:

Dr. Daza Vergaray,Alfredo (orcid.org/0000-0002-2259-1070)

LÍNEA DE INVESTIGACIÓN:

Auditoría De Sistemas Y Seguridad De La Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2022

Dedicatoria

Este proyecto está dedicado a nuestros padres, familiares y maestros que siempre creyeron en nosotros y brindaron su apoyo cuando lo necesitábamos. Nos han enseñado que tener conocimiento es el primer paso, pero hay que aplicarlo para generar un impacto positivo en la sociedad.

Agradecimiento

Agradecemos a nuestra institución de educación superior por brindarnos acceso a las bases de datos más grandes que existen, así como a cada uno de nuestros profesores a lo largo de la carrera y en especial al Doctor Alfredo Daza Vergaray y al ingeniero Oscar Manuel Bravo Carbajal por su apoyo y asistencia en la investigación y desarrollo de este proyecto, respectivamente.

Índice de contenidos

Índice de tablas

índice de gráficos y figuras

Resumen

Como objetivo, esta investigación tuvo identificar que tecnología blockchain, pública o privada basada en Ethereum, tiene mejor rendimiento y proporciona un alto nivel de seguridad, aplicada al Internet de las Cosas (IoT). Se utilizó un análisis comparativo con enfoque cuantitativo-experimental. En la primera fase, se crearon los dispositivos IoT y también una interfaz de programación de aplicaciones (API). En la segunda fase, se crearon dos redes Blockchain de prueba, Privada y Pública. Por último, en la tercera fase, se creó el FrontEnd y se realizaron las pruebas para obtener los resultados. Con respecto al rendimiento se tomó en cuenta el tiempo de ida y vuelta (TIV), donde la BC privada destaca con 0.05 milisegundos; en el porcentaje de consumo de recursos de la CPU, la BC privada obtuvo un menor porcentaje con 27.63%; y en la eficacia, ambas BC obtuvieron un 100% de efectividad; para la seguridad se observó la disponibilidad de los datos, donde se obtuvo un 100%; y el nivel de seguridad que brinda cada blockchain, también es muy alto. Dados los resultados, se concluye que las blockchains privadas son las más adecuadas para la integración.

Palabras Claves: Blockchain (BC), Internet de las cosas(IoT), Pública, Privada, Seguridad, Rendimiento, tiempo de ida y vuelta (TIV), Recursos, Eficacia, Disponibilidad.

Abstract

The objective of this research was to identify which blockchain technology, public or private based on Ethereum, has the best performance and provides a high level of security, applied to the Internet of Things (IoT). A comparative analysis with a quantitative-experimental approach was used. In the first phase, the IoT devices were created and also an application programming interface (API). In the second phase, two test Blockchain networks, Private and Public, were created. Finally, in the third phase, the FrontEnd was created and the tests were carried out to obtain the results. Regarding the performance, the round trip time (TIV) was taken into account, where the private BC stands out with 0.05 milliseconds; in the percentage of CPU resource consumption, the private BC obtained a lower percentage with 27.63%; and in efficacy, both BC obtained 100% effectiveness; for security, the availability of the data was observed, where 100% was obtained; and the level of security that each blockchain provides is also very high. Given the results, it is concluded that private blockchains are the most suitablefor integration.

Keywords: Blockchain (BC), IoT, Public, Private, Security, Performance, TIV, Resources, Efficiency, Availability.

I. INTRODUCCIÓN

El Internet de las cosas está revolucionando la forma en que vivimos y también representa cada vez más una gran amenaza para la seguridad de las empresas y personas en todo el mundo. La manera en la que estas manejan los datos hoy en día tiene dos principales retos por superar, la seguridad de datos, así como también la privacidad de sus usuarios registrados, pues con la creciente ola de ataques cibernéticos que hoy en día existe y según Gartner (2017), una empresa líder en investigación y asesoría digital, estimaba que para el año 2020 más del 25% de todos los ataques cibernéticos contra las empresas a nivel mundial ocurriría a través de dispositivos IoT (p. 13). Sin embargo, según Extreme Networks (2020), el 70% de las empresas sufrieron ataques cibernéticos mediante el uso de dispositivos IoT ese mismo año. Partiendo de dicha premisa, si no se implementa una nueva manera de manejar los datos en una red de IoT, que sea más segura, los atacantes seguirán aprovechando estas falencias para usar los dispositivos IoT a su conveniencia. Así mismo Gartner, en una investigación más reciente (2021), advierte que los ciberataques mediante IoT van a llegar a tal nivel, que en el año 2025 los atacantes tendrán el escenario, la tecnología y la capacidad de hacer daño físico o incluso llegar a acabar con la vida de las personas mediante el uso de estos dispositivos que cada vez se vuelven más comunes de tener tanto en los hogares mediante el IoT como en las empresas mediante el IIoT (párr. 2).

En el ámbito internacional, en Italia, Sicari (2015), publicó un artículo en el cual nos comenta que, en este caso, cumplir con los requisitos de seguridad y privacidad juega un papel fundamental. Esos requisitos incluyen privacidad y autenticación de datos, control de acceso a la red IoT, privacidad y confianza entre los usuarios y las cosas, y el cumplimiento de las políticas de seguridad y privacidad (p. 146). Las medidas que se toman ahora para evitar las vulnerabilidades antes mencionadas de IoT no son directamente aplicables a esta tecnología debido a los actuales estándares de comunicación en la red que existen. Por lo tanto, se requiere una nueva infraestructura, que sea resistente para hacer frente a las amenazas de seguridad en este entorno tan cambiante y en constante crecimiento.

Zeña (2021), en su investigación para llegar al grado de ingeniero de sistemas, en su tesis nos habla sobre la comparación de dos protocolos que son los más utilizados en la industria de la internet de las cosas (IoT), con la intención de demostrar que protocolo es el más seguro para utilizar en los dispositivos biomédicos y de alguna manera incrementar la seguridad de los mismos ante ataques cibernéticos, evidenciando sus resultados con sus propias pruebas (p. 42).

La conectividad de Internet con las cosas que nos rodean en nuestra vida diaria, tales como cámaras de seguridad, interruptores de luz y otros dispositivos que pertenecen a la familia de IoT, a los que además se puede consultar y manipular desde cualquier lugar, posibilitando formas de interactuar en un espacio determinado sin estar presentes mientras a medida que los usamos, estos objetos constantemente obtienen información de forma continua a través de sus sensores. Nos facilitan la vida, pero hay personas con habilidades de informática avanzadas que pueden aprovechar estos dispositivos para obtener información de los usuarios sin el consentimiento de los mismos, vulnerando las bases de datos de las grandes organizaciones que prestan servicios de IoT, La revista CIO (2016) nos dice que el problema con muchos productos de seguridad de IoT en el mercado es que se centran en la comodidad a expensas de la seguridad. La gente quiere que una cámara de seguridad tenga seguridad en la red por razones de privacidad (párr. 7). Pero esta debe ser parte de cada uno de los dispositivos de IoT. Estas personas antes mencionadas pueden capturar información tal como nombres de usuario, contraseñas, datos personales, números de tarjetas de crédito, entre muchos otros. Esto hace que los usuarios y las empresas no confíen plenamente en los dispositivos IoT por temor a ser víctimas de estos atacantes. “[...] los desarrolladores y fabricantes, tienen la responsabilidad de valorar la seguridad en el transcurso de la concepción y desarrollo de tecnologías implementadas con IoT, debido a que no únicamente se habla de pérdida o robo de información, sino al control de dispositivos remotamente, denegación de servicio, y otras funcionalidades que brindan los dispositivos IoT cada vez en mayor medida, esto conllevando al menoscabo de vidas humanas u ocasionar la detención colectiva” (Zeña, 2021, p. 14).

La falta de seguridad en dispositivos IoT en la empresa GUIMARTBOT SAC plantea un desafío importante, pues los dispositivos que maneja, así como lo mencionamos en párrafos anteriores, se encuentran vulnerables. Además, la necesidad de adopción de estos mismos es cada vez mayor, por consiguiente, el riesgo de recibir ataques a través de ellos aumenta de igual manera. Por otro lado, mientras las empresas que desarrollan la tecnología IoT buscan nuevas formas de proteger la infraestructura donde se guardan y manejan los datos, del mismo modo, los atacantes también idean nuevas formas de vulnerar esa seguridad, logrando acceder a información confidencial, hacerse con el control de acceso a los dispositivos o sensores y así al final, de una u otra manera, afectando la integridad de la información que estos dispositivos envían o reciben, y hasta la disponibilidad de los mismos para su dueño. De ello Sanchez (2020), nos dice, “La necesidad de proteger y clasificar la información al interior de la infraestructura de IoT por parte de los dueños de la tecnología IoT, ha despertado en los atacantes investigar nuevas formas o mecanismos de manipular, extraer o eliminar la información que se procesa allí [...] donde sí llegan a lograr atacar, esto puede ocasionar consecuencias en términos legales, económicos, sociales e incluso ambientales”. Esto conlleva a la empresa GIMARBOT SAC a la necesidad de buscar otras infraestructuras o tecnologías más robustas para hacer frente a estos problemas.

A modo de demostración, se aplicó el instrumento de evaluación que se muestra en el anexo 10, con el cual se realizaron unas pruebas con un dispositivo IoT, donde se realizó una simulación de un ataque a un dispositivo IoT para determinar latencia en la respuesta del dispositivo, la eficacia respecto a la cantidad de transacciones exitosas y fallidas (cuando el dispositivo responde a los comandos que se le envían de manera exitosa y sin contratiempos), el porcentaje de disponibilidad y el Nivel de seguridad. Además, aunque nuestra herramienta de recolección de datos no nos permite medir una vez aplicada la solución, cabe destacar que al aplicar este test a un dispositivo IoT, también que el usuario llega a perder el control del mismo por completo, lo que demuestra cuán inseguro realmente es el IoT que se usa y en el que se confía habitualmente, este test se muestra en la figura N.º 22 (Anexo 12) y también en este enlace que se muestra en la figura N.º 22 a modo de video. Donde se muestra, cuáles son las fallas y

vulnerabilidades que el dispositivo IoT tiene y de las que una persona ajena al usuario real, puede sacar provecho mediante el uso de estas para perjudicar al usuario.

La empresa GUIMARTBOT SAC está expuesta a ciberataques, como se muestra en el anexo 12, mediante el uso de sus dispositivos que cuentan con una conexión a internet, las empresas que brindan soporte a estos dispositivos tratan sus datos mediante el uso tradicional basado en la nube, y estas pueden tener un insuficiente interés de inversión en seguridad, además los datos, dentro de estas empresas pueden ser susceptibles a manipulación, filtración, fallos en los servidores en los que se manejan. Además, con la anteriormente mencionada creciente ola de ataques enfocados a los dispositivos IoT, que según resultados del informe realizado por el laboratorio de Palo Alto, el 57% de los dispositivos IoT todo el mundo tienen múltiples vulnerabilidades que pueden ser explotadas por los atacantes, a pesar de que los ciberdelincuentes no los usan para atacar al dispositivo en sí, pero con el objetivo de usarlos como "trampolín para el movimiento lateral para atacar otros sistemas en red", la empresa GUIMARTBOT SAC, siente desconfianza respecto a su seguridad de los datos, es por ello que busca una nueva alternativa de solución con la aplicación de la tecnología Blockchain y para ello necesita dar con el tipo de tecnología blockchain que es apropiada para el IoT.

Ante esto, en la problemática general, ¿Qué tipo de tecnología blockchain tiene un mejor rendimiento y proporciona mayor seguridad al realizar el intercambio de información con el IoT en la empresa GUIMARTBOT SAC?, y como problemas específicos, ¿Qué tecnología blockchain tendrá el menor tiempo de latencia en el intercambio de información con el IoT en la empresa GUIMARTBOT SAC?, ¿Cuál tecnología blockchain consumirá menos recursos durante el intercambio de información de los dispositivos IoT de la empresa GUIMARTBOT SAC?, ¿Cual tecnología blockchain será la más eficaz para permitir la comunicación con los dispositivos IoT en la empresa GUIMARTBOT SAC?, ¿Qué tipo de tecnología blockchain podrá mejorar la disponibilidad de la información en los dispositivos IoT en la empresa GUIMARTBOT SAC?, y ¿Cuál tecnología blockchain podrá mejorar el nivel de seguridad en mayor medida para proteger los dispositivos IoT en la empresa GUIMARTBOT SAC?.

Esta investigación se justifica mediante la relevancia social, ya que permite determinar cuál es la mejor tecnología blockchain que se adapte a la integración con los dispositivos IoT, así permitiendo que los desarrolladores centren sus esfuerzos en crear nuevas soluciones involucrando ambas tecnologías. Por otro lado, los usuarios del IoT van a tener acceso a sus dispositivos con un nivel de seguridad alto y haciendo uso de tecnología blockchain que ofrece un mejor rendimiento a comparación de los protocolos actuales. Esta misma tecnología (BC), permite encriptar la información con la que los dispositivos trabajan para comunicarse con el lado del usuario, de esta manera, brindando privacidad a los datos que el usuario manda a la red sin la posibilidad de que puedan ser interceptados, alterados, robados, eliminados o ser usados de manera indebida, lo cual, al final beneficia en gran medida a todos los dueños de estos dispositivos.

También este proyecto se justifica a nivel práctico, ya que permite determinar que tecnología blockchain nos ayuda a que la integración de blockchain-IoT sea más ágil y segura, haciendo uso de nuevas tecnologías como los contratos inteligentes o Smart contracts los cuales permiten tener programas corriendo dentro de las Blockchains, lo que permite el manejo de los dispositivos de manera segura y eficaz, añadiendo una capa más de seguridad a la tecnología IoT, brindando los beneficios de la tecnología blockchain al IoT. De esta manera se ayuda a superar los retos más importantes del IoT (Seguridad, escalabilidad, control de acceso, entre otros beneficios que no se estudian a fondo en esta comparativa). De modo que, esta investigación puede servir de guía para desarrolladores o empresas interesadas en integración BC-IoT. Por otro lado, también se cuenta con el fin de posicionar una nueva integración de dos tecnologías tan relevantes y necesarias en la actualidad, ahora despertando el interés sobre este tema a próximos investigadores sobre la tecnología de la cadena de bloques o blockchain.

Nuestra investigación sobre la implementación de la tecnología blockchain a los dispositivos IoT se justifica de manera económica, permitió una disminución de los gastos en la adquisición de antivirus que prometen seguridad para los dispositivos IoT, pues actualmente la empresa incurre en gastos en licencias anuales por software de seguridad, dado que los contratos inteligentes (Smart contract), ayudan en la optimización de los procesos de los dispositivos IoT, siendo

estos pre-programados para ejecutar determinados parámetros cumpliendo ciertas condiciones que el dueño del contrato previamente define, y solo él y quienes le asigne, puede manejar este contrato mediante una verificación que utiliza metamask (un servicio de encriptación que te permite contar con una llave privada y una pública para realizar transacciones dentro de la red Ethereum), logrando la inmutabilidad de los datos, y siendo intrínsecamente seguros. De este modo se eliminó diferentes tipos de mecanismos de seguridad (bases de datos espejo, los mismos servidores y la infraestructura completa, así como también en hardware como en software), que antes se usaba para resguardar la información.

Para el presente trabajo se planteó el siguiente Objetivo General: Identificar qué tecnología blockchain tiene el mejor rendimiento y seguridad al realizar el intercambio de información con el Internet de las cosas (IoT), en la empresa GUIMARTBOT SAC. También se plantearon los siguientes objetivos específicos, el primero fue identificar qué tipo de blockchain tiene un menor tiempo de ida y vuelta (TIV), durante el intercambio de información con el dispositivo IoT en la empresa GUIMARTBOT SAC. El segundo fue identificar qué tipo de blockchain consume menos recursos durante el intercambio de información con el dispositivo IoT de la empresa GUIMARTBOT SAC. El tercero fue determinar qué tecnología blockchain es la más eficaz para permitir la comunicación con los dispositivos IoT en la empresa GUIMARTBOT SAC. El cuarto fue identificar qué tipo de blockchain mejora la disponibilidad en la información en los dispositivos IoT de la empresa GUIMARTBOT SAC. Y por último fue determinar qué tecnología blockchain mejora el nivel de seguridad de la información manejada en los dispositivos IoT en la empresa GUIMARTBOT SAC.

En esta investigación se formuló la siguiente Hipótesis General: Existen diferencias significativas respecto al rendimiento y seguridad entre la blockchain pública y la privada cuando son aplicadas a los dispositivos IoT en GUIMARTBOT SAC y con también se plantearon las siguientes hipótesis específica, la primera fue: La tecnología blockchain pública y privada tienen diferencias significativas en la latencia en relación al TIV durante el intercambio de información con los dispositivos IoT de la empresa GUIMARTBOT SAC. La segunda fue: Existen diferencias significativas entre la tecnología blockchain pública y privada respecto a su

rendimiento en relación al consumo de recursos al aplicarse al IoT en la empresa GUIMARTBOT SAC. La tercera fue: La tecnología blockchain pública y privada tienen diferencias significativas en rendimiento en relación a la eficacia al aplicarse al IoT en la empresa GUIMARTBOT SAC. La cuarta fue: La tecnología blockchain pública y privada tiene diferencias significativas en la seguridad respecto a la disponibilidad de la información en los dispositivos IoT de la empresa GUIMARTBOT SAC. Y, por último, la tecnología blockchain pública y privada tienen diferencias significativas en el nivel de seguridad al aplicarse al IoT en la empresa GUIMARTBOT SAC.

II. MARCO TEÓRICO

Durante el desarrollo de este capítulo en adelante se usarán los términos listados a continuación.

TABLA N.º 1: *Diccionario de términos*

Diccionario de términos:	
TIV:	Tiempo de Ida y Vuelta del comando que enviamos a la BC.
BC:	Blockchain.
IoT:	Internet de las cosas o Internet of Things por su traducción al inglés.
VsCode:	Visual Studio Code, un IDE donde se desarrolla el código para que todo funcione correctamente.
IDE:	Ambiente integrado de desarrollo o Integrated Development Environment en inglés.
ETH:	Moneda virtual que se usa en la red Ethereum.
IIoT:	Internet de las cosas industrial o Industrial Internet of Things por su traducción al inglés.
HDD:	Memoria de disco duro o Hard Disk Drive por su traducción al inglés.
IBM:	Se refiere a la empresa International Business Machines Corporation.
ISO:	Organización internacional para la estandarización o International Organization for Standardization.
EVM:	Estas siglas provienen de ETHEREUM VIRTUAL MACHINE, la cual es la máquina virtual de Ethereum que está respaldada por la red Ethereum.
POW:	Protocolo de consenso de una red blockchain y con el que anteriormente trabajaba Ethereum.
POS:	Protocolo de consenso de una red blockchain y con el que actualmente trabaja Ethereum.
PCR:	Porcentaje de consumo de recursos.
API:	(Application Programming Interface), sirve para intercambiar datos y funcionalidades de manera fácil y segura con el lado del usuario o FrontEnd.
RAM:	(Random-access memory) es una forma de memoria de computadora que generalmente se usa para almacenar datos temporales de trabajo y código de máquina.
FrontEnd:	Es la parte de un sistema de información con la que el usuario interactúa directamente para recibir o utilizar las capacidades del back-end del sistema host.
BackEnd:	La programación Backend es un tipo específico de programación en el que se configuran todos los aspectos lógicos de un sitio web o aplicación.

Fuente: Elaboración propia

Para sustentar el desarrollo del presente trabajo de investigación se recurrió a las siguientes fuentes:

Delgado (2018), en su investigación “Aplicación de Blockchain para la seguridad de los datos del IoT” tiene como objetivo utilizar la blockchain para aprovechar la privacidad y la seguridad que brinda esta misma, y así poder aliviar algunos de los problemas que tiene IoT con respecto a la seguridad de sus datos, implementando una Blockchain para poder procesar y almacenar los datos de los sensores IoT de manera descentralizada y segura con Hyperledger Fabric. En esta investigación se realizó en 3 máquinas virtuales junto con una placa de Arduino. Primero se realizaron pruebas con una primera configuración de las máquinas virtuales (1 CPU, 3,75GB de RAM, 80GB de HDD) si los resultados fueron que se el 5% de uso de CPU, 1 KB/s en red. No se tiene grandes procesos la máquina con una transacción equiespaciada de 1 min, la transacción de los datos fue exitosa en 2 seg. Luego se programan 3 dispositivos los cuales están programados para enviar 1 y transacción por seg. Aumentando el doble de transacciones por 10 min. Esto hacía que se duplicarán las transacciones. Además, en un momento se comenzaron a rechazar las transacciones dado el alto estrés que estaba sometido la CPU. En tanto Kafka no presento un uso alto de su CPU, solo presento el 65% del mismo, mientras que el tiempo de latencia es de 3 segundos por respuesta aprox. Después se realizó pruebas con diferentes características de las máquinas virtuales (8vCPU y 16 GB RAM), el tiempo de latencia se mantiene en 1 segundo, hasta 800 transacciones por segundo y después la red va decayendo a medida que aumentan las transacciones. Esto concluye que las máquinas virtuales requieren de las Cores de CPU para realizar procesos desde la versión 1.2 de Hyperledger Fabric. En esta investigación se llegó a la conclusión que la sinergia entre la tecnología IoT y blockchain es posible gracias a BC privadas. De esta investigación se tomará cuenta los resultados y definición de algunos programas a utilizar en esta investigación dado que son importantes para este presente proyecto.

Castro (2021) en su investigación titulada “Aplicabilidad de tecnologías Blockchain diseñadas para entornos IoT” tiene como objetivos analizar la ejecutabilidad de algunas redes de tecnologías Blockchain que menciona como campo principal la IoT, con eso poder realizar un caso práctico que pueda probar

lo mencionado anteriormente. Se usó un estudio analítico y un desarrollo iterativo donde se desarrollará de forma incremental, para una aplicación de internet de las cosas sobre una plataforma blockchain que sea la más idónea. Con el resultado de las pruebas realizadas se desarrolló un programa para Raspberry Pi, que permite leer los datos de BC y actuar en base a ellos (contrató inteligente). Pero también se llegó a la conclusión que las tecnologías blockchain que aún no son suficientemente maduras para los entornos de la IoT. Esto quiere decir que se logra desarrollar un programa con las tecnologías blockchain y IoT, pero aún no es un procedimiento que funcione al 100%, ya que se debe mejorar algunas herramientas y algunas aplicaciones. De esta investigación se tomará cuenta los resultados y definición de algunos programas a utilizar en esta investigación dado que son importantes para este presente proyecto.

Conteron (2021) en su investigación titulada “Sistema de Smart home aplicado IoT y Blockchain” el objetivo de este trabajo fue implementar un sistema de casa inteligente ejecutando internet de las cosas y BC, valorar la seguridad y la confidencialidad de la información de acceso en la integración de blockchain con IoT, para obtener los resultados, se realizó el análisis por medio de las respuestas entre el blockchain y los dispositivos IoT, también se realizaron pruebas de seguridad a la BC para garantizar la integridad de los datos tanto de envío como de respuesta entre los dispositivos IoT y la BC. Los resultados de las pruebas son de 0,4023 milisegundos de demora, lo que significa que no se pierde información y la confirmación del usuario es inmediata, como cabría esperar de un sistema en tiempo real. La integridad de los dispositivos IoT y la solución propuesta le permite lograr sus objetivos de seguridad y resistir ataques de intermediarios, DoS y suplantación de identidad. Además, Vyper ha sido elegido como el lenguaje que permitirá contratos inteligentes más seguros, serán fácil de programar y serán legibles porque restringe libremente las acciones permitidas en otros lenguajes De esta investigación se tomará cuenta los resultados y definición de algunos programas a utilizar en esta investigación dado que son importantes para este presente proyecto.

Restrepo, Olaya (2018) en su investigación titulada “Desarrollo de un prototipo basado en blockchain aplicado a la plataforma IoT sobre un sistema

embebido” que tiene como objetivo desarrollar un prototipo basado en un sistema embebido de bajo costo en una plataforma IoT que permita la interacción con una red de cadena de bloques, en esta investigación se logró la interacción de ambas la tecnología BC y los dispositivos IoT, se optimizo los recursos para que puedan aprovechar las características únicas que ofrece blockchain, ya que se ha demostrado que es posible realizar funciones JSON-RPC utilizando un archivo json generado desde un sistema integrado para usar y registrar respuestas de manera similar, realizar acciones en base a ella y utilizando un contrato inteligente, es posible establecer el valor de PPM permitido desde el sitio web de forma segura, Como resultado el contrato inteligente se puede utilizar de forma remota por medio del programa NodeJs, entre otros programas el cual tiene el usuario y contraseña que permite ingresar un nodo de esa red. De esta investigación se tomará cuenta los resultados y definición de algunos programas a utilizar en esta investigación dado que son importantes para este presente proyecto.

Sanchez (2020) en su investigación para obtener el grado de magíster titulado “Defensa contra intrusos en redes de dispositivos IoT usando técnicas de blockchain y machine learning” tuvo como objetivo desarrollar una estructura que permite la detección y prevención de ataques de intrusos en redes IIoT basada en tecnología BC (blockchain o cadena de bloques), y Machine Learning. En esta investigación se enfocó en evaluar y determinar cuáles son los parámetros adecuados para optimizar el tiempo y la eficiencia. En los resultados de esta investigación se ve que el sistema desarrollado es capaz de detectar los ataques bajo una cierta identificación, este modelo es muy flexible y responde muy bien al aumento de cargas y escalabilidad, mientras que las fluctuaciones de rendimiento son mínimas. De esta investigación se tomará cuenta los resultados y definición de algunos programas a utilizar en esta investigación dado que son importantes para este presente proyecto.

Chen, Nguyen y Sekiya (2021) en su artículo titulado “Un estudio experimental sobre el rendimiento de blockchain privado en aplicaciones IoT” tiene como objetivo medir el rendimiento de una blockchain privada que está aplicada a aplicaciones IoT, este artículo se enfocó en evaluar y determinar el rendimiento de la blockchain privada en Ethereum, para esto se realizaron dos pruebas para llegar

a las conclusiones, primero se realizó por medio de una blockchain con nodos conectados dentro de una misma red, se realizó utilizando unas placas de Raspberry Pi conectadas a un computador, después se realizó por medio de máquinas virtuales, que también fueron utilizados como dispositivos IoT, como conclusión se obtuvo que la cadena de bloques privada basada en Ethereum es una tecnología con mucho potencial para que se pueda aplicar en la tecnología IoT, sin embargo, la blockchain es considerado como pesado para los dispositivos IoT. De esta investigación se tomará cuenta los resultados y definición de algunos programas a utilizar en esta investigación dado que son importantes para este presente proyecto.

Zeña (2021) en su investigación titulada “Comparación de protocolos de comunicación en internet de las cosas, determinando el nivel de seguridad ante ataques en dispositivos biométricos” El objetivo de esta investigación es comparar protocolos de capa de aplicación en IoT para medir la protección contra ataques a dispositivos biométricos. La investigación es de tipo de cuantitativa porque incluye muchos números en indicadores expresados como porcentajes. De acuerdo a los resultados de este estudio, resulta que los protocolos más utilizados en la industria IoT son MQTT y COAT, sin embargo, uno de ellos brinda mayor seguridad, protección y privacidad en la implementación, de acuerdo a los resultados del COAP, brinda mejor protección contra ataques biométricos, ya que al compararlos el promedio de la latencia con el MQTT, que obtuvo 22221,45 ms y COAP 7182,56 ms, siendo este último el de menor latencia, esto concluye que tiene mayor especificidad y eficiencia. Asimismo, al ver los resultados por peticiones fallidas se obtiene que el protocolo COAP arroja un 19.37% mientras que el MQTT 28.12%, dando como conclusión que el protocolo COAP es más seguro a los ataques de dispositivos biométricos. Con estos resultados se llegó a la conclusión que el protocolo COAP es el más seguro frente a los ataques DOS. De esta investigación se tomará cuenta los resultados y definición de algunos programas a utilizar en esta investigación dado que son importantes para este presente proyecto.

Para que el proyecto tenga un adecuado respaldo se ha tomado referencias teóricas:

Por ejemplo**,** en esta sección se aborda el tema central de esta investigación, la tecnología Blockchain que según Reyna (2018, p. 2) nos dice que Blockchain es un mecanismo que permite que las transacciones sean verificadas por un grupo confiable. Proporciona un libro mayor que es distribuido, inmutable, transparente, seguro y auditable, por otro lado, Puliafito (2018, p. 3) nos comenta, el objetivo de Blockchain es liberar a las personas de cualquier confianza que ahora los usuarios están obligados a dar a los intermediarios que regula y gestiona gran parte de los datos. Según Dorri (2017, p. 1) Blockchain es un libro contable Inmutable de bloques que respalda a Bitcoin y mantiene las transacciones de la red. Cuenta con participantes en la red que son conocidos por una clave pública modificable (PK) y administran la BC de forma distribuida.

La información dentro de una blockchain se organiza por medio de una cadena de bloques, que son un conjunto de transacciones, los bloques son de tamaño limitado para facilitar el minado. Una vez que la transacción es validada, se añade un nuevo bloque a la cadena y dentro de este bloque lleva el HASH del anterior bloque y también se creó un nuevo HASH para que así en una futura transacción se pueda utilizar de cabecera en el siguiente bloque.

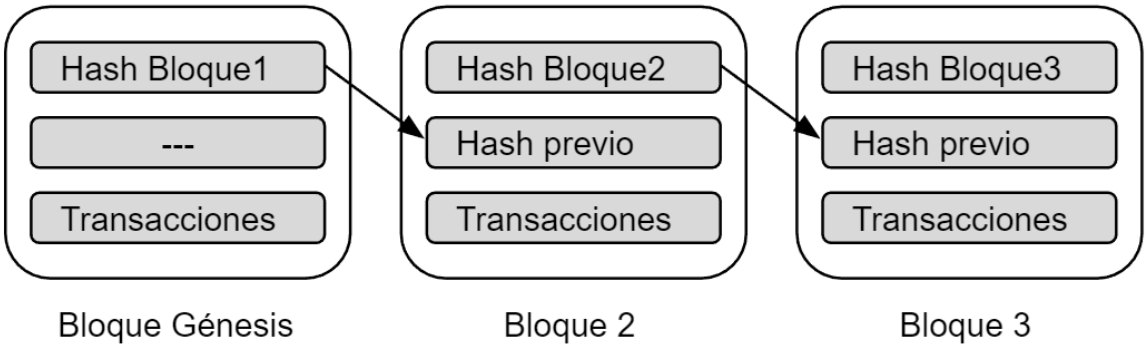


Figura N.º 1: Funcionamiento del hash dentro de una cadena de bloques.
Fuente: Elaboración propia

Además, la tecnología blockchain cuenta con diversas características, de las cuales se explican a continuación:

La tecnología blockchain tiene un diseño, donde su red no depende de un intermediario manteniendo así la información consistente en el tiempo, es decir, se puede garantizar que los datos no serán alterados una vez que ya estén dentro de la blockchain, este diseño ayuda a solucionar varios problemas como por ejemplo que personas no autorizadas puedan modificar, alterar o añaden nuevos datos sin

la verificación de la persona autorizada, también evita que un nodo malintencionado pueda estafar o engañar en una transacción a los demás nodos mandando datos alterados de previas transacciones (Mereles, 2019, p. 11).

Por otra parte, se cuenta con la descentralización que es la parte más esencial de la tecnología blockchain, esto hace posible que una o varias personas no puedan controlar o hacer cambios al sistema, de esta manera los usuarios tienen la posición de que directamente puedan almacenar sus documentos, criptomonedas, Smart contracts u otro tipo de información, sin que se necesite a un tercero para ser la autoridad intermediaria de confianza. Esto genera confianza en este sistema. También hace que este sistema sea fiable al ejecutarse de forma distribuida, es decir, tiene menos tendencia que si tiene una avería inutilice todo el sistema por completo, como el que podría ser provocado por un ataque DDoS. Este sistema reduce el control de datos y las tareas de registro, evitando la duplicación de registros y datos, es decir que solo existe un registro distribuido (Bashir, 2018, p. 42).

Por otro lado, también cabe tener en cuenta un tipo diferente de blockchain, que es la Blockchain Privada, siendo aquella creada por una entidad u organización para su propio uso. El acceso de personas ajenas a la entidad es totalmente restringido, esto quiere decir que no pueden ni ver, ni poder escribir. Cada nodo de esta red está controlado por dicha entidad, que es la encargada del mantenimiento y gestión. Las características de esta red hacen que se vuelva muy valiosa para la empresa, ya que pueden hacer aplicaciones de la blockchain para sus procesos, aprovechando las ventajas de seguridad e inmutabilidad de datos, sin que se pueda filtrar algún tipo de información. Debido a que el mantenimiento de esta es privada, está encargada de la entidad además puede utilizar protocolos de consenso más eficientes que primen el rendimiento y la escalabilidad que caracteriza a la cadena de bloques (Fernandez, 2021, p. 60).

También se tomará en cuenta que es un nodo en una cadena de bloques (BC), puede realizar diversas cosas según el rol que este asuma. Este puede validar y proponer transacciones, también puede minar y agilizar el protocolo de consenso y proteger la Blockchain. También puede verificar simples pagos, validación y muchas otras funciones, según el blockchain que se utiliza, Un Nodo también

pueden realizar las firmas digitales, esto se realiza cuando se realiza una transacción y luego los nodos por medio de claves privadas pueden firmar digitalmente, esto como prueba de son propietarios legítimos del activo que se desea transferir de una persona a otra en la BC (Bashir, 2018, p. 494).

Dentro de las características que los nodos hacen dentro de la blockchain es la base de datos distribuidos, cada nodo de la red tiene que replicar la base de datos la blockchain. El nodo seguirá perteneciendo a la blockchain siempre y cuando siga sincronizado a la cadena de bloques. Uno de los puntos a analizar es que la base de datos que es distribuida, es alimentada por los bloques, quiere decir que, si una transacción no es confirmada o sincronizada a la cadena de bloques, esta será rechazada y considerada como no válida dentro de la blockchain (Rojo, 2020, p. 1).

Una característica importante de la blockchain es el hash, Según Alija (2017, p. 7) Es la huella digital única de la transacción. A través de la transacción, se puede entender cualquier cosa digital que se requiera poner en la cadena de bloques. Puede ser un giro postal, una fotografía o un capítulo de un libro que escribimos. El beneficio de la función hash es que no importa qué tipo de información quieras enviar (o hacer una transacción), la longitud y el tipo de esa información no importa, el hash es una marca única y siempre tiene la misma estructura posible y se puede encontrar, comparar y contrastar en cualquier momento. Además, se le conoce como la “resistencia a la colisión”. Esta es la capacidad del hash para que nadie pueda encontrar dos hashes idénticos. Y así es como se puede comprobar la autenticidad de las cosas, esta es la principal característica del hash.

Ejemplo: En ambos casos solo ha cambiado un número (el 0 por número 1 se cambió en el segundo caso), y el resultado del hash es totalmente diferente. Lo mismo ocurre en cualquier otra frase ingresada al algoritmo.

TABLA N.º 2: *Ejemplo de encriptación con el algoritmo hash de Ethereum*

Frase a encriptar	Frase hasheada
frase00	7e99697c5b209ad7f44a2dc448ae78b759dbdc6418e0c4aeba8c2673ff270596

frase01	2e632518b214f612c0e764eaa15ab0d54a145716657ae48134cdb6a93b94334b

Fuente: Elaboración propia

Además del hash, la blockchain también hace uso de un protocolo de consenso, el cual es la manera en la que todos los nodos de una blockchain llegan a un acuerdo entre la interrogante de que, si el bloque es verídico o no, para ser agregado a la cadena de bloques para siempre, sin la posibilidad de modificarlo como ya se mencionó en la explicación de la inmutabilidad que tiene blockchain.

Utilizan diferentes algoritmos para llegar a un consenso. Es una serie de pasos realizados por la mayoría de los nodos en la cadena de bloques para acordar el valor propuesto. El mecanismo de consenso estuvo en el centro de atención y se hizo popular con la llegada de blockchain y Bitcoin (Bashir, 2018, p. 253). Con relación a la blockchain el protocolo de consenso es el núcleo de la blockchain que garantiza su funcionamiento. En la red los nodos realizan las transacciones en toda la red y llegan a un consenso sobre las transacciones aceptadas siguiendo el protocolo de consenso (Ding, 2019, p. 3).

Otro tema importante a tocar para este proyecto son los Smart contracts o contratos inteligentes, que como individual es un programa capaz de ejecutar y forzar un evento de forma automática o desde un evento, sin necesidad de intermediario. Los contratos inteligentes o Smart Contracts pueden ser creados por personas físicas o jurídicas, pero también pueden ser creados por máquinas o programas que funcionan de forma autónoma. Tienen un valor independiente de las autoridades, esto se debe a que su código es visible para todos y no se puede modificar usando la tecnología blockchain. Esto hace que sean inmutables, descentralizados y transparentes. Tienen muchos casos de uso como las gestiones de identidades, los mercados de capitales, financieras comerciales, gestión de registro, seguros y el gobierno electrónico (Christidis, 2016, p. 1). Con respecto a la blockchain, los contratos inteligentes surgen de la propiedad inteligente, es un método utilizado en la blockchain para lograr un acuerdo entre las partes, sin la necesidad de depender de terceros para tener la confianza (Bashir, 2018, p. 75). En este caso los Smart Contracts o contratos inteligentes nos ayudará a poder interactuar con la blockchain, será quien nos ayude con la interacción con los

dispositivos IoT, ya que por medio de estos se mandará las funciones requeridas por el cliente, aparte que se desplegará el Smart Contract con la Blockchain pública y privada y la interacción entre ambas será directa. Esta interacción nos ayudará a sacar los resultados para poder medir los indicadores como la latencia y las transacciones exitosas.

Por otro lado, el Internet de las cosas o IoT, es una tecnología basada en la conexión de objetos a través de Internet, en la que intercambian, procesan y sintetizan información sobre su entorno físico y esto aporta un valor añadido al usuario, finalmente, el sistema puede responder de forma autónoma y adecuada. El propósito de IoT es proporcionar una infraestructura que cruce la barrera entre el mundo físico y el mundo digital. La integración de sensores y dispositivos en objetos cotidianos, ahora conectados a Internet a través de redes cableadas o inalámbricas, ha creado un nuevo mundo de interacción (Andres, 2018, p. 19-20).

También se tomará en cuenta la criptografía este ocupa de técnicas de cifrado o codificación a determinados mensajes con el fin de hacerlos ininteligibles a personas no autorizadas, actualmente se utilizan la seguridad a las comunicaciones, a la información. En ese sentido, se encarga de dar a los sistemas las siguientes características: autenticación, confidencialidad, integridad, vinculación (Nespral, 2021, p. 48).

La Criptografía se divide en dos partes:

La Criptografía Simétrica Es la cual usa la misma clave para cifrar y descifrar mensajes en el emisor y receptor, es bueno ponerse de acuerdo las dos partes, cuando llegan a un acuerdo el remitente cifra el mensaje y el receptor tiene que descifrar con la misma clave (Nespral, 2021, p. 49).

Por otra parte, la criptografía asimétrica También conocida como clave pública o de dos claves, ambas claves pertenecen a un usuario, una clave es pública, esta se la puede entrar a cualquier persona, la otra clave es privada que esa es solo la del usuario, además los métodos criptográficos garantizan que esas claves solo que puedan generar una sola vez, de modo que dos personas es casi imposible que puedan tener la misma pareja de claves (Nespral, 2021, p. 49).

Un tema importante a ver es sobre Ethereum que es una plataforma computacional confiable, junto con una moneda nativa, que se establece sobre una red descentralizada de igual a igual. Cualquier contenido digital que pueda ser controlado por alguien puede guardarse en un contrato inteligente de Ethereum, que luego se transfiere entre pares sin necesidad de un tercero o intermediario, como un banco, bolsa o gobierno central. Los datos almacenados en los contratos inteligentes son seguros y de fácil acceso, aunque el costo y la estructura de la tienda están más relacionados con las aplicaciones relacionadas con los metadatos porque guardar datos reales es demasiado costoso. La máquina virtual Ethereum se utiliza principalmente para dirigir contratos inteligentes, así como para establecer un consenso entre todos los participantes.

Otro tema a tocar será el Metamask que en comparación de otras carteras de escritorio, Metamask viene como extensión de Chrome o Firefox, esto significa que está disponible para todos los usuarios de escritorio que tenga acceso a estas plataformas, esta es una aplicación que almacena las claves en el disco duro de su computadora, por lo que se categoriza como una cartera de escritorio, una de las características más destacada que brinda acceso a DApps que se ejecutan en la cadena de bloques ethereum. Lo malo es que no admite Smart contracts (Woods, 2021, p. 200).

Por otro lado, también se tomó en cuenta el lenguaje de programación solidity, Aunque Ethereum admite muchos lenguajes diferentes para crear Smart Contracts, el más conocido y más utilizado es Solidity. Este es un lenguaje de alto nivel, su sintaxis es muy parecida a JavaScript. Las diferentes características de Solidity se muestran a continuación. En primer lugar, para iniciar un hilo en Solidity, se hace con una palabra patentada "contrato", similar a una clase que puede contener funciones, modificadores y más tipos de datos como cualquier lenguaje de programación. Tenga en cuenta que este lenguaje permite que los contratos se hereden (Schupfer, 2017, p. 16).

En este trabajo otra herramienta que se tomó en cuenta es Infura, es un conjunto de Interfaces de Programación de aplicaciones (APIs) que ayuda a tener acceso a diferentes redes de Ethereum como: Rinkeby, Mainnet, Gorli, Ropsten, Kovan y Sepolia, tambien a los IPFS a través de HTTPS (protocolo de seguro de

transferencia de hipertexto) y el WebSockets. Esto nos ayuda a poder implementar la red descentralizada de la red de Ethereum, este programa es utilizado para hacer simulaciones (Infura, 2020, p. 1).

Remix es una herramienta que nos ayudará con los Smart contract, Remix es un IDE más popular y con mejor capacidad. Fue desarrollado por el mismo equipo de Ethereum, nos permite implementar, compilar, desplegar y depurar los contratos inteligentes en diferentes redes de prueba de Ethereum como por ejemplo Rinkeby (Remix, 2019, p. 1).

También se tomará en cuenta la herramienta Visual studio code (VsCode), ya que es un editor de código ligero, pero potente al ejecutarlo en el escritorio, lo bueno que esta herramienta está disponible tanto para Windows como para MacOS y Linux. También viene incorporado soporte para JavaScript, node.js y TypeScript, y también bastantes extensiones eso hace posible que se puedan utilizar otros lenguajes como C, C#, Java, Python, Go y PHP (Visual Studio Code, 2020, p. 1).

Arduino, es otra herramienta que se utilizara para este proyecto, ya que es una herramienta de Hardware libre, que está basada en una placa con un microcontrolador. Su software y hardware son flexibles por esa razón es fácil de usar. Este hardware fue diseñado para que se pueda adaptar a las necesidades que el usuario lo pueda utilizar, tanto como para aficionados o expertos en robótica o equipos electrónicos (Arduino, 2015, p. 1).

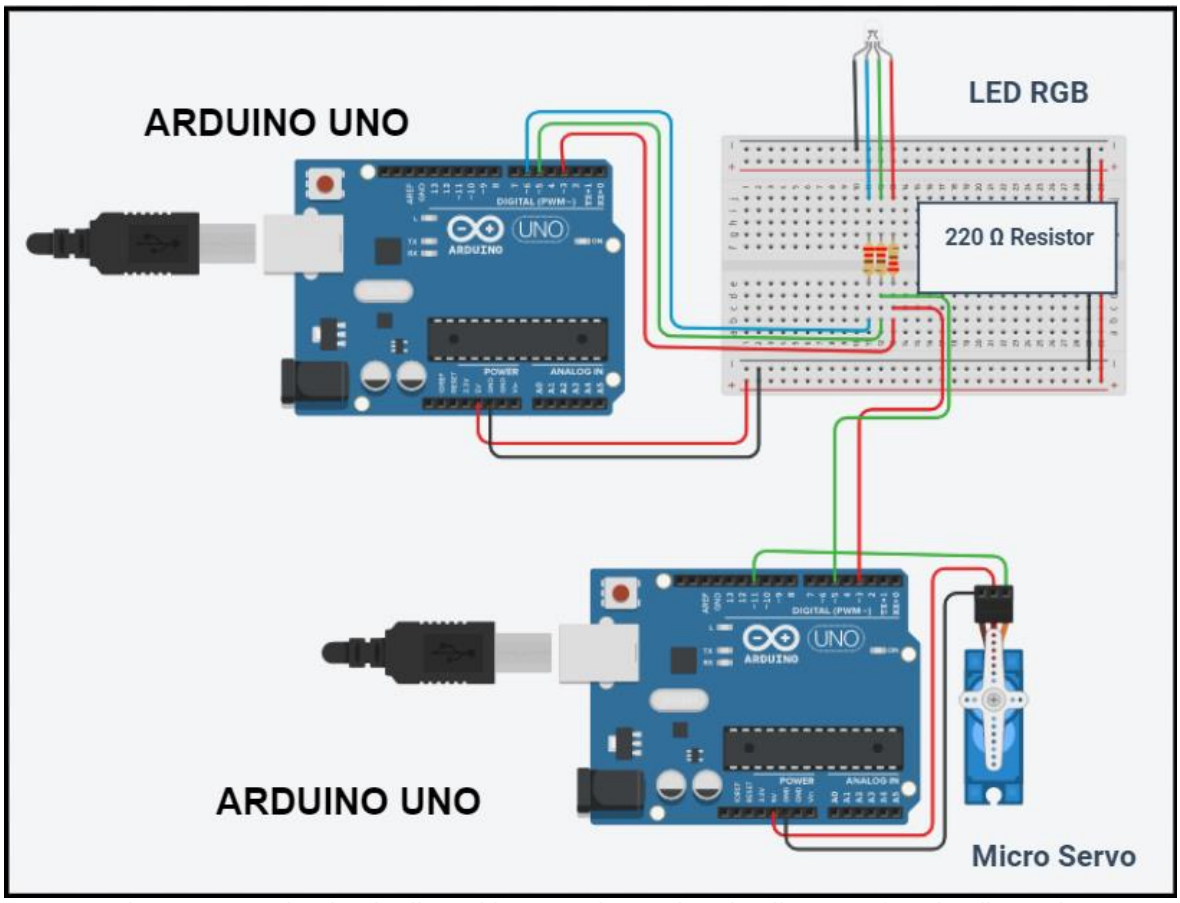


Figura N.º 2: Circuito de dispositivos IoT (Cerradura inteligente y foco inteligente)
Fuente: Elaboración propia en Dashboard | Tinkercad

PoS o Proof-of-Stake este es un protocolo de consenso utilizado en la cadena de bloques, es alternativo a PoW, y está pensado para ahorrar energía, en este caso los mineros con más prioridad son los que tienen más criptomonedas, por lo tanto, estos mineros no van a tener la intención de corromper la cadena y van a ser los elegidos para así minar los siguientes bloques (Rojas, 2018, p. 44).

PoW o prueba de trabajo es un protocolo de consenso utilizado en una cadena de bloques o blockchain, este protocolo de consenso se basa en exigir a los nodos de la red con un coste computacional elevado la verificación de las transacciones y así crear un nuevo bloque, la dificultad de este protocolo es demasiado difícil de resolver, pero muy fácil de verificar si ha sido resuelto correctamente, que si un nodo de la red resuelve el problema los demás nodos solamente deberán verificar si es correcto y aceptar o no el nuevo bloque en la cadena (Lodeiro,2020, p. 22).

Geth o Go Ethereum, esta es una herramienta que nos ayudará mucho en este proyecto, esta es una aplicación que se utiliza para poder ejecutar un nodo en Ethereum, esto permite que este nodo de Ethereum sea privado y autosuficiente. Se puede usar para poder consultar sobre la cadena de bloques, transferir ETH entre las cuentas y hasta proteger la red. Es un software rápido, de código abierto y ligero (Ethereum, 2022, p. 1).

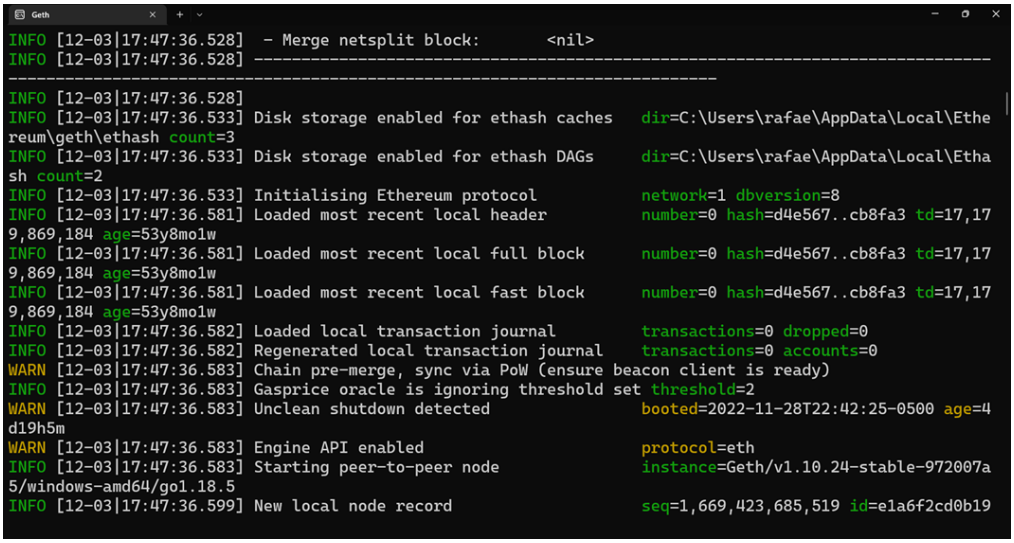


Figura N.º 3: Herramienta Geth en ejecución
Fuente: Elaboración propia

La máquina virtual de Ethereum (EVM) es lo que gestiona la computación y el estado para todos los contratos. Un Smart Contract es sólo un conjunto de declaraciones de código de operación, que se ejecutan secuencialmente por el EVM. Esta herramienta virtual se puede considerar como un ordenador global descentralizado donde se ejecutan todos los contratos inteligentes. Aunque se comporta como un ordenador grande, es realmente una red de máquinas más pequeñas que están constantemente comunicándose entre sí (Ethereum, 2020, p. 1).

IIoT o Internet de las cosas industrial, surgió como concepto general de la aplicación de IoT o internet de las cosas al sector industrial. Es una generalización de la industria 4.0, que parece concentrarse en la eficiencia de los procesos industriales. IIoT incluye todas las operaciones industriales, no solo en la eficiencia del proceso, sino también en la gestión de activos, mantenimientos […] (Madakam, 2019, p. 2).

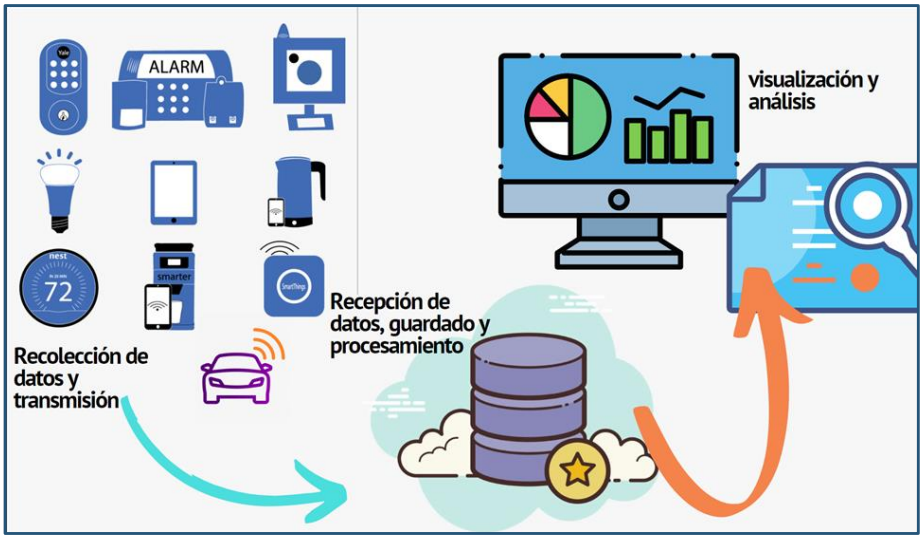


Figura N.º 4: Funcionamiento actual del IoT
Fuente: Elaboración propia

El ataque del 51% (o attacks 51% en inglés), es una definición que tiene relevancia, ya que es un ataque que puede sufrir una blockchain, este se da al poseer el control de la mayor parte de la potencia de cómputo de la blockchain o cadena de bloques, de esta manera los atacantes podrán evitar las confirmaciones de las nuevas transacciones, como también pueden aceptar confirmaciones de nuevas transacciones manipuladas, pueden hacerse pagos entre usuarios, con el control de más de la mitad de la red pueden revertir transacciones y hasta podrán hacer gastar el doble de lo requerido (Stanislav, 2019, p. 30).

También amerita hacer énfasis en técnicas de hacking regulares para sistemas informáticos que hoy en día se encuentran presentes en el día a día de los usuarios de internet, como lo es el phishing, este es un ataque donde obtiene las credenciales de los usuarios, lo logran cuando el atacante manda correo a usuarios que sean propietarios de billeteras digitales, estos correos contienen enlaces falsos, donde el usuario si entra, el atacante puede tener acceso a sus claves tanto como pública y privada (McAfee, 2018, p. 6).

Un tema importante que se toma en este proyecto es la seguridad, pues, es el tema principal en que esta tecnología destaca. Blockchain es una solución segura, pues lo demuestra en Bitcoin hasta el momento, que no ha presentado ningún problema de seguridad importante que pueda poner en peligro la red. La seguridad de una blockchain se basa en lo siguiente: Permite tener historiales de transacciones con la seguridad de que no se pueden cambiar ni eliminar, también

la firma digital de cada transacción que garantiza la autoría de la transacción, facilitando la identificación del remitente ya se puede asociar su firma a cada transacción que hace, y todos los nodos tienen su propia copia de la red blockchain, cualquier modificación al bloque se puede detectar fácilmente, simplemente comparando el bloque o la transacción sospechosa con la copia en cualquier otro nodo de la red (Romero, 2018, p. 25).

Para garantizar la confidencialidad, las claves públicas permanecerán anónimas, las personas podrán ver el dinero que se transfiere de un lugar a otro sin tener que saber quiénes están involucrados en esas transferencias. Además, se genera un nuevo par de claves para cada transmisión. El punto es que al asociar a una persona con su clave pública puedes encontrar otras transacciones pertenecientes a ese usuario (Nakamoto, 2008, p. 6).

Otra definición que se tomara en cuenta es el Rendimiento, este es relativo, una forma fiable de medir el rendimiento de un equipo es por el tiempo de ida y vuelta, para realizar estas pruebas se debe cargar el programa y comparar los tiempos de ida y vuelta con un computador similar, de esta manera se identificará si el equipo es óptimo (Universidad Europe de Madrid, 2016, p. 11).

También se tomó en cuenta el tiempo de ida y vuelta (TIV), es el tiempo transcurrido desde que la información parte del emisor hasta que el receptor haya recibido la confirmación, determina la velocidad, también es un indicador clave para la red, ya que si ocurre algún cambio dentro del tiempo de ida y vuelta puede significar que puede haber ataques hacia la red (Kim, 2022, p. 1).

Por otro lado, se tomó en cuenta los Recursos, es un punto importante de evaluar, ya que se encarga de dar funcionalidad a la cadena de bloques, en este punto se observa el uso de la memoria, puesto que la cadena de bloques cuando ejecuta transacciones y se cambia el estado de la EVM, esto se mantiene ejecutado junto a las transacciones pendientes, es un punto importante de evaluar, ya que se encarga de dar funcionalidad a la cadena de bloques (Sekiya, 2021, p. 6).

También se tomó en cuenta la Eficacia, que es la capacidad de lograr las metas u objetivos dentro del tiempo establecido, también cuando se cumple el objetivo con el menor recurso posible (Fernandez, 2018, p. 36).

Por otro lado, se tomó en cuenta que la privacidad es un derecho fundamental que ayuda a construir confianza entre los usuarios y los servicios en línea. Es un derecho importante que facilita la autonomía personal, la dignidad y la libertad de expresión. Aunque no existe una definición aceptada de la privacidad en el contexto de Internet, se acuerda generalmente que la privacidad es el derecho de controlar cuándo, cómo y en qué medida los datos personales pueden ser compartidos con terceros. (Aguilar, 2021, p. 320).

Dentro de la blockchain se generan muchos registros de las transacciones y de esto Christensson (2014) nos dice que los registros son áreas de almacenamiento temporal integradas en la CPU. Algunos registros se usan internamente y no se puede acceder a ellos fuera del procesador, mientras que otros son accesibles para el usuario. La mayoría de las arquitecturas de CPU modernas contienen ambos tipos de registros(párr. 1).

Las transacciones se tratan de un intercambio de información entre dos entes, en este caso entre dispositivos específicamente, de modo que exista la comprensión y la efectiva comunicación entre las dos partes para recibir y enviar la información correspondiente (Solomon, 2003, p. 17). En este punto relacionado con la blockchain la cadena de bloques puede registrar transacciones entre múltiples partes, esto proporciona configuraciones de red flexibles, y reduce el riesgo de fallas en la red (Zha, 2019, p. 18).

La integridad, valida que la información está completa y correcta, eso quiere decir que no está alterado o modificado. Un dato puede ser íntegro por no auténtico: Se puede diseñar una situación en la que se compruebe la integridad de la información utilizando la función CRC (Comprobación de Redundancia Cíclica), en ese caso, podría alterarse la información (corrigiendo un error detectado, por ejemplo), re-calcular el CRC y presentar ese nuevo conjunto, que parecería íntegro, pero ha perdido la autenticidad (Lopez, 2012, p. 205).

Sobre la el control de acceso, Pérez (2018), nos comenta que, para administrar el control de acceso, se implementa un programa que sirve prevención ante la seguridad física, así mismo se necesita crear una base de datos con la

información del grupo de individuos con su respectivo nivel de acceso para ingresar a determinadas áreas (p. 12).

También se tomarán en cuentas las nuevas tecnologías, ya que desde sus inicios han demostrado ser muy útiles en varios ámbitos como por ejemplo económicos y sociales, y con el pasar del tiempo se van consolidando y mejorando a la vez de que se desarrollan nuevas tecnologías (Pinzon, 2017, p. 2), esto ayuda a mejorar los servicios, y, por lo tanto, demuestra la importancia de que las empresas se sometan a esta transformación digital y se adapten a este nuevo entorno con el fin de obtener todos los beneficios derivados de las nuevas tecnologías propuestas.

Otro punto a tomar en cuenta es la exposición de la información, se define como un incidente que ocasiona que una persona no autorizada tenga en su poder información o datos confidenciales de una organización, estos solo deberían estar disponibles para integrantes de la misma (Bortnik, 2010, p. 1), un hecho sonado en el mundo con respecto a la exposición de información fue en el 2010 con Wikileaks, que sufrió una gran exposición o fuga de información. Esto hizo ver lo difícil que es mantener la confidencialidad de la información, esto deja ver que grandes empresas con herramientas robustas y personal especializado han sufrido casos de exposición o fuga de información (Amaya, 2015, p. 1).

La corrupción de la información se refiere a los errores de la información que ocurren durante la escritura, almacenamiento, transmisión o procesamiento, que realiza cambios en los datos originales. Existen tipos de Malware que pueden dañar archivos intencionalmente. Cuando los archivos sufren este daño o alteración de la información, estos datos producen resultados inesperados en el sistema o la aplicación que acceda a ellos, ya que los resultados pueden variar (Molina, 2022, p. 8).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Para el desarrollo de esta investigación se contó con un análisis comparativo de 2 Blockchains, no existe un pre-test ni post-test, sino que se comparan los resultados obtenidos de parte de la interacción de los dispositivos IoT con ambas tecnologías blockchain a estudiar y de esta manera poder determinar que tecnología blockchain es la que tiene un mejor rendimiento y un nivel alto de seguridad.

La presente investigación es de enfoque cuantitativo, como respaldo al uso de este enfoque se tiene a Hernandez (2014, p.10), que dice sobre esto que es secuencial y probatorio y cada paso precede al siguiente sin poder "saltar" o evitar pasos. El orden es estricto, aunque por supuesto se puede anular una etapa. Parte de la idea va acotando, y después de definir los límites, se establecen los objetivos y las preguntas de investigación, se realiza una revisión de la literatura y se desarrolla un marco teórico. La problemática de la empresa ha sido poco estudiada según nuestra exploración entre las investigaciones que antes se han hecho respecto al tema. El presente estudio se está investigando desde una perspectiva que permita dar solución a la problemática de la empresa (con la tecnología blockchain), de una manera innovadora, ya que esta tecnología promete brindar soluciones que el IoT requiere hoy en día.

Así también, se contó con un diseño experimental, debido a que, en este estudio las variables fueron manipuladas con el objetivo de conocer cuál es la influencia que tiene una sobre otra. En este tipo de investigación, se manipulan una o más de las variables del estudio para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas.

Grupo	Tratamiento	Observaciones BC privada	Observaciones BC pública
G	X	C_1	C_2

$G = x(C_1C_2)$

Donde:

X: Comparación de las tecnologías Blockchain aplicadas al IoT
C_1: Blockchain privada - Rendimiento y seguridad
C_2: Blockchain pública - Rendimiento y seguridad

Figura N.º 5: Modo de aplicación de la investigación
Fuente: Elaboración propia

3.2. Variables y operacionalización:

La variable independiente es “Tecnología Blockchain aplicada al IoT”, ya que dentro del mundo de las empresas de tecnología existe un interés cada vez mayor en la adopción de esta tecnología para potenciar el internet de las cosas.

Tanto así que hasta empresas que se dedican a crear grandes sistemas informáticos que funcionan de manera centralizada como lo es IBM, ahora forma parte de esta gran adopción, pues en su último informe titulado “Device Democracy: Saving the Future of the Internet of Things”, esta empresa identifica el valor de la Tecnología BLOCKCHAIN, mencionando que al usar la tecnología Blockchain, se abren maneras de comerciar completamente nuevas debido a que cada dispositivo o nodo en la red podría funcionar como una micro-empresa autónoma, es decir que este podría prestar su servicio de capacidad de procesamiento o incluso hasta energía a un precio que no se podría conseguir en una red convencional con intermediarios. De esta variable salen dos dimensiones las cuales son Repartimiento, Registro de transacciones y cantidad de transacciones exitosas, de las cuales por la primera dimensión cuenta con dos indicadores como: Uso de protocolos de consenso ligeros y Uso de nuevas tecnologías, por la segunda dimensión cuenta con un indicador que es el Tiempo y por último la dimensión de Cantidad de transacciones exitosas contará con un indicador que será Cantidad de transacciones exitosas.

Por otro lado, la variable dependiente, es “Rendimiento y seguridad”, donde Jimenez (2017, p. 12) nos comenta que el rendimiento se encarga de monitorear el tiempo de ida y vuelta, acceso a datos[...], gestionando los recursos y los procesos

ineficientes. Es de esta manera que se midió el rendimiento de ambas blockchain y de esta variable se tendrán en cuenta 3 indicadores relacionados que serán: la latencia, se midió por el tiempo de ida y vuelta, los recursos, los cuales se midieron de acuerdo al porcentaje de la CPU que se necesita para realizar las transacciones y también la eficacia, la cual se midió mediante la cantidad de transacciones exitosas o fallidas. Por otro lado, la seguridad informática es la encargada de proteger el control de acceso a los datos, su integridad y su disponibilidad al momento que se requiera de estos mismos (Romero, 2018, p. 13). Es justamente en lo que IoT padece hoy en día según estadísticas de diversas fuentes como Gartner y otros estudios encontrados en esta investigación.

3.3. Población, Muestra, Muestreo, unidad de análisis

Según Arias (2016, párr.1) se entiende como población de un estudio o investigación, en general, se entienden todos los casos definidos, están adecuadamente limitados y disponibles, que suponen un modelo de referente para la muestra y tienen características predefinidas. Cabe señalar que cuando se refiere a la población de prueba, no solo se habla de humanos, sino que también se pueden tener en cuenta [dispositivos IoT], en el presente caso de estudio.

En el proyecto se tomó en cuenta como nuestra población los 3 dispositivos IoT. Todos estos fueron utilizados para medir los indicadores antes mencionados y que se aprecian de manera más clara en el cuadro de operacionalización de variables, GUIMARTBOT SAC.

Según Álvarez (2011, p. 122), la muestra es un conjunto de objetos o sujetos que proviene de una población; es decir es un subgrupo de la población, se define como un conjunto de elementos que cumple con determinadas especificaciones de una población se puede definir diferentes muestras.

El muestreo, como nos comenta Lui (2016, p. 1), es la técnica usada para poder definir, partir o agrupar la población en diferentes conjuntos (muestra), según Etikan (2015, p. 2) de este parte el muestreo probabilístico, donde se define como la probabilidad sin restricción de ser elegido en una muestra, es decir que cualquier objeto de la población que cumpla con los requisitos para ser muestreados.

Sin embargo, se hizo uso del muestreo no probabilístico por conveniencia que, según Manterola (2017, p. 2), permitirá seleccionar aquellos casos accesibles que acepten ser incluidos, esto fundamentado en la conveniente accesibilidad y proximidad de los sujetos para el investigador, que nos permite utilizar toda la población incluyendo los dispositivos, las blockchains y la computadora donde se ejecuta el proceso.

Se utilizó como unidad de análisis a cada uno de estos. Como lo define Gomez y Sena (2005, p. 5), esto se refiere a los objetos o sujetos de análisis, indica de quienes o quien se está hablando, respecto de quien o quienes se quiere construir conocimiento, también Lanzetta (2013), comenta que presenta un componente teórico como empírico. También debe existir coherencia con el problema de investigación, los objetos de investigación y el enfoque teórico.

3.4. Técnicas e instrumentos de recolección de datos

En este caso se hizo uso de 4 instrumentos de observación adaptados a cada blockchain e indicador medido, que se encuentran en el Anexo 10, Tamayo (2004, p.50), define el instrumento de observación como, un formato en el cual nos ayuda a recolectar los datos en sistemática y que se pueden registrar en forma uniforme, nos ayuda a obtener una revisión clara y objetiva de los hechos, agrupa la información según las necesidades específicas, se hace respondiendo a la estructura de las variables. Se utilizó este instrumento para medir el tiempo de ida y vuelta. En estos instrumentos se midió el tiempo que demora el comando en ir y volver de la blockchain, esto incluye, su trayectoria hacia el Smart Contract, su ejecución del Smart contract, la validación del comando por parte de la blockchain, la aplicación del consenso, y la respuesta que el Smart Contract regresa al front end. Por otra parte, se observa también la cantidad de transacciones exitosas y fallidas de los distintos dispositivos IoT (Led, Smart Light y Cerradura inteligente), con los diferentes tipos de blockchain (pública y privada), y, por último, la disponibilidad: Es con esta que se observa cuantas veces el usuario tiene acceso al estado del dispositivo.

3.5. Procedimientos

Para la recolección de los datos, primero se envió una carta de aceptación del proyecto a la empresa Guimartbot SAC, esta se observa en el Anexo 5. Después que la empresa aceptó el proyecto, se comienza con la recolección de datos, Primero se identificó que dispositivos IoT se iban a interactuar con ambas blockchain, en este caso será la cerradura, un led inteligentes y un Smart light, después se creó una red de prueba para la BC pública en Infura, luego se creó una blockchain privada de ethereum en una computadora, luego se buscó la forma de interactuar la tecnología IoT y ambas blockchain a través de Smart contracts para cada dispositivo, una vez ya realizado esto se comenzó a llenar los 4 instrumentos de observación, dos instrumentos de observación para medir el rendimiento de la blockchain pública y 2 para la privada, donde se observó el tiempo de ida y vuelta, el porcentaje de consumos de recursos de la CPU y también la eficacia de las transacciones donde dentro de esta última se vio las transacciones exitosas y las fallidas y al final también se midió la seguridad de ambas blockchain. Después del llenado de los instrumentos se pasó a analizar sus resultados para sacar el promedio y la media de cada resultado y así poder comparar ambas blockchain aplicadas al IoT, y poder demostrar que blockchain es la más recomendable para que pueda ser aplicada al IoT.

3.6. Método de análisis de datos

Para analizar los datos recaudados para el proyecto, se ha desarrollado una vista dentro del proyecto donde mostramos un análisis esquemático. Para la comparación del rendimiento entre la blockchain (BC) pública y la BC privada se usó un gráfico de líneas como se observa en la figura N.º 14, para el tiempo de ida y vuelta (TIV), se utilizaron dos gráficos de líneas (uno para la BC privada y otro para la BC pública), como se muestran en las figuras 12 y 13 respectivamente, por último se utilizó un gráfico de barras para mostrar el porcentaje de eficacia en el envío de transacciones comparando la BC pública con la BC privada. Luego se mostró con más detalle en la misma vista, más abajo, la comparación entre las dos BCs: el Tiempo de Ida y Vuelta de la información que va desde el front end hacia las BCs, el porcentaje de consumo de recursos que generan los procesos de ejecución necesarios para realizar el manejo de los dispositivos IoT haciendo uso

de las diferentes BCs, y la eficacia que estas dos BCs brindan al momento de brindar su servicio al IoT.

3.7. Aspectos éticos

Este proyecto se adhiere a la ética del investigador, basado en las normas que actualmente gobiernan en todo el mundo. Buscamos respetar todos los trabajos intelectuales que se pueden citar en este trabajo, haciendo una referencia correcta a los diferentes autores. Todas las fuentes de información se citarán de acuerdo con el manual ISO y la guía de la Universidad de César Vallejo para la escritura de investigaciones y tesis, así como con la RESOLUCIÓN DE LA JUNTA DE LA UNIVERSIDAD N.º 0101-2022/UCV que se ve en el Anexo 8, de esta forma se garantiza un trabajo de calidad, con información auténtica y veraz, para los futuros investigadores puedan leer esta investigación.

IV. RESULTADOS

Para esta parte se contrastará la información obtenida de los instrumentos de recolección de datos con los objetivos de la investigación.

Objetivo general: Identificar qué tecnología blockchain tiene el mejor rendimiento y seguridad al realizar el intercambio de información con el IoT en la empresa GUIMARTBOT SAC**.**

Figura N.º 6: Obteniendo el tiempo de ida y vuelta dentro de la BC privada
Fuente: Elaboración propia

Aquí se muestra como la BC privada está interactuando y se van creando cada bloque dentro de la BC privada, así mismo se muestra su respectivo tiempo de ida y vuelta (TIV), de esta manera obtuvimos que en el promedio del TIV es de 0.05 milisegundos por cada transacción realizada, de esta manera podemos determinar que cuenta con un menor tiempo de latencia.

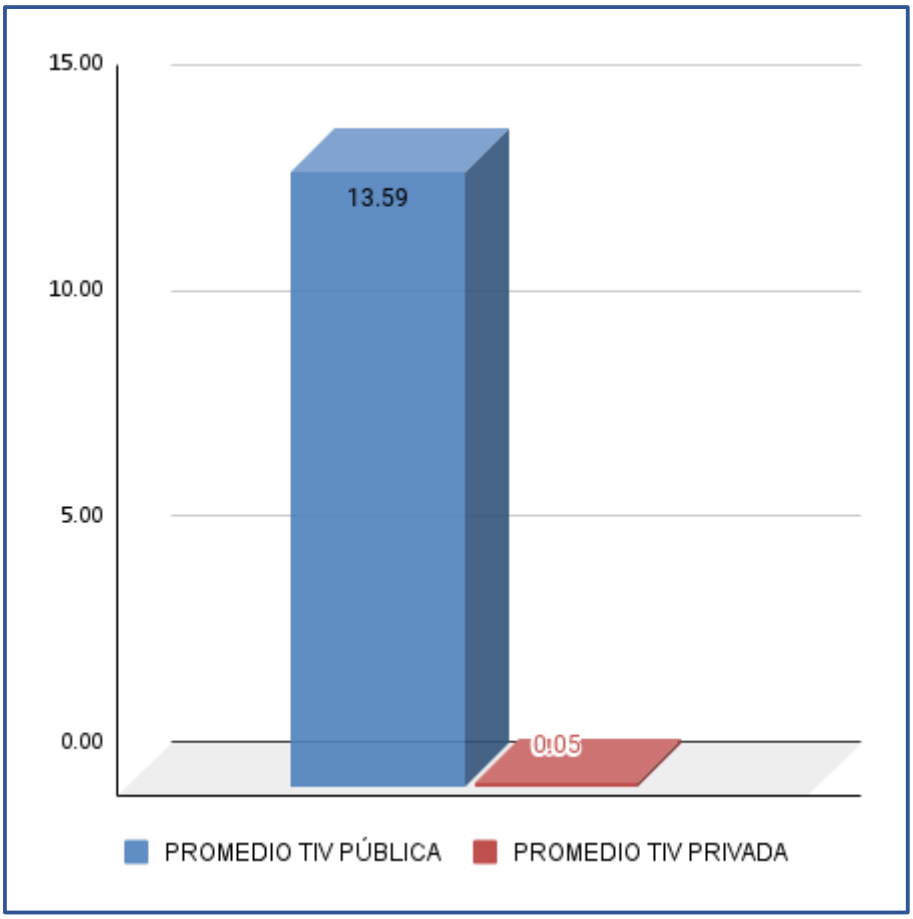


Figura N.º 7: Comparación – Promedio TIV (privada vs publica)
Fuente: Elaboración propia

Aquí se muestra el promedio de los resultados con respecto al tiempo de ida y vuelta (TIV), tanto cuando se realizaron las pruebas con la blockchain (BC) pública, como con la BC privada cuando interactúan con el dispositivo IoT “Smart Lock”, donde obtuvimos que el promedio del TIV es de 13.59 segundos por transacción realizada, de esta manera podemos determinar que la BC pública cuenta con un tiempo mayor en comparación con el BC privada.

Figura N.º 8: Vista general de los resultados en el front End
Fuente: Elaboración propia

Aquí se muestra como la Blockchain (BC) pública y privada interactúa con el dispositivo IoT en este caso es un “Smart Lock”, en nuestro front-end muestra su respectivo tiempo de ida y vuelta (TIV) de cada BC, también el porcentaje de recursos de la CPU que utiliza cada BC en las transacciones y la eficacia de cada transacción realizada, de esta manera con los datos recolectados podemos determinar que BC es la indicada para la interacción con la tecnología IoT.

```
Comando obtenido publicaclose
127.0.0.1 - - [03/Dec/2022 01:56:40] "GET /api/Public/smartLock/getState HTTP/1.1" 200 -
El porcentaje es:  30.1
################################################################
SignedTransaction(rawTransaction=HexBytes
('0xf8ce8201278459682f07827dde9476508615457cee3bb2ea93ae01bcf7c13ec16af980b864601d9256000000000000000
00000000000000000000000000000000000000000000002000000000000000000000000000000000000000000000000000000
000000000000046f70656e000000000000000000000000000000000000000000000000000000008401546d71a06cd0c65f158e3
da5f3cd20b49e5dae44c5f0660fbdd45d8116c99a411924eca8a03f44ef9f97ad008deb77e621da6e66413f9e639db459885e
61be2e3559e2c666'), hash=HexBytes
('0xaaf4ae5881be191f630918e61d8a5e8897f798bf8475127260839f02c579eea8'),
r=49218660945708344397558107626683553883373533378531392935314793109062158707880,
s=28617508881132440628529299894903517834735054682032445117808925635915154638438, v=22310257)
127.0.0.1 - - [03/Dec/2022 01:56:59] "POST /api/Public/smartLock/sendState/open HTTP/1.1" 200 -
Comando obtenido publicaopen
127.0.0.1 - - [03/Dec/2022 01:57:01] "GET /api/Public/smartLock/getState HTTP/1.1" 200 -
```

Figura N.º 9: Demostración de la encriptación de la información en la blockchain pública
Fuente: Elaboración propia

En la figura N.º 9 se muestra el nivel de seguridad de la blockchain (BC) pública interactuando con el dispositivo IoT “Smart Lock”, a través de la información encriptada que se envía hacia la BC pública. En la figura, se muestra el mensaje encriptado dentro de la BC pública, como también el Hash de la transacción realizada, la cuenta del contrato, la cuenta desde donde se envía la transacción y el porcentaje del recursos consumido de esa transacción realizada. De esa manera demostrando el alto nivel de seguridad de la informacion que se maneja en la ejecución de una transacción realizada para controlar un dispositivo de IoT.

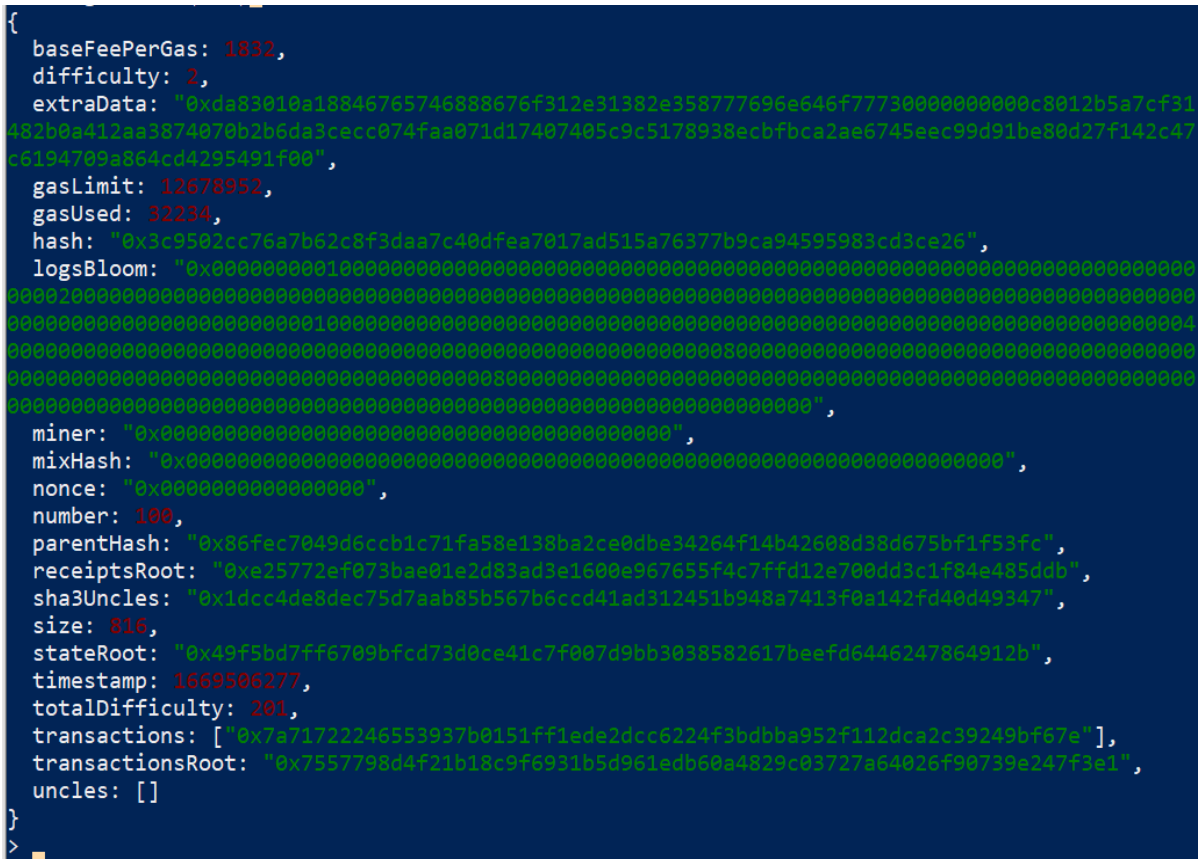


Figura N.º 10: Demostración de la encriptación de la información en la blockchain privada
Fuente: Elaboración propia

En la figura N.º 10 se muestra la información de la transacción de la blockchain (BC) privada cuando interactúa con el dispositivo IoT “Smart Lock”, dentro de la blockchain local de pruebas (GETH), en la misma, también está incluido el mensaje encriptado, demostrando el alto nivel de seguridad que brinda la BC privada basada en Ethereum, se muestra el se muestra en HASH del bloque anterior, como tambien el nuevo HASH, y el número del bloque.

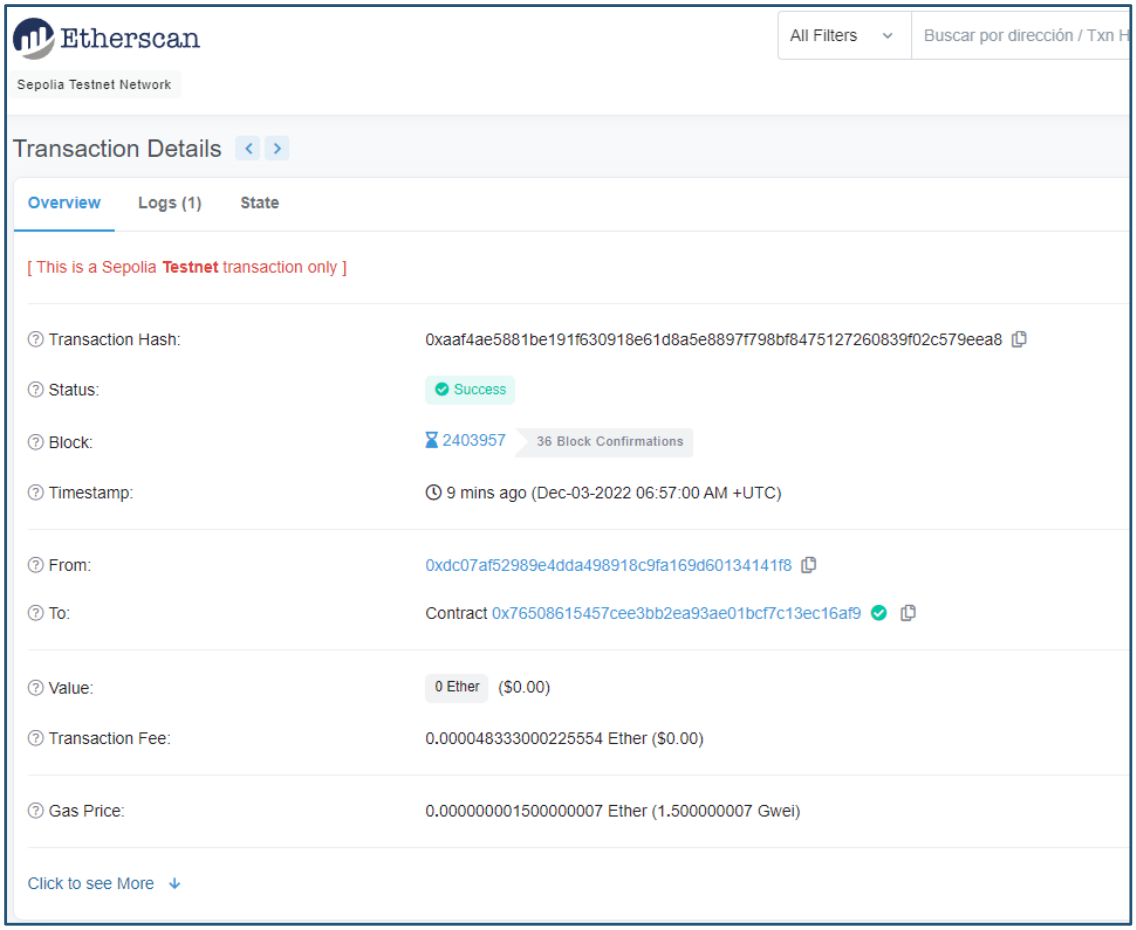


Figura N.º 11: Demostración de la disponibilidad de la BC pública
Fuente: Elaboración propia

Cada transacción realizada en la blockchain publica se guarda permanentemente en la misma, el usuario que tenga la llave privada del contrato inteligente que se maneja dentro de la BC tiene acceso en todo momento a la informacion que el Smart Contract maneje. En el caso de la presente investigación, cuando se aplicaron los instrumentos de recolección de datos a las transacciones realizadas para manejar el dispositivo “Cerradura o SmartLock”, se observó que siempre se logró acceder a dicha informacion dentro del contrato, lo que se obtenía era el estado la cerradura (Bloqueada o Desbloqueada), ello demostrando un nivel de disponibilidad de la informacion alto.

Los resultados obtenidos indican que la tecnología BC privada tiene un mejor desempeño respecto al tiempo que le toma al comando ir y regresar de la red BC, con respecto a al porcentaje de recursos que consumen, determinamos que la BC privada consume menos recursos que la BC pública, por el lado de la eficacia, ambas BC fueron 100% eficaces en las transacciones realizadas, en el nivel de seguridad ambas blockchain presentan un nivel de seguridad alto, ya que ambas cuenta con las mismas características como la encriptación y el uso de las claves públicas y privadas, con respectos la disponibilidad de la información observamos que cada vez que llamamos al contrato inteligente para que nos brinde el último estado del dispositivo, esté siempre respondió inmediatamente, por lo tanto, amabas blockchain muestran una disponibilidad de la información alta, así como también se puede decir que ambas blockchain pueden aplicarse a los dispositivos IoT; sin embargo, la privada brinda una mejor experiencia al usuario por su velocidad de respuesta (baja latencia).

Hipótesis general: Existen diferencias significativas respecto al rendimiento y seguridad entre la blockchain pública y la privada cuando son aplicadas a los dispositivos IoT en GUIMARTBOT SAC

Respecto a lo mencionado anteriormente se puede decir que la hipótesis general es correcta, existen diferencias significativas, ya que, en promedio, el TIV de la blockchain privada es más de 270 veces más rápido que la blockchain pública, debido a que el promedio del tiempo de ida y vuelta (TIV) en la BC privada es de 0.05 milisegundos, mientras que en la BC pública es de 13.59 segundos por cada transacción realizada aplicada al IoT. En el caso del porcentaje de consumo de recursos se demuestra que la BC privada consume menos recursos que la BC pública. Con respecto a la eficacia cuenta con un 100%, la interacción entre ambas tecnologías se ejecuta con normalidad, con respectos a la seguridad la blockchain pública y privada tiene un nivel de seguridad alto. Se concluye de esta manera que la BC privada cuenta con una diferencia significativa en comparación con la BC pública.

Objetivo específico 1: Identificar qué tipo de blockchain tiene un menor tiempo de ida y vuelta (TIV), durante el intercambio de información con el dispositivo IoT en la empresa GUIMARTBOT SAC

Los resultados obtenidos sobre el TIV se muestran en la siguiente tabla de resultados del tiempo de ida y vuelta de la blockchain **pública** de ethereum aplicado a un dispositivo IoT “Cerradura”.

Tabla N.º 3: *Resultados del tiempo de ida y vuelta (BC pública)*

__id__	blockchain_type	device	duration
0001	Public	SmartLock	16.877
0002	Public	SmartLock	33.183
0003	Public	SmartLock	18.142
0004	Public	SmartLock	24.891
0005	Public	SmartLock	17.544
0006	Public	SmartLock	24.584
0007	Public	SmartLock	10.612
0008	Public	SmartLock	4.274
0009	Public	SmartLock	7.275
0010	Public	SmartLock	4.902
0011	Public	SmartLock	8.099
0012	Public	SmartLock	17.726
0013	Public	SmartLock	8.230
0014	Public	SmartLock	20.868
0015	Public	SmartLock	6.291
0016	Public	SmartLock	9.267
0017	Public	SmartLock	19.764
0018	Public	SmartLock	22.326
0019	Public	SmartLock	21.764
0020	Public	SmartLock	12.085
0021	Public	SmartLock	21.298
0022	Public	SmartLock	20.834
0023	Public	SmartLock	13.439
0024	Public	SmartLock	7.742
0025	Public	SmartLock	24.771
0026	Public	SmartLock	8.677
0027	Public	SmartLock	22.670
0028	Public	SmartLock	8.579
0029	Public	SmartLock	7.913
0030	Public	SmartLock	8.797
0031	Public	SmartLock	27.862
0032	Public	SmartLock	12.784

Fuente: Elaboración propia

A continuación, se muestra la figura N.º 12, que representa al tiempo de ida y vuelta de la blockchain pública de Ethereum aplicado a un dispositivo IoT “Cerradura”.

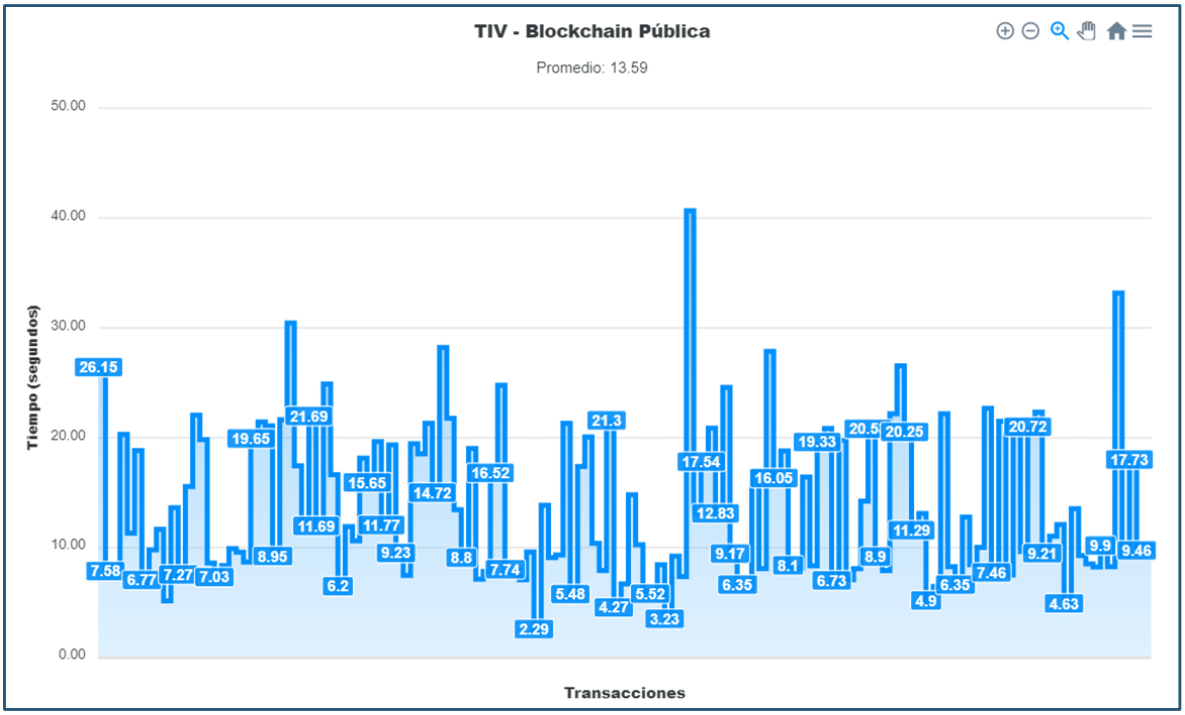


Figura N.º 12: Figura del TIV del dispositivo IoT con la BC pública
Fuente: Elaboración propia

Según lo observado en la tabla N.º 03 y en la figura N.º 12 conforme con los resultados obtenidos de transacciones realizadas a la blockchain pública de Ethereum aplicado al dispositivo IoT “Smart Lock”, donde se obtiene que el promedio del tiempo de ida y vuelta (TIV) de la BC pública es de 13.29 segundos por cada transacción realizada al ser aplicada al dispositivo IoT. Esto demuestra que el tiempo de ida y vuelta de la blockchain pública tiene un tiempo prudente dentro de la interacción con el dispositivo IoT.

Por otro lado, también se presentan los resultados del tiempo de ida y vuelta de la blockchain privada de ethereum aplicado a un dispositivo IoT “Cerradura”.

Tabla N.º 4: *Tiempo de ida y vuelta de la (BC privada)*

__id__	blockchain_type	device	duration
0001	Private	SmartLock	0.063
0002	Private	SmartLock	0.043
0003	Private	SmartLock	0.042
0004	Private	SmartLock	0.057
0005	Private	SmartLock	0.053
0006	Private	SmartLock	0.047
0007	Private	SmartLock	0.046
0008	Private	SmartLock	0.066
0009	Private	SmartLock	0.055
0010	Private	SmartLock	0.049
0011	Private	SmartLight	0.060
0012	Private	SmartLock	0.040
0013	Private	SmartLock	0.043
0014	Private	SmartLock	0.056
0015	Private	SmartLock	0.062
0016	Private	SmartLock	0.049
0017	Private	SmartLock	0.042
0018	Private	SmartLock	0.057
0019	Private	SmartLight	0.064
0020	Private	SmartLock	0.044
0021	Private	SmartLock	0.056
0022	Private	SmartLock	0.053
0023	Private	SmartLock	0.052
0024	Private	SmartLock	0.062
0025	Private	SmartLock	0.052
0026	Private	SmartLock	0.044
0027	Private	SmartLock	0.043
0028	Private	SmartLock	0.041
0029	Private	SmartLock	0.060
0030	Private	SmartLock	0.056
0031	Private	SmartLock	0.049
0032	Private	SmartLock	0.044

Fuente: Elaboración propia

A partir de estos resultados se realizó la figura N.º 13, que representa el porcentaje de los recursos utilizados por la blockchain privada de Ethereum aplicado a un dispositivo IoT “Cerradura” (en milisegundos).

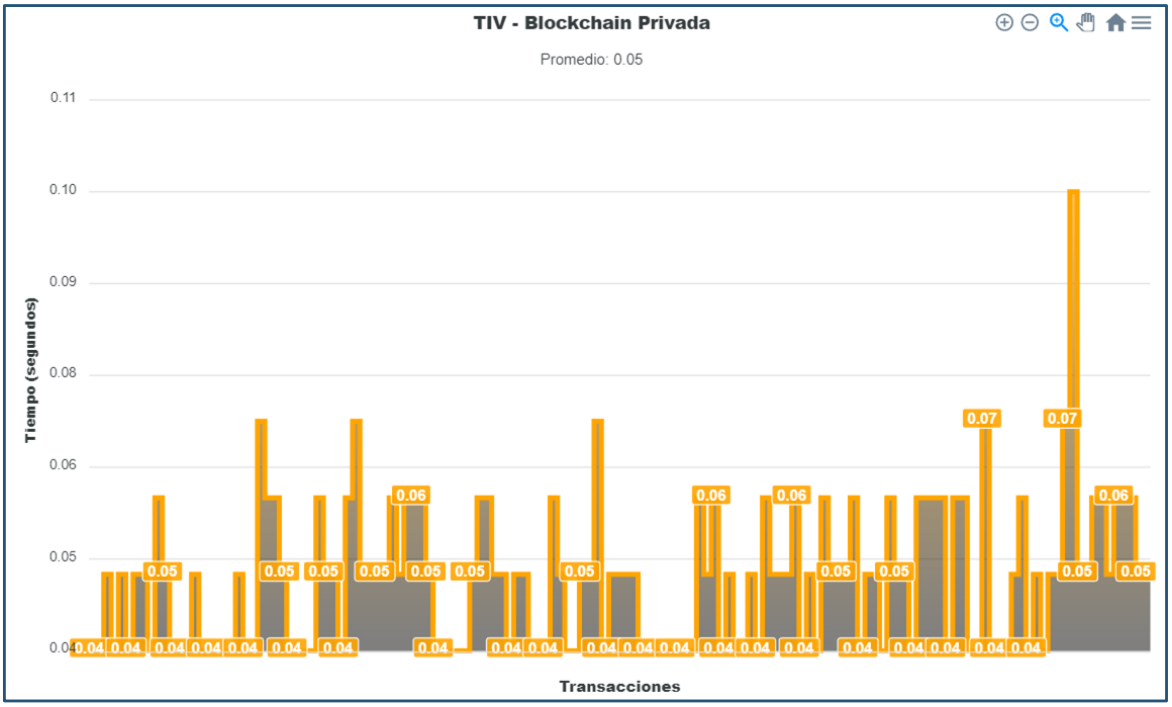


Figura N.º 13: Figura del TIV del dispositivo IoT con la BC privada
Fuente: Elaboración propia

Según lo observado en la tabla N.º 4 y en la figura N.º 13 los resultados obtenidos por las transacciones realizadas en la blockchain privada aplicado al dispositivo IoT “Cerradura”, determinamos que el promedio del tiempo de ida y vuelta (TIV) es de 0.05 milisegundos por transacción realizada en la blockchain.

En este caso, de acuerdo a lo observado en los resultados, vemos que el promedio del TIV con respectos a la blockchain Pública basada en Ethereum es de 13.59 segundos por transacción realizada aplicada al dispositivo IoT, este tiempo puede variar según la máquina donde se esté ejecutando, por el lado de la blockchain privada basada en Ethereum aplicado a dispositivo IoT, determinamos que el promedio del tiempo de ida y vuelta es de 0.05 milisegundos por cada transacción realizada. De esta manera determinamos que la BC privada es más de 270 veces más rápida que la BC pública, de esta manera concluimos que la BC privada tiene un menor TIV.

Hipótesis Específica 1: La tecnología blockchain pública y privada tienen diferencias significativas en la latencia en relación al TIV durante el intercambio de información con los dispositivos IoT de la empresa GUIMARTBOT SAC.

Respecto a la hipótesis específica según los resultados mostrados, decimos que la hipótesis específica 1 es aceptada, ya que el promedio del tiempo de ida y vuelta (TIV) de la blockchain pública basada en Ethereum es 13.59 segundos por transacción realizada aplicada a los dispositivos IoT, por otro lado, la blockchain privada basada en Ethereum el promedio del TIV es de 0.05 milisegundos por transacción realizada, dicho esto si existen diferencias significativas entre ambas blockchain, ya que la blockchain privada es 271.8 veces más rápida que la BC pública.

Objetivo específico 2: Identificar qué tipo de blockchain consume menos recursos durante el intercambio de información con el dispositivo IoT de la empresa GUIMARTBOT SAC.

Los resultados del rendimiento relacionado con los recursos (BC privada vs. Pública) obtenidos fueron los siguientes:

Tabla de resultados del porcentaje de los recursos utilizados por la blockchain privada de Ethereum aplicado a un dispositivo IoT “Smart Lock”.

Tabla N.º 5: *Resultados del rendimiento relacionado al consumo de recursos (BC privada)*

__id__	blockchain_type	device	pcr	__id__	blockchain_type	device	pcr
0001	Private	SmartLock	20.9%	0001	Public	SmartLock	28.9%
0002	Private	SmartLock	35.6%	0002	Public	SmartLock	29.5%
0003	Private	SmartLock	24.6%	0003	Public	SmartLock	47.4%
0004	Private	SmartLock	33.1%	0004	Public	SmartLock	55.6%
0005	Private	SmartLock	39.7%	0005	Public	SmartLock	28.7%
0006	Private	SmartLock	45.7%	0006	Public	SmartLock	23.7%
0007	Private	SmartLock	29.3%	0007	Public	SmartLock	25.8%
0008	Private	SmartLock	27.7%	0008	Public	SmartLock	30.8%
0009	Private	SmartLock	25.6%	0009	Public	SmartLock	24.4%
0010	Private	SmartLock	44.6%	0010	Public	SmartLock	29.5%
0011	Private	SmartLight	52.7%	0011	Public	SmartLock	26.5%
0012	Private	SmartLock	18.7%	0012	Public	SmartLock	24.0%
0013	Private	SmartLock	22.4%	0013	Public	SmartLock	28.2%
0014	Private	SmartLock	27.4%	0014	Public	SmartLock	22.1%
0015	Private	SmartLock	18.0%	0015	Public	SmartLock	32.1%
0016	Private	SmartLock	21.2%	0016	Public	SmartLock	29.7%
0017	Private	SmartLock	9.0%	0017	Public	SmartLock	28.0%
0018	Private	SmartLock	16.7%	0018	Public	SmartLock	27.5%
0019	Private	SmartLight	40.3%	0019	Public	SmartLock	30.6%
0020	Private	SmartLock	17.0%	0020	Public	SmartLock	36.7%
0021	Private	SmartLock	24.8%	0021	Public	SmartLock	28.5%
0022	Private	SmartLock	30.6%	0022	Public	SmartLock	27.6%
0023	Private	SmartLock	30.5%	0023	Public	SmartLock	33.8%
0024	Private	SmartLock	22.2%	0024	Public	SmartLock	29.3%
0025	Private	SmartLock	36.9%	0025	Public	SmartLock	38.9%
0026	Private	SmartLock	22.7%	0026	Public	SmartLock	26.3%
0027	Private	SmartLock	26.2%	0027	Public	SmartLock	26.1%
0028	Private	SmartLock	24.8%	0028	Public	SmartLock	18.6%
0029	Private	SmartLock	30.9%	0029	Public	SmartLock	24.6%
0030	Private	SmartLock	22.3%	0030	Public	SmartLock	22.4%
0031	Private	SmartLock	23.8%	0031	Public	SmartLock	25.6%

Fuente: Elaboración propia

A continuación, se presenta la figura N.º14 con los resultados del porcentaje de los recursos utilizados por la blockchain privada y pública de Ethereum aplicado a un dispositivo IoT (Cerradura).

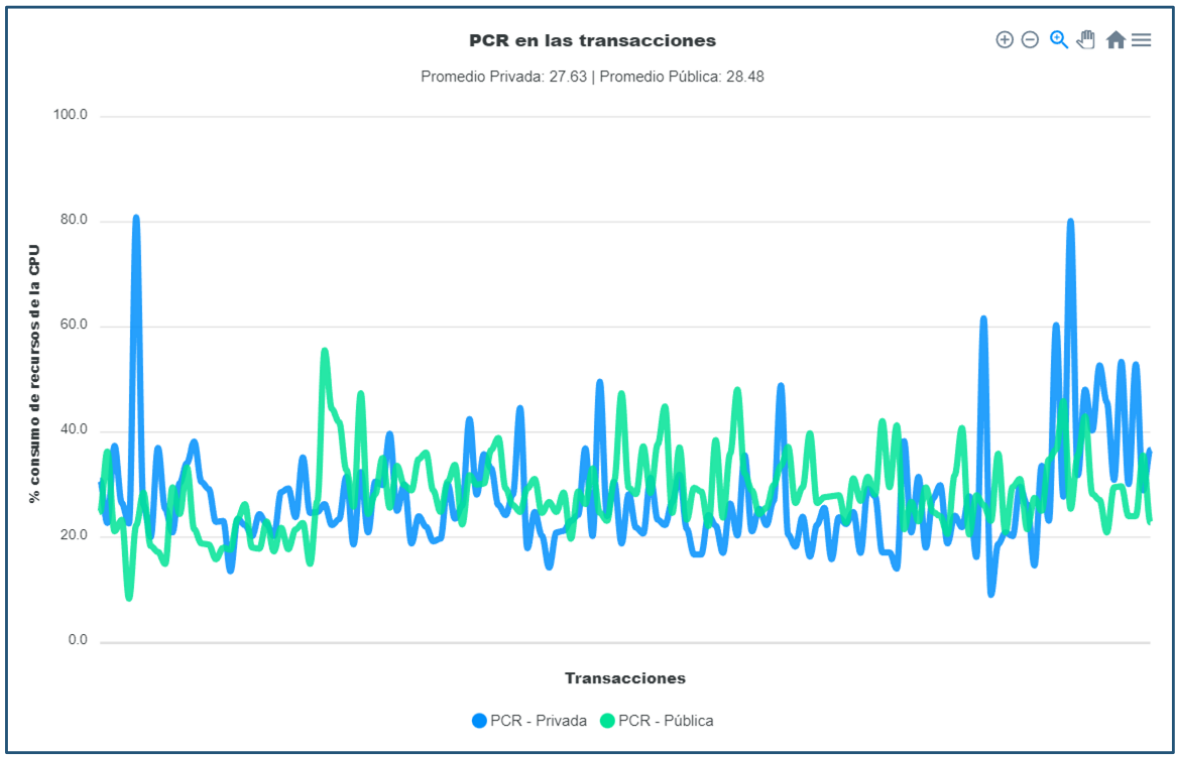


Figura N.º 14: Figura de los recursos utilizados del dispositivo IoT con la BC privada vs BC pública
Fuente: Elaboración propia

Según lo observado en la tabla N.º 5 y en la figura N.º 14 conforme con los resultados obtenidos de 146 transacciones realizadas por cada Blockchain (BC) de Ethereum (292 en total), aplicada al dispositivo IoT (Cerradura), donde se muestra el promedio del porcentaje del uso de la CPU en la BC pública es de 28.48% y el de la BC privada de 27.63% al realizar las transacciones. Visualizando un gráfico muy inestable con la BC privada, mientras que con la pública la computadora donde se realizaron las pruebas se mantuvo más estable. Esto demuestra que el porcentaje de uso de la CPU dentro de la blockchain pública y privada no se diferencian por mucho, pero la BC privada si genera inestabilidad en la misma durante la interacción con el dispositivo IoT.

Hipótesis específica 2: Existen diferencias significativas entre la tecnología blockchain pública y privada respecto a su rendimiento en relación al consumo de recursos al aplicarse al IoT en la empresa GUIMARTBOT SAC.

Respecto esta hipótesis específica según los resultados mostrados, decimos que la hipótesis específica 2 es nula, ya que el promedio del porcentaje que consume de la CPU la BC privada es de 27.63% por cada transacción al aplicarse con el dispositivo IoT, por otro lado, el promedio del porcentaje que consume de la CPU la BC pública es de 28.48% por cada transacción al aplicarse con el dispositivo IoT, de esta manera determinamos que no existen diferencias significativas entre ambas BCs.

Objetivo específico 3: Determinar qué tecnología blockchain es la más eficaz para permitir la comunicación con los dispositivos IoT en la empresa GUIMARTBOT SAC.

Como resultados del rendimiento relacionado con la eficacia en la BC pública se obtuvo la siguiente tabla donde se ha aplicado a un dispositivo IoT (Cerradura).

Tabla N.º 6: *Resultados del rendimiento relacionado a la eficacia (BC pública)*

N.º TRANSACCIÓN	Nombre	Eficacia BC pública	
		Eficaz	No eficaz
1	Cerradura	x	
2	Cerradura	x	
3	Cerradura	x	
4	Cerradura	x	
5	Cerradura	x	
6	Cerradura	x	
7	Cerradura	x	
.	.	.	.
.	.	.	.
.	.	.	.
146	Cerradura	x	

Fuente: Elaboración propia

En esta tabla N.º 6 se muestra los resultados enfocados en la eficacia en el momento que se realiza una transacción aplicada a un dispositivo IoT con la

blockchain pública de Ethereum, como se muestra todas las transacciones fueron eficaces de esta manera determinamos que es 100% eficaz.

Tabla de resultados relacionada con la eficacia de la blockchain privada de Ethereum aplicado a un dispositivo IoT (Cerradura).

Tabla N.º 7: *Resultados del rendimiento relacionado a la eficacia (BC privada)*

N.º TRANSACCIÓN	Nombre	Eficacia BC privada	
		Eficaz	No eficaz
1	Cerradura	x	
2	Cerradura	x	
3	Cerradura	x	
4	Cerradura	x	
5	Cerradura	x	
6	Cerradura	x	
7	Cerradura	x	
.	.	.	.
.	.	.	.
.	.	.	.
146	Cerradura	x	

Fuente: Elaboración propia

En esta tabla N.º 7 se muestra los resultados obtenidos del instrumento de recolección de datos respecto a la eficacia en el momento que se realiza una transacciones aplicadas a un dispositivo IoT con la blockchain (BC) privada de Ethereum, como se muestra en esta misma, todas las transacciones fueron eficaces y de esta manera determinamos que es 100% eficaz.

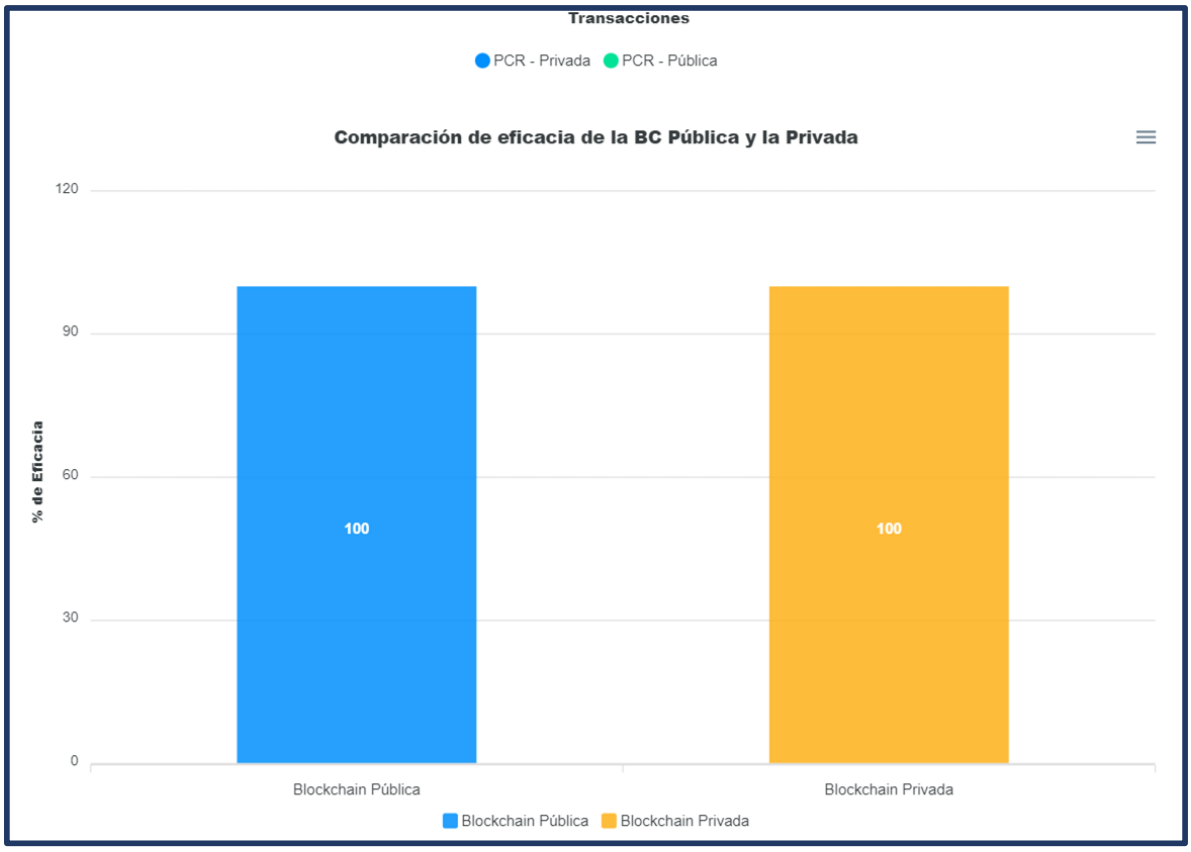


Figura N.º 15: Porcentaje de eficacia de las blockchains basadas en Ethereum

Como se muestra en la tabla N.º 6 y 7, son los resultados obtenidos sobre el rendimiento enfocado en la eficacia, estos resultados son obtenidos cuando se realizan transacciones aplicadas al dispositivo IoT con la blockchain privada de Ethereum, como se muestra a todas las transacciones fueron realizadas exitosamente, esto quiere decir que la eficacia con la BC privada es del 100% eficaz.

En este caso, de acuerdo a lo recaudado por los instrumentos de observación se muestra que la blockchain pública de Ethereum aplicada a los dispositivos IoT, todas las transacciones fueron exitosas, tanto en la BC pública como en la privada, de esta manera se determina que ambas blockchain son eficaces para que se pueda aplicar al IoT.

Hipótesis Específica 3: La tecnología blockchain pública y privada tienen diferencias significativas en rendimiento en relación a la eficacia al aplicarse al IoT en la empresa GUIMARTBOT SAC.

Respecto a la hipótesis específica según los resultados mostrados, decimos que la hipótesis específica 3 es aceptada, ya que la blockchain privada de ethereum aplicada a los dispositivos IoT fueron exitosas, de esta manera la hipótesis específica 3 es aceptada.

Objetivo específico 4: Determinar qué tecnología blockchain mejora el nivel de seguridad de la información manejada en los dispositivos IoT en la empresa GUIMARTBOT SAC.

En la figura N.º 16 se muestra el nivel de seguridad brindada por las BCs basadas en ethereum aplicadas a los dispositivos IoT. Donde se muestra que el nivel de seguridad en alto, por la manera en la que el mensaje es protegido en el transcurso de su camino hacia y desde la BC, con un método de encriptación llamado SHA3, de esa manera ayudando a que la información recibida por el dispositivo IoT sea segura y privada.

Tabla N.º 8: *Resultados del nivel de seguridad y disponibilidad (BC pública)*

Instrumento #3: Observación de la seguridad de la Blockchain Pública			
Ficha de Registro			
Tipo de Prueba	Obserbación		
Lugar	Guimartbot SAC		
Motivo de Investigación	Demostrar la seguridad de la blockchain pública		
Investigadores	Farfan Rosales, Handerson; Lopez Cordova, Rafael		
Fecha de Inicio:		Fecha de Fin	

Variable	Indicadores	Medida	Blockchain
Seguridad	Nivel de seguridad	Ordinal	Pública
	Disponibilidad	Ordinal	

		Dispositivo	Seguridad	Disponibilidad	
# TRANSACCIÓN	Fecha	Nombre	Nivel de seguridad	Nivel de disponibilidad	
				Exitoso	Fallido
1	19/11/2022	Cerradura	Alto	X	
2	19/11/2022	Cerradura	Alto	X	
3	19/11/2022	Cerradura	Alto	X	
4	19/11/2022	Cerradura	Alto	X	
5	19/11/2022	Cerradura	Alto	X	
6	19/11/2022	Cerradura	Alto	X	
7	19/11/2022	Cerradura	Alto	X	
8	19/11/2022	Cerradura	Alto	X	
9	19/11/2022	Cerradura	Alto	X	
10	19/11/2022	Cerradura	Alto	X	
11	19/11/2022	Cerradura	Alto	X	
12	19/11/2022	Cerradura	Alto	X	
13	19/11/2022	Cerradura	Alto	X	
14	19/11/2022	Cerradura	Alto	X	
15	19/11/2022	Cerradura	Alto	X	

Fuente: Elaboración propia

Como se muestra en la tabla N.º 8, se demuestra el nivel de seguridad cada vez que se realizaron las transacciones dentro de la Blockchain publica basada en Ethereum, como se muestra el nivel de seguridad que brinda es alto.

Tabla N.º 9: *Resultados del nivel de seguridad y disponibilidad (BC privada)*

Variable	Indicadores		Medida	Blockchain	
Seguridad	Nivel de seguridad		Ordinal	Privada	
	Disponibilidad		Ordinal		
		Dispositivo	Seguridad	Disponibilidad	
# TRANSACCIÓN	Fecha	Nombre	Nivel de seguridad	Nivel de disponibilidad	
				Exitoso	Fallido
1	19/10/2022	Cerradura	Alto	x	
2	19/10/2022	Cerradura	Alto	x	
3	19/10/2022	Cerradura	Alto	x	
4	19/10/2022	Cerradura	Alto	x	
5	19/10/2022	Cerradura	Alto	x	
6	19/10/2022	Cerradura	Alto	x	
7	19/10/2022	Cerradura	Alto	x	
8	19/10/2022	Cerradura	Alto	x	
9	19/10/2022	Cerradura	Alto	x	
10	19/10/2022	Cerradura	Alto	x	
11	19/10/2022	Cerradura	Alto	x	
12	19/10/2022	Cerradura	Alto	x	
13	19/10/2022	Cerradura	Alto	x	
14	19/10/2022	Cerradura	Alto	x	
15	19/10/2022	Cerradura	Alto	x	
16	19/10/2022	Cerradura	Alto	x	

Fuente: Elaboración propia

Como se muestra en la tabla N.º 9, se demuestra el nivel de seguridad cada vez que se realizaron las transacciones dentro de la Blockchain privada basada en Ethereum, como se muestra el nivel de seguridad que brinda es alto.

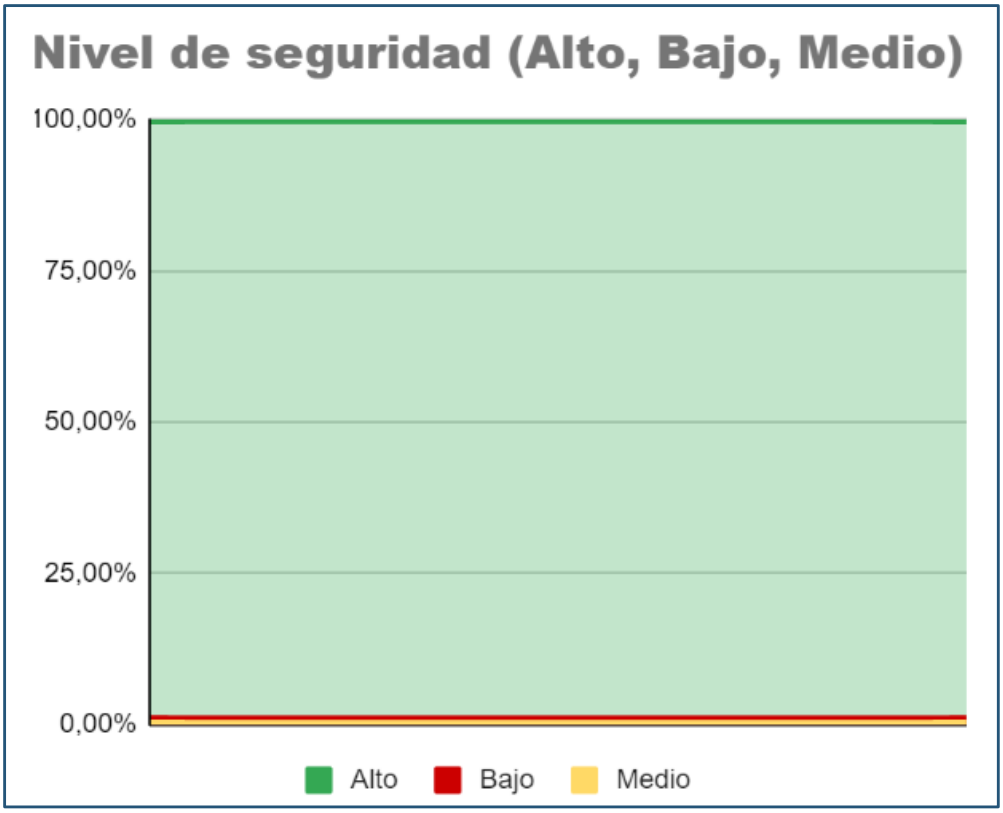


Figura N.º 16: Nivel de seguridad en ambas BCs, respecto a la encriptación de la información.
Fuente: Elaboración propia

En este gráfico se muestra el nivel de seguridad brindada por la blockchain privada de Ethereum aplicada a los dispositivos IoT, en este caso aplicada a la Cerradura (SmartLock), se muestra que el nivel de seguridad en alta a partir de datos extraídos de cada transacción realizada respecto al su encriptamiento de la información, gracias a que las características que presenta la blockchain como la encriptación, de esa manera ayuda que la información recibida por el dispositivo IoT sea seguro y privado.

En este caso, de acuerdo a lo recaudado se muestra que la blockchain pública de Ethereum aplicado a los dispositivos IoT, muestra que el nivel de seguridad de dicha blockchain es alto, en todas las transacciones si vio que el nivel de seguridad es alto, en la blockchain privada de Ethereum también se observó que en cada transacción realizada para las pruebas, el nivel de la seguridad también fue alta.

Hipótesis específica 4: La tecnología blockchain pública y privada tienen diferencias significativas en el nivel de seguridad al aplicarse al IoT en la empresa GUIMARTBOT SAC.

Según los resultados mostrados, decimos que la hipótesis específica es rechazada, como se muestra en las pruebas realizadas en la blockchain (BC) pública y privada, ambas tecnologías tuvieron un nivel de seguridad alta, por ambas tecnologías cuenta con las mismas características para brindar un nivel de seguridad alto, por esa razón la determinamos que no existen diferencias significativas entre ambas BC.

Objetivo específico 5: Identificar qué tipo de blockchain mejora la disponibilidad en la información en los dispositivos IoT de la empresa GUIMARTBOT SAC.

Por otra parte, también se demuestra que la información está siempre disponible para la API en cualquier momento que esta solicite acceso. Para manejar los dispositivos IoT se tiene acceso al estado de todos los dispositivos en todo momento.

Figura N.º 17: Disponibilidad de la información del estado del dispositivo en las BCs
Fuente: Elaboración propia

En este caso, de acuerdo a lo recaudado por los instrumentos de observación mostrados en las tablas N.º 8 y 9, con respecto a la blockchain pública de ethereum aplicada a los dispositivos IoT y de esta manera se observó que la información está disponible en todo momento, por el lado de la blockchain privada de Ethereum así como también por el lado de la BC pública.

Hipótesis específica 5: La tecnología blockchain pública y privada tiene diferencias significativas en la seguridad respecto a la disponibilidad de la información en los dispositivos IoT de la empresa GUIMARTBOT SAC.

Según los resultados mostrados, decimos que la hipótesis específica es rechazada, como se muestra en las pruebas realizadas, la blockchain pública de Ethereum aplicada a los dispositivos IoT, ya conectado por medio del front-end cada vez que se va a realizar alguna función hacia el dispositivo IoT, el front-end obtiene el último estado o envío realizado a la blockchain, de esta manera la disponibilidad de la información está visible en cada función que se realizó en el caso de ambas Blockchains.

V. DISCUSIÓN

Con respecto al objetivo general se determinó qué tecnología blockchain tiene el mejor rendimiento y seguridad con respecto a la tecnología BC pública, al realizar el intercambio de información con el IoT en la empresa GUIMARTBOT SAC. Según los resultados obtenidos, observamos que el tiempo promedio de la BC privada en ethereum es de 0.05 milisegundos, mientras que en la BC pública de Ethereum es de 13.59 segundos, es decir que la BC privada es unas 145.8 veces más rápida que la pública. Este trabajo se corroboran por los resultados de Delgado (2018), donde mide la latencia de una blockchain privada aplicada también al IoT a través de un simulador IoT basado en un chip Arduino ESP-32 que envía datos a la red Blockchain a través de una API REST, obtuvo como resultado que la latencia en promedio, de Hyperledger Fabric para concretar una transacción es de 2 segundos por cada una. La presente investigación, basada en la BC privada de Ethereum, realiza las mismas transacciones en promedio 40.8 veces más rápido. Así mismo, los resultados que muestra Conteron (2021) indica que la transacción se realiza en 0,4023 ms, esto debido a que cuenta con una computadora con mejores características (16 GB RAM, Core i7, y una tarjeta de video GTX 1050 4GB), teniendo en cuenta lo antes indicado, el resultado obtenido en este estudio es de 0.05 milisegundos, por cuál indicamos que tiene un tiempo de ida y vuelta parecido. De esta manera determinamos que la BC privada es la indicada para la integración con la tecnología IoT.

En lo que respecta al objetivo específico 1, se obtuvo que en promedio el TIV es de 17,403 ms. Este resultado se corrobora con los de Chen, Nguyen y Sekiya (2021) donde realizaron dos pruebas con diferentes nodos de una blockchain privada, y llegaron a obtener como resultados el tiempo de ida y vuelta (TIV) el tiempo de 149.53 milisegundos en el primer nodo y el tiempo de 71.23 milisegundos en el segundo nodo por cada una de las transacciones que realizaban dentro de su red de pruebas, comparando esto con los resultados obtenidos relacionados con el rendimiento respecto al tiempo de y vuelta (TIV), se puede determinar que existe una leve diferencia de (0.05 milisegundos) cuando comparamos sus resultados con los de las pruebas realizadas en este proyecto. Por otro lado, Zeña (2021) dentro de su trabajo que estaba enfocado en comparar los dos tipos de protocolos más

conocidos que utiliza la tecnología IoT los cuales son el MQTT (Message Queue Telemetry Transport), y COAP (Constrained Application Protocol), y así determinar cual tiene el menor tiempo de ida y vuelta (TIV), donde al analizar y comparar los resultados obtenidos, concluyó que el protocolo MQTT demora en promedio unos 22221,45 milisegundos por cada transacción que realiza, mientras que el protocolo COAP cuenta con un tiempo de demora de 7182,56 milisegundos por cada transacción realizada, de esta manera el concluye que el protocolo COAP tiene un mejor rendimiento con respecto al TIV. Cabe destacar que estos eran protocolos diseñados para los dispositivos IoT que no tienen que ver con ningún tipo de blockchain, comparándolos el TIV obtenido en los resultados del rendimiento de la BC Privada tiene un tiempo estimado de 0.05 milisegundos por cada transacción que se realiza, de esta manera corroboramos que nuestra BC privada basada en Ethereum presenta un mejor rendimiento. Resaltando así el alto rendimiento que una BC privada ofrece al momento de ser aplicada al IoT mediante el uso de Smart Contracts.

En lo que respecta al objetivo específico 2, gracias a los datos obtenidos observamos que el porcentaje promedio de los recursos utilizados de la CPU por la blockchain privada basada en Ethereum aplicado a los dispositivos IoT, es de 27.63 % al momento de realizar las transacciones. En contraste, Delgado (2018) en su investigación donde realizó dos pruebas para estudiar el rendimiento de la BC privada, está hecha en diferentes configuraciones de las máquinas virtuales, en la primera obtuvo como resultado que la blockchain privada de Hyperledger Fabric utilizó el 5% de los recursos de la CPU, de esta manera comparando la primera prueba con los resultados de la presente investigación, observamos que el uso de los recursos de nuestra blockchain privada es mayor, esto debido a que la configuración de la máquina virtual tiene características con más capacidad que la computadora utilizada en el trabajo, en la segunda prueba que realizó obtuvo como resultado que la blockchain privada de Hyperledger Fabric utilizó el 65% de los recursos de la CPU, en esta prueba realizó un cambió por una configuración más baja y de esta manera al comparar el rendimiento de la BC privada con respecto a los recursos que gasta, teniendo en cuenta lo mencionado anteriormente los resultados indican que la nuestra BC privada consume menos recursos, pero esto

siempre está relacionado con las características que puede tener la máquina que se utilizará para implementar la BC privada y los respectivos nodos de esta tecnología.

En lo que respecta al objetivo específico 3, se obtuvo como resultado que la BC privada basada en Ethereum al realizar las transacciones fue 100% eficaz, de esta manera comparando con los resultados obtenidos por Zeña (2021) con respecto en la eficacia, dentro de los resultados obtenidos en su investigación para ver la eficacia de los protocolos utilizados en la tecnología IoT, determinó que el protocolo COAP tuvo un 19.37% de transacciones fallidas al aplicarse al IoT, mientras que el protocolo MQTT tuvo un 28,12% de transacciones fallidas al ser puestos a prueba, comparando ambos protocolos determinamos que el protocolo COAP es más eficaz que el MQTT, de igual manera se observa que ambos protocolos cuentan con un 100% de eficacia. Teniendo en cuenta lo mencionado anteriormente, y comparando con los resultados obtenidos en este proyecto, esta BC privada basada en Ethereum fue un 100% eficaz al ejecutar cada una de las transacciones realizadas al ser puesta a prueba con el IoT, de esta manera se determina que la tecnología blockchain privada como también la pública frente a los protocolos del IoT tiene mejor eficacia en las transacciones realizadas. Por otro lado, corroborando los resultados y conclusiones de Castro (2021), él nos comenta que la tecnología blockchain es la más idónea para que se pueda aplicar a la tecnología IoT y así poder mitigar esas vulnerabilidades con las que cuenta esta última, también Conteron (2021) llegó a la conclusión que la tecnología blockchain se conecta de forma eficaz, haciendo referencia a una característica de la tecnología Blockchain donde la información no se pierde y, por otro lado, la confirmación del usuario es inmediata, también Oloya (2018) nos comenta que la interacción de ambas la tecnología BC y los dispositivos IoT, logra una optimización de los recursos para que puedan aprovechar las características únicas que ofrece blockchain, ya que se ha demostrado que es posible realizar funciones JSON-RPC utilizando un archivo JSON generado desde un sistema integrado para usar y registrar respuestas de manera similar. Realizar acciones con base a ella y utilizando un contrato inteligente, permitiendo la conexión de ambas tecnologías de una manera óptima, respaldando también los resultados.

En lo que respecta al objetivo específico 4. En las pruebas realizadas se observó que el nivel de seguridad es alto, ya que cuando interactuamos por medio de la BC privada, esta nos muestra los mensajes encriptados, de acuerdo a los resultados obtenidos por Sanchez (2020) en su investigación que tuvo como objetivo desarrollar una estructura que permita la detección y prevenir los ataques que pueda sufrir la red de IoT, obtuvo como resultados que efectivamente, la tecnología blockchain brindó una seguridad muy alta contra los ataques simulados dentro de su investigación, también siendo respaldada por Lecuit (2019) nos comenta que la tecnología blockchain utiliza mecanismos criptográficos de seguridad para acceder, firmar, encriptar transacciones y bloques. Las claves privadas se pueden vincular a identidades de usuario o elementos intermedios (p. 2). Por otra parte, Kim y Chandra (2020) afirman que la tecnología de Blockchain tiene el potencial de revolucionar muchas industrias proporcionando una transacción de usuario rápida y segura de extremo a extremo, sin la participación de cualquier confianza de terceros o autoridades centrales (p. v). De esta manera se corrobora que la tecnología blockchain brinda un nivel de seguridad alto gracias a las características con las que cuenta, donde destaca la encriptación de la información, sus protocolos de consenso que pone el nivel de seguridad dentro de la cadena de blockchain y también la inmutabilidad de la información con la que cuenta. Ante lo antes mencionado anteriormente determinamos que la BC privada basada en Ethereum nos da un nivel de seguridad alto.

En lo que respecta al objetivo específico 5. El resultado fue que ambos tipos de tecnologías Blockchain (BC) cuentan con un 100% de disponibilidad de la información que los dispositivos IoT o el usuario requiera en cualquier momento, siempre y cuando las blockchain se encuentren en funcionamiento al momento de recibir la consulta, como si de una base de datos se tratase, con la única diferencia que esta base de datos no sufrirá caídas como si lo hacen las bases de datos regulares, Piscini y Lory (2018) dicen que la disponibilidad de la información es una de las fortalezas de BC porque si un nodo deja de funcionar no sucede nada, pues existen muchos otros que cuentan con la misma información dentro de la red BC (p. 11). De esta manera la respuesta al usuario es inmediata y la información que se obtiene, permanecen de manera perpetua dentro de la red BC, en esta

investigación se guardó el estado del dispositivo en la BC y es este mismo el que se guarda y es visible a todo momento que sea requerido, por ejemplo: En la cerradura (SmartLock), se tienen estado de tipo bloqueado y desbloqueado, y es así como el usuario puede interactuar con el dispositivo, sabiendo cuál es su estado. Como sostén para lo antes mencionado Tapscoot (2017) nos comenta que la información digitalizada se puede subir a la blockchain y de esta manera la integridad y la disponibilidad de la información aumentará notablemente, y evitar pérdidas, mejorando el procesamiento de documentación (p. 142), de esta manera concluimos que la BC privada brindan una disponibilidad muy alta.

VI. CONCLUSIONES

En síntesis, gracias a los resultados obtenidos en la investigación presentamos las conclusiones:

Primera: La tecnología blockchain privada basada en Ethereum cuenta con un mejor rendimiento y un nivel de seguridad que la BC pública, ya que la BC privada es mucho más rápida en el rendimiento con respecto a al TIV, el consumo de recursos está dentro de lo normal y tiene una eficacia del 100%, con respecto a la seguridad ambas cuentan con seguridad alta. Se determinó que la BC privada es la indicada para poder integrar con la tecnología IoT, ya que la IoT necesita que su tiempo de conformidad sea lo más corto posible, esto quiere decir que el TIV tiene que ser el menor posible.

Segunda: La tecnología blockchain (BC) privada basada en Ethereum tiene un menor tiempo de latencia en relación con el tiempo de ida y vuelta (TIV) con respecto a una BC pública, debido a que al comparar ambos resultados, la BC privada por cada transacción realizada demora en promedio 0.05 milisegundos, mientras que la tecnología blockchain pública tiene un tiempo aproximado por cada transacción de 13.59 segundos.

Tercera: Con respecto al consumo de recursos de la CPU, se determinó que la tecnología blockchain (BC) privada basada en Ethereum consume menos recursos en comparación con la blockchain pública de Ethereum, esto puede variar debido a la máquina donde se realice, realizadas la pruebas obtuvimos que el consumo promedio de la BC privada es de 27.63%, mientras que la BC pública tiene un promedio de 28.48% del consumismo de recursos de la CPU. De esta manera, la BC privada consume menos recursos.

Cuarta: Con respecto a la eficacia, ambas tecnologías cuenta con una eficacia del 100%, ya que tanto la BC privada como la BC pública al realizar las transacciones todas fueron exitosas, de esta manera se determina que ambas blockchain son eficaces al aplicarse con la tecnología IoT, de esta

manera determinamos que la BC privada tiene un mejor rendimiento que la BC pública.

Quinta: Con respecto al nivel de seguridad, ambas tecnologías de blockchain de Ethereum cuentan con un nivel de seguridad alto, ambas tienen las mismas características como la encriptación, protocolos de consenso que hace que la dificultad de la cadena de bloques sea alta a la hora de poder encontrar el HASH, pero determinamos que la BC pública es la más segura, puesto que la BC pueden sufrir ataques, como el ataque del 51%, sobre este ataque la BC pública es más complicada que lo pueda sufrir, ya que cuenta con una red de nodos más grande (millones de nodos), en cambio, la blockchain privada es más limitada, por esta razón la BC es más segura.

VII. RECOMENDACIONES

Una vez que fueron prestadas las conclusiones finales, se hacen las recomendaciones para las investigaciones futuras relacionadas a Blockchain:

Primera: Se recomienda hacer uso de la tecnología blockchain en las empresas, debido a que en Latinoamérica son pocas las organizaciones que están interesadas en la implementación de esta, sin embargo, sería una buena opción para mejorar en gran medida la seguridad, de esta manera aumentar la confianza de los clientes y elimina el riesgo de que terceros puedan atacar.

Segunda: Se recomienda hacer uso de los Smart Contracts en diferentes áreas que se utilice los dispositivos IoT o la tecnología internet de las cosas industriales (IIoT), de esta manera se podrá optimizar los recursos, así como reducir los costos, brindando una mayor seguridad de la información con la seguridad que blockchain proporciona a estos mismos.

Tercera: Para obtener mejores resultados con la tecnología de blockchain aplicada a la IoT, se puede realizar pruebas con más tráfico en la red, ya que en este tipo de investigaciones se usa el Internet como un puente de conexión. También se puede probar con la otro tipo de tecnología blockchain híbrida, que combina las características de las tecnologías de blockchain públicas y privadas. Esto podría ser otra opción, tomando lo mejor de cada una de ellas, para ayudar a resolver los problemas de seguridad a los que se enfrenta el IoT.

Cuarta: Para futuras investigaciones, se propone que la investigación presente sea implementada o aplicadas a otras tecnologías como, por ejemplo, puede ser aplicado en el ámbito político frente al incremento de corrupción, varios especialistas muestran que la tecnología blockchain puede ser un importante para poder eliminar con esta tecnología la corrupción.

Quinta: Tomar en cuenta que esto también puede variar por las características de la computadora donde se esté corriendo la BC, el tiempo de ida y vuelta (TIV), el porcentaje de los recursos que consume, pueden varias por las características de la computadora, en este caso se utilizó una

computadora con las siguientes características 8 RAM, disco duro de 1 Terabytes, tarjeta de video GT 730, si se realiza en máquina de menos características el resultado con respecto a los indicadores mencionados será mayor, por el otro lado si se realizan las pruebas en una computadora con mejores características el resultado será menor.

REFERENCIAS

Acurio Conteron, Oswaldo David; SISTEMA DE SMART HOME APLICANDO IoT Y BLOCKCHAIN; Ecuador - Ambato; Universidad Técnica de Ambato. (2021);195 PP.

Alija, A. (2017). Descubriendo las claves de Blockchain. 14. https://datos.gob.es/sites/default/files/doc/file/descubriendo_las_claves_de_blockchain.pdf

Alvarez Rojas, Luis Rodrigo; análisis de la tecnología blockchain, su entorno y su impacto en modelos de negocios; Valparaíso - Chile; Universidad Técnica Federico Santa Maria; 2018; pp 94.

AMAYA, C. G. (2015 de 01 de 08). welivesecurity. Recuperado el 15 de 03 de 2016, de http://www.welivesecurity.com: http://www.welivesecurity.com/la-es/2015/01/08/10- anos-fuga-de-informacion.

Arduino (2015), Arduino Página Oficial, Disponible: http:/www.arduino.ccs

Argamon, S. E. (n.d.). Computational Register Analysis and Synthesis.

Arias-Gómez, J., Ángel Villasís-Keever, M., & Guadalupe Miranda-Novales, M. (2016). Metodología de la investigación. www.nietoeditores.com.mx ISSN: 0002-5151 DOI: https://doi.org/10.29262/ram.v63i2.181.

Arturo, C., Álvarez, M., Surcolombiana, U., De, F., Sociales, C., Humanas, Y., de Comunicación Social, P., Periodismo, Y., & Monje Álvarez, C. A. (2011). METODOLOGÍA DE LA INVESTIGACIÓN CUANTITATIVA Y CUALITATIVA Guía didáctica.

Barrio Andrés Moisés (2018); Internet de las Cosas ;Editorial Reus, 2018 Primera Edición ; 132 PP. ISBN:8429020381, 9788429020380.

Bashir Imran; Mastering Blockchain Second Edition Distributed ledger technology, decentralization, and smart contracts explained; segunda edición; India - Munbai; 2018; 647 PP. ISBN 978-1-78883-904-4.

Beltran Bejarano, Juan Carlos; Pineda Conejo, Andre Katerine; Quevedo Vega, Andres Felipe; ANÁLISIS DE LOS RIESGOS QUE CAUSAN LA FUGA DE INFORMACIÓN EN LA EMPRESA ASESORIAS CONTABLES Y REVISORÍA FISCAL JAA SAS. Bogotá - Colombia, Universidad Católica de Colombia [2016],59 pp.

BORTNIK, S. (13 de 04 de 2010). www.welivesecurity.com. Recuperado el 28 de 04 de 2016, de www.welivesecurity.com: http://www.welivesecurity.com/la-es/2010/04/13/que-es-lafuga-de-informacion/.

Carrasco Dias, S. (2019). Metodología de la Investigación científica. Lima - Perú: Editorial San Marcos.

Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción-acción). Julio 2020. https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173.

Christensson, Per. "Register Definition." TechTerms. Sharpened Productions, 30 January 2014. Web. 29 June 2022. <https://techterms.com/definition/register>.

Christidis, K., & DevetsikIoTis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. In IEEE Access (Vol. 4, pp. 2292–2303). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2016.2566339

DIAZ PINZON, Beatriz Helena et al. Contribución de las iniciativas de tecnologías de la información en las organizaciones: una revisión de la literatura. Innovar [online]. 2017, vol.27, n.66 [citado 2022-06-29], pp.41-55. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-50512017000400041&lng=es&nrm=iso. ISSN:0121-5051.https://doi.org/10.15446/innovar.v27n66.66710

Diccionario panhispánico de dudas. Ipso Facto [Internet]. Real Academia Española. Madrid: RAE; 2019 [citado el 20 de octubre de 20222]. P.1. Disponible en: Search | Real Academia Española (rae.es)

DING, S., CAO, J., LI, C., FAN, K. y LI, H., 2019. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access, vol. 7, pp. 38431-38441. ISSN 21693536. DOI 10.1109/ACCESS.2019.2905846.

Dioni Nespral, Roberto Fernández Hergueda (2021);Blockchain: El modelo descentralizado hacia la economía digital;Ediciones de la U, 2021;Primera edición; 324 PP. ISBN: 9587922832, 9789587922837.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (Part of CPS Week), 173–178. https://doi.org/10.1145/3054977.3055003.

Eterovic, J., Cipriano, M., & Torres, L. (n.d.). Seguridad en Internet de las Cosas usando soluciones Blockchain.

ETIKAN, Ilker. Comparision of Snowball Sampling and Sequential Sampling Technique [en línea]. ECOSMedCrave: Nicosia, 18 de Noviembre del 201. [Fecha de consulta: 20 de Abril de 2020].

F. Schüpfer, “Design and Implementation of a Smart Contract Application”, Master Thesis, Agosto 2017. [En línea]. Disponible en: https://files.ifi.uzh.ch/CSG/staff/Rafati/Florian-Schupfer-MA.pdf.

Gamarro, Lozano Pablo., Aplicabilidad de tecnologías Blockchain diseñadas para entornos IoT; España - Málaga ; Universidad de Málaga [2021]; 100 PP.

Gartner (2017). Leading the IoT [Internet],EEUU, Mark Hung, 2017. [Fecha de consulta: 20 de octubre de 2022]. Disponible en : https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Global IT Research Institute, IEEE Communications Society, & Institute of Electrical and Electronics Engineers. (n.d.). The 19th International Conference on Advanced Communications Technology: “Opening Era of Smart Society” : ICACT 2017 : Phoenix Park, Pyeongchang, Korea (South) : Feb. 19-22, 2017 : proceeding & journal.

Godoy, R. (2014). Seguridad de Información. Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Gómez Rojas, Gabriela y De Sena Angélica (2005): “Niveles de análisis y falacia ecológica en las primeras aproximaciones a la tarea investigativa”, ponencia presentada en IV Jornadas de Sociología de la Univ. Universidad Nacional de La Plata, Departamento de Sociología. La Plata.

HERNANDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C. y BAPTISTA LUCIO, M. del P., 2010. Definición del alcance de la investigación a realizar: exploratoria, descriptiva, correlacional o explicativa [en línea]. S.l.: s.n. ISBN 9786071502919. Disponible.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). Metodología de la Investigación Científica sexta edición. México: Editorial Mc Grawll Hill Education.

Hernández, R., & Mendoza, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (Primera ed.). México: McGrawHill.

It Digital Security (2020), Un 70% de las organizaciones ha sufrido ciberataques a través de IoT: ¿y ahora qué?[Internet], Madrid. [Fecha de consulta: 20 de octubre de 2022]. Disponible en: https://www.itdigitalsecurity.es/actualidad/2020/02/un-70-de-las-organizaciones-ha-sufrido-ciberataques-a-traves-de-iot-y-ahora-que

Infura, Consensis [disponible on-line: https://infura.io/], consultado el 14 de julio de 2020.

KIM, S., CHANDRA, G., & EDITORS, D. (2020). Advanced Applications of Blockchain Technology. Electronic ISSN 2197-6511, Disponible en: https://link.springer.com/book/10.1007/978-981-13-8775-3.

Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815–1823. https://doi.org/10.1016/j.procs.2018.05.140.

LIU, Yingna [et al.]. Knowledge, attitudes, and perceptions of autism spectrum disorder in a stratified sampling of preschool teachers in China [en línea]. BMC Psychiatry, 16, p.142, 2016. [Fecha de consulta: 22 de Junio del 2020]. Disponible en: https://doi.org/10.1186/s12888-016-0845-2.

Lopez-Vazquez, C. (2012). La autenticidad e integridad de la información geográfica Geochemestry lake modelling View project Numerical modelling of Atmospheric pollution View project. https://www.researchgate.net/publication/236012522.

Luis Joyanes Aguilar (2021);Internet de las cosas: Un futuro hiperconectado: 5G, inteligencia artificial, Big Data, Cloud, Blockchain y ciberseguridad;Marcombo, 2021;384 páginas;ISBN 8426733646, 9788426733641.

Luque Lodeiro, Ruben; Blockchain; estado del arte, tendencia y retos; Oviedo - España; Universidad de Oviedo; 2020; pp 153

Mahmoudie, R., Parsa, S., & Rahmani, A. M. (2022). The Application of Private Blockchain to Increase Security and Privacy in Internet of Things (IoT). Int. J. Industrial Mathematics, 14(3). https://doi.org/10.30495/ijim.2022.65634.1574.

McAfee. (2018). Informe sobre amenazas contra blockchain.

Mereles, Eduardo & Ortellado Juan;Uso de blockchain en la administración pública; Montevideo - Uruguay; Universidad de la República Uruguay, 2019; pp 91.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Obtenido de https://bitcoin.org/es/.

Narbayeva, S., Bakibayev, T., Abeshev, K., Makarova, I., Shubenkova, K., & Pashkevich, A. (2020). Blockchain Technology on the Way of Autonomous Vehicles Development. Transportation Research Procedia, 44, 168–175. https://doi.org/10.1016/j.trpro.2020.02.024.

OTZEN, T. y MANTEROLA, C., 2017. Técnicas de Muestreo sobre una Población a Estudio. International Journal of Morphology, vol. 35, no. 1, pp. 227-232. ISSN 07179502. DOI 10.4067/S0717-95022017000100037.

Özyılmaz, K. R., Doğan, M., & Yurdakul, A. (2018). IDMoB: IoT Data Marketplace on Blockchain. https://doi.org/10.1109/CVCBT.2018.00007.

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. In Sensors (Switzerland) (Vol. 18, Issue 8). MDPI AG. https://doi.org/10.3390/s18082575.

Remix, Remix IDE. Welcome to Remix documentation. Disponible en: ¡Welcome to Remix's documentation! — Remix - Ethereum IDE 1 documentation (remix-ide.readthedocs.io)

Remix Documentation [En línea]. Disponible en: https://remix.readthedocs.io/en/latest/. [Último acceso: Septiembre 2022].

Restrepo, Esteban Adrian;Olaya, Daniel Arturo; DESARROLLO DE UN PROTOTIPO BASADO EN BLOCKCHAIN APLICADO A LA PLATAFORMA IoT SOBRE UN SISTEMA EMBEBIDO, Colombia - Bogotá; Universidad Distrital Francisco José de Caldas [2018]; 88 PP.

Reyes Delgado Diego; «APLICACIÓN DE BLOCKCHAIN PARA LA SEGURIDAD DE LOS DATOS DEL INTERNET OF THINGS» ; Chile - Valparaíso ;UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA [2018]; 75 PP.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046.

Rojo, M. (2020). Blockchain: Visión tecnológica. Recuperado el 23 de Marzo del 2020 de https://www2.deloitte.com/es/es/pages/technology/articles/blockchain-vision- tecnologica.html.

ROMERO, M.I., FIGUEROA, G.L., VERA, D.S., ÁLAVA, J.E., PARRALES, G.R., ÁLAVA, C.J., MURILLO, Á.L. y CASTILLO, M.A., 2018. Mecanismo Correctivos en seguridad informática. S.l.: s.n. ISBN 9788494930614. DOI: http://dx.doi.org/10.17993/IngyTec.2018.46.

Rose, K., Eldridge, S., & Chapin, L. (2015). OCTUBRE DE 2015 Para entender mejor los problemas y desafíos de un mundo más conectado.

SAN JOSE, C., 2020. 7 out of 10 Organizations Have Seen Hacking Attempts via IoT | Extreme Networks, Inc. [en línea], Disponible en: https://investor.extremenetworks.com/news-releases/news-release-details/7-out-10-organizations-have-seen-hacking-attempts-iot.

S. Madakam, T. Uchiya, Industrial Internet of Things (IIoT): Principles, Processes and Protocols, in: Springer, Cham, 2019: pp. 35–53. https://doi.org/10.1007/978-3- 030-24892-5_2.

Samaniego, M., & Deters, R. (2017). Blockchain as a Service for IoT. Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, IThings-GreenCom-CPSCom-Smart Data 2016, 433–436. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.

SANTILLAN MOLINA, Alberto Leonel; VINUEZA OCHOA, Nelly Valeria y BENAVIDES SALAZAR, Cristian Fernando. Derecho, informática y corrupción. Un enfoque a la realidad ecuatoriana. Dilemas contemp. educ. política valores [online]. 2021, vol.9, n.spe1 [citado 2022-06-30], 00106. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-78902021000800106&lng=es&nrm=iso. Epub 31-Ene-2022. ISSN 2007-7890. https://doi.org/10.46377/dilemas.v9i.3017.

Scott Nelson. (2016); What door locks teach us about IoT cybersecurity.EEUU- San Diego .Disponible en: What door locks teach us about IoT cybersecurity | CIO

Sengupta, S., Kim, H., & Rexford, J. (2022). Continuous in-network round-Trip time monitoring. SIGCOMM 2022 - Proceedings of the ACM SIGCOMM 2022 Conference, 473–485. https://doi.org/10.1145/3544216.3544222

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead. In Computer Networks (Vol. 76, pp. 146–164). Elsevier B.V. https://doi.org/10.1016/j.comnet.2014.11.008. ISSN: ISSN 1389-1286.

Sitanskiy Stanislav; Análisis de seguridad de los principales sistemas de criptomonedas; Valencia - España; Universidad Politécnica de Valencia; 2019; pp 50.

Solomon, C. (2003). Transactional Analysis Theory: the Basics (Vol. 33, Issue 1).

Tamayo, M. (2004). El proceso de la investigación científica: Incluye evaluación y administración de proyectos de investigación. México, D.F.: Editorial Limusa.

TAPSCOTT, D., TICOLL, D. y LOWY, A., 2016. Blockchain Revolution How the technology Behind Bitcoin is changing money, business, and the world S.l.: s.n. ISBN 9781101980132.

UCV, 2022. Resolución De Consejo Universitario. Universidad César Vallejo [en línea], no. 044, pp. 12. Disponible en: https://www.ucv.edu.pe/wp-content/uploads/2020/09/RCUN°470-2022-UCV-Aprueba-actualizacion-del-Codigo-de-Etica-en-Investigacion-V01.pdf.

U.S. Department of Homeland Security, S. and T. D. (2015). Access Control Technologies Handbook Prepared by Space and Naval Warfare Systems Center Atlantic. www.firstresponder.gov/SAVER.

Unknown. (n.d.). Federal Information Security Modernization Act of 2014. Retrieved June 28, 2022, from https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

Vargas Sanchez Henry Fabian, Defensa contra intrusos en redes de dispositivos IoT usando técnicas de Blockchain y Machine Learning;Tesis (Magister en Seguridad de la Información); Colombia - Bogotá ;Universidad de los Andes [2020].

Venkata, B., Reddy, R., & Reddy, B. V. R. (2019). Block chain: A Game Changer for Securing IoT Data. https://www.researchgate.net/publication/335029128.

WANG, X., ZHA, X., NI, W., LIU, R.P., GUO, Y.J., NIU, X. y ZHENG, K., 2019. Survey on blockchain for Internet of Things. 1 febrero de 2019. S.l.: Elsevier B.V.

Welcome to Infura docs. Disponible en: Welcome to Infura docs - Infura Docs

Woods Nick (2021); Ethereum Para Principiantes: La Guía Completa Para Comprender Ethereum; Babelcube Inc.,2021(primera edición);78 PP. ISBN 1667409212, 9781667409214.

XU, R., CHEN, Y., BLASCH, E. y CHEN, G., 2018. BlendCAC: A Blockchain-ENabled Decentralized Capability-based Access Control for IoTs. [en línea], Disponible en: http://arxiv.org/abs/1804.09267.

Zeña Zeña, Edison Omar; COMPARACIÓN DE PROTOCOLOS DE COMUNICACIÓN EN INTERNET DE LAS COSAS, DETERMINANDO EL NIVEL DE SEGURIDAD ANTE ATAQUES EN DISPOSITIVOS; Perú - Pimentel; Universidad Señor de Sipán [2021];91 PP.

ANEXOS

Anexo 1: Fuentes de recolección de información

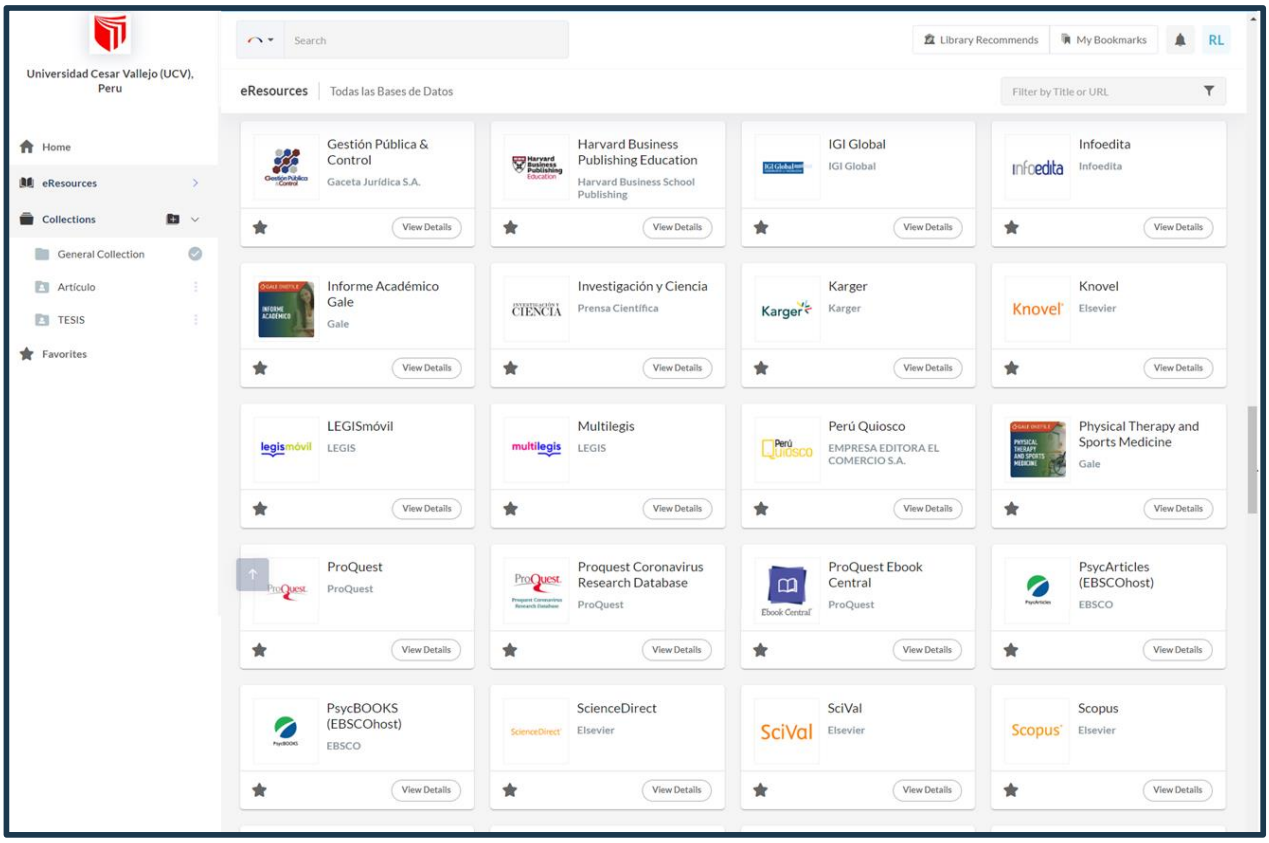


Figura N.º 18: Portal MyLOFT - UCV

Anexo 2:

Matriz de consistencia

Título: Comparación del rendimiento y seguridad que brindan las Blockchains aplicadas al IoT en Guimartbot SAC Lima 2022

Autores: FARFAN ROSALES HANDERSON JOEL y LOPEZ CORDOVA RAFAEL

TABLA N.º 10: *Matriz de consistencia*

Problema	Objetivo	Hipótesis	Metodología	Variables
Problema General: ¿Qué tipo de tecnología blockchain proporciona un mayor rendimiento y mejora la seguridad en los dispositivos IoT de la empresa GUIMARTBOT SAC? **Problema Específico:** A. ¿Cuál tecnología blockchain tendrá la menor latencia en el intercambio de información con el IoT en la empresa GUIMARTBOT SAC? B. ¿Qué tipo de tecnología blockchain consumirá menos recursos durante el	**Objetivo General:** Determinar qué tecnología blockchain tiene mejor rendimiento y seguridad al realizar el intercambio de información con el IoT en la empresa GUIMARTBOT SAC. **Objetivo Específico:** A. Identificar qué tipo de blockchain tiene un menor tiempo de ida y vuelta (TIV), durante el intercambio de información con el dispositivo IoT en la empresa GUIMARTBOT SAC.	**Hipótesis General:** Existen diferencias significativas respecto al rendimiento y seguridad entre la blockchain pública y la privada cuando son aplicadas a los dispositivos IoT en GUIMARTBOT SAC. **Hipótesis Específica:** A. La tecnología blockchain pública y privada tienen diferencias significativas en la latencia en relación al TIV durante el intercambio de información con los dispositivos IoT de la empresa GUIMARTBOT SAC.	**Tipo de investigación:** Aplicada **Tipo de Enfoque:** Cuantitativo **Tipo de Diseño:** Experimental	**Variable independiente:** Tecnologías Blockchain y IoT **Variable Dependiente** Rendimiento y seguridad **Indicadores:**

intercambio de información de los dispositivos IoT de la empresa GUIMARTBOT SAC? C. ¿Cuál tecnología blockchain será la más eficaz para permitir la comunicación con los dispositivos IoT en la empresa GUIMARTBOT SAC? D. ¿Qué tecnología blockchain podrá mejorar la disponibilidad de la información en los dispositivos IoT en la empresa GUIMARTBOT SAC? E. ¿Cuál tecnología blockchain podrá mejorar la seguridad de la información manejada en los dispositivos IoT en la empresa GUIMARTBOT SAC?	B. Identificar qué tipo de blockchain consume menos recursos durante el intercambio de información con el dispositivo IoT de la empresa GUIMARTBOT SAC. C. Determinar qué tecnología blockchain es la más eficaz para permitir la comunicación con los dispositivos IoT en la empresa GUIMARTBOT SAC. D. Identificar qué tipo de blockchain mejora la disponibilidad en la información en los dispositivos IoT de la empresa GUIMARTBOT SAC. E. Determinar qué tecnología blockchain mejora el nivel de seguridad de la información manejada en los dispositivos IoT en la empresa GUIMARTBOT SAC.	B. Existen diferencias significativas entre la tecnología blockchain pública y privada respecto a su rendimiento en relación al consumo de recursos al aplicarse al IoT en la empresa GUIMARTBOT SAC. C. La tecnología blockchain pública y privada tienen diferencias significativas en rendimiento en relación a la eficacia al aplicarse al IoT en la empresa GUIMARTBOT SAC. D. La tecnología blockchain pública y privada tiene diferencias significativas en la seguridad respecto a la disponibilidad de la información en los dispositivos IoT de la empresa GUIMARTBOT SAC. E. La tecnología blockchain pública y privada tienen diferencias significativas en el nivel de seguridad al aplicarse al IoT en la empresa GUIMARTBOT SAC.		1. TIV promedio. 2. Porcentaje de consumo de recursos. 3. Consenso de la red BC. 4. Porcentaje de disponibilidad 5. Nivel de seguridad.

Fuente: Elaboración propia

Anexo 3:

Tabla de operacionalización de variables

TABLA N.º 11: *Tabla de operacionalización de variables*

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	Dimensiones (sub variables)	INDICADORES	ESCALA DE MEDICIÓN
Blockchain IoT	**Blockchain** es una base de datos distribuida donde cada nodo de la red ejecuta y registra transacciones agrupadas en bloques (Nakamoto, 2008). **IoT** es la interconexión en red de todos los objetos cotidianos, que están equipados con algún tipo de inteligencia (Salazar, 2016).	Modelo que permite gestionar los datos, sin intermediarios. Tecnología que permite controlar dispositivos mediante el uso de internet.			
Rendimiento	La RAE (Real academia española), define Rendimiento como la proporción entre el producto o el resultado obtenido y los medios utilizados". Es así que se monitoreó el tiempo en el TIV, y el	La medida en relación al tiempo y recursos con los que un sistema cumple con el objetivo para el que fue creado.	Latencia (kim, 2022, p. 1)	TIV: Tiempo de ida y vuelta (kim, 2022, p. 1)	RAZÓN
			Recursos (Sekiya, 2021, p. 6)	PCR: Porcentaje de consumo de recursos(Sekiya, 2021, p. 6)	RAZÓN

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	Dimensiones (sub variables)	INDICADORES	ESCALA DE MEDICIÓN
	acceso a los datos de la BC.		Eficacia (Fernandez, 2018)	Cantidad de transacciones exitosas	ORDINAL
				Cantidad de transacciones fallidas	
Seguridad	Los pilares de la seguridad informática son la confidencialidad, la integridad y la disponibilidad de la información, logrando así sacarle el máximo rendimiento con el mínimo riesgo (Romero, 2018).		Disponibilidad (Nakamoto, 2008)	Porcentaje de disponibilidad (Nakamoto, 2008)	RAZÓN
			Seguridad (Romero, 2018)	Nivel de seguridad (Romero, 2018)	ORDINAL

Fuente: Elaboración propia

Anexo 4: Diagrama Causa Efecto

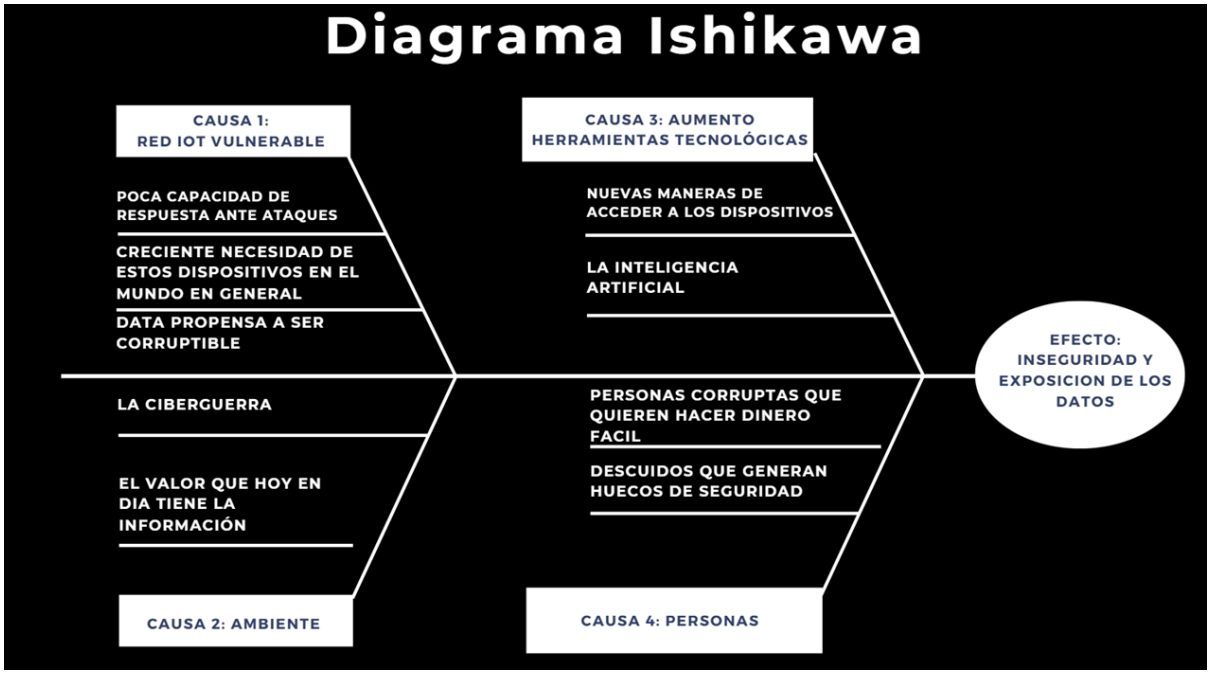
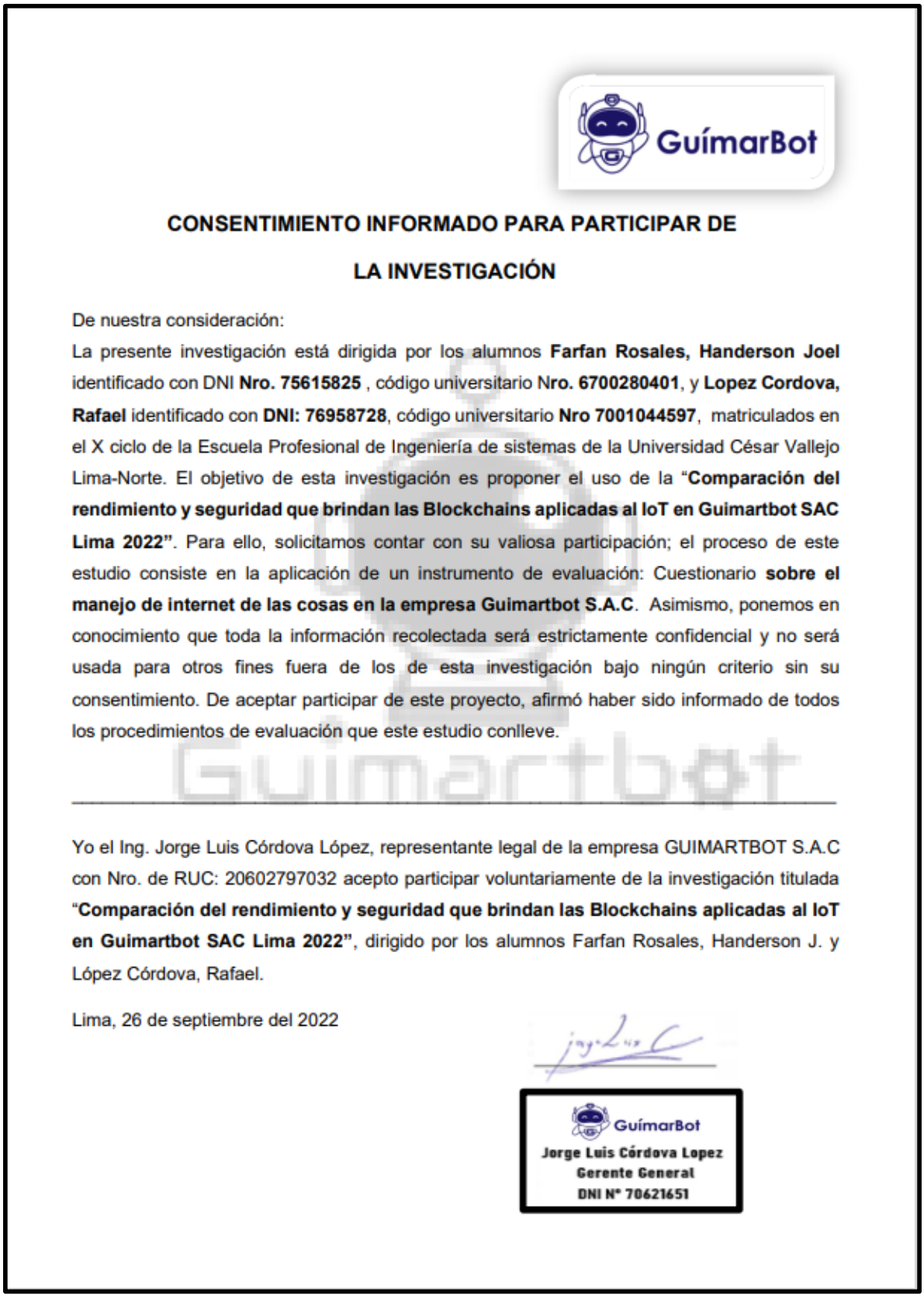


Figura N.º 19: Diagrama de causa y efecto
Fuente: Elaboración propia

Anexo 5: Consentimiento Informado



GuímarBot

CONSENTIMIENTO INFORMADO PARA PARTICIPAR DE

LA INVESTIGACIÓN

De nuestra consideración:

La presente investigación está dirigida por los alumnos **Farfan Rosales, Handerson Joel** identificado con DNI **Nro. 75615825** , código universitario N**ro. 6700280401**, y **Lopez Cordova, Rafael** identificado con **DNI: 76958728**, código universitario **Nro 7001044597**, matriculados en el X ciclo de la Escuela Profesional de Ingeniería de sistemas de la Universidad César Vallejo Lima-Norte. El objetivo de esta investigación es proponer el uso de la "**Comparación del rendimiento y seguridad que brindan las Blockchains aplicadas al IoT en Guimartbot SAC Lima 2022"**. Para ello, solicitamos contar con su valiosa participación; el proceso de este estudio consiste en la aplicación de un instrumento de evaluación: Cuestionario **sobre el manejo de internet de las cosas en la empresa Guimartbot S.A.C**. Asimismo, ponemos en conocimiento que toda la información recolectada será estrictamente confidencial y no será usada para otros fines fuera de los de esta investigación bajo ningún criterio sin su consentimiento. De aceptar participar de este proyecto, afirmó haber sido informado de todos los procedimientos de evaluación que este estudio conlleve.

Guimartbot

Yo el Ing. Jorge Luis Córdova López, representante legal de la empresa GUIMARTBOT S.A.C con Nro. de RUC: 20602797032 acepto participar voluntariamente de la investigación titulada "**Comparación del rendimiento y seguridad que brindan las Blockchains aplicadas al IoT en Guimartbot SAC Lima 2022"**, dirigido por los alumnos Farfan Rosales, Handerson J. y López Córdova, Rafael.

Lima, 26 de septiembre del 2022

GuímarBot
Jorge Luis Córdova Lopez
Gerente General
DNI N° 70621651

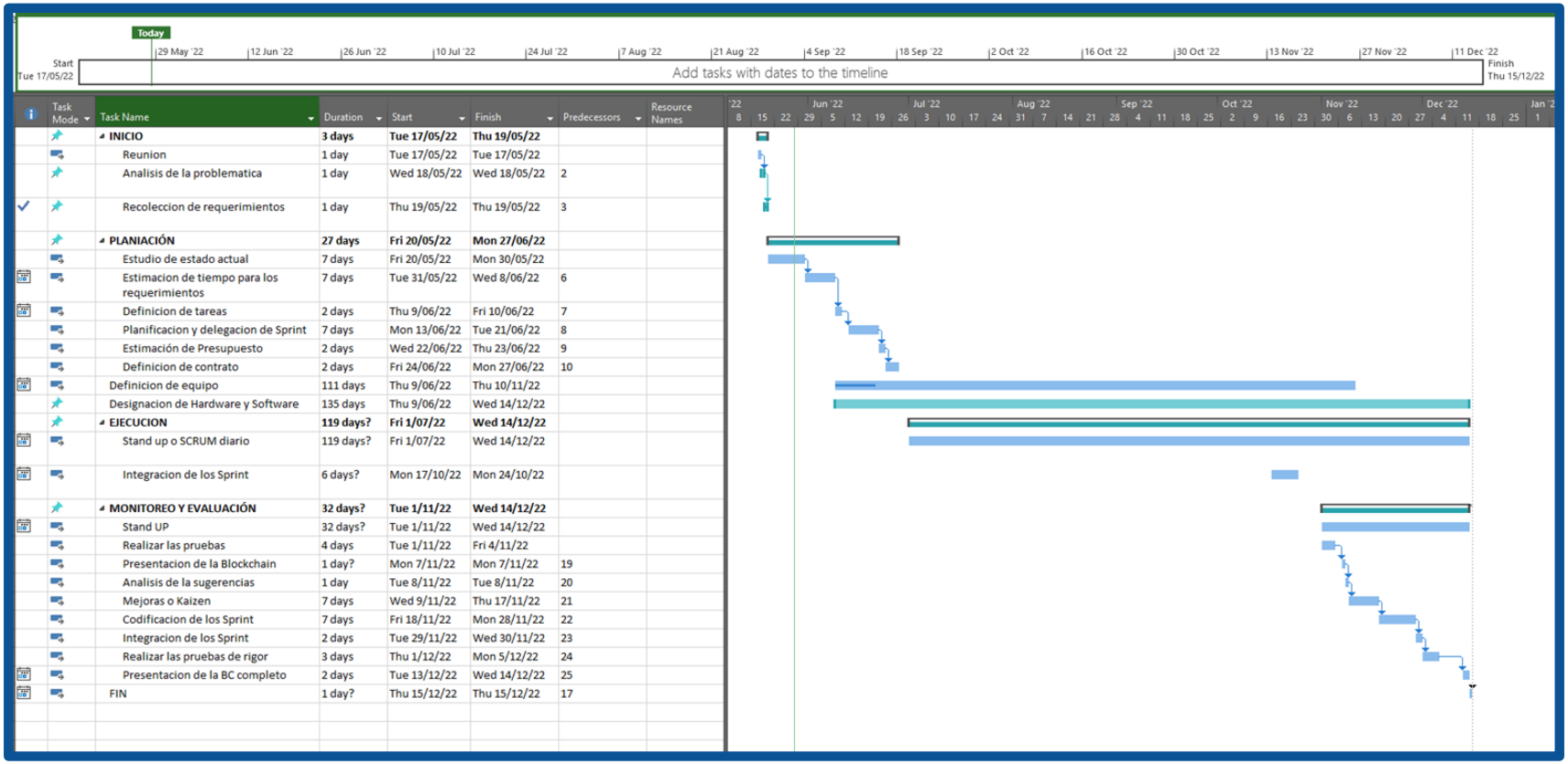
Figura N.º 20: Consentimiento informado

Anexo 6: Conducta Responsable

Figura N.º 21: Prueba de conducta responsable - Investigador 1

Figura N.º 22: Prueba de conducta responsable - Investigador 2

Anexo 7: Diagrama de Gantt



Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names
	INICIO	**3 days**	**Tue 17/05/22**	**Thu 19/05/22**		
	Reunion	1 day	Tue 17/05/22	Tue 17/05/22		
	Analisis de la problematica	1 day	Wed 18/05/22	Wed 18/05/22	2	
	Recoleccion de requerimientos	1 day	Thu 19/05/22	Thu 19/05/22	3	
	PLANIACIÓN	**27 days**	**Fri 20/05/22**	**Mon 27/06/22**		
	Estudio de estado actual	7 days	Fri 20/05/22	Mon 30/05/22		
	Estimacion de tiempo para los requerimientos	7 days	Tue 31/05/22	Wed 8/06/22	6	
	Definicion de tareas	2 days	Thu 9/06/22	Fri 10/06/22	7	
	Planificacion y delegacion de Sprint	7 days	Mon 13/06/22	Tue 21/06/22	8	
	Estimación de Presupuesto	2 days	Wed 22/06/22	Thu 23/06/22	9	
	Definicion de contrato	2 days	Fri 24/06/22	Mon 27/06/22	10	
	Definicion de equipo	111 days	Thu 9/06/22	Thu 10/11/22		
	Designacion de Hardware y Software	135 days	Thu 9/06/22	Wed 14/12/22		
	EJECUCION	**119 days?**	**Fri 1/07/22**	**Wed 14/12/22**		
	Stand up o SCRUM diario	119 days?	Fri 1/07/22	Wed 14/12/22		
	Integracion de los Sprint	6 days?	Mon 17/10/22	Mon 24/10/22		
	MONITOREO Y EVALUACIÓN	**32 days?**	**Tue 1/11/22**	**Wed 14/12/22**		
	Stand UP	32 days?	Tue 1/11/22	Wed 14/12/22		
	Realizar las pruebas	4 days	Tue 1/11/22	Fri 4/11/22		
	Presentacion de la Blockchain	1 day?	Mon 7/11/22	Mon 7/11/22	19	
	Analisis de la sugerencias	1 day	Tue 8/11/22	Tue 8/11/22	20	
	Mejoras o Kaizen	7 days	Wed 9/11/22	Thu 17/11/22	21	
	Codificacion de los Sprint	7 days	Fri 18/11/22	Mon 28/11/22	22	
	Integracion de los Sprint	2 days	Tue 29/11/22	Wed 30/11/22	23	
	Realizar las pruebas de rigor	3 days	Thu 1/12/22	Mon 5/12/22	24	
	Presentacion de la BC completo	2 days	Tue 13/12/22	Wed 14/12/22	25	
	FIN	1 day?	Thu 15/12/22	Thu 15/12/22	17	

Figura N.º 23: Diagrama de Gantt
Fuente: Elaboración propia

Anexo 8: Resolución De Consejo Universitario

UNIVERSIDAD CÉSAR VALLEJO

RESOLUCIÓN DE CONSEJO UNIVERSITARIO N.° 0101-2022/UCV

Trujillo, 15 de febrero de 2022

VISTO: el oficio N° 075-2022-VI-UCV, remitido por el Dr. Jorge Salas Ruiz, vicerrector de investigación de la Universidad César Vallejo S.A.C. y el acta del Consejo Universitario de sesión extraordinaria, del 15 de febrero del presente año, que aprueba la actualización del Reglamento de Investigación de la Universidad César Vallejo S.A.C., versión 03; y

CONSIDERANDO:

Que el Estatuto, el Reglamento General y los demás reglamentos universitarios son normas institucionales que regulan las relaciones que se establecen entre las unidades académicas y administrativas de la universidad, con la finalidad de encauzar los esfuerzos individuales para alcanzar la visión, misión y objetivos institucionales, por lo que están sujetos a aprobar y poner en vigencia las normas situacionales que permitan lograr los propósitos institucionales;

Que, mediante Resolución de Consejo Universitario Nº 0722-2021/UCV, de fecha 29 de octubre de 2021, se aprobó el Reglamento de Investigación de la Universidad César Vallejo S.A.C. versión 02 y se dispuso su entrada en vigencia a partir del día siguiente de la publicación de la resolución de consejo universitario que lo aprueba;

Que, mediante Oficio N° 075-2022-VI-UCV, el Dr. Jorge Salas Ruiz, vicerrector de investigación de la Universidad César Vallejo S.A.C., en cumplimiento de las funciones inherentes a su cargo ha presentado el Reglamento de Investigación de la Universidad César Vallejo S.A.C. actualizado, que ha sido elaborado con la participación de los miembros de la Comisión de Normas, y tomando en consideración las normativas internas del área de investigación, quedando expedito para su aprobación mediante acuerdo del Consejo Universitario;

Que, elevado el expediente al Consejo Universitario, en su sesión extraordinaria del 15 de febrero del presente año, ha evaluado la solicitud de actualización presentada por el vicerrector de investigación y, encontrándola conforme con la visión, misión y objetivos institucionales, ha dispuesto su aprobación, difusión y aplicación; por lo que, debe emitirse la correspondiente resolución de consejo universitario;

Estando a lo expuesto y de conformidad con las normas estatutarias y reglamentarias vigentes.

SE RESUELVE:

Art. 1°. --- APROBAR, la actualización del **Reglamento de Investigación de la Universidad César Vallejo S.A.C., versión 03**, norma legal institucional que consta de 5 títulos, 22 capítulos, 68 artículos, 1 disposición complementaria y 4 disposiciones finales; y disponer su entrada en vigencia a partir del día siguiente de la publicación de la presente resolución, norma institucional cuyo texto forma parte de la presente resolución como anexo n.º 01.

Art. 2º.--- DEJAR SIN EFECTO todas las normas institucionales que se opongan a las modificaciones aprobadas mediante la presente resolución.

Figura N.º 24: Resolución de consejo universitario
Fuente: UCV

UNIVERSIDAD CÉSAR VALLEJO

Art. 3°.--- ENCARGAR al profesional responsable del Sistema de Gestión de la Calidad la difusión de la actualización del Reglamento de Investigación de la Universidad César Vallejo S.A.C., aprobado por la presente norma institucional y coordinar la actualización de los procedimientos de gestión de la calidad correspondientes.

Art. 4°.--- DISPONER que los órganos académicos y administrativos de la Universidad brinden las facilidades del caso para el cumplimiento de la presente resolución de Consejo Universitario.

Regístrese, comuníquese y cúmplase.

RECTORADO UNIVERSIDAD CÉSAR VALLEJO

Dra. JEANNETTE TANTALEAN RODRIGUEZ
Rectora

SECRETARÍA GENERAL UNIVERSIDAD CÉSAR VALLEJO

Abog. ROSA LOMPARTE ROSALES
Secretaria General

DISTRIBUCIÓN: Rectora, presidenta ejecutiva, VA, VBU, VI, VC, gerente Gral., decanos, directores de escuela, Dir. De Admisión, Dir. De Marketing, Dir. Grados y Títulos, Dir. Registros Académicos, DGC, Dir. EPG, Dir. FG, Dir. Planificación y Desarrollo Institucional, Dir. Asesoría Legal, directores generales de la sede y filiales, archivo.

JCTR/rpach: asg.

Figura N.º 25: Resolución de consejo universitario
Fuente: UCV

Anexo 9: Propuesta de Desarrollo

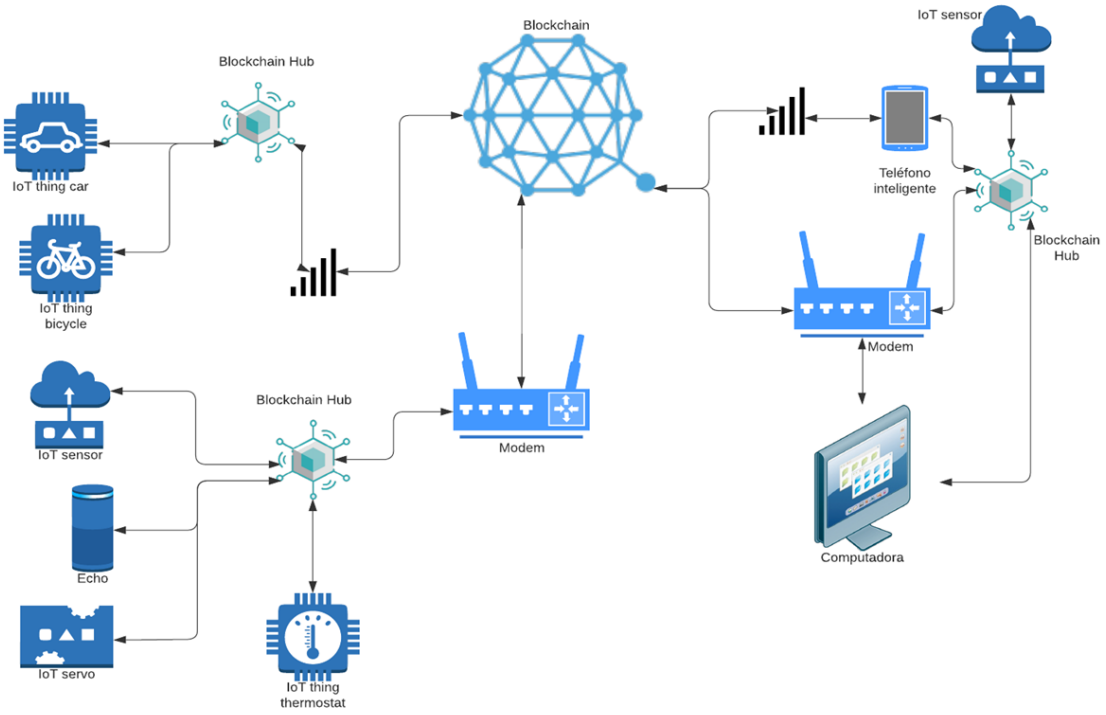


Figura N.º 26: Arquitectura de la propuesta
Fuente: Elaboración propia

Anexo 10: Instrumento de observación

TABLA N.º 12: *Instrumento de observación de rendimiento de la BC Pública*

Instrumento #2: Observación de Rendimiento de la Blockchain Pública						
Ficha de Registro						
Tipo de Prueba		Obserbación				
Lugar		Guimartbot SAC				
Motivo de Investigación		Demostrar el rendimiento de la Blockchain Pública				
Investigadores		Farfan Rosales. Handerson; Lopez Cordova. Rafael				
Fecha de Inicio:			Fecha de Fin			

Variable	Indicadores	Medida	Tipo de blockchain
Rendimiento	TIV	Razón	PÚBLICA
	PCR	Razón	
	EFICACIA	Razón	

		Dispositivo	RENDIMIENTO			
# TRANSACCIÓN	Fecha	Nombre	TIV (segundos)	PCR	EFICACIA	
					Eficaz	No eficaz
1	22/10/2022	Cerradura	16,877	28,9%	x	
2	22/10/2022	Cerradura	33,183	29,5%	x	
3	22/10/2022	Cerradura	18,142	47,4%	x	
4	22/10/2022	Cerradura	24,891	55,6%	x	
5	22/10/2022	Cerradura	17,544	28,7%	x	
6	22/10/2022	Cerradura	24,584	23,7%	x	
7	22/10/2022	Cerradura	10,612	25,8%	x	
8	22/10/2022	Cerradura	4,274	30,8%	x	
9	22/10/2022	Cerradura	7,275	24,4%	x	
10	22/10/2022	Cerradura	4,902	29,5%	x	
11	22/10/2022	Cerradura	8,099	26,5%	x	
12	22/10/2022	Cerradura	17,726	24,0%	x	
13	22/10/2022	Cerradura	8,230	28,2%	x	
14	22/10/2022	Cerradura	20,868	22,1%	x	
15	22/10/2022	Cerradura	6,291	32,1%	x	
16	22/10/2022	Cerradura	9,267	29,7%	x	
17	22/10/2022	Cerradura	19,764	28,0%	x	
18	22/10/2022	Cerradura	22,326	27,5%	x	
19	22/10/2022	Cerradura	21,764	30,6%	x	
20	22/10/2022	Cerradura	12,085	36,7%	x	
21	22/10/2022	Cerradura	21,298	28,5%	x	
22	22/10/2022	Cerradura	20,834	27,6%	x	
23	22/10/2022	Cerradura	13,439	33,8%	x	
24	22/10/2022	Cerradura	7,742	29,3%	x	
25	22/10/2022	Cerradura	24,771	38,9%	x	

Fuente: Elaboración propia

TABLA N.º 13: *Instrumento de observación de rendimiento de la BC Privada*

Instrumento #2: Observación de Rendimiento de la Blockchain Privada			
Ficha de Registro			
Tipo de Prueba	Obserbación		
Lugar	Guimartbot SAC		
Motivo de Investigación	Demostrar el rendimiento de la blockchain privada		
Investigadores	Farfan Rosales, Handerson; Lopez Cordova, Rafael		
Fecha de Inicio:	19/10/2022	Fecha de Fin	19/10/2022

Variable	Indicadores	Medida	Tipo de blockchain
Rendimiento	TIV	Razón	PRIVADA
	PCR	Razón	
	EFICACIA	Ordinal	

		Dispositivo	RENDIMIENTO			
# TRANSACCIÓN	Fecha	Nombre	TIV (milisegundos)	PCR	EFICACIA	
					Eficaz	No eficaz
1	19/11/2022	SmartLock	0,063	20,9%	1	0
2	19/11/2022	SmartLock	0,043	35,6%	1	0
3	19/11/2022	SmartLock	0,042	24,6%	1	0
4	19/11/2022	SmartLock	0,057	33,1%	1	0
5	19/11/2022	SmartLock	0,053	39,7%	1	0
6	19/11/2022	SmartLock	0,047	45,7%	1	0
7	19/11/2022	SmartLock	0,046	29,3%	1	0
8	19/11/2022	SmartLock	0,066	27,7%	1	0
9	19/11/2022	SmartLock	0,055	25,6%	1	0
10	19/11/2022	SmartLock	0,049	44,6%	1	0
11	19/11/2022	SmartLock	0,060	52,7%	1	0
12	19/11/2022	SmartLock	0,040	18,7%	1	0
13	19/11/2022	SmartLock	0,043	22,4%	1	0
14	19/11/2022	SmartLock	0,056	27,4%	1	0
15	19/11/2022	SmartLock	0,062	18,0%	1	0
16	19/11/2022	SmartLock	0,049	21,2%	1	0
17	19/11/2022	SmartLock	0,042	9,0%	1	0
18	19/11/2022	SmartLock	0,057	16,7%	1	0
19	19/11/2022	SmartLock	0,064	40,3%	1	0
20	19/11/2022	SmartLock	0,044	17,0%	1	0
21	19/11/2022	SmartLock	0,056	24,8%	1	0
22	19/11/2022	SmartLock	0,053	30,6%	1	0
23	19/11/2022	SmartLock	0,052	30,5%	1	0
24	19/11/2022	SmartLock	0,062	22,2%	1	0
25	19/11/2022	SmartLock	0,052	36,9%	1	0
26	19/11/2022	SmartLock	0,044	22,7%	1	0

Fuente: Elaboración propia

TABLA N.º 14: *Instrumento de observación de seguridad de la BC Pública*

Instrumento #3: Observación de la seguridad de la Blockchain Pública			
Ficha de Registro			
Tipo de Prueba	Obserbación		
Lugar	Guimartbot SAC		
Motivo de Investigación	Demostrar la seguridad de la blockchain pública		
Investigadores	Farfan Rosales, Handerson; Lopez Cordova, Rafael		
Fecha de Inicio:		Fecha de Fin	

Variable	Indicadores	Medida	Blockchain
Seguridad	Nivel de seguridad	Ordinal	Pública
	Disponibilidad	Ordinal	

		Dispositivo	Seguridad	Disponibilidad	
# TRANSACCIÓN	Fecha	Nombre	Nivel de seguridad	Nivel de disponibilidad	
				Exitoso	Fallido
1	19/11/2022	Cerradura	Alto	X	
2	19/11/2022	Cerradura	Alto	X	
3	19/11/2022	Cerradura	Alto	X	
4	19/11/2022	Cerradura	Alto	X	
5	19/11/2022	Cerradura	Alto	X	
6	19/11/2022	Cerradura	Alto	X	
7	19/11/2022	Cerradura	Alto	X	
8	19/11/2022	Cerradura	Alto	X	
9	19/11/2022	Cerradura	Alto	X	
10	19/11/2022	Cerradura	Alto	X	
11	19/11/2022	Cerradura	Alto	X	
12	19/11/2022	Cerradura	Alto	X	
13	19/11/2022	Cerradura	Alto	X	
14	19/11/2022	Cerradura	Alto	X	
15	19/11/2022	Cerradura	Alto	X	
16	19/11/2022	Cerradura	Alto	X	
17	19/11/2022	Cerradura	Alto	X	
18	19/11/2022	Cerradura	Alto	X	
19	19/11/2022	Cerradura	Alto	X	
20	19/11/2022	Cerradura	Alto	X	
21	19/11/2022	Cerradura	Alto	X	
22	19/11/2022	Cerradura	Alto	X	
23	19/11/2022	Cerradura	Alto	X	
24	19/11/2022	Cerradura	Alto	X	
25	19/11/2022	Cerradura	Alto	X	
26	19/11/2022	Cerradura	Alto	X	
27	19/11/2022	Cerradura	Alto	X	
28	19/11/2022	Cerradura	Alto	X	

Fuente: Elaboración propia

TABLA N.º 15: *Instrumento de observación de seguridad de la BC Privada*

Instrumento #3: Observación de la seguridad de la Blockchain Privada			
Ficha de Registro			
Tipo de Prueba	Obserbación		
Lugar	Guimartbot SAC		
Motivo de Investigación	Demostrar la seguridad de la blockchain privada		
Investigadores	Farfan Rosales, Handerson; Lopez Cordova, Rafael		
Fecha de Inicio:		Fecha de Fin	

Variable	Indicadores	Medida	Blockchain
Seguridad	Nivel de seguridad	Ordinal	Privada
	Disponibilidad	Ordinal	

		Dispositivo	SEGURIDAD		
# TRANSACCIÓN	Fecha	Nombre	Nivel de seguridad	Nivel de disponibilidad	
				Exitoso	Fallido
1	19/10/2022	Cerradura	Alto	X	
2	19/10/2022	Cerradura	Alto	X	
3	19/10/2022	Cerradura	Alto	X	
4	19/10/2022	Cerradura	Alto	X	
5	19/10/2022	Cerradura	Alto	X	
6	19/10/2022	Cerradura	Alto	X	
7	19/10/2022	Cerradura	Alto	X	
8	19/10/2022	Cerradura	Alto	X	
9	19/10/2022	Cerradura	Alto	X	
10	19/10/2022	Cerradura	Alto	X	
11	19/10/2022	Cerradura	Alto	X	
12	19/10/2022	Cerradura	Alto	X	
13	19/10/2022	Cerradura	Alto	X	
14	19/10/2022	Cerradura	Alto	X	
15	19/10/2022	Cerradura	Alto	X	
16	19/10/2022	Cerradura	Alto	X	
17	19/10/2022	Cerradura	Alto	X	
18	19/10/2022	Cerradura	Alto	X	
19	19/10/2022	Cerradura	Alto	X	
20	19/10/2022	Cerradura	Alto	X	
21	19/10/2022	Cerradura	Alto	X	
22	19/10/2022	Cerradura	Alto	X	
23	19/10/2022	Cerradura	Alto	X	

Fuente: Elaboración propia

Anexo 11: Dispositivo IoT para la simulación del ataque

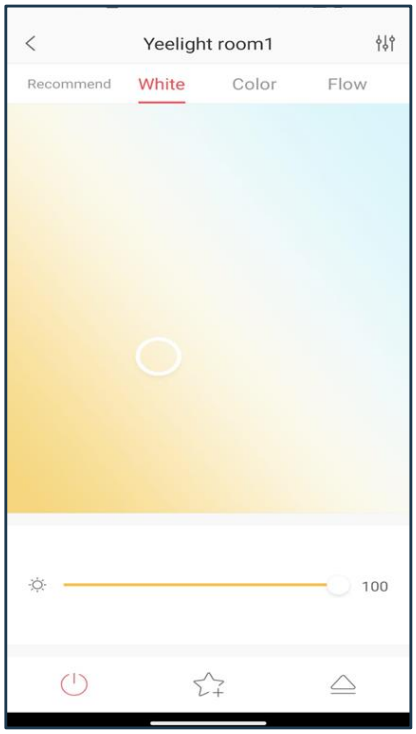


Figura N.º 27: Prueba - App del foco inteligente
Fuente: App Yeelight

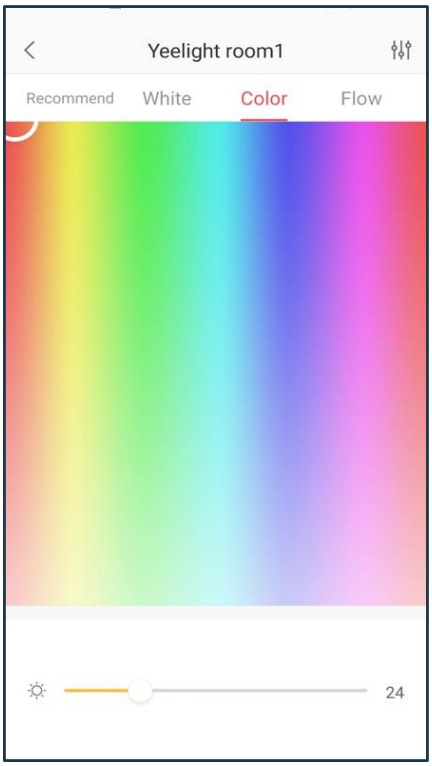


Figura N.º 28: Prueba - App del foco inteligente 2
Fuente: App Yeelight

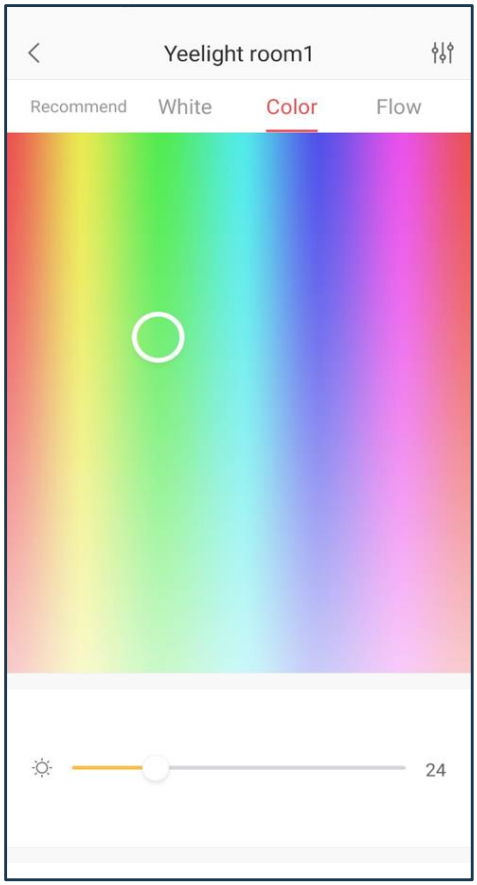


Figura N.º 29: Prueba - App del foco inteligente 3
Fuente: App Yeelight

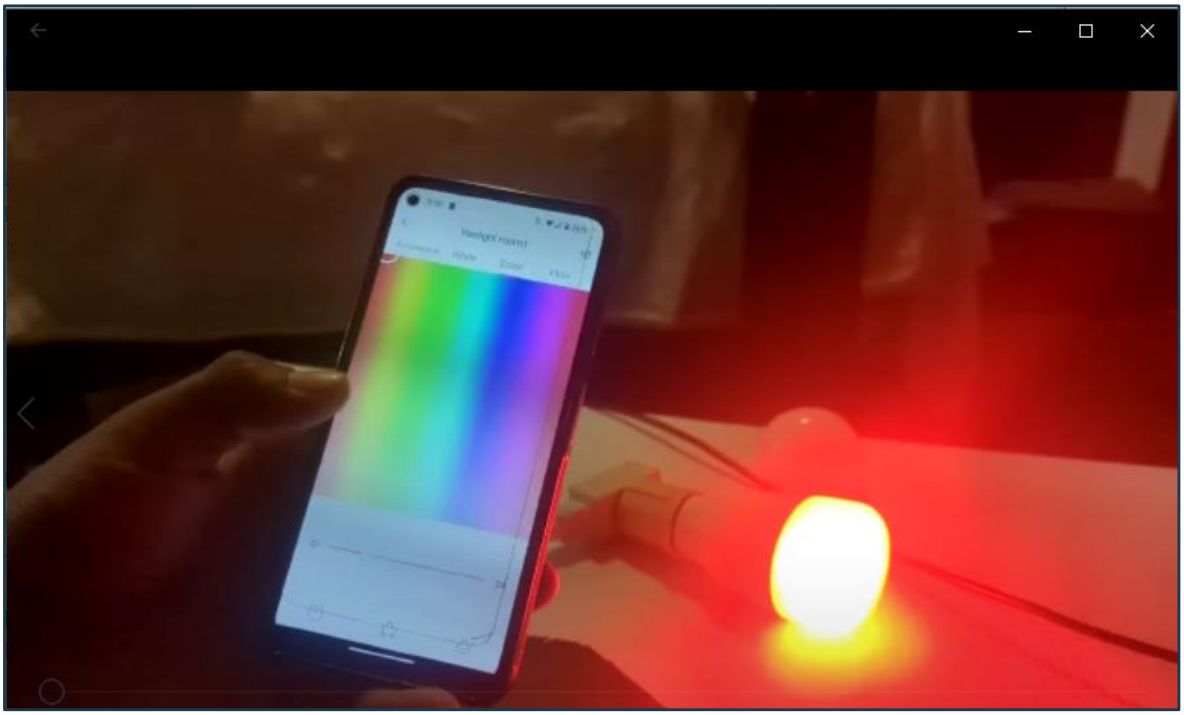


Figura N.º 30: Muestra del uso del foco inteligente
Fuente: Elaboración propia

Anexo 12: Simulación de ataque

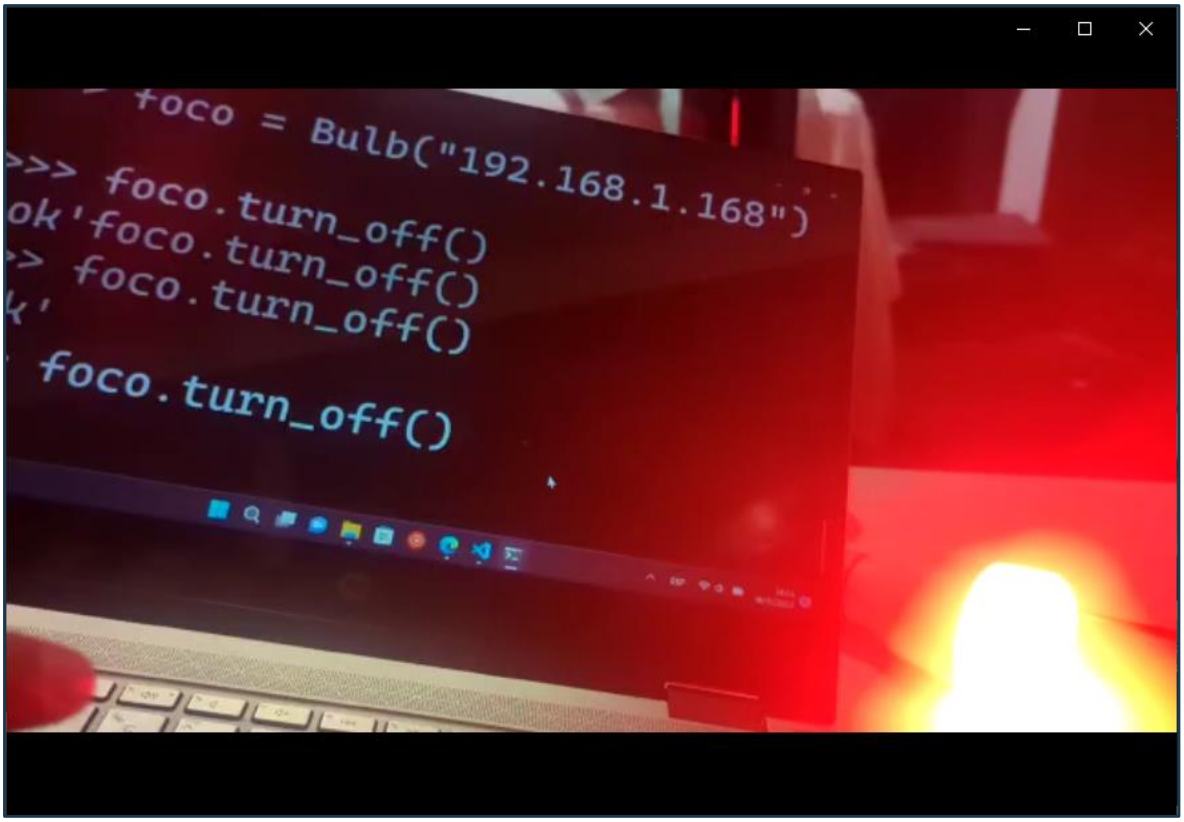


Figura N.º 31: Simulación de ataque 1
Fuente: Elaboración propia

Figura N.º 32: Simulación de ataque 2
Fuente: Elaboración propia

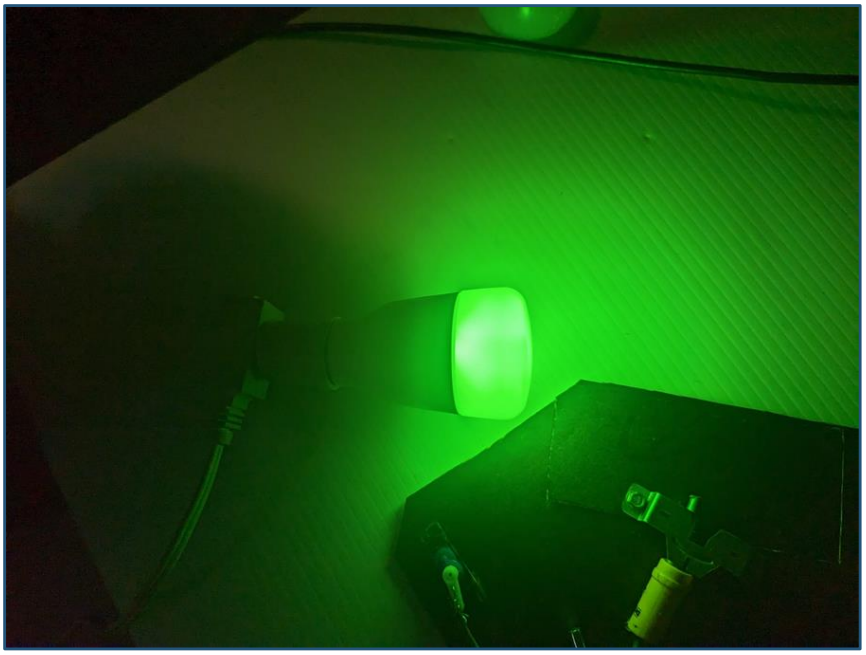


Figura N.º 33: Simulación de ataque 3
Fuente: Elaboración propia

Figura N.º 34: Simulación de ataque 4
Fuente: Elaboración propia

Anexo 13: Esquema de conexiones para la cerradura

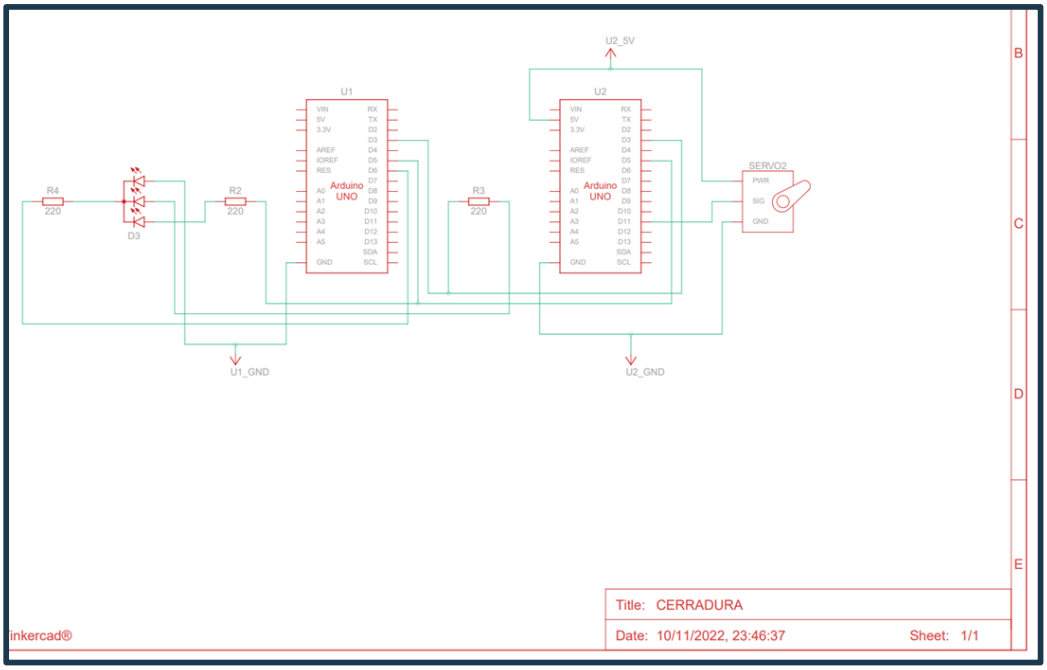


Figura N.º 35: Esquema de la cerradura

Fuente: Elaboración propia (**Link al diagrama Tinkercad**)

Anexo 14: Diseño de la cerradura

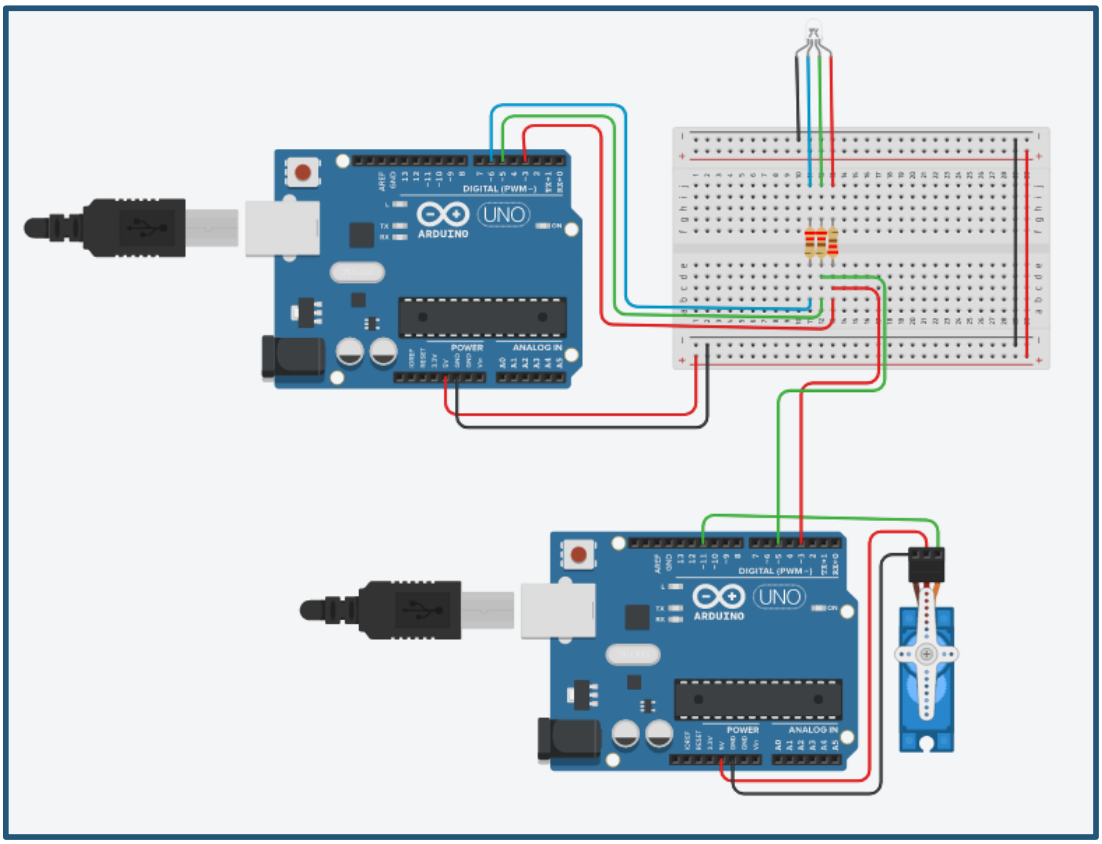


Figura N.º 36: Diseño de la cerradura

Fuente: Elaboración propia

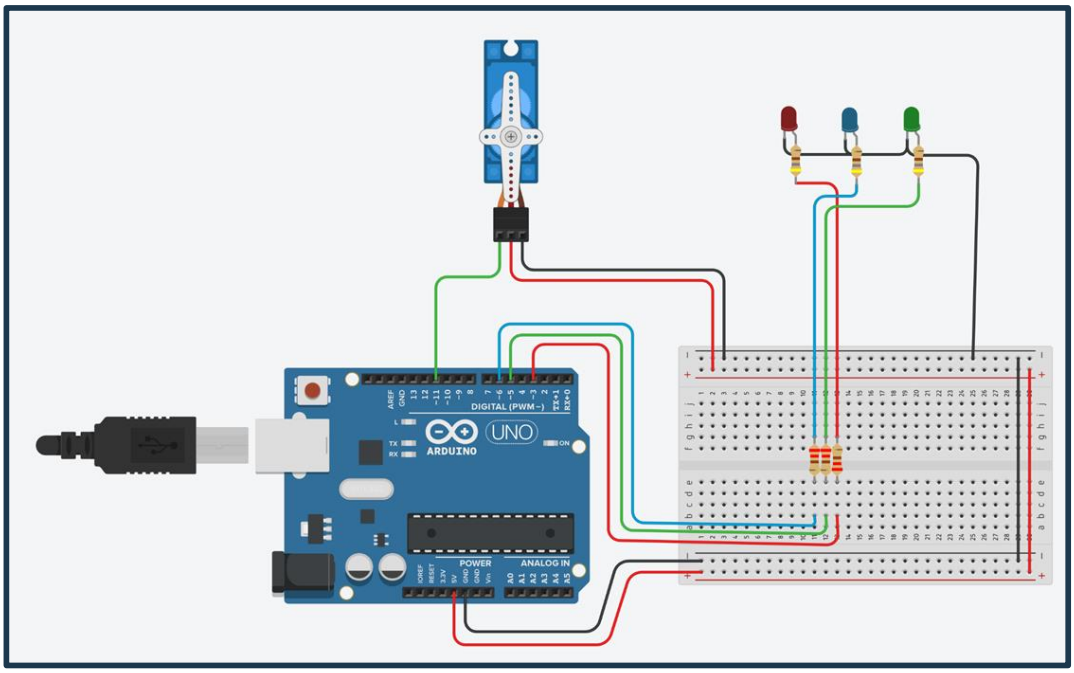


Figura N.º 37: Diseño 2 de la cerradura y foco inteligente con un solo Arduino
Fuente: Elaboración propia

Anexo 15: Validación instrumentos

UNIVERSIDAD CÉSAR VALLEJO

Estimado Validador:

Me es grato dirigirme a usted, a fin de solicitar su inapreciable colaboración como experto para validar el cuestionario anexo, el cual será aplicado a los trabajadores de la empresa Guimartbot S.A.C., por cuanto considero que sus observaciones y subsecuentes aportes serán de utilidad.

El presente instrumento tiene como finalidad recoger información directa para la investigación que se realiza en los actuales momentos, titulado: **"Tecnología Blockchain para mejorar la seguridad y privacidad de dispositivos IoT de la empresa Guimartbot S.A.C Lima 2022"**, esto con el objeto de presentarla como requisito para poder aplicar el pre-test y posterior pos-test en la empresa y obtener resultados precisos para nuestra investigación de noveno ciclo.

Para efectuar la validación del instrumento, usted deberá leer cuidadosamente cada enunciado y sus correspondientes alternativas de respuesta, en donde se solo se puede seleccionar una alternativa de acuerdo al criterio personal y profesional del actor que responda al instrumento. Por otra parte, se le agradece cualquier sugerencia relativa a redacción, contenido, pertinencia y congruencia u otro aspecto que se considere relevante para mejorar el mismo.

Gracias por su aporte

Figura N.º 38: Carta de presentación
Fuente: Elaboración propia

Tabla N.º 16: *Evaluación de expertos 1*

TABLA DE EVALUACION DE EXPERTOS

I. **DATOS GENERALES:**

Apellidos y Nombre del Experto: Iván Michell Castillo Jiménez

Título y/o Grado: Ingeniero Informático , Dr. En Tecnologías de la Información y Comunicaciones

Doctor……(X)	Magister……..( )	Ingeniero……..( )	Otros……..especifique

Institución donde Labora: Universidad Cesar Vallejo Sede Piura

Autores: Farfan Rosales, Handerson Joel y Lopez Cordova, Rafael.

Fecha : 06/07/2022

Nombre del instrumento motivo de evaluación:

Título de la investigación : Comparación de las Blockchains aplicadas al IoT en relación al rendimiento y seguridad en la empresa Guimartbot SAC Lima 2022

II. **ASPECTOS DE VALIDACIÓN:**

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81- 100%
Claridad	Está formulado con el lenguaje apropiado.				80	
Objetividad	Está expresado en conducta observable		50			
Actualidad	Es adecuado al avance de la ciencia.			70		
Organización	Existe una organización lógica.				80	
Suficiencia	Comprende los aspectos de cantidad y calidad.			70		
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico.					90
Consistencia	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				80	
Coherencia	Entre los índices, indicadores, dimensiones.					90
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr.				80	
Pertinencia	El instrumento es adecuado al tipo de investigación.				80	
Promedio de Validación			50	70	80	90

III. **Promedio de Valoración: 72.5%**

IV. **Observaciones :Ninguna**

Dr. Ing. Iván Michell Castillo Jiménez

Fuente: Elaboración propia

Tabla N.º 17: *Evaluación de expertos 2*

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES:

Apellidos y Nombre del Experto: Sara Edith Castillo Olsson

Título y/o Grado: Doctor

Doctor……(x)	Magister……..( )	Ingeniero……..( )	Otros……..especifique

Institución donde Labora: Universidad Cesar Vallejo Sede Lima Norte.

Autores: Farfan Rosales, Handerson Joel y Lopez Cordova, Rafael.

Fecha:08/07/2022

Nombre del instrumento motivo de evaluación:

Título de la investigación:

Comparación de las Blockchains aplicadas al IoT en relación al rendimiento y seguridad en la empresa Guimartbot SAC Lima 2022

II. ASPECTOS DE VALIDACIÓN:

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81- 100%
Claridad	Está formulado con el lenguaje apropiado.				80	
Objetividad	Está expresado en conducta observable			70		
Actualidad	Es adecuado al avance de la ciencia.			70		
Organización	Existe una organización lógica.				80	
Suficiencia	Comprende los aspectos de cantidad y calidad.			70		
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico.					90
Consistencia	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa				80	
Coherencia	Entre los índices, indicadores, dimensiones.					90
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr.				80	
Pertinencia	El instrumento es adecuado al tipo de investigación.				80	
Promedio de Validación				70	80	90

III. Promedio de Valoración: 80%

IV. Observaciones

Fuente: Elaboración propia

Tabla N.º 18: *Evaluación de expertos 3*

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES:

Apellidos y Nombre del Experto: Alfredo Daza Vergaray

Título y/o Grado:Doctor

Doctor.....(X)	Magister.....( )	Ingeniero.....( )	Otros.....especifique

Institución donde Labora: Universidad Cesar Vallejo Sede Lima Norte.

Autores: Farfan Rosales, Handerson Joel y Lopez Cordova, Rafael.

Fecha : 08/07/2022

Nombre del instrumento motivo de evaluación:

Título de la investigación :

Comparación de las Blockchains aplicadas al IoT en relación al rendimiento y seguridad en la empresa Guimartbot SAC Lima 2022

II. ASPECTOS DE VALIDACIÓN:

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81- 100%
Claridad	Está formulado con el lenguaje apropiado.					
Objetividad	Está expresado en conducta observable					
Actualidad	Es adecuado al avance de la ciencia.					
Organización	Existe una organización lógica.					
Suficiencia	Comprende los aspectos de cantidad y calidad.					
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico.					
Consistencia	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa					
Coherencia	Entre los índices, indicadores, dimensiones.					
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr.					
Pertinencia	El instrumento es adecuado al tipo de investigación.					
Promedio de Validación						

TABLA #14: Evaluación de expertos

Elaboración propia

III. Promedio de Valoración:

IV. Observaciones

Fuente: Elaboración propia

Tabla N.º 19: *Evaluación de expertos 4 parte 01*

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES:

Apellidos y Nombre del Experto: GONZALES SANCHEZ SANTIAGO RAUL

Título y/o Grado: DOCTOR EN MEDIO AMBIENTE Y DESARROLLO SOSTENIBLE

Doctor……(X)	Magister……..( )	Ingeniero……..( )	Otros……..especifique

Institución donde Labora: Universidad Cesar Vallejo Sede Lima Norte.

Autores: Farfan Rosales, Handerson Joel y Lopez Cordova, Rafael.

Fecha: 07.07.2022

Nombre del instrumento motivo de evaluación: Trabajo de Tesis

Título de la investigación:

Fuente: Elaboración propia

Tabla N.º 20: *Evaluación de expertos 4 parte 02*

II. ASPECTOS DE VALIDACIÓN:

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-50%	Bueno 51-70%	Muy bueno 71-80%	Excelente 81-100%
Claridad	Está formulado con el lenguaje apropiado.				75%	
Objetividad	Está expresado en conducta observable				75%	
Actualidad	Es adecuado al avance de la ciencia.			70%		
Organización	Existe una organización lógica.				75%	
Suficiencia	Comprende los aspectos de cantidad y calidad.				75%	
Intencionalidad	Adecuado para valorar aspectos del sistema metodológico y científico.			70%		
Consistencia	Está basado en aspectos teóricos, científicos acordes a			70%		

Fuente: Elaboración propia

Tabla N.º 21: *Evaluación de expertos 4 parte 03*

	la tecnología educativa					
Coherencia	Entre los índices, indicadores, dimensiones.				**75%**	
Metodología	Responde al propósito del trabajo bajo los objetivos a lograr.					**80%**
Pertinencia	El instrumento es adecuado al tipo de investigación.				**75%**	
Promedio de Validación				**70%**	**75%**	**80%**

III. **Promedio de Valoración: 75%**
IV. **Observaciones:**

Fuente: Elaboración propia

Anexo 16: Diseño Front-end en Figma

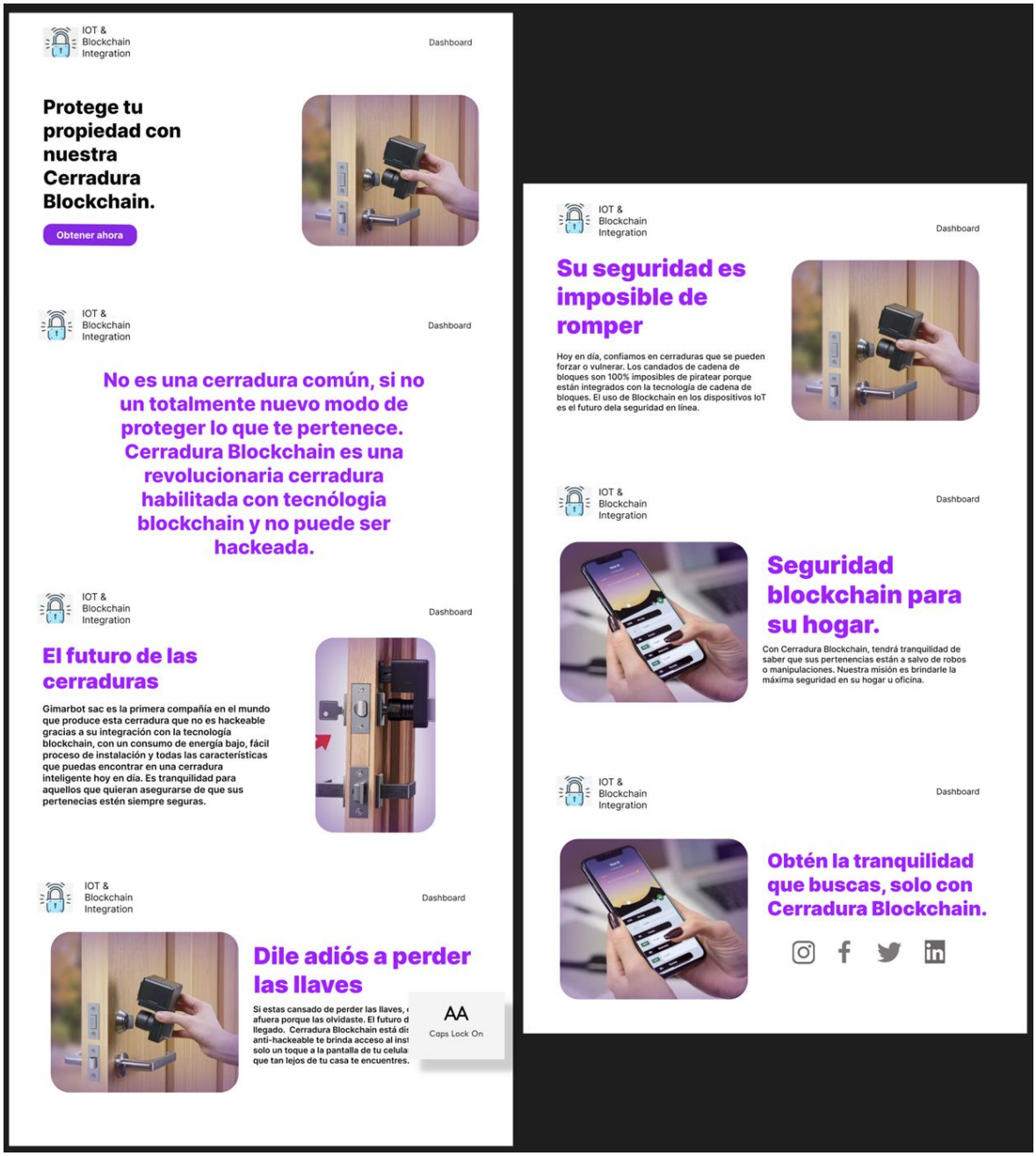


Figura N.º 39: Diseño del Front-End
Fuente: Elaboración propia

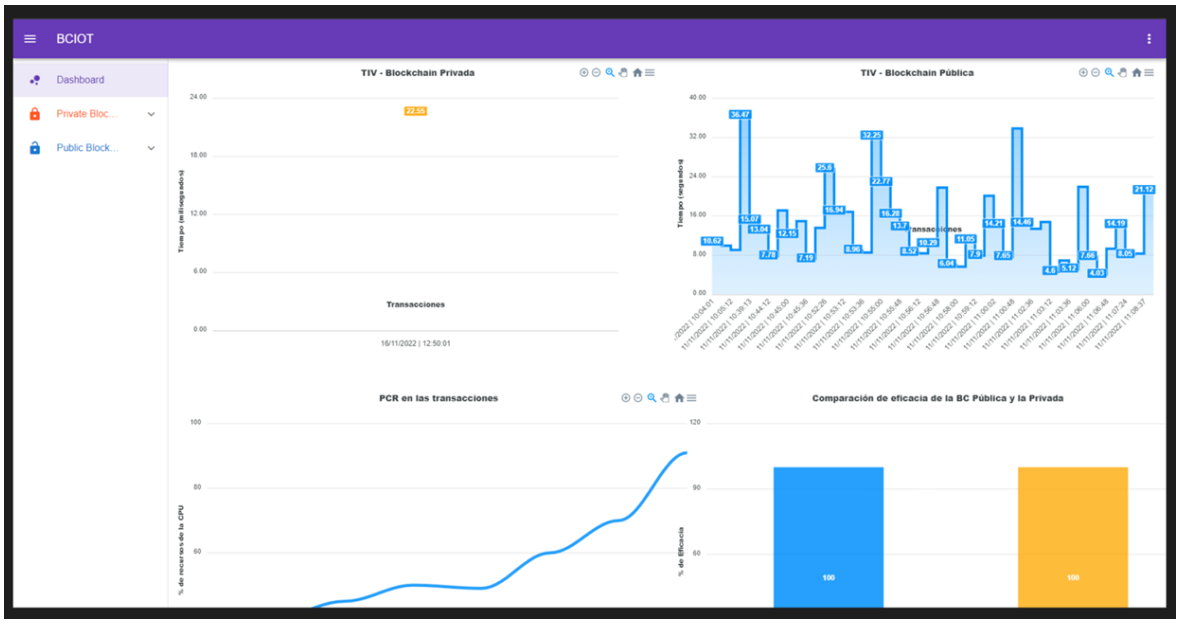


Figura N.º 40: Diseño del Front-End Dashboard
Fuente: Elaboración propia

Anexo 17: Estructura de rutas - Back-end

Figura N.º 41: Estructura de la API
Fuente: Elaboración propia

Anexo 18: Smart Contracts

Código Smart contract LED

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract LedIoT {

    string public commandLED;
    event manejarLED(string commandLED);

    function enviarcommandLED(string memory _commandLED) public {
        commandLED = _commandLED;
        emit manejarLED(_commandLED);
    }

    function getcommandLED() public view returns(string memory){
        return commandLED;
    }
}
```

Código Smart contract Cerradura

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract lockIoT {

    string public commandLOCK;
    event manejarLOCK(string commandLOCK);

    function enviarcommandLOCK(string memory _commandLOCK) public {
        commandLOCK = _commandLOCK;
        emit manejarLOCK(_commandLOCK);
    }

    function getcommandLOCK() public view returns(string memory){
        return commandLOCK;
    }
}
```

Código Smart contract Smart light (Foco inteligente)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract smartLight {

    string public commandSML;
    event manejarSML(string commandSML);

    function enviarcommandSML(string memory _commandSML) public {
        commandSML = _commandSML;
        emit manejarSML(_commandSML);
    }

    function getcommandSML() public view returns(string memory){
        return commandSML;
    }
}
```

Anexo 19: Prueba de la BC privada

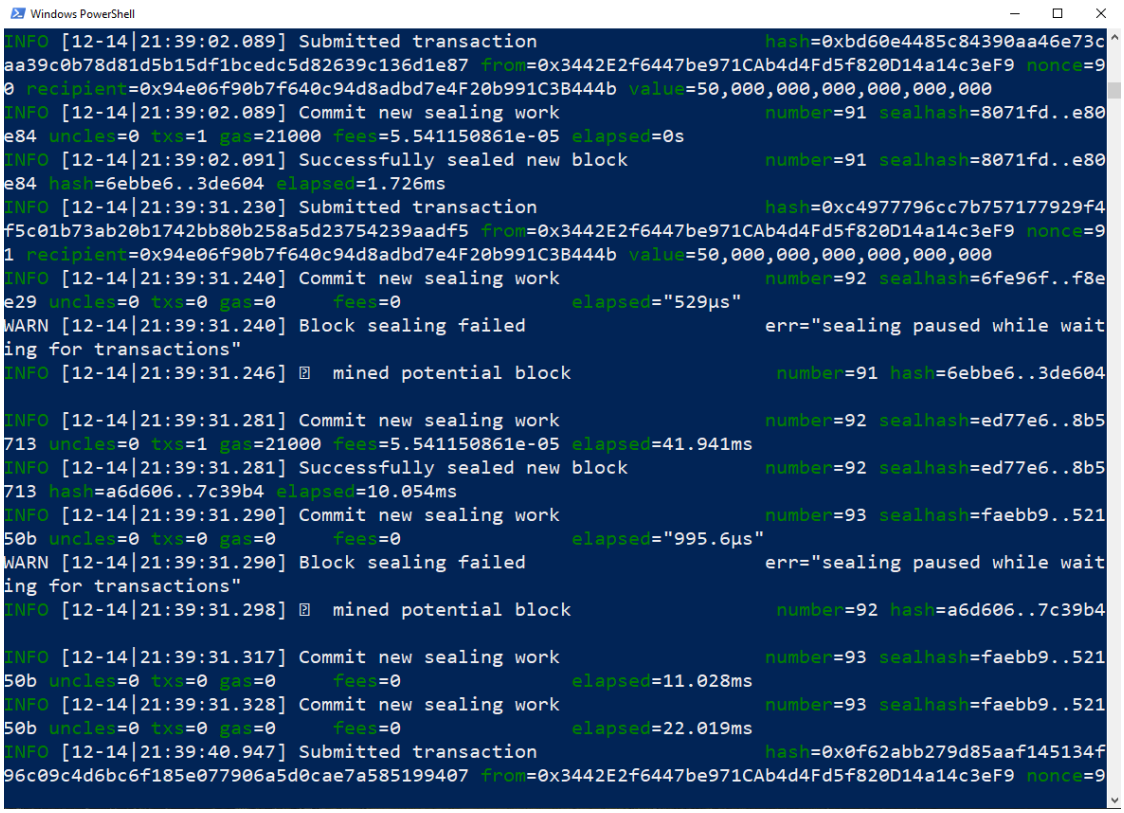


Figura N.º 42: Prueba de las transacciones en la BC privada
Fuente: Elaboración propia

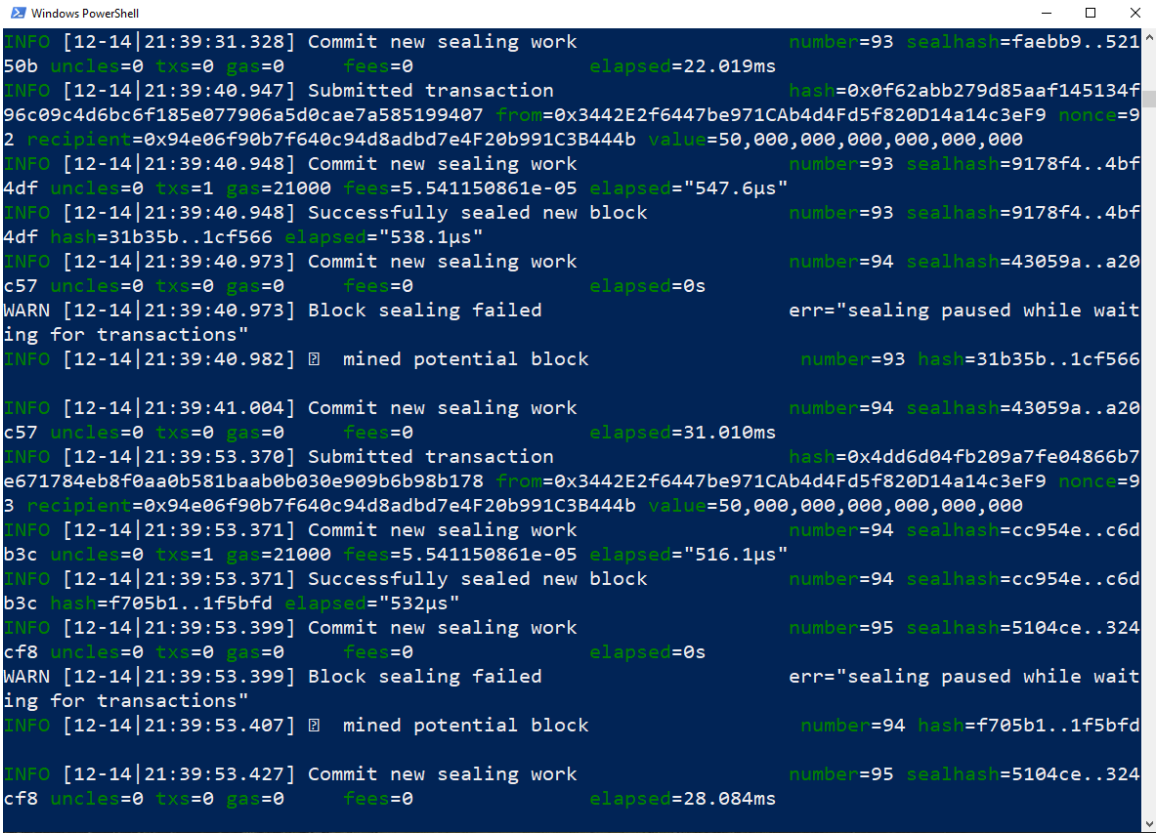


Figura N.º 43: Prueba de las transacciones en la BC privada
Fuente: Elaboración propia

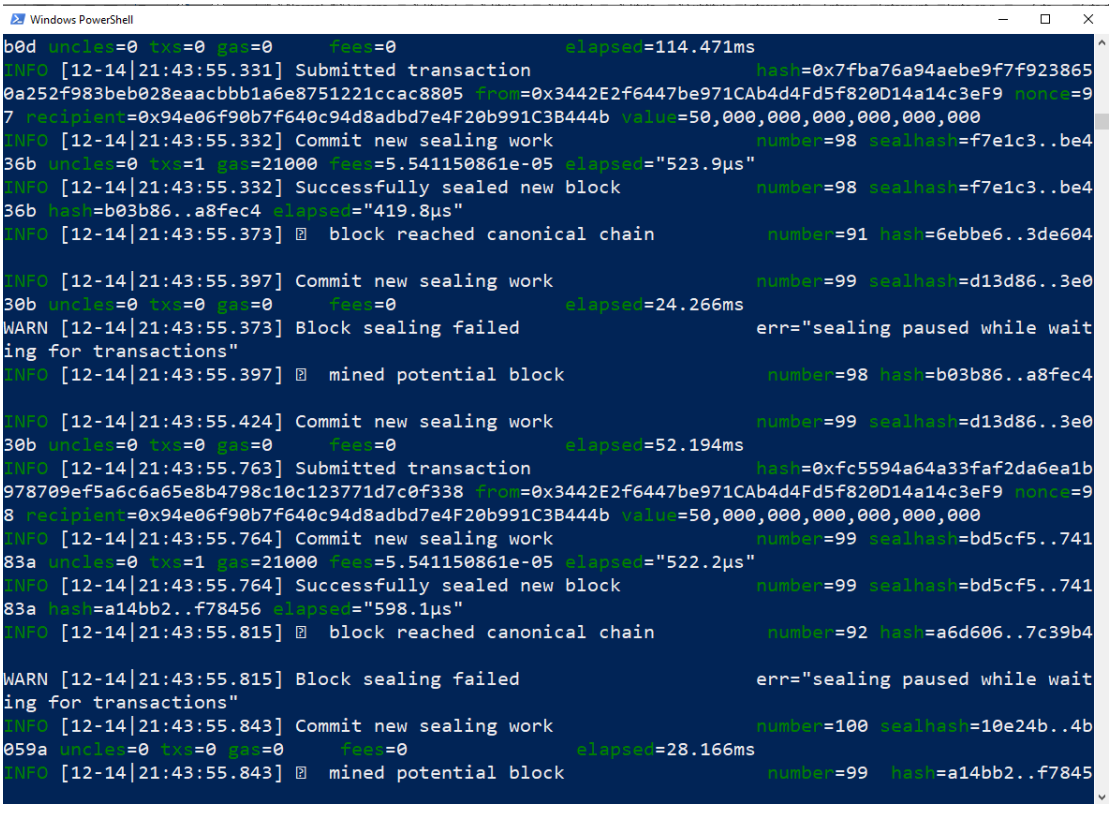


Figura N.º 44: Prueba de las transacciones en la BC privada
Fuente: Elaboración propia

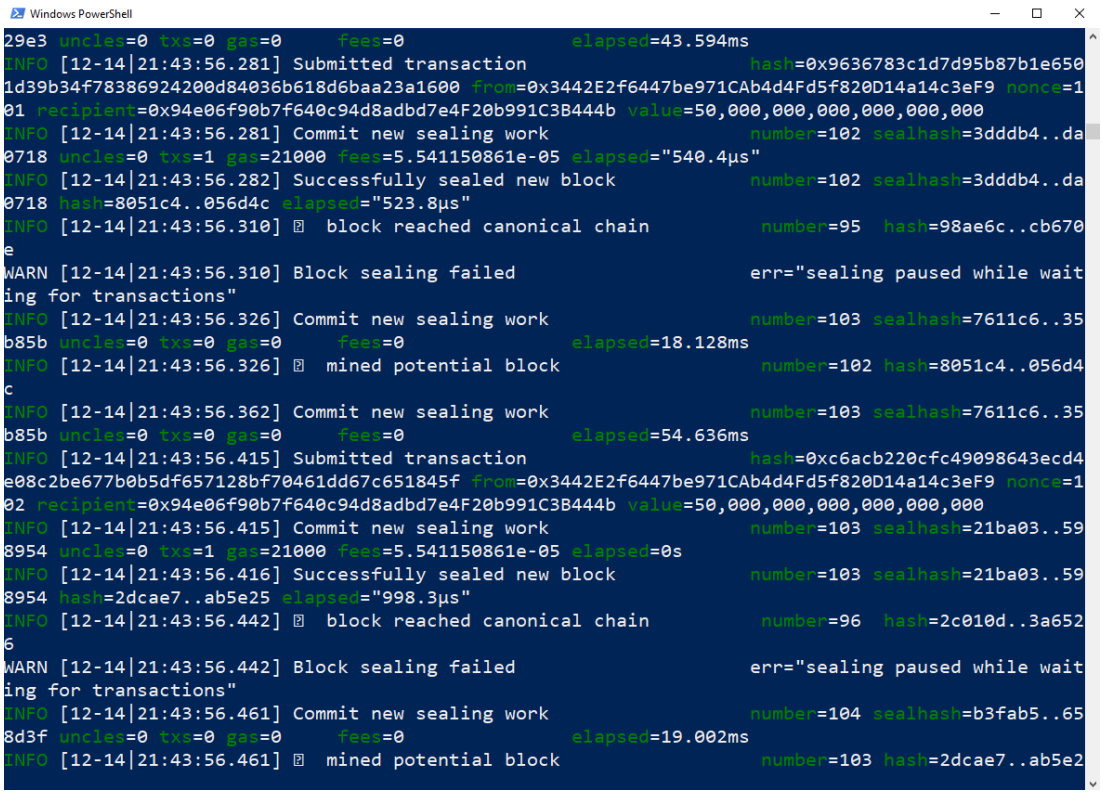


Figura N.º 45: Prueba de las transacciones en la BC privada
Fuente: Elaboración propia

Anexo 20: Interfaz

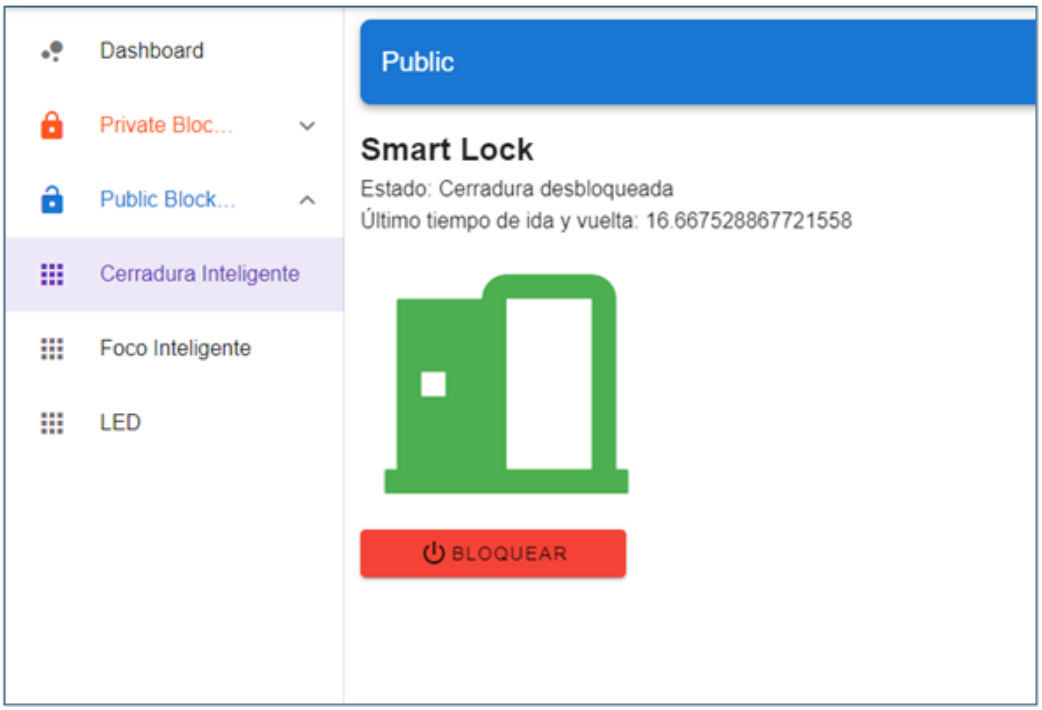


Figura N.º 46: Interfaz - Cerradura blockchain Publica
Fuente: Elaboración propia

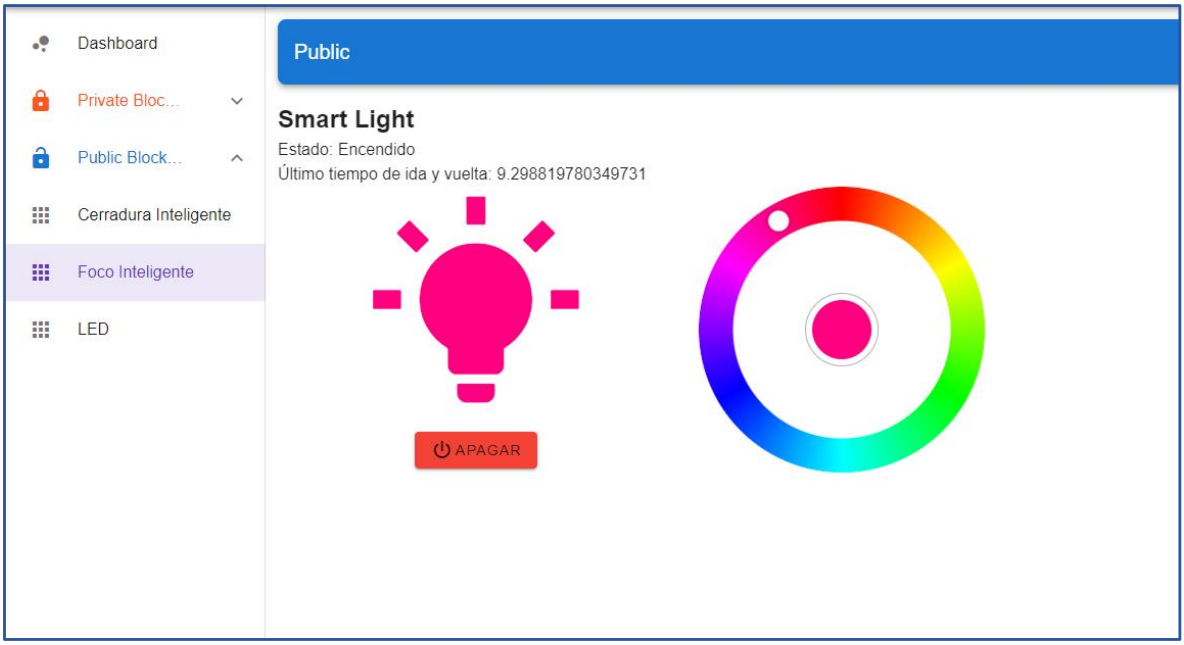


Figura N.º 47: Interfaz – Smart Light blockchain Publica
Fuente: Elaboración propia

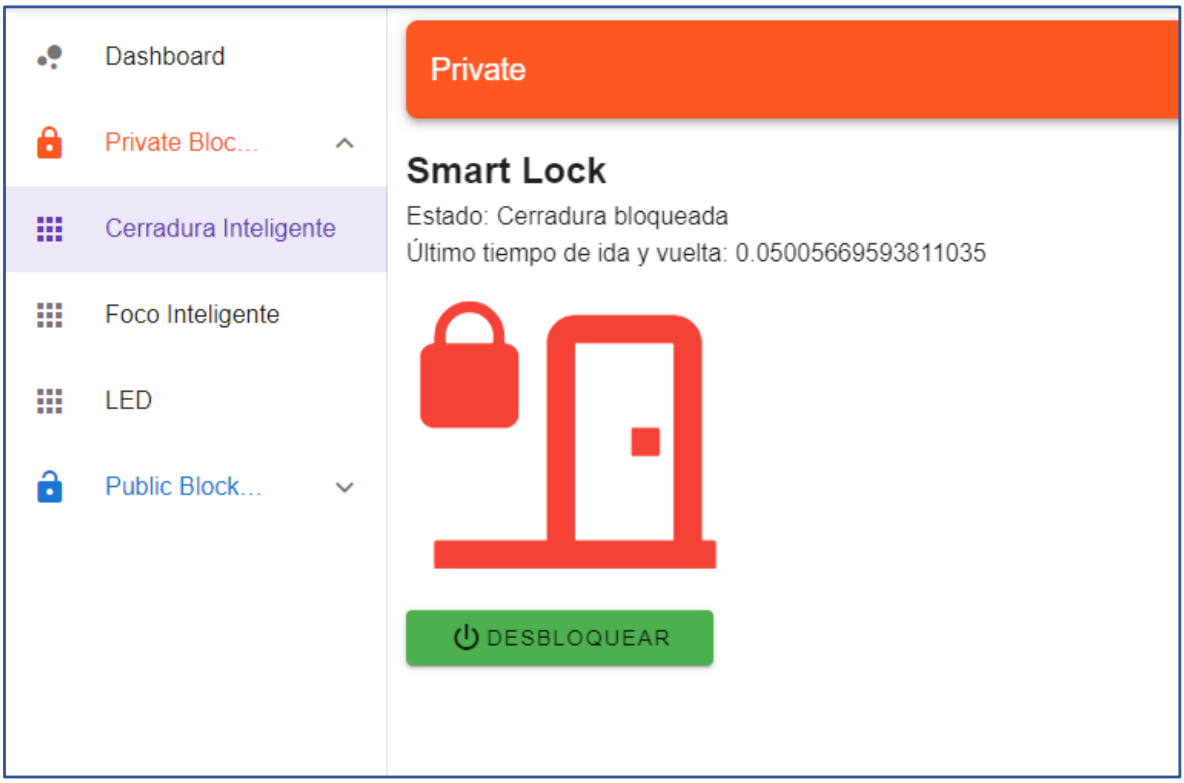


Figura N.º 48: Interfaz - Cerradura blockchain Privada
Fuente: Elaboración propia

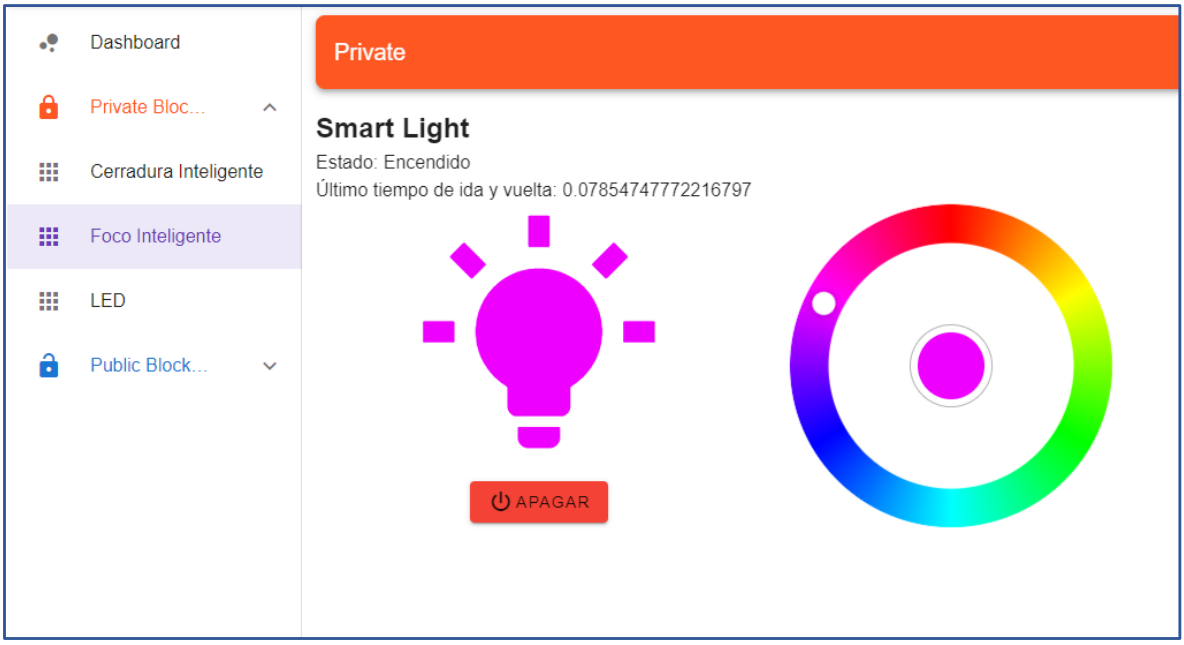


Figura N.º 49: Interfaz – Smart Light blockchain Publica
Fuente: Elaboración propia

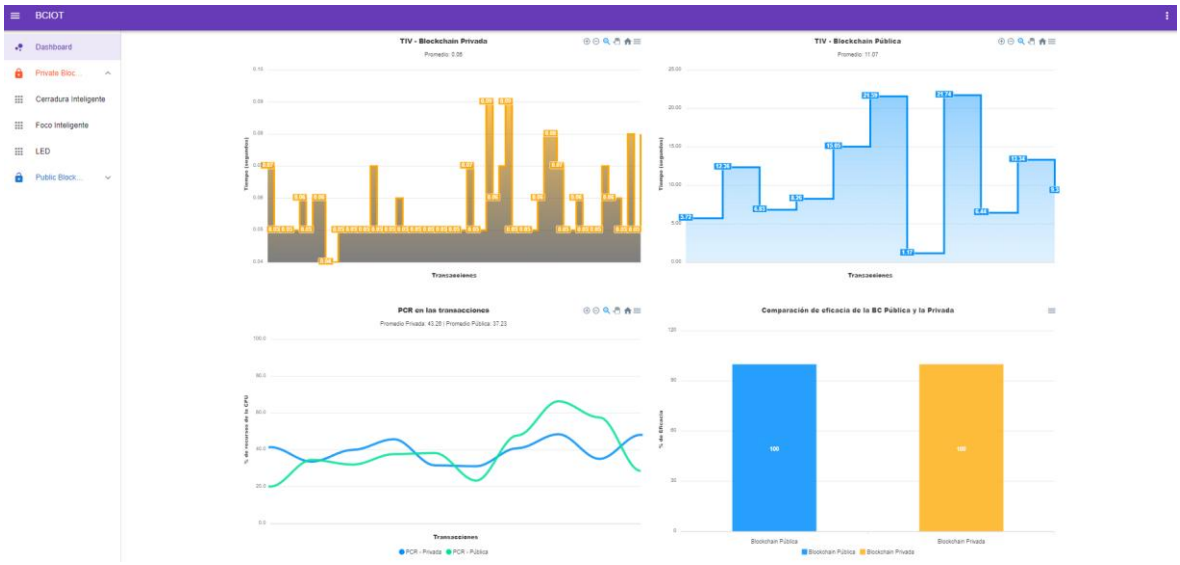


Figura N.º 50: Interfaz - Comparación blockchain Publica - Privada
Fuente: Elaboración propia

Anexo 21: Metodología de desarrollo

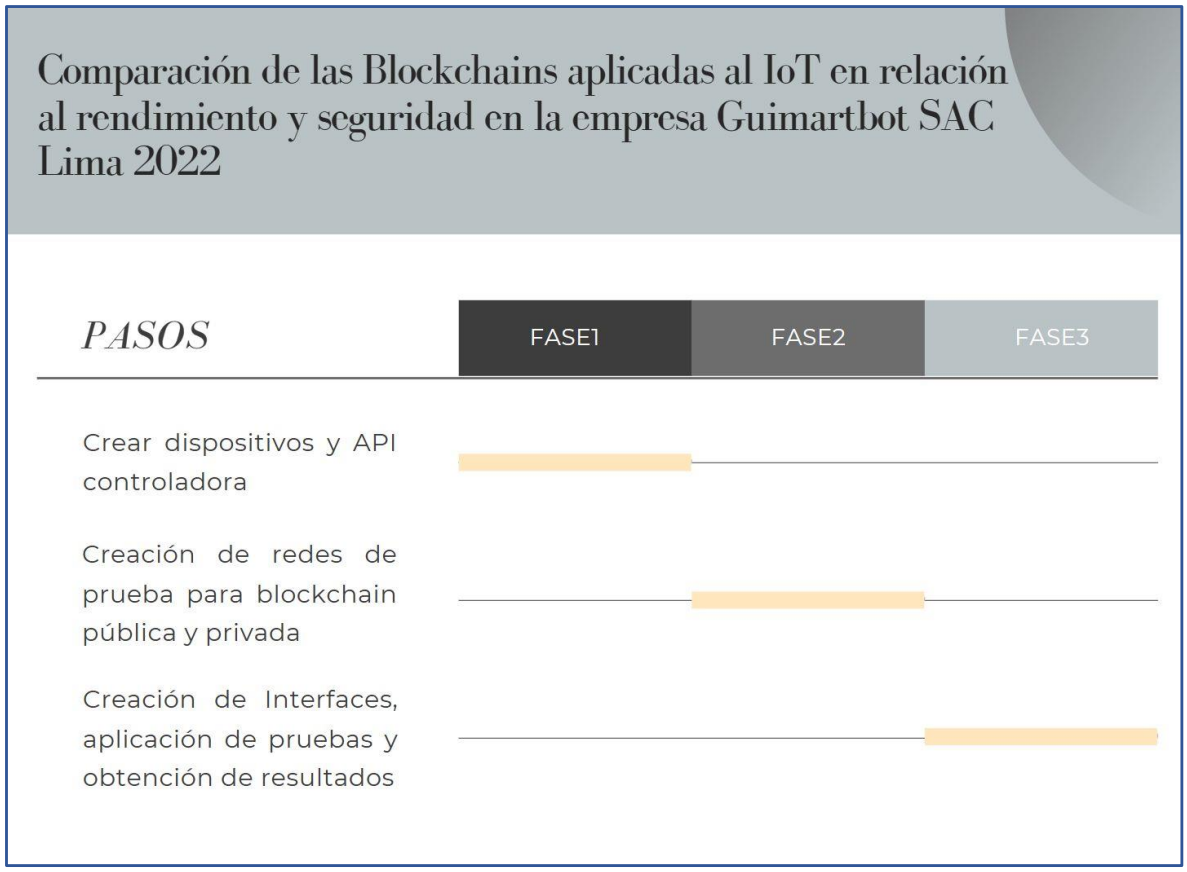


Figura N.º 51: Flujograma de la Metodología utilizada para el desarrollo de esta investigación
Fuente: Elaboración propia

En la primera fase se crearon los dispositivos IoT y también se creó un controlador de API, el cual es responsable por proporcionar servicios de comunicación para aplicación y controlar tanto los recursos físicos de dos dispositivos IoT como los recursos de sistema web. Este fue el encargado de distribuir y brindar acceso a las rutinas de servicios basados en aplicación y los de infraestructura de hardware.

En la segunda fase se diseñaron las redes de prueba. Estas permitieron la simulación de la MAIN NET de Ethereum, donde se desplegaron los Smart Contracts para los dispositivos IoT tanto en la BC privada (creada localmente), como en la pública (en una red de pruebas llamada Infura).

En la tercera fase, se realizó la creación de interfaces de usuario, es una de las más importantes de las tareas que se realiza en un proyecto de desarrollo de software. Si esta tarea se hace bien, el producto terminado tendrá una interfaz

amigable que asegurará que los usuarios puedan interactuar con su software fácilmente y rápidamente. Si se hace mal, existen problemas de usabilidad y el producto no tendrá un buen rendimiento. Luego se aplicaron las pruebas que se habían preparado con anterioridad en los Instrumentos de observación mostrados en la tabla N.º 12,13,14 y 15 para que al final se obtengan los resultados a analizar en los mismos.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, DAZA VERGARAY ALFREDO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Comparación de las Blockchains aplicadas al IoT en relación al rendimiento y seguridad en la empresa Guimartbot SAC Lima 2022", cuyos autores son FARFAN ROSALES HANDERSON JOEL, LOPEZ CORDOVA RAFAEL, constato que la investigación tiene un índice de similitud de 10.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 18 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
DAZA VERGARAY ALFREDO **DNI:** 40466240 **ORCID:** 0000-0002-2259-1070	Firmado electrónicamente por: ADAZAVE el 18-12-2022 22:11:08

Código documento Trilce: TRI - 0494456

INVESTIGA UCV