ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

DESARROLLO DE UNA DAPP CON TECNOLOGÍA BLOCKCHAIN PARA LA VERIFICACIÓN DE DOCUMENTOS ELECTRÓNICOS. CASO PRÁCTICO: GRANJA AVÍCOLA IVANNA.

Trabajo de Titulación

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN SOFTWARE

AUTOR:

KEVIN ANDRES GALLARDO ESPINOZA

Riobamba – Ecuador

2023

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

DESARROLLO DE UNA DAPP CON TECNOLOGÍA BLOCKCHAIN PARA LA VERIFICACIÓN DE DOCUMENTOS ELECTRÓNICOS. CASO PRÁCTICO: GRANJA AVÍCOLA IVANNA.

Trabajo de Titulación

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN SOFTWARE

AUTOR: KEVIN ANDRES GALLARDO ESPINOZA

DIRECTOR: DR. DANILO MAURICIO PASTOR RAMIREZ

Riobamba – Ecuador

2023

Yo, KEVIN ANDRES GALLARDO ESPINOZA, declaro que el presente Trabajo de Titulación es de mi autoría y los resultados de este son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 23 de junio de 2023

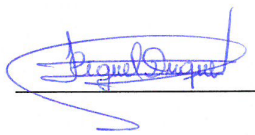
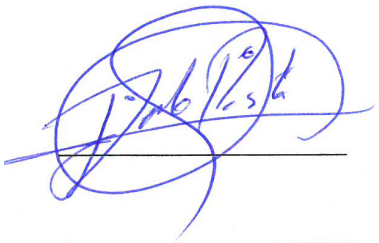
Kevin Andrés Gallardo Espinoza
070573480-4

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA SOFTWARE

El Tribunal de Trabajo de Titulación certifica que: El Trabajo Titulación: **DESARROLLO DE UNA DAPP CON TECNOLOGÍA BLOCKCHAIN PARA LA VERIFICACIÓN DE DOCUMENTOS ELECTRÓNICOS. CASO PRÁCTICO: GRANJA AVÍCOLA IVANNA**, realizado por el señor: **KEVIN ANDRES GALLARDO ESPINOZA,** ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Ing. Miguel Angel Duque Vaca **PRESIDENTE DEL TRIBUNAL**		23-JUN-2023
Dr. Danilo Mauricio Pastor Ramírez **DIRECTOR DEL TRABAJO DE TITULACIÓN**		23-JUN-2023
Ing. Marco Vinicio Ramos Valencia **ASESOR DEL TRABAJO DE TITULACIÓN**		23-JUN-2023

DEDICATORIA

El presente trabajo va dedicado a mis padres como resultado de todo su amor y sacrificio que me han entregado en esta etapa de mi vida, este logro no hubiese sido posible sin su ayuda. Y finalmente, a la persona más importante en mi vida, mi hijo Israel, quién se ha convertido en mi motor y mi fuerza para lograr mis metas.

Kevin

AGRADECIMIENTO

Agradecer primeramente a Dios por permitirme llegar a una de mis metas académicas. Gracias a mis padres y hermana por el apoyo incondicional, el esfuerzo y la confianza que han puesto en mí. También agradezco a mi pareja por todo el apoyo y su compañía durante esta etapa. Agradezco a los docentes que han sido parte de mi formación académica, a mis compañeros y amigos por hacer de ésta una experiencia única.

Kevin

ÍNDICE DE CONTENIDO

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

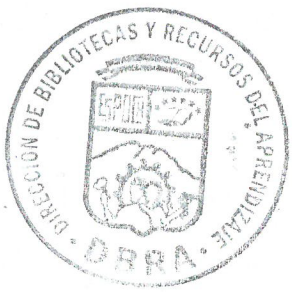
ÍNDICE DE ILUSTRACIONES

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo enfocó en el desarrollo de una Dapp para verificar la autenticidad de documentos electrónicos para la empresa "Granja Avícola Ivanna", con la finalidad de verificar la autenticidad de sus documentos. En el proceso de desarrollo se comparó la funcionalidad de las aplicaciones convencionales y Dapp dónde la principal diferencia es la descentralización y el almacenamiento de información. Luego de analizar su funcionamiento y con el objetivo de generar su arquitectura, en este proceso se evaluaron diferentes redes Blockchain dónde se utilizó Ethereum Goerli como red para el funcionamiento de la Dapp. Para evaluar la seguridad de la Dapp, se utilizó la norma ISO 25010:2011 y se midió el grado de cumplimiento para las subcategorías de confidencialidad, integridad y autenticidad. Se obtuvo un grado de cumplimiento admisible del 87.5% para confidencialidad e integridad, lo que indica que la Dapp cumple con los criterios establecidos para estas subcategorías. En cuanto a autenticidad, se obtuvo un grado de cumplimiento admisible del 62.5%, lo que sugiere que hay margen de mejora en esta subcategoría. La evaluación de la seguridad del producto según la norma ISO 25010:2011 mostró que la Dapp cumple con los criterios de confidencialidad e integridad, y que hay margen de mejora en la subcategoría de autenticidad.

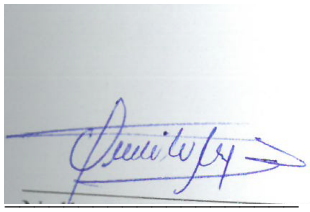
Palabras clave: <APLICACIONES DESCENTRALIZADAS>, <BLOCKCHAIN>, <ETHEREUM>, <GOERLI>, <SEDURIDAD DE LA INFORMACIÓN>, <NORMA ISO 25010>, <AUTENTICIDAD>, <CONFIDENCIALIDAD>.



SUMMARY

The present work focused on the development of a Dapp to verify the authenticity of electronic documents for the company "Granja Avicola Ivanna", in order to verify the authenticity of its documents. In the development process, the functionality of conventional and Dapp applications was compared, where the main difference is decentralization and information storage. After analyzing its operation and with the objective of generating its architecture, in this process different Blockchain networks were evaluated where Ethereum Goerli was used as a network for the operation of the Dapp. To evaluate the security of the Dapp, the ISO 25010:2011 standard was used and the degree of compliance was measured for the subcategories of confidentiality, integrity and authenticity. An admissible degree of compliance of 87.5% was obtained for confidentiality and integrity, which indicates that the Dapp meets the criteria established for these subcategories. Regarding authenticity, an admissible degree of compliance of 62.5% was obtained, which suggests that there is room for improvement in this subcategory. The product security assessment according to ISO 25010:2011 showed that the Dapp meets the confidentiality and integrity criteria, and that there is room for improvement in the authenticity subcategory.

Keywords: <DECENTRALIZED APPLICATIONS>, <BLOCKCHAIN>, <ETHEREUM>, <GOERLI>, <INFORMATION SECURITY>, <ISO 25010 STANDARD>, <AUTHENTICITY>, <CONFIDENTIALITY>



Nelly Padilla P. Mgs
0603818717
DOCENTE FIE

INTRODUCCIÓN

En la actualidad, la gestión de documentos electrónicos se ha vuelto cada vez más común en diversos campos debido a su importancia en transacciones financieras, registros médicos y certificaciones académicas. A pesar de esto, la vulnerabilidad a la alteración y la falsificación de estos documentos puede comprometer su validez e integridad. Por tanto, la tecnología Blockchain se presenta como una solución prometedora que proporciona una capa adicional de seguridad a los documentos electrónicos, creando registros inmutables y descentralizados que no pueden ser modificados o falsificados sin dejar un rastro visible. Además, su descentralización elimina la necesidad de una autoridad central para verificar la autenticidad de los documentos, lo que hace que sea más resistente a la corrupción y el fraude.

En particular, la industria avícola ha tomado interés en la utilización de Blockchain para garantizar la autenticidad de los registros y cumplir con los requisitos legales. Las aplicaciones descentralizadas basadas en Blockchain, conocidas como Dapps, han surgido como una alternativa atractiva para mejorar la seguridad y la transparencia en la gestión de documentos electrónicos.

Por lo tanto, el objetivo principal es desarrollar una dApp para verificar la autenticidad de los documentos electrónicos de la empresa "Granja Avícola Ivanna" y evaluar su seguridad según los estándares internacionales establecidos. Esta solución innovadora utiliza la tecnología Blockchain para garantizar la autenticidad y la seguridad de los documentos electrónicos y las Dapps basadas en Blockchain ofrecen una alternativa interesante para mejorar la gestión de estos documentos en el ámbito empresarial.

CAPÍTULO I

1. DIAGNÓSTICO DEL PROBLEMA

1.1. Antecedentes

Según el libro "Smart legal Contracts y Blockchain" publicado en julio del 2019 nos dice que en la actualidad la tecnología de Blockchain resulta ser la tecnología más disruptiva por su potencial de automatización a gran escala y por su capacidad de permear en numerosos ámbitos de la vida de las personas. Estas cadenas de bloques surgen de la combinación y aplicación conjunta de numerosas herramientas tecnológicas existentes, puede decirse que no constituye una tecnología nueva sino más bien una nueva expresión de la ya existente (Vilalta, 2019).

Entonces para poder entender cómo funciona una solución Blockchain podemos apoyarnos en el aporte del libro "Blockchain", dónde se conoce como Blockchain al conjunto de soportes o máquinas que implementan ese software y donde se desenvuelve su funcionamiento; y, sobre todo, a la propia red interconectada de los nodos, puntos de conexión o máquinas, que, gestionadas por personas o, en su caso, por otras máquinas de forma automática (en última instancia, claro, bajo control de personas físicas o jurídicas) configuran una red, plataforma o espacio de intercambio de información para vincular bloques o series de datos enlazados criptográficamente (Ibáñez, 2018).

La Blockchain surgió en el sector de servicios financieros como plataforma descentralizada para soportar criptomonedas como el bitcoin, pero su evolución permite conectar a las partes de cualquier negociación mediante nuevos modos para hacer contratos inteligentes. Ya que es un libro mayor distribuido, elimina el requerir a organizador oficial, reduciendo costes, retrasos y complejidad, teniendo así el potencial de soportar múltiples usos en diferentes sectores en los que la confianza de un intermediario central resulta costosa, lenta y vulnerable a los ataques (García, 2018).

De acuerdo con Windley (2014), menciona que la identidad en Internet está rota. Hay demasiadas fugas de privacidad. Demasiados negocios y casos que están siendo pobremente atendidos por las soluciones actuales.

La identidad digital en la actualidad, la privacidad tanto como la veracidad de la información son muy importantes, tanto que se convierten en información sensible que en situaciones son puntos

débiles donde se puede dar alteraciones de información no solo de manera digital sino también de manera física.

Dada esta situación se puede recurrir a alguna tecnología para solucionar este inconveniente como por ejemplo una Blockchain, la cual permite tenerse basa en integrar ficheros informáticos, relacionados matricialmente por identificadores o códigos, conforme combinaciones producidas con cálculos, en varios ordenadores y de formatos idénticos en todos (Ibáñez, 2016).

En cuanto a las ventajas que plantea la Blockchain podemos destacar, fundamentalmente, su inmutabilidad como registro de datos. Ello puede otorgarle, en principio, una función registral muy segura jurídicamente hablando, sin la necesidad de que exista una autoridad central superior que autorice, compruebe y efectúe la transacción de que se emplee. Asimismo, proporciona gran seguridad en la transmisión de datos gracias a la criptografía, se reducen los riesgos de robo o filtración de la información en gran medida gracias al anonimato y codificación de las transacciones, se reducen los costes de transacción y se produce la liquidación de estas en tiempo real; además, se elimina el error humano y existe un aumento de la transparencia y fiabilidad de las operaciones (Martín, 2021).

Con base en los antecedentes, la "Granja Avícola Ivanna" es una empresa dedicada a la producción y comercialización de aves de corral. Como muchas empresas en la actualidad, Ivanna maneja gran cantidad de información digital, incluyendo documentos electrónicos como facturas, recibos, certificados, entre otros. Esta información es esencial para el correcto funcionamiento de la empresa, ya que es necesaria para llevar un registro preciso de los procesos productivos y las transacciones comerciales.

Sin embargo, Ivanna se ha enfrentado a problemas de seguridad en su manejo de la información. Los documentos digitales no están adecuadamente protegidos y existe la posibilidad de que sean alterados o falsificados sin dejar rastro. Esto representa un riesgo para la integridad de la información y puede llevar a pérdidas económicas importantes para la empresa. Además, la falta de transparencia en el manejo de la información también puede afectar la confianza de los clientes en la empresa y su reputación en el mercado.

Ante esta situación, se hace necesaria la implementación de medidas que permitan garantizar la seguridad y autenticidad de los documentos electrónicos en Ivanna. La tecnología Blockchain surge como una solución efectiva para prevenir la alteración y falsificación de los documentos, a través de la creación de registros inmutables y descentralizados. La implementación de una aplicación descentralizada basada en Blockchain permitirá a Ivanna mejorar la seguridad y

transparencia en el manejo de la información, y aumentar la confianza de sus clientes y proveedores en la empresa a través de la verificación de su información.

1.2. Formulación del problema

¿Cómo se puede asegurar documentos electrónicos utilizando tecnología Blockchain?

1.3. Sistematización del problema

¿Cómo es el funcionamiento de una aplicación descentralizada con tecnología Blockchain?

¿Cuál es el tipo de Blockchain apropiado para el progreso de la aplicación descentralizada?

¿Qué herramientas se encuentran disponibles para el crecimiento de la aplicación descentralizada?

¿Cómo las aplicaciones descentralizadas pueden verificar la autenticidad de un documento electrónico?

1.4. Justificación del trabajo de titulación

1.4.1. Justificación teórica

La rectitud, accesibilidad y confidencialidad, son imprescindibles para los usuarios debido a que, las personas no se sienten seguras al revelar tanta información personal (Sullivan, y otros, 2017). Acorde con este autor se puede manifestar que en el manejo de las identidades digitales el principal desafío es la certeza de la investigación.

En la actualidad, la automatización de procesos se está volviendo cada vez más común por varias razones, como la creciente exigencia de los usuarios por niveles más altos de satisfacción, la competencia más dura en el mercado y la rápida evolución tecnológica que ofrece numerosas herramientas y oportunidades para la innovación. Esto ha llevado a una tendencia hacia la mecanización de procesos en muchas áreas (Rosero, 2019).

Dentro del mundo empresarial se maneja una gran cantidad de información reflejada en documentos físicos o electrónicos. Los cuales representan un riesgo de alta prioridad dentro de la empresa al ser sujeto de alteración, eliminación. En la actualidad existen muchas alternativas para

mitigar este riesgo, cómo lo es la digitalización de documentos físicos, el almacenamiento en la nube, o a su vez dentro de sistemas informáticos centralizados dónde se guarda gran cantidad de información. Estas innovaciones tecnológicas representan un gran avance para las empresas, pero el riesgo no se ha corregido en su totalidad, esto debido que la información hasta cierto punto asegurada seguirá desatando métodos, y tecnologías para poder ser obtenida. La tecnología Blockchain se presenta como una alternativa de seguridad que resuelve esta problemática desde un entorno descentralizado, dónde la información está en distribuida en su totalidad.

Una de las ventajas que proporciona el registrar información con la tecnología Blockchain es la inmutabilidad, ya que una vez almacenados los datos en la Blockchain estos se distribuyen por toda la red, una red hasta cierto punto desconocida porque se basa en una arquitectura descentralizada, distribuida en nodos. La información puede ser consultada dentro de estos nodos o bloques y verificar su autenticidad e inmutabilidad.

La seguridad y autenticidad de la información son aspectos críticos para cualquier empresa, especialmente en la industria avícola donde la calidad y seguridad de los productos son de gran importancia para la salud pública y el cumplimiento de regulaciones y leyes. Los documentos digitales, como facturas, recibos, certificados, entre otros, son cada vez más comunes en el mundo empresarial, y su integridad es esencial para garantizar la transparencia y confianza en las transacciones comerciales.

Sin embargo, estos documentos pueden ser vulnerables a manipulaciones y alteraciones, lo que puede poner en riesgo la integridad y seguridad de la información. La tecnología blockchain surge como una solución prometedora para garantizar la integridad y autenticidad de los documentos digitales, gracias a su capacidad de crear registros descentralizados e inmutables.

Por lo tanto, este proyecto es importante porque busca aplicar la tecnología blockchain en la industria avícola para mejorar la seguridad y confiabilidad en el manejo de documentos electrónicos, lo que puede tener un impacto significativo en la calidad y seguridad de los productos avícolas, así como en el cumplimiento de regulaciones y leyes. Además, la investigación en este tema puede proporcionar una base teórica para el uso de blockchain en otras industrias y sectores que requieren de la integridad y autenticidad de la información.

1.4.2. Justificación aplicativa

La empresa avícola actualmente no cuenta con un sistema o base de datos específico para registrar sus documentos importantes, como facturas, guías de remisión, planes de vacunación, certificados, pagos, fotografías, permisos, fórmulas e informes. Estos documentos se almacenan en diferentes plataformas como equipos de cómputo, correos electrónicos, redes sociales, e incluso algunos documentos se mantienen en papel y son archivados de forma manual. Esta falta de un sistema específico expone estos documentos a riesgos de vulnerabilidad, alteración o pérdida.

Para abordar esta problemática y garantizar la integridad y autenticidad de los documentos electrónicos de la empresa avícola, se propone desarrollar una aplicación descentralizada utilizando la tecnología Blockchain. La aplicación permitirá agregar todos los datos importantes que entran y salen del negocio a la red Blockchain, lo que permitiría verificar su autenticidad y mejorar la seguridad y veracidad de la información en los procesos de la empresa.

La tecnología Blockchain ofrece múltiples ventajas para mejorar los procesos en diferentes áreas, incluyendo la salud, la educación y la administración pública, protegiendo el recurso más importante que es la información. Por lo tanto, se plantea la elaboración de un proyecto técnico que contemple el desarrollo de una Dapp dónde Entre los módulos más importantes en esta aplicación descentralizada tenemos:

- Autenticación de usuarios
- Cargar documentos
- Visualización de documentos
- Validación de documentos

De esta forma, se podrá asegurar la autenticidad de los documentos de la empresa avícola y mejorar la eficiencia y seguridad en sus procesos.

El siguiente proyecto está basado con las líneas de investigación de EIS en las líneas trasversales en programa de Ingeniería de software en el ámbito de mantenimiento y evolución del software. En las líneas de ESPOCH se ubica en el eje de TICS en la línea de investigación de líneas trasversales – técnicas de la investigación y comunicación en donde el proyecto de ingeniería de software.

En tanto que en el PND se ubica en coordenada 2, ahorro y provecho de la colectividad con el objetivo 5 que es Promocionar el rendimiento y capacidad para el desarrollo económico sustentable de modo distributivo y altruista fundándose en la política: 5.6 que es fomentar el estudio, la enseñanza, la preparación, el crecimiento y la transmisión tecnológica, la mejora y el acometimiento, la defensa de la posesión intelectual, para incitar la renovación de la principal productividad mediante la asociación a través de la administración pública, productiva y las escuelas universitarias.

1.5. Objetivos

1.5.1. General

Desarrollar una DAPP con tecnología Blockchain para la verificación de documentos electrónicos.

1.5.2. Específicos

- Analizar la operatividad de las aplicaciones descentralizadas que utilizan tecnología Blockchain.

- Seleccionar el tipo de red Blockchain adecuado para el progreso de la aplicación descentralizada.

- Implementar los módulos de las aplicaciones descentralizadas que permitan la comprobación de los documentos.

- Evaluar la seguridad de las aplicaciones descentralizadas mediante la norma ISO 25010:2011 respecto a las subcaracterísticas de integridad, autenticidad y confidencialidad.

CAPÍTULO II

2. FUNDAMENTOS TEÓRICOS

2.1. Blockchain

La llamada “cadena de bloques” es un protocolo criptográfico, usado inicialmente para crear la divisa Bitcoin. En pocas palabras, se fundamenta en incorporar archivadores electrónicos, afines matricialmente por cifrado o codificación (por ejemplo, clave alfanumérica), conforme composiciones ocasionadas con cálculos, en diversos ordenadores y de modo idéntico por completo. Ya que una cifra competente de internautas participa en el sistema, admite la irreversible, perfecta y simultánea caracterización del contenido asociado a aquellos archivos (Ibáñez, 2016).

Dicho de otra manera, blockchain es cotejar con una central de reseñas como se lo concreta a continuidad: Una sucesión de unidades es esencialmente una sede de documentos distribuida de registros en representación de "bloques" cifrados (conjuntos de datos más pequeños), o un libro público de las transacciones o eventos digitales que se ejecutan y comparten entre las partes participantes, y que pueden ser verificados en alguna ocasión en el futuro. Cada transacción en el libro público se verifica por aprobación del mayor número de los colaboradores en el sistema. Una vez interpuesta, la pesquisa jamás consigue ser eliminada. La sucesión de componentes contiene un registro cierto y demostrable de cada transacción realizada y sus bloques pueden ser utilizados para coordinar una acción o verificar un evento (Galvez et al., 2018).

Según algunos escritores, la tecnología blockchain es considerada como el invento más significativo en el ámbito tecnológico desde la creación de Internet. Por otra parte, para Rosero (2019) establece ya sea debido a su capacidad para transformar la forma en que la sociedad lleva a cabo transacciones e interactúa sin la necesidad de una tercera parte que garantice la seguridad, o gracias a los beneficios intrínsecos que ofrece, como la inmutabilidad, la auditabilidad, la moralidad de las transacciones y la autenticación, la tolerancia a fallos, entre otros, la tecnología Blockchain es altamente valorada. De la misma manera para Makhdoom et al. (2020) alude que lo verídico es que este conjunto de técnicas va ganando interés en diversas áreas en donde podría ser aplicada entre las que se incluyen el almacenamiento distribuido en el centro de datos, propiedad intelectual, espacio virtual de los objetos, administración del vínculo de abastecimiento, atención médica, propiedad y repartición de regalías, organizaciones autónomas descentralizadas.

La unidad fundamental de Blockchain es el bloque que se compone de una estructura como se muestra en la **Figura 1-2**, donde se registra muchas de las transacciones ejecutadas en un periodo de tiempo determinado (Singh et al., 2018).

Dichos bloques se conforman de modo que cada bloque nuevo está criptográficamente conectado al bloque anterior:

- El encabezado, que incluye metadatos como, un número de referencia de bloque único, la hora en que se creó el bloque y un enlace al bloque anterior.
- El contenido, generalmente una lista validada de activos digitales y declaraciones de instrucciones, como las transacciones perpetradas, sus montos y las direcciones de los fragmentos en esas transacciones (Makhdoom et al., 2020).

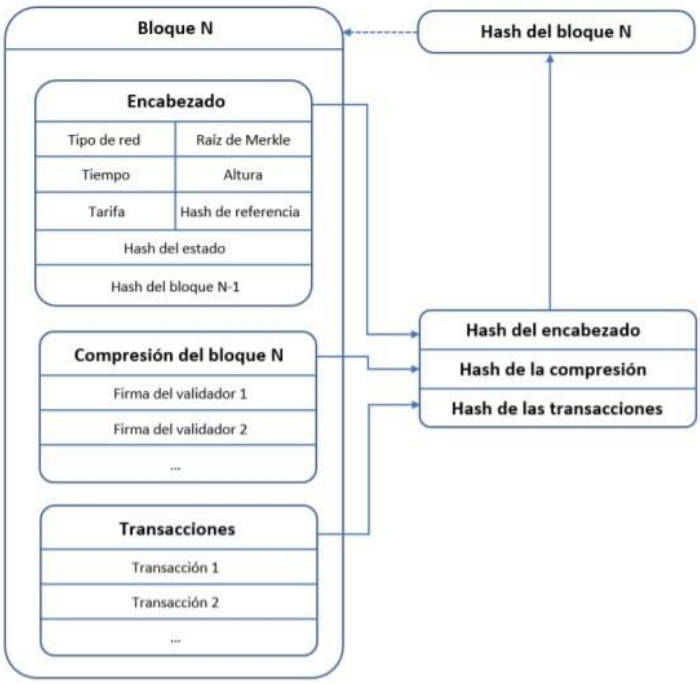


Ilustración 2-1: Estructura de un bloque

Fuente: (Rosero, 2019)

Ello simboliza que la cadena irá creciendo a medida que se le vayan añadiendo nuevos bloques, por su parte provocará que aumente la porción de espacio de almacenamiento que ocupa aunque se puede considerar una perspectiva positiva en este escenario, la idea es que la tecnología blockchain se vuelve más resistente y segura a medida que aumenta la cantidad de datos almacenados en ella. Esto en parte debido a que, una vez ingresada una transacción en la blockchain, ésta nunca podrá borrarse cada bloque de la cadena de bloques contiene el hash del bloque anterior, lo que significa que, si alguien intenta manipular un bloque, tendría que cambiar

los hashes de todos los bloques anteriores para hacerlo. Esto hace que sea extremadamente difícil y costoso falsificar o alterar datos almacenados en la cadena de bloques (Singh et al., 2018).

Es posible acceder a la secuencia completa y detallada de los componentes de la cadena de bloques, lo que permite la visualización de todas las transacciones registradas, incluyendo la primera transacción del sistema. Además, cualquier entidad tiene la capacidad de verificar y recopilar esta información en cualquier momento. ello se puede conseguir puesto que a algunas características que presenta Blockchain como, por ejemplo: autónoma, transparente, distribuida, integra, redundante, inmutable, confiable y pública (Reyna et al., 2018).

En 2008, Satoshi Nakamoto (o un grupo de personas acreditadas bajo este nombre) definió la sucesión inicial de bloques que posteriormente fue implementada como un componente central de la moneda digital conocida como "Bitcoin" en 2009. Esta sucesión de bloques funciona como un libro público que registra todas las transacciones realizadas en la red (Wang et al., 2019).

2.2. Arquitectura de la sucesión de bloques

Dado que una sucesión de bloques son una red de malla descentralizada de computadoras conectadas entre sí, en vez de utilizar un servidor central, hay una cadena de capas que gobiernan las operaciones de la serie de bloques y crean los protocolos para la aplicación de Blockchain.

Según los autores Muzammal et al. (2019) y Min (2019) una arquitectura de Blockchain se dispone de los cinco módulos, detallados a continuación:

- Almacén de datos: es almacén de datos en la tecnología blockchain es una organización de datos que se basa en una secuencia de bloques y que replica los datos en cada nodo de la red blockchain. Esta tecnología ayuda a crear una cadena de bloques en plataformas de datos compartidos y distribuidos, lo que significa que no dependen de una red cliente-servidor controlada por una autoridad central. Al no depender de esta red, no es necesario que los interesados realicen un proceso de autenticación para verificar la escritura de nuevos datos. En cambio, se requiere un consenso entre los participantes de esta red peer-to-peer.

- Consenso: la blockchain es un sistema que permite el cambio de estados mediante la realización de transacciones, las cuales son agrupadas en bloques que son firmados y procesados conjuntamente. Cada bloque define la transición del sistema de un estado a otro. Además, la blockchain utiliza un mecanismo de consenso para confirmar y validar

las transacciones y evitar la corrupción de la información almacenada en la serie de bloques. Por lo tanto, la selección del mecanismo de consenso es fundamental para garantizar la seguridad y la integridad de la información en la blockchain.

- Validación: La integridad de la cadena de bloques se garantiza mediante un proceso de validación de transacciones, que son transferencias de valor entre dos partes. Para que una transacción sea validada, primero debe haber un acuerdo entre las partes involucradas y luego ser transmitida a la red P2P. Para ser validada, la transacción debe cumplir con tres controles: en primer lugar, debe ser criptográficamente válida, es decir, su firma debe ser verificable; en segundo lugar, debe tener un formato válido, lo que significa que todos los campos incluidos en la transacción deben cumplir con los requisitos correspondientes; y en tercer lugar, debe tener una etapa válida, lo que significa que se deben cumplir todas las restricciones impuestas a la transacción.

- Red de Blockchain: La blockchain es una red descentralizada en la que los nodos se comunican entre sí para intercambiar información, en particular transacciones, utilizando un protocolo de difusión seguro que garantiza la confidencialidad y la integridad de los datos transmitidos.

- Seguridad y privacidad: la seguridad de Blockchain se basa en gran medida en técnicas de criptografía. Esta tecnología utiliza mecanismos criptográficos para proteger la autenticidad, la integridad y la confidencialidad de las transacciones, los bloques y la cadena de bloques. La clave pública criptográfica puede estar vinculada a la identidad del usuario o a resúmenes intermedios. Por ejemplo, la billetera digital que se utiliza en la plataforma para preservar el anonimato de las transacciones.

2.3. Árboles de Merkle

Según Buterin (2019) una característica clave de la escalabilidad de la tecnología Blockchain es que los bloques se almacenan en una estructura de datos de múltiples niveles, donde las transacciones se agrupan en bloques y cada bloque se conecta al bloque anterior mediante un valor hash. Debido a que los bloques solo están disponibles hacia adelante, cualquier cambio en el valor hash de un bloque afecta a todos los bloques posteriores y, por lo tanto, compromete la integridad de toda la cadena de bloques.

Un sistema logra ser aún más robusto si se almacena cada hash en una arboleda hash de manera que cada valor se combina con los anteriores en solamente un hash nuevo para lograr así que sea

muy difícil alterar los hashes anteriores. Un árbol Merkle, además acreditado como un árbol hash de dos elementos, es una organización de datos utilizada para resumir y verificar de manera eficiente la integridad de un gran conjunto de datos. Este árbol como se muestra en la **Figura 2-2**, está integrado por un grupo de nodos con una gran cantidad de nodos de hoja en el fragmento inferior del árbol que sujeta los datos subyacentes, un grupo de nodos intermedios en el que cada nodo es el hash de sus dos hijos, y, para terminar, un solo nodo raíz, igualmente desarrollado a partir del hash de sus dos hijos, que personifica la "parte superior" del árbol (Buterin, 2019).

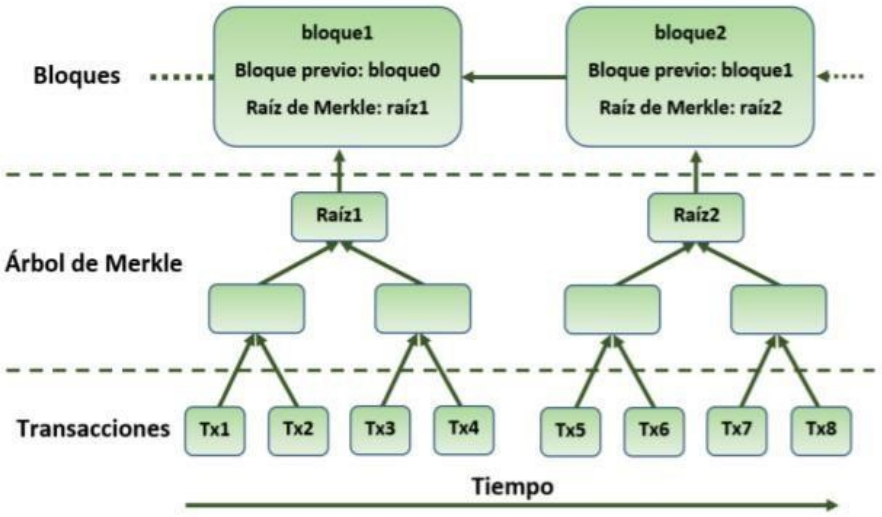


Ilustración 2-2: Estructura genérica de una transacción de Blockchain

Fuente: (Buterin, 2019)

Se construye un árbol de Merkle mediante el uso de hash recursivos en pares de nodos hasta que solo queda un hash, el cual se llama la raíz de Merkle. Esta raíz de Merkle proporciona pruebas indudables de que algunas transacciones han tenido lugar y se obtiene al vincular cada transacción con otra, mezclando los datos, emparejando el resultado con otro par y repitiendo este proceso exhaustivamente hasta que todos los datos de la transacción se encuentren contenidos en un hash final y no quede ningún par para combinar. El resumen de 32 bytes generado al final del proceso del árbol de Merkle se almacena en los encabezados del bloque y representa todas las transacciones contenidas en él de manera completa. En otras palabras, la raíz de Merkle es el hash resultante de los hashes de todas las transacciones presentes en el bloque (Burgwinkel, 2016).

2.4. Contratos inteligentes

Un contrato inteligente es un programa informático que se ejecuta en la blockchain y tiene como finalidad facilitar, ejecutar y hacer cumplir los términos de un acuerdo sin necesidad de intermediarios de confianza. Su principal ventaja es la automatización de la ejecución de los

términos del acuerdo una vez que se cumplen las condiciones especificadas. Esto resulta en un costo de transacción más bajo en comparación con los sistemas tradicionales que requieren un tercero de confianza para hacer cumplir y ejecutar los términos del acuerdo. Los contratos inteligentes pueden considerarse como un método para liberar activos digitales a ciertos participantes una vez que se cumplen las reglas previamente definidas (Alharby et al., 2017).

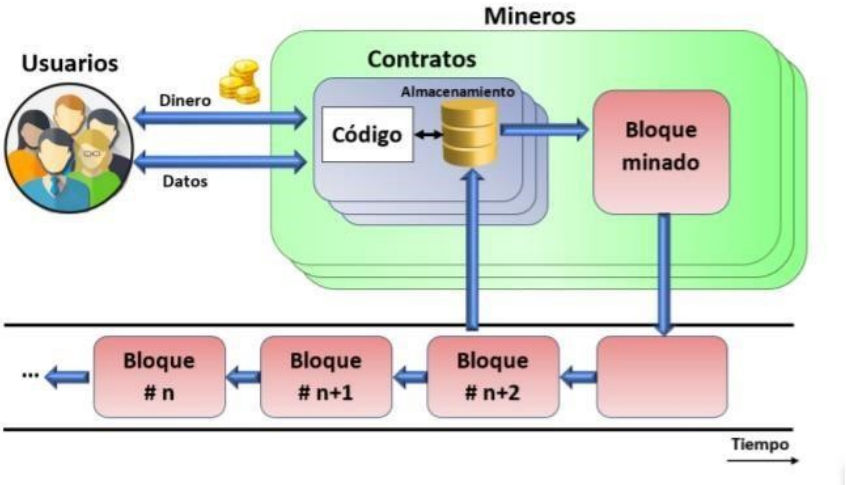


Ilustración 2-3: Sistema de los contratos inteligentes

Fuente: (Alharby et al., 2017)

Los contratos inteligentes son componentes complejos que poseen un saldo de cuenta, un almacenamiento privado y un código ejecutable. El estado del contrato, que incluye tanto el almacenamiento como el saldo, se mantiene en una sucesión de bloques y se actualiza en cada ciclo que se invoca el contrato. Según se muestra en la Ilustración 2-3, los contratos inteligentes son capaces de realizar cualquier tipo de cálculo arbitrario y, en algunos casos, incluso pueden llamar a otros contratos inteligentes (Peyrott, 2017).

Hay varias plataformas disponibles para el desarrollo de contratos inteligentes, entre ellas Ethereum, Bitcoin y NXT, que proporcionan diferentes características y funcionalidades para la creación de estos contratos. Estas plataformas permiten el uso de lenguajes de programación de alto nivel, lo que facilita la creación de contratos inteligentes y permite una mayor personalización y flexibilidad en la implementación de los términos y condiciones del acuerdo. Cada plataforma tiene sus propias ventajas y limitaciones, por lo que es importante considerar cuidadosamente cuál plataforma es la mejor para cada caso particular.

2.5. Operatividad de las aplicaciones descentralizadas

2.5.1. Descripción de las aplicaciones descentralizadas

Según el autor Hurtado (2022) una Dapp o aplicación descentralizada es un tipo de aplicación que opera en una red descentralizada de ordenadores y computadoras. La información generada por esta aplicación se almacena en una red de ordenadores que permite que esta información se mantenga segura y accesible. La red descentralizada es una tecnología blockchain universalmente aceptada conocida como DLT.

En términos simples, una Dapp puede entenderse como la unión de dos componentes: un Smart Contract que sirve como base para la aplicación, y una interfaz de usuario que permite a los usuarios interactuar con el Smart Contract en una red descentralizada. Esta combinación permite el desarrollo de aplicaciones descentralizadas con la capacidad de ejecutar automáticamente los términos del contrato y garantizar la transparencia y accesibilidad de la información en la red Blockchain.

2.5.2. Funcionamiento de las aplicaciones descentralizadas

Se puede decir que las aplicaciones descentralizadas son completamente portátiles, ya que se pueden ejecutar desde cualquier nodo de la red en la que se alojan. La interacción entre la aplicación y la red descentralizada se logra mediante el uso de librerías que actúan como intermediarias entre el Smart Contract desplegado y la interfaz de usuario. El autor Gómez (2021) muestra un diseño de las aplicaciones descentralizadas se muestra en la Ilustración 2-4:

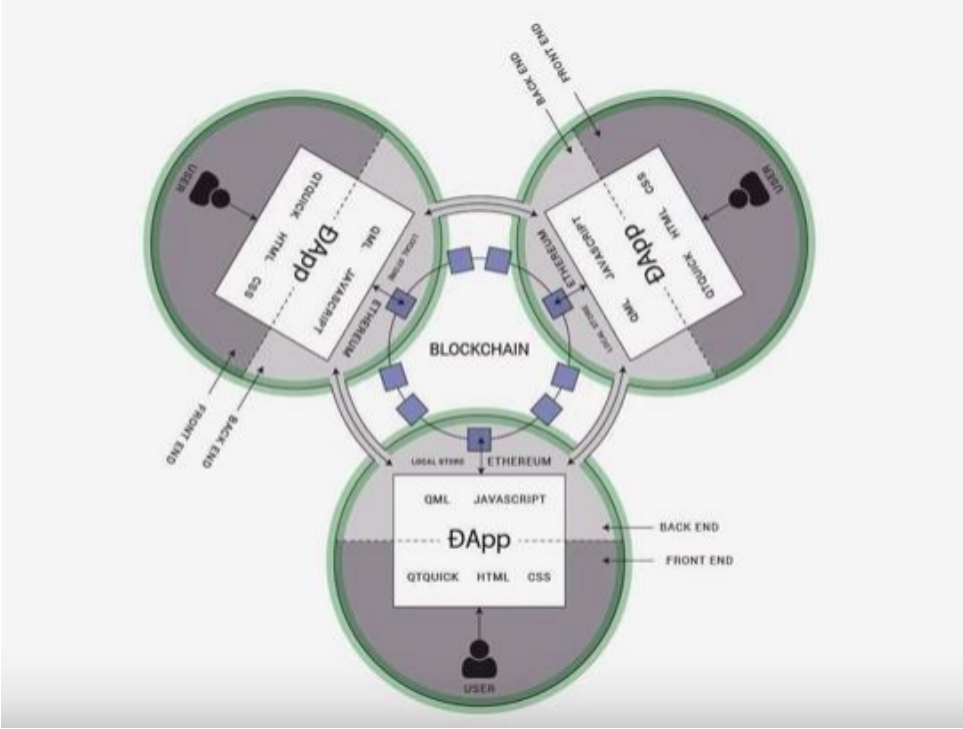


Ilustración 2-4: Esquema de trabajo de Dapps.

Fuente: (Gómez, 2021)

Una Dapp opera de manera similar a una red blockchain, donde cada usuario de la aplicación es un nodo en la red y es responsable de supervisar las operaciones que se llevan a cabo en ella. La comunicación de la Dapp se realiza a través de la blockchain, que registra cada acción que se realiza en el Smart Contract que controla la aplicación. La validación o rechazo de las transacciones realizadas por los usuarios de la Dapp depende de la lógica implementada en el Smart Contract, con el objetivo de asegurar que todas las partes actúen dentro de los límites establecidos por el contrato.

El Smart Contract en cuanto a este caso, es una posición intermedia que se responsabiliza de confirmar la eficacia de cada relación. En el momento en que hay una operación nueva en la Dapp, la información que existe en la plataforma se renueva en cada nodo. Con ello se garantiza que la investigación quede almacenada en cada una (Mougayar, 2019).

Cada participante de la red blockchain contribuye a mantener en funcionamiento la aplicación mediante los recursos de su ordenador, lo que asegura que la plataforma esté disponible las 24 horas del día, los 7 días de la semana. Esto se debe a la complejidad de mantener todos los nodos de la red blockchain inactivos al mismo tiempo.

2.5.3. Comparación de las Apps vs Dapps

La adopción de la tecnología blockchain ha generado un impacto significativo en el desarrollo y uso de aplicaciones en línea. En particular, las aplicaciones descentralizadas (dapps) han ganado popularidad como una alternativa más segura y resistente a los riesgos de seguridad inherentes a las aplicaciones convencionales. A diferencia de las apps tradicionales, que dependen de servidores centralizados y son controladas por una entidad única, las dapps operan de manera autónoma y descentralizada en una red blockchain. Este nuevo enfoque de las aplicaciones ofrece una solución diferente a los problemas que han afectado a las apps tradicionales, tales como la seguridad y la protección de los datos del usuario. El presente estudio compara las características y funcionamiento de las Apps y las Dapps, examinando su metodología y forma de almacenamiento de información, para comprender sus diferencias y cómo las dapps han revolucionado la forma en que interactuamos con la tecnología en línea.

Tabla 2-1: Tabla comparativa entre las Apps y Dapps

	APPS	**DAPPS**
Metodología de funcionamiento	La app tradicional tiene como desventaja los posibles hackeos ya sea a las cuentas de los usuarios como también de las empresas propietarias..	Funciona de forma autónoma sin que ninguna entidad la controle, desistiendo el poder de decisión sobre la misma, en su grupo de usuarios
Almacenamiento de información	Su información se almacena en servidores o en la sede central. Existe el riesgo de que si la empresa propietaria desaparece, así mismo desaparecería la información.	Los datos se almacenan en una red Blockchain, logrando que la información de las transacciones ejecutadas quede encriptado y almacenado de manera inmutable, pública y segura.

Fuente: Revisión de metodologías ágiles para el desarrollo de software (2013)

La tabla compara dos aspectos clave entre las aplicaciones convencionales y las aplicaciones descentralizadas (dapps) basadas en blockchain. En cuanto a la metodología de funcionamiento, las apps tradicionales son vulnerables a hackeos y están controladas por una entidad central, mientras que las dapps funcionan de forma autónoma y descentralizada en una red blockchain. En cuanto al almacenamiento de información, las apps convencionales almacenan la información en servidores o en la sede central, lo que puede ser un riesgo si la empresa propietaria desaparece, mientras que las dapps almacenan los datos de manera encriptada e inmutable en una red blockchain, lo que garantiza su seguridad y permanencia.

Las aplicaciones descentralizadas (Dapps) se diferencian de las aplicaciones tradicionales (Apps) por su enfoque descentralizado en una red blockchain, lo que les proporciona mayor seguridad y

privacidad. En este sentido, la tecnología blockchain ofrece encriptación y autenticación para garantizar la integridad de los datos, lo que minimiza el riesgo de ataques de hackers. Además, las dapps reducen la dependencia de terceros y permiten que los usuarios tengan control total sobre sus datos, sin necesidad de confiar en una entidad central.

Otro beneficio de las dapps es su transparencia, ya que todas las transacciones en una red blockchain son públicas y verificables, lo que resulta útil para aplicaciones que requieren alta confianza y seguridad, como los sistemas de votación. Las dapps son una opción interesante para aquellos que buscan una solución más segura, confiable y autónoma para sus necesidades de aplicación en línea. En general, las dapps ofrecen una alternativa más segura y resistente a los riesgos de seguridad que presentan las apps tradicionales.

2.6. Selección del tipo de red Blockchain

Cuando se está implementando una solución blockchain, es fundamental tomar una decisión importante: seleccionar el tipo de red blockchain. Hay diversos tipos de redes blockchain disponibles, cada una con sus propias ventajas y desventajas. Por lo tanto, es crucial elegir la red adecuada para la aplicación específica, ya que esto puede tener un impacto significativo en la seguridad, la escalabilidad y el rendimiento de la solución. En esta sección se presentan algunas consideraciones clave que se deben tener en cuenta al seleccionar el tipo de red Blockchain más apropiado.

2.6.1. Tipos de redes Blockchain

Existen diferentes tipos de redes blockchain que se pueden clasificar en función de cómo se distribuyen los datos y quién tiene acceso a ellos. La elección de la tipología adecuada dependerá de las necesidades específicas de cada aplicación y de los objetivos que se quieran alcanzar. Es importante tener en cuenta las características y limitaciones de cada tipo de red al momento de seleccionar la más adecuada para una solución blockchain. De esta manera tenemos:

- **Blockchain Públicas:** En el tipo de blockchain de carácter abierto, cualquiera puede unirse y participar. Esto permite a los usuarios acceder libremente a los datos y realizar transacciones. Sin embargo, dado que un gran número de usuarios no verificados pueden participar, se requiere un cifrado y confirmación audaz para garantizar la seguridad. Como resultado, la expansión de la red puede ser lenta y difícil. A pesar de esto, el blockchain público establece una organización distribuida perfecta, y los participantes son pseudoanónimos. Sin embargo, debido a que no es adecuado para valores financieros

que requieren una investigación centralizada del proceso de gestión, puede no ser la opción adecuada en ciertos escenarios. Permiten también que cualquier persona participe y mantenga un registro distribuido, con permisos para validar la integridad mediante un mecanismo de consenso. Son completamente distribuidas y abiertas, lo que significa que cualquier persona puede unirse, contribuir y salir del sistema libremente. Por lo tanto, este proceso funciona bajo nodos anónimos y no confidenciales (Viriyasitavat et al., 2019).

- **Blockchain Privadas:** Para esta Blockchain privadas son aquellas en las que el control y la manipulación del Blockchain están en manos de un único poder centralizado, lo que resulta adecuado para sistemas en los que se desea gestionar el Blockchain de manera centralizada (Oh et al., 2017).

  Estos registros son compartidos y verificados simultáneamente por un grupo específico de nodos que previamente han sido autorizados a participar en el proceso. En este sentido, los nodos que deseen unirse al sistema deben ser previamente preparados y autorizados por el poder central. Las blockchain privadas son particularmente útiles en sistemas cerrados, en los que todos los nodos son completamente confidenciales y solo el poder central tiene la máxima autoridad para controlar el acceso a los nodos autorizados. En resumen, las Blockchain privadas son sistemas en los que el control y la autoridad están centralizados en una única entidad poderosa afirma (Viriyasitavat et al., 2019).

- **Blockchain Hibridas (Consorcio):** La tecnología Blockchain Híbrida (Consorcio) representa un tipo de blockchain intermedio entre los modelos públicos y privados. A diferencia de las redes privadas donde el poder está en manos de una sola entidad, en las Blockchain Híbridas son los nodos preestablecidos quienes tienen el control. De esta forma, se logra mantener la estructura distribuida de las redes públicas y se aumenta la seguridad al limitar la intervención en la toma de decisiones, superando así los problemas de velocidad y escalabilidad que presentan las Blockchain públicas. Así, las Blockchain Híbridas pueden ser adecuadas para transacciones entre instituciones financieras (Oh, et al., 2017).

2.6.2. Parámetros de comparación de redes blockchain

Actualmente existen varias redes blockchain, dónde podemos desplegar aplicaciones. Es importante conocer la clase de blockchain a utilizar antes de comenzar un proyecto, tienen cierta similitud, pero hay características que las hacen distintas entre sí. El autor de la Tabla 2-2 rescata

4 propiedades importantes a tomar en cuenta si realizamos una comparativa entre la tipología de Blockchain antes de elegir una red:

Tabla 2-2: Comparación entre redes de tipo públicas, privadas e híbridas

Propiedad	**Tipos de redes blockchain**		
	Pública	**Privada**	**Híbrida**
Productores	Cualquier usuario	Una entidad	Conjunto de nodos seleccionados
Permisos	Públicos	Públicos, parcialmente públicos o restringidos	Públicos, parcialmente públicos o restringidos
Inmutabilidad	Prácticamente garantizada	No asegurada	No asegurada
Centralización	No	Si	Parcial

Fuente: (Luque, 2020)

2.6.3. Comparación de tipos de redes Blockchain

La tecnología blockchain ha adquirido gran popularidad en los últimos años debido a sus beneficios en cuanto a transparencia, seguridad y descentralización. Existen diferentes tipos de redes blockchain, cada una con características únicas y diversas aplicaciones en el mundo de la tecnología.

En esta comparación, se examinarán los tipos más comunes de redes blockchain, incluyendo blockchain público, privado y consorcio. Cada tipo de red tiene diferentes niveles de acceso, control y descentralización, lo que puede influir en su uso y aplicaciones en distintos contextos.
En este análisis, se explorará cómo funcionan cada uno de estos tipos de redes blockchain, sus ventajas y desventajas, y las posibles aplicaciones para cada uno de ellos. Al comparar estos tipos de redes blockchain, se espera proporcionar una mejor comprensión de cuándo y cómo utilizarlos en diferentes escenarios.

Tabla 2-3: Tabla comparativa de tipos de redes Blockchain

TIPOS DE BLOCKCHAIN	ABIERTA	Pública sin permisos	Abierta a cualquiera	Cualquiera	Cualquiera	Bitcoin y Ethereum
		Pública sin permisos	Abierta a cualquiera	Participantes autorizados	Todos o parte de los participantes autorizados	Libro de la cadena de suministro visible al público
	CERRADA	Consorcio	Restringido a un grupo autorizado de participantes	Participantes autorizados	Todos o parte de los participantes autorizados	Múltiples bancos que operan un libro de contabilidad compartido
		Empresa privada autorizada	Totalmente privada o restringida a un conjunto limitado de nodos autorizados	Sólo para operadores de red	Sólo para operadores de red	Libro externo de cuentas bancarias compartido entre la sociedad matriz y las subsidiarias.

Fuente: Blockchain Technology (2016)

La blockchain pública es altamente segura debido a la descentralización y la verificación de múltiples participantes. Además, es completamente transparente ya que todas las transacciones son públicas y no pueden ser alteradas. Sin embargo, su proceso de validación descentralizado puede hacer que sea más lenta y costosa, y también hay una falta de privacidad en las transacciones. Además, la gobernanza puede ser un problema, ya que no hay una autoridad central que tome decisiones. Algunas posibles aplicaciones incluyen criptomonedas, votación y registro de propiedades.

La blockchain privada, por otro lado, es más rápida y eficiente debido a su menor cantidad de participantes, y ofrece mayor privacidad y control para los usuarios autorizados. Sin embargo, tiene un menor nivel de seguridad debido a su limitado número de participantes, lo que puede hacerla menos confiable. Además, la gobernanza puede ser un problema si los participantes no están de acuerdo con las decisiones tomadas. Algunas posibles aplicaciones incluyen redes de suministro, votación y registro de identidad.

La blockchain consorcio se encuentra en un punto intermedio entre la blockchain pública y privada, y puede ofrecer mayor eficiencia y privacidad debido a la colaboración entre organizaciones. Además, las organizaciones participantes tienen un mayor control y gobernanza compartida. Sin embargo, también tiene algunos desafíos, como la necesidad de un tercero para validar transacciones en algunos casos, y la gobernanza puede ser un problema si los participantes no están de acuerdo con las decisiones tomadas. Algunas posibles aplicaciones incluyen redes de suministro compartidas entre varias organizaciones, registro de identidad compartido y sistema de seguimiento y registro de activos compartido (Narayanan, et al., 2016).

2.6.4. Selección de la red blockchain para el desarrollo del proyecto

En el proyecto en desarrollo se ha elegido la red pública y abierta de Ethereum para garantizar la inmutabilidad de la información. Ethereum es un entorno de blockchain público que permite la creación de contratos inteligentes personalizados mediante la programación de un lenguaje Turing completo. La plataforma Ethereum es capaz de soportar restricciones de retirada, bucles, contratos financieros y escenarios de contingencia. La complejidad de los contratos inteligentes de Ethereum se expresa en un código de bytes basado en componentes y se ejecuta en la máquina virtual Ethereum (EVM). Se pueden utilizar varios lenguajes de alto nivel (como Solidity, Serpent y LLL) para escribir contratos inteligentes en Ethereum. El código de estos lenguajes se puede compilar en EVM Byte Codés y ejecutar en la plataforma. Actualmente, Ethereum es la plataforma más común para el desarrollo de contratos inteligentes (Alharby et al., 2017).

La tecnología de Ethereum es capaz de respaldar la implementación de contratos inteligentes, los cuales están anclados en la tecnología Blockchain y, por lo tanto, son inmutables una vez implementados. Sin embargo, existe una instrucción en la máquina virtual de Ethereum llamada SELFDESTRUCT, que permite desactivar el código del contrato inteligente. Cuando se ejecuta, esta instrucción transfiere el ether almacenado en el contrato a un destino específico y borra todos los datos almacenados en el contrato. Es importante tener en cuenta que esta acción no altera el historial de transacciones previas realizadas en la Blockchain (Dika, 2017).

La continuación de elementos Ethereum tiene algunas redes de prueba, y 2key Network tiene una versión que opera en la malla de prueba Goerli. El punto de prueba Goerli admite que los progresos de blockchain experimenten su labor en un ambiente en vivo, pero sin la necesidad de tokens ETH reales y 2KEY de red primordial. Es así como brinda la capacidad de concordar continuamente la red 2key sin afrontar ningún valor serio de gas o exponer la red primordial 2KEY (Radu, 2020).

2.7. ISO/IEC 25010

El modelo de calidad es el marco fundamental para evaluar la calidad de un producto software. Este modelo identifica las características de calidad que se deben considerar al evaluar las propiedades de un producto software específico. La calidad del producto software se define como la medida en que satisface los requisitos del usuario y aporta valor. Los requisitos incluyen la función, el rendimiento, la confiabilidad, la mantenibilidad y otros aspectos relevantes, los cuales se representan en el modelo de calidad. Este modelo permite categorizar la calidad del producto en características y sus características para su evaluación (ISO 25010, 2020).

El modelo de calidad del producto conceptualizado por la ISO/IEC 25010 se compone por ocho características de calidad identificadas en la figura (**Ilustración 2-5**):

Ilustración 2-5: Características de la calidad del producto de software ISO 25010

Fuente: (ISO 25010, 2020)

2.7.1. Seguridad

Según el aporte de la ISO 25010 (2020) se trata de la capacidad de proteger la información y los datos para que sólo sean accesibles por aquellos que estén autorizados, impidiendo que terceros no autorizados los lean o modifiquen. En cuanto a las Sub-características, se dividen en:

- **Confidencialidad**: Garantiza que los datos e información no autorizados no estén al alcance de terceros, ya sea de forma accidental o intencionada.
- **Integridad**: Evita que los datos o programas informáticos sean accedidos o modificados sin autorización.
- **No repudio**: Permite demostrar las acciones o eventos realizados para evitar que sean negados posteriormente.

- **Responsabilidad**: Facilita el seguimiento de las acciones de una entidad de manera precisa.
- **Autenticidad**: hace posible la identificación precisa de un sujeto o recurso.

2.8. Herramientas y plataformas de desarrollo

NodeJS

Admitido como un ambiente de elaboración de JavaScript orientado a eventos asíncronos, Node.js está diseñado para edificar estudios en red escalables (Oktian et al., 2021).

NPM (Node Package Manager)

Npm es la búsqueda de software más grandiosa del mundo. Los promotores de código directo de todos los continentes emplean Npm para colaborar y arrebatar ofrecidos paquetes, y diversas organizaciones igualmente utilizan Npm para gestionar el progreso exclusivo (Yavari et al., 2020).

Visual Studio Code

Visual Studio Code es un impresor de código fuente impalpable pero recia que se elabora en su estudio y está utilizable para Windows, macOS y Linux. Comparece con soporte asociado para JavaScript, TypeScript y Node.js y posee un delicado ambiente de amplificaciones para otros lenguajes (como C ++, C #, Java, Python, PHP, Go) y períodos de realización (como .NET y Unity) (Microsoft, 2020).

Solidity

Solidity constituye un lenguaje de valioso horizonte encaminado a centros para efectuar tratados inteligentes. Los tratados inteligentes son presentaciones que presiden el procedimiento de las enumeraciones centralmente del estado Ethereum. Solidity fue influenciado por C ++, Python y JavaScript y está planteada para asentar a la máquina virtual Ethereum (EVM). Solidity está estático tipado, permite sucesión, bibliotecas y tipos complicados determinados por el usuario, entre otras peculiaridades. Con Solidity obtiene establecer tratados para rutinas como votación, crowdfunding, concursos a exasperas y billeteras con variadas firmas (Cuesta, 2021).

Truffle

Truffle se faculta de dirigir sus aparatos convenidos para que no obtenga que hacerlo. Contiene sustentáculo para ejecuciones personificadas, enlaces de bibliotecas y diligencias complicadas de Ethereum (Amir et al., 2021).

Ganache

Un vínculo de mecanismos personales para el progreso de Ethereum que logra usar para efectuar contratos, desenvolver sus aplicaciones y establecer pruebas. Está favorable tanto como una diligencia de escritorio como un instrumento de línea de instrucciones (primariamente destacada como TestRPC) (Mansour et al., 2021).

Infura

Infura suministra las herramientas y la construcción que ayudan a los desarrolladores manejar de forma fácil su aplicación de Blockchain desde los inicios de pruebas hasta que se implementa la escala, proporcionando acceso fácil y seguro a Ethereum e IPFS (Amir et al., 2021).

Ipfs

Constituye uno de los sistemas de archivos descentralizados para la construcción de la próxima generación de Internet, se encuentran las monedas de archivos y diversos proyectos de tipo Web3 populares se basan en IPFS. También conocido como el disco duro para blockchain y Web3, aunque posee una capacidad extendida (Makhdoom et al., 2020).

CAPÍTULO III

3. MARCO METODOLÓGICO

La metodología que se desarrolla hace referencia a los medios que contribuyen con la obtención de datos y la información que se pretende llevar a cabo en el progreso de mismo. Dando a conocer los procedimientos, medios y técnicas que se requieren para el diseño metodológico mediante la aplicación de una DAAP, además de un detalle de las herramientas utilizadas para construir la propuesta.

3.1. Contexto de la investigación

La Granja Avícola "Ivanna", es una microempresa dedicada a la producción y comercialización de pollos de engorde, ubicada en el cantón Marcabelí, provincia de El Oro. Al igual que todas las microempresas, sin importar la actividad a la que se dediquen, las granjas avícolas también interactúan con documentación como, por ejemplo: facturas, recibos, notas de venta, guías de remisión, permisos, documentos de control, etc. Con los avances que ha tenido la tecnología en el entorno, la mayoría de los documentos se manejan en formato digital, lo que desde un punto de vista podría generar desconfianza, ya que esta información podría ser alterada o eliminada, siendo esta una de las problemáticas que se encuentran a menudo en la actualidad.

3.2. Alcance de la investigación

3.2.1. Hipótesis

Hi: Un modelo descentralizado que almacene la información de manera inalterable podrá contrarrestar inconvenientes como la alteración o pérdida de información dentro de la avícola.

Ho: Una vez que toda la información esté dentro de una Blockchain, fácilmente podrá ser verificada por otras entidades, teniendo la confianza de que está segura.

3.3. Diseño de la investigación

La presente investigación tiene como objetivo principal demostrar la efectividad del desarrollo de una DAPP utilizando tecnología Blockchain para la verificación de documentos electrónicos. Se realizará un estudio experimental para evaluar la capacidad de la DAPP en garantizar la autenticidad, integridad y confidencialidad de los documentos en un contexto específico. A través

de la implementación y análisis detallado de la DAPP, se busca obtener resultados que respalden la utilización de la tecnología Blockchain como una solución confiable para la verificación de documentos electrónicos.

3.4. Población

La población objetivo está constituida por tres desarrolladores de sitios web, se justifica debido a que ellos poseen un conocimiento en el desarrollo de software y en temas de seguridad informática. Como parte de su formación, han adquirido habilidades y conocimientos especializados en programación y en el manejo de herramientas de seguridad que les permiten desarrollar aplicaciones seguras y confiables.

Por otro lado, los usuarios finales de la DAPP pueden no tener el mismo nivel de conocimiento en estas áreas. Por lo tanto, se considera que la opinión y experiencia de los desarrolladores resulta valiosa para evaluar la efectividad de la aplicación en términos de seguridad y confiabilidad. Además, su aporte puede ser de gran ayuda para identificar posibles mejoras o ajustes que deban realizarse en la DAPP para mejorar su desempeño y garantizar su éxito en el mercado. Debido a que los problemas de seguridad se deben tomar en consideración en la etapa del desarrollo del software.

3.5. Métodos y técnicas de investigación

3.5.1. Método

El método del estudio es inductivo deductivo, debido a que parte del desarrollo de la tecnología Blockchain de tal manera que pueda ser aplicada en una DAPP en el tema de verificación de documentos electrónicos.

Para la ejecución del estudio se llevó a cabo el siguiente proceso

1. Revisión Bibliográfica
2. Revisión documental
3. Diseño y selección de red Blockchain
4. Desarrollo de la DAPP
5. Evaluación de seguridad de la DAPP basada en la ISO 25010:2011

3.5.2. Técnicas

Las técnicas que se utilizan en este estudio están basadas en fuentes de información bibliográfica y documental utilizando pruebas y observación de resultados como una fuente primaria, además la revisión de fuentes secundarias que abarcan las leyes de la constitución, tesis de investigación con relación a la temática de estudio, revistas electrónicas, artículos científicos, entre otros.

A continuación, se enlistan las técnicas que se utilizaron en el presente estudio:

- Recopilación de información en fuentes primarias y secundarias como herramientas para conocer acerca de la temática de estudio.
- Realización de pruebas experimentales en el lugar del estudio del caso.
- Aplicación de la encuesta
- Observación de los resultados principales con relación a las pruebas realizadas
- Análisis de los resultados identificados en la investigación

3.5.3. Instrumentos

- Documentos bibliográficos
- Cuestionario
- Guía de observación

Considerando que la población con la que se trabaja es muy pequeña se desarrolló un cuestionario identificando las subcategorías que se van a tomar en cuenta de acuerdo con las características de la Norma ISO 25010:2011, todo este análisis basado en una metodología para evaluar la seguridad de las aplicaciones según (Alvarez et al., 2021).

Como se ha mencionado previamente, la norma ISO 25010 define cinco subcategorías para establecer los indicadores del instrumento de evaluación de seguridad. En base a estas subcategorías, se seleccionaron 3 subcategorías establecieron los indicadores correspondientes para cada sección del instrumento. La Tabla 3-1 presenta las subcategorías de la característica Seguridad de la Norma ISO 25010, los indicadores de evaluación correspondientes y la sección del instrumento de recolección de datos con la que están relacionados:

Tabla 3-1: Relación Sub-características/indicador

Calidad del producto Subcategoría para la característica de Seguridad	**INDICADOR**
Confidencialidad	El grado en que el sistema protege los datos y la información no autorizados del acceso accidental o deliberado.
Integridad	El grado en que el sistema puede evitar modificaciones no autorizadas de datos o información.
Autenticidad	El grado en que el sistema demuestra la identidad del sujeto.

Realizado por: Kevin G., 2023

Cuestionario como instrumento de evaluación

El proceso de recolección de datos se llevó a cabo mediante un instrumento que se estructuró en 3 secciones. Cada sección estaba diseñada para contener cuatro preguntas, lo que da un total de 12 preguntas en el cuestionario completo. Para garantizar la objetividad en las respuestas de los entrevistados, se utilizó un enfoque dicotómico en la formulación de las preguntas. Cada sección del cuestionario se enfocó en una subcaracterística específica y se asoció con un indicador correspondiente**.** Las preguntas de cada subcaracterística del cuestionario pueden ser verificadas en el **Anexo A**.

Con base a la metodología propuesta por (Mex-Alvarez, et al., 2021) , se creó una herramienta de medición para categorizar la aceptación del porcentaje obtenido de los criterios positivos totales. La Tabla 3-2 presenta los diferentes rangos y criterios propuestos para tal fin.

Tabla 3-2: Clasificación de criterios según porcentaje de respuestas positivas

CRITERIOS	**Rango de respuestas positivas**
Inelegible	0 <= X < 40%
Mínimo permitido	40 <= X < 60%
Admisible	60 % <= X < 90 %
Excelente	90 < X <= 100%

Realizado por: Kevin G., 2023

3.6. Aplicación de la metodología ágil SCRUM

Esta metodología presenta un marco de trabajo que ayuda a mejorar la productividad en un equipo de trabajo de forma efectiva y ágil, incrementa el desarrollo de las necesidades y proporciona roles de uso, basadas en transparencia, inspección y adaptación (Navarro et l., 2013).

El período de trabajo Scrum se define mediante un Sprint, que corresponde a la ventana de tiempo para crear versiones usadas en el producto en la **figura 1-3**, Cada Sprint contiene artefactos que constituyen las actividades que realiza el grupo como: Product Backlog; Sprint Backlog; Monitoreo de avance e incremento.

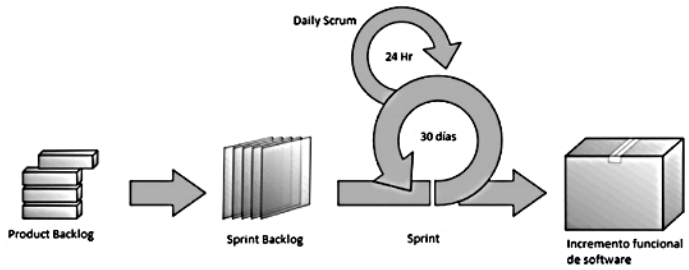


Ilustración 3-1: Metodología Scrum: fases de un Sprint

Fuente: (Navarro et al., 2013)

3.6.1. Proceso SCRUM

Los procesos de Scrum muestran las actividades específicas y la sistematización del proyecto.

Tabla 3-3: Procesos fundamentales SCRUM

FASE	PROCESOS FUNDAMENTALES DE SCRUM
INICIO	Creación del proyecto Identificación de Scrum Formación de equipos Desarrollo de épica Creación del producto Planificar lanzamiento
PLANIFICACIÓN Y ESTIMACIÓN	Creación de usuarios Comprometer usuarios Identificación de actividades Estimación de actividades Creación Sprint Backlog
IMPLEMENTACIÓN	Creación de entregables Realizar levantamiento Refinación de producto
REVISIÓN Y RETROSPECTIVA	Demostración y validación Retrospectiva Producto
LANZAMIENTO	Envió de entregables Retrospectiva proyecto

Fuente: (Stracquadaini, 2017)

3.7. Planificación

3.7.1. Personas y roles involucrados en el proyecto

Los roles descritos en la Tabla 3-4 son los definidos en base a la metodología SCRUM. Teniendo en total 3 roles, como (Product Owner) tenemos a la Granja Avícola "Ivanna" que participa como el dueño del sistema. El (Scrum Master) es el director del proyecto y por último el desarrollador que se encargara de la codificación de las funcionalidades del sistema.

Tabla 3-4: Roles del proyecto.

Persona	**Rol**
Iván Gallardo	Product Owner
Ing. Danilo Pastor	Scrum Master
Kevin Gallardo	Desarrollador

Realizado por: Kevin G., 2023

Se utilizó el método de talla de ropa conocido como T-Shirt Sizes para realizar la estimación de las tareas, en la Tabla 5 se detallan la talla y los puntos estimados que se designarán a la duración que se tendrá en cada Sprint, también se establece que la duración del sprint equivale a 40 puntos una semana, ya que se trabajará 8 horas al día los cinco días laborables de la semana.

Tabla 3-5: Método de la camiseta.

Talla	**Puntos estimados**	**Horas de trabajo**
S	5	5
M	10	10
L	20	20
XL	40	40

Realizado por: Kevin G., 2023

Se establecieron por el momento 11 requisitos funcionales para el desarrollo del sistema de adopción, cada uno de estos representan una historia de usuario conocido como HU-01, para las historias técnicas se representan como HT-03. El Product Backlog, contiene las 7 historias de

usuario y 4 historias técnicas, cada una de estas historias están priorizadas con las etiquetas: ALTA, MEDIA Y BAJA como se puede observar en la tabla 6:

Tabla 3-6: Descripción de historias de usuario y técnicas

ID	DESCRIPCIÓN	PRIORIDAD	PUNTOS ESTIMADOS	TALLA
HT_01	Como desarrollador deseo diseñar la arquitectura de la dapp	ALTA	40	XL
HT_02	Como desarrollador deseo registrarme en el proveedor Infura.	ALTA	40	XL
HT_03	Como desarrollador deseo configurar el entorno de desarrollo para el cliente front-end	MEDIA	20	L
HT_04	Como desarrollador deseo configurar el entorno de desarrollo para los contratos inteligentes(backend)	MEDIA	20	L
HT_05	Como desarrollador deseo configurar el Endpoint dentro del proveedor de blockchain	ALTA	40	XL
HT_06	Como desarrollador deseo configurar una cuenta con la billetera virtual para acceder a la blockchain	MEDIA	20	L
HT_07	Como desarrollador necesito diseñar la interfaz de usuario para la dapp	ALTA	40	XL
HU_01	Como desarrollador deseo codificar una función en el contrato inteligente para la carga de información en la blockchain.	ALTA	40	XL
HU_02	Como desarrollador deseo codificar una función en el contrato inteligente para traer de información de la red blockchain.	ALTA	40	XL

HU_03	Como desarrollador deseo desplegar el contrato inteligente en la red blockchain	ALTA	40	XL
HU_04	Como desarrollador instalar las dependencias necesarias para interactuar con la web	ALTA	40	XL
HU_05	Como usuario público deseo iniciar sesión en la dapp a través de Metamask	MEDIA	20	L
HU_06	Como usuario requiero cargar un nuevo documento.	ALTA	40	XL
HU_07	Como usuario requiero visualizar la información de documentos existentes en la red de blockchain.	MEDIA	20	L
HU_08	Como usuario requiero cargar un documento en verificación de documentos.	ALTA	40	XL
HU_09	Como usuario requiero validar la autenticidad de un documento.	ALTA	40	XL
HU_10	Como usuario requiero recargar gas en los sitios faucet de ethereum	MEDIA	20	L
TOTAL		560		

Realizado por: Kevin G., 2023

3.8. Sprint Backlog

Tabla 3-7: Sprint Backlog

SPRINT	ID	Fecha Inicio	Fecha Fin	PUNTOS ESTIMADOS	TOTAL
1	HT_01	26/09/2022	03/10/2022	40	100
	HT_02	03/10/2022	10/10/2022	40	
	HT_03	10/10/2022	17/10/2022	20	
2	HT_04	17/10/2022	24/10/2022	20	120
	HT_05	24/10/2022	31/10/2022	40	
	HT_06	31/10/2022	07/11/2022	20	
	HT_07	07/11/2022	14/11/2022	40	
3	HU_01	14/11/2022	21/11/2022	40	120
	HU_02	21/11/2022	28/11/2022	40	
	HU_03	28/11/2022	05/12/2022	40	
4	HU_04	05/12/2022	12/12/2022	40	120
	HU_05	12/12/2022	19/12/2022	20	
	HU_06	19/12/2022	26/12/2022	40	
	HU_07	26/12/2022	02/01/2023	20	
5	HU_08	02/01/2023	09/01/2023	40	100
	HU_09	09/01/2023	16/01/2023	40	
	HU_10	16/01/2023	20/01/2023	20	

Realizado por: Kevin G., 2023

Las historias técnicas, historias técnicas y las pruebas de aceptación se encuentran localizadas al final del documento en el anexo B.

3.9. Análisis de riesgos

En esta sección se analizarán las características de los riesgos, con sus respectivos parámetros y rangos de probabilidad, que puedan presentarse mientras se desarrolla el proyecto de integración curricular

3.9.1. Determinación de la probabilidad

Para poder realizar la gestión de riesgos tomaremos como referencia a la ISO 27001 dónde tomamos como referencia a todos sus indicadores (ISO-27001, 2013).

La presente tabla nos indica los rangos de probabilidad de los riesgos.

Tabla 3-8: Rango de probabilidad.

Rango de Probabilidad	Descripción	Valor
1 % a 30 %	Baja	1
30 % a 70 %	Media	2
70 % a 100 %	Alta	3

Realizado por: Kevin G., 2023

3.9.2. Determinación del impacto

En la presente tabla se detalla la cantidad de tiempo, que podría tardar cada riesgo que pudiera presentarse, dándole un valor de 1-4 según su impacto en el proyecto como explicamos a continuación:

Tabla 3-9: Determinación del impacto

Impacto	Retraso	Impacto técnico	Valor
Bajo	1 semana	Retraso menor	1
Moderado	3 semanas	Retraso considerable	2
Alto	1 mes	Retraso critico	3
Critico	Más de un mes	Suspensión del proyecto	4

Realizado por: Kevin G., 2023.

3.9.3. Determinación de exposición de riesgos

Como se puede observar en la presente tabla se ha identificado la posibilidad de que un riesgo se presente y afecte el proyecto de integración curricular, mediante notación visual en este caso con verde para baja, amarilla para media y roja como punto crítico de afectación.

Tabla 10-3. Exposición de riesgos

Exposición de riesgo	Valor	Color
Baja	1 -2	1
Media	2- 3	2
Critica	Mayor de 4	3

Realizado por: Kevin G., 2023

3.9.4. Priorización de riesgos

Tabla 3-10: Priorización de riesgos.

ID	Descripción	Prioridad	Valor de exposición	Prioridad
R01	Falta de compromiso del personal con el cronograma de trabajo establecido	CRITICA	9	1
R02	Requisitos son mal interpretados por el equipo del proyecto	CRITICA	9	1
R03	Mala estimación del tiempo de desarrollo de los requerimientos	BAJA	2	3
R04	Los requerimientos no superan las pruebas funcionales	MEDIA	4	2
R05	Cambio de requerimientos para el desarrollo del proyecto	MEDIA	4	2
R06	Retiro inesperado del desarrollador	CRITICA	6	1
R07	Pérdida de información	BAJA	2	3
R08	Robo o daño de los equipos de cómputo.	MEDIA	3	2

Realizado por: Kevin G., 2023

3.10. Desarrollo del aplicativo

3.10.1. Arquitectura de la aplicación descentralizada

Para el presente trabajo se implementó una arquitectura para aplicaciones descentralizadas, dónde un cliente está conectado a la red de Blockchain a través de la web3 pasando por un proveedor Blockchain llamado Infura. Esta arquitectura requiere de librerías para que un navegador pueda acceder a la información en la Blockchain. Cabe destacar que la arquitectura presentada sólo

puede funcionar en un navegador web, estrictamente en un dispositivo que admita extensiones para conectar billeteras virtuales e interactuar con la Blockchain. En la siguiente figura 2-3 se aprecia un resumen de la arquitectura usada:

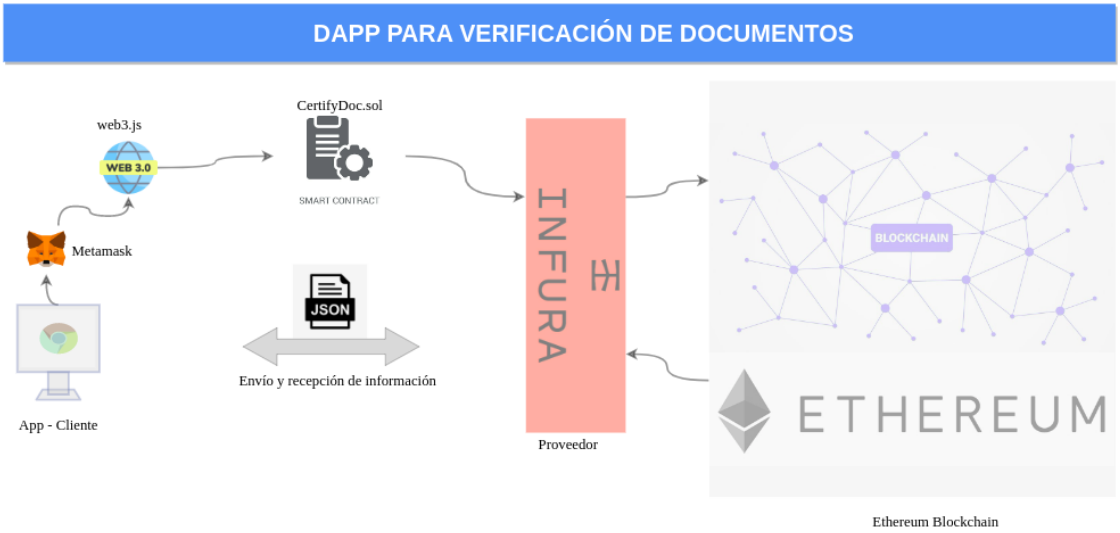


Ilustración 3-2: Arquitectura de la Dapps

Realizado por: Kevin G., 2023

3.10.2. Diseño de las interfaces de la aplicación descentralizada

Con la finalidad de agilizar el desarrollo dentro de la planificación se optó por el Framework de Next.js en el cuál no se necesita configurar cosas repetitivas como el enrutamiento desde cero ya que este Framework nos proporciona un enrutador incorporado. Es importante también mencionar librerías (figura 3-3) como: web3, Wallet, Ehers, Hardhat, Openzeppelin, etc. las cuales son indispensables para el funcionamiento del proyecto porque ayudan a comunicarse a la Dapps con el contrato inteligente desplegado en la red de Blockchain.

```
"dependencies": {
  "@portis/web3": "^4.0.7",
  "@walletconnect/web3-provider": "^1.8.0",
  "authereum": "^0.1.14",
  "eslint": "8.27.0",
  "eslint-config-next": "13.0.3",
  "ethers": "^5.7.2",
  "fortmatic": "^2.4.0",
  "next": "13.0.3",
  "react": "18.2.0",
  "react-dom": "18.2.0",
  "react-socks": "^2.2.0",
  "semantic-ui-css": "^2.5.0",
  "semantic-ui-react": "^2.1.3",
  "web3": "^1.8.1",
  "web3-provider": "^1.0.0",
  "web3modal": "^1.9.10"
}
```

Ilustración 3-3: Dependencias del proyecto

Realizado por: Kevin G., 2023

A continuación, se describirá las principales vistas de la aplicación descentralizada;

En la figura 4-3 se muestra la pantalla principal del aplicativo dónde se tiene la facilidad de ir a verificar un documento a través de un botón, cabe recalcar que para esa funcionalidad no es necesario Loguearse en el aplicativo. Otro aspecto importante es el inicio de sesión en la Wallet por la parte superior derecha, dónde la Dapps establecerá conexión con el contrato inteligente para poder cargar documentos.

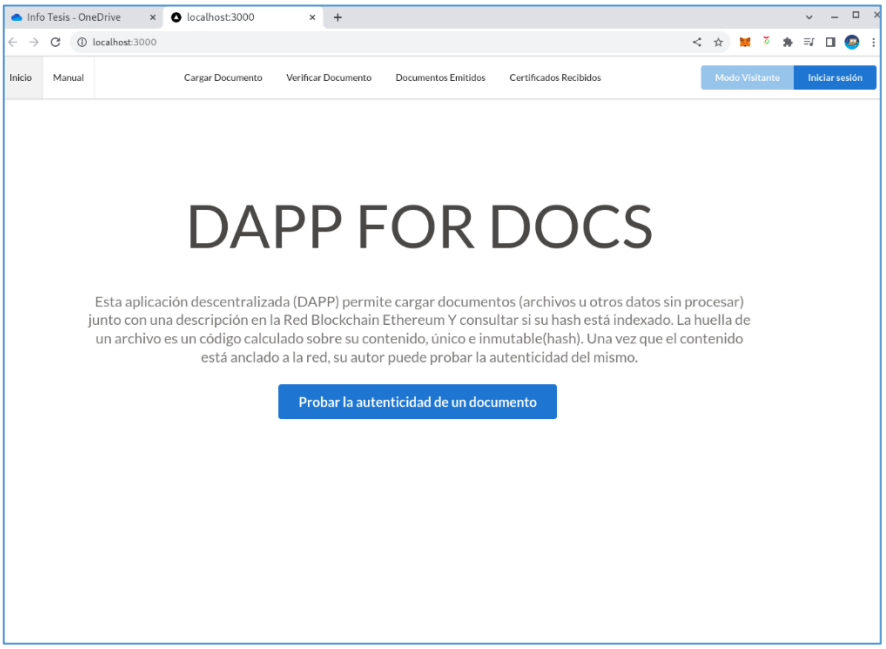


Ilustración 3-4: Pantalla principal de la Dapps

Realizado por: Kevin G., 2023

3.10.3. Diseño del contrato inteligente para la aplicación descentralizada

Para el funcionamiento de la aplicación descentralizada existe un contrato inteligente simple, desarrollado en Solidity, que relaciona un hash (del documento anclado para verificación) con un registro de Blockchain que consta de un hash, un emisor, un receptor, descripción, la fecha y la hora. En la interfaz, el hash se toma de un documento cargado desde el cliente.

CertifyDoc.sol

ardhat > contracts > CertifyDoc.sol

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.7.0 <0.9.0;


contract CertifyDoc {
    /**struct que contien un certificado con la información del documento que se desea anclar a blockchain */
    struct certificate {
        bytes32 docHash;
        address issuer;
        address recipient;
        uint datetime;
        string description;
    }
    /** array de certificados. */
    certificate[] public certificates; //

    /** evento que retorna información del documento anlcado dado su hash y su identificador de persona */
    event CertificateIssued(bytes32 indexed docHash, uint indexed index);

    /**Varios Hashmap para almancenar información de hash, emisores, receptores, para varios documentos */
    mapping(bytes32 => uint[]) public docHashMap;


    mapping(address => uint[]) public issuerMap;


    mapping(address => uint[]) public recipientMap;


    mapping(bytes32 => address) public docHashOwnerMap;
/**Funcion que ancla un vcertificado en la red de blockhain */
    function certify(bytes32 _docHash, address _recipient, string memory _description) public {

            certificate storage newCertificate = certificates.push();
            newCertificate.docHash = _docHash;
            newCertificate.issuer = msg.sender;
            newCertificate.recipient = _recipient;
            newCertificate.description = _description;
            newCertificate.datetime = block.timestamp;

```

Ilustración 3-5: Contrato inteligente

Realizado por: Kevin G., 2023

3.10.4. Contrato inteligente desplegado en la red Goerli Blockchain

La Ilustración 3-5 muestra a través de Ehterscan el contrato inteligente desplegado en la red Goerli Testen de Ethereum Blockchain. El contrato inteligente es un programa informático que se ejecuta automáticamente cuando se cumplen ciertas condiciones, y que permite establecer acuerdos confiables y transparentes entre diferentes partes sin la necesidad de intermediarios. En la figura se puede observar información general sobre sus características y también sobre las transacciones asociadas a este contrato.

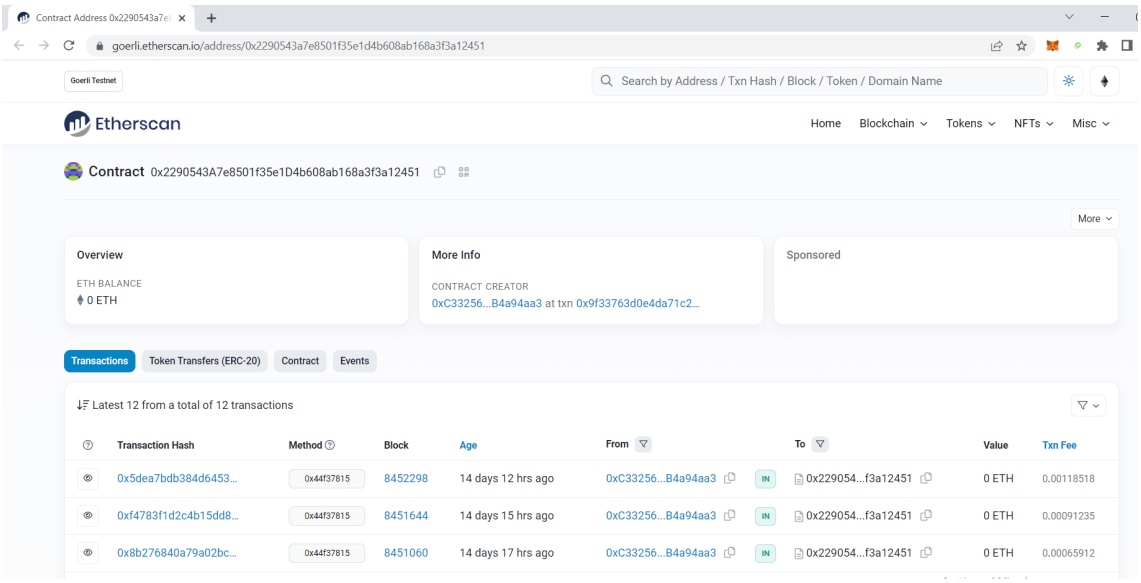


Ilustración 3-6: Contrato inteligente desplegado

Realizado por: Kevin G., 2023

CAPÍTULO IV

4. RESULTADOS

En el presente capítulo se desarrolla la evaluación de la seguridad de la aplicación descentralizada mediante la norma ISO25010:2011 con relación a las Sub-características que se han determinado siendo estas integridad, autenticidad y confidencialidad, de esta manera se procede a realizar la comprobación de la hipótesis.

Los resultados que se muestran a continuación se detallan con el análisis, utilizando las técnicas y métodos definidos para dar cumplimiento a los objetivos y a la hipótesis planteada.

4.1.1. Confidencialidad

Con relación a la confidencialidad de la Dapps se han desarrollado cuatro preguntas, las cuales permuten determinar la seguridad que existe en la privacidad, a continuación, en la tabla 1 se muestra la frecuencia con respecto a la pregunta 1 ¿El sistema ofrece al usuario la opción de privacidad de datos?

Tabla 1-4. Privacidad de datos

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	0	0%
FALSO	3	100%
TOTAL	3	100%

Realizado por: Kevin G., 2023

Con relación a la privacidad de los datos del usuario en el Tabla 1-4 se observa que el 100% de los evaluadores no identifican que pueda existir tal aspecto, pues la Dapps se encuentra desplegada en una red pública.

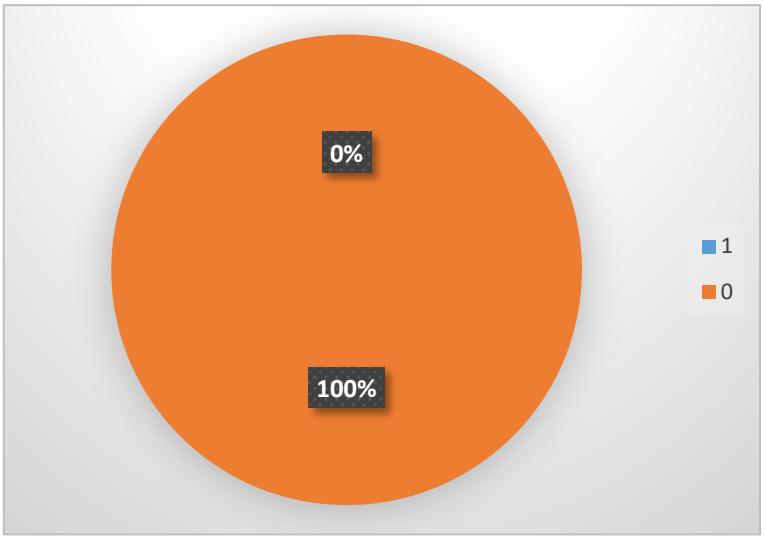


Ilustración 4-1: Privacidad de datos

Realizado por: Kevin G., 2023

En la siguiente tabla 2 se describe los resultados que se obtienen con respecto a la pregunta 2, en el sistema, ¿hay alguna forma de que los usuarios no registrados accedan a los datos de los usuarios registrados?

Tabla 4-1: Usuarios no registrados con acceso a datos

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	0	0%
FALSO	3	100%
TOTAL	3	100%

Realizado por: Kevin G., 2023

En cuanto a la posibilidad de que un usuario que no se encuentra registrado pueda tener acceso a los datos de usuarios que si se encuentran registrados se determina en el gráfico 2-4 que el 100% de los evaluadores afirman que no existe tal posibilidad, debido a que para interactuar con la Dapps y su información en la red Blockchain, es necesario que el usuario se registre con su billetera, cree su cuenta, y luego si interactuar con la Dapps.

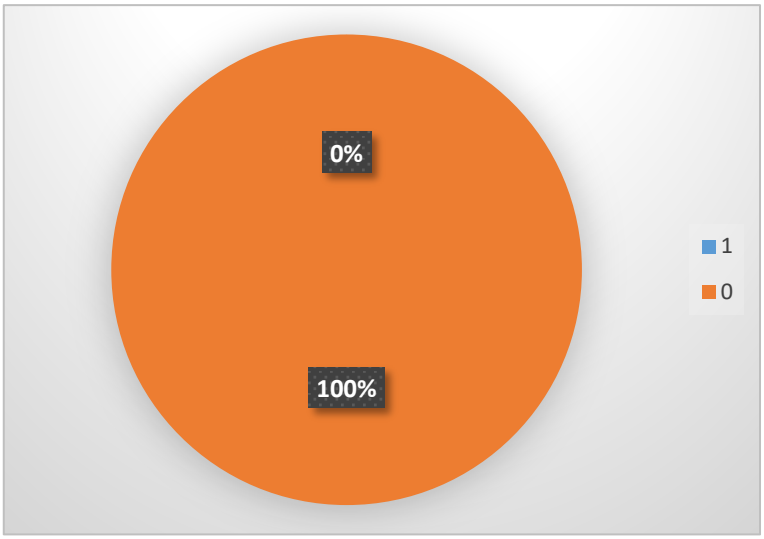


Ilustración 4-2: Usuarios no registrados con acceso a datos

Realizado por: Kevin G., 2023

A continuación, en la tabla 3 se describe la respuesta de los evaluadores con relación a la pregunta, en el sistema, ¿hay alguna forma de que los administradores del sitio web puedan ver la información personal de los usuarios?

Tabla 4-2: Acceso a información personal

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	3	100%
FALSO	0	0%
TOTAL	3	100%

Realizado por: Kevin G., 2023

En el gráfico 3-4 se determina que el 100% de los evaluadores concuerda con la interrogante con relación a que, si los administradores del sitio web podrán tener acceso de la información personal de los usuarios, debido a que no existen jerarquías en la Dapps, además existe un contrato de validación de la información.

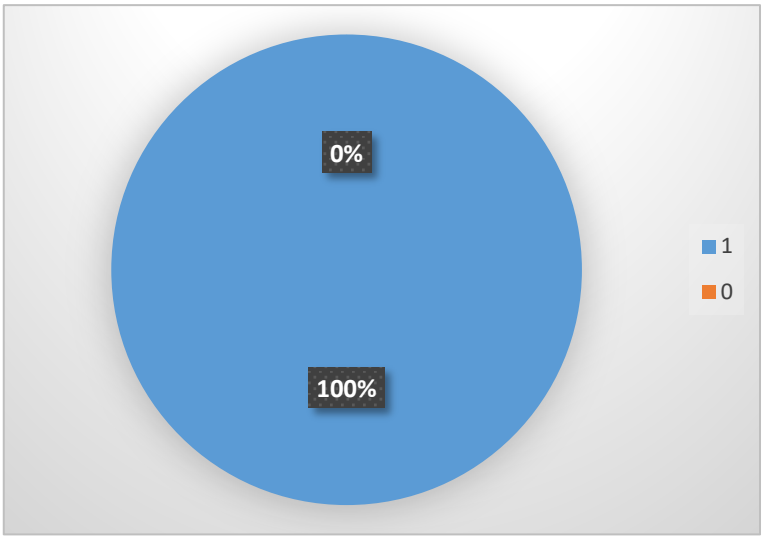


Ilustración 4-3: Acceso a información personal

Realizado por: Kevin G., 2023

Con respecto a la confidencialidad en la tabla 4 se describe la respuesta a la pregunta 4 ¿El sistema 17 almacena en la base de datos un control de acceso?

Tabla 4-3: Control de acceso

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	0	0%
FALSO	3	100%
TOTAL	3	100%

Realizado por: Kevin G., 2023

A continuación, en el Ilustración 4-4. Con respecto al control de acceso al sistema que se almacenan en la base de datos el 100% de los evaluadores demuestran que es falso, debido a que no se interactúa con una base de datos, el control de acceso se maneja mediante una billetera asociada a una cuenta Ethereum.

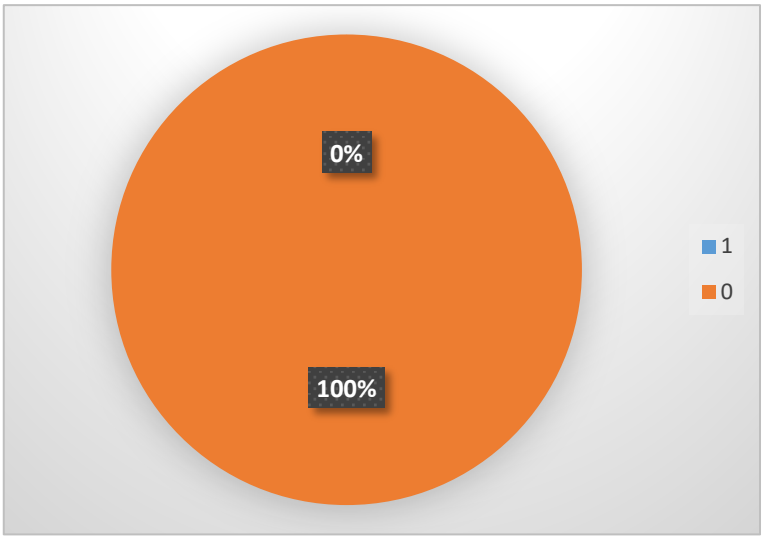


Ilustración 4-4: Control de acceso

Realizado por: Kevin Gallardo, 2023.

A continuación, en la tabla 5 se detalla el cálculo de la media de cada pregunta de acuerdo con la respuesta de los evaluadores, además de la media general con relación a las preguntas que verifican la confidencialidad de la Dapps.

Tabla 4-4: Media de evaluación de preguntas de confidencialidad

EVALUADORES	PREGUNTA 1	PREGUNTA 2	PREGUNTA 3	PREGUNTA 4
1	2	2	1	2
2	2	2	1	2
3	2	2	1	2
SUMA	6	6	3	6
MEDIA	2	2	1	2
Media general				1,75
Verdad=1; Falso=2				

Realizado por: Kevin G., 2023

El resultado de la media de cada pregunta y la media general se muestran en el gráfico 5-4 donde se obtuvo que el valor de la media general es de 1.75 sobre 2 acerca de las preguntas de identificación de confidencialidad lo que representa que la confidencialidad de la Dapps es **admisible** situado entre 60 % <= X < 90 % obteniendo un porcentaje de 87.5%.

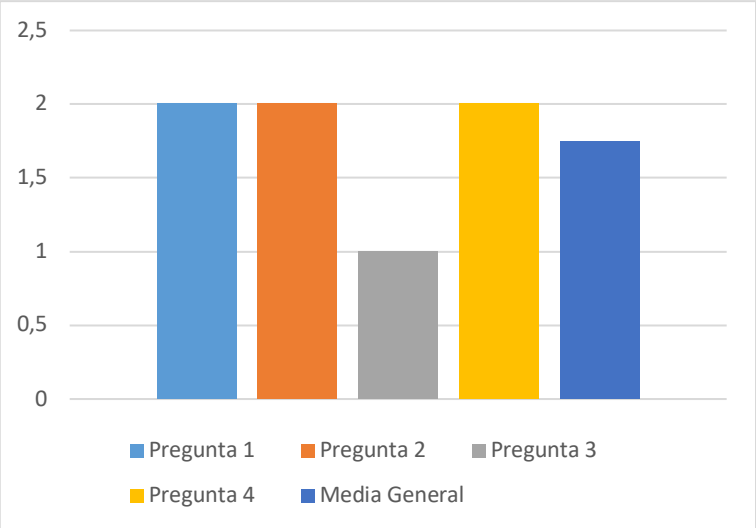


Ilustración 4-5: Media de evaluación de preguntas de confidencialidad

Realizado por: Kevin G., 2023

4.1.2. Integridad

Con respecto a la evaluación de la integridad de la Dapps a continuación en la tabla 6 se describe la respuesta por parte de los evaluadores a la pregunta 5, ¿El sistema considera un paso de autenticidad?

Tabla 4-5: Sistema de autenticidad

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	3	100%
FALSO	0	0%
TOTAL	3	100%

Realizado por: Kevin G., 2023

En el gráfico 6-4 se identifica que el 100% de los evaluadores mencionan que es verdad que el sistema considera un paso de autenticidad, puesto que cada billetera maneja una frase de recuperación y una llave privada de acceso.

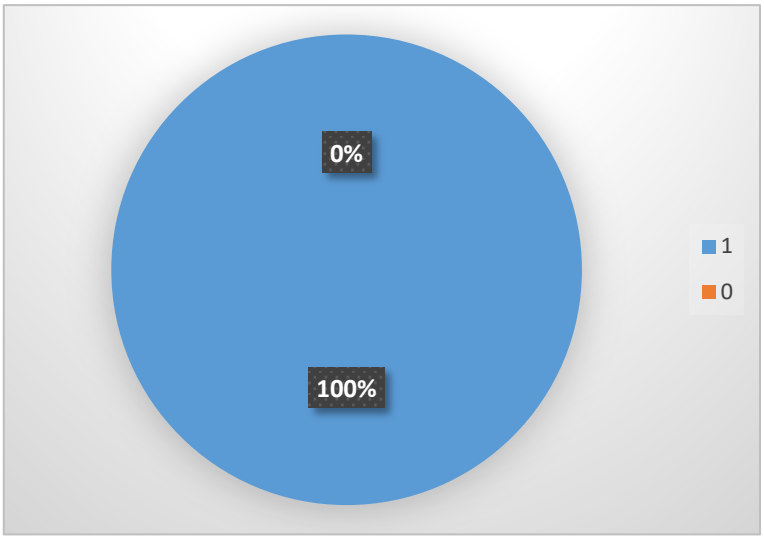


Ilustración 4-6: Sistema de autenticidad

Realizado por: Kevin Gallardo, 2023.

En cuanto a la posibilidad de del cambio de datos del usuario, en la tabla 7 se muestran los resultados de la pregunta 6, ¿El sistema solicita una confirmación de contraseña al cambiar los datos del usuario?

Tabla 4-6: Confirmación de contraseña

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	0	0%
FALSO	3	100%
TOTAL	3	100%

Realizado por: Kevin G., 2023

Con respecto a la solicitud de la confirmación de contraseña para realizar cambios en los datos del usuario en el gráfico 7-4 el 100% de los evaluadores han determinado que es falso debido a que ninguna información puede ser alterada, pues se consideran los datos de usuario a la dirección de la cuenta Ethereum que aloja la billetera.

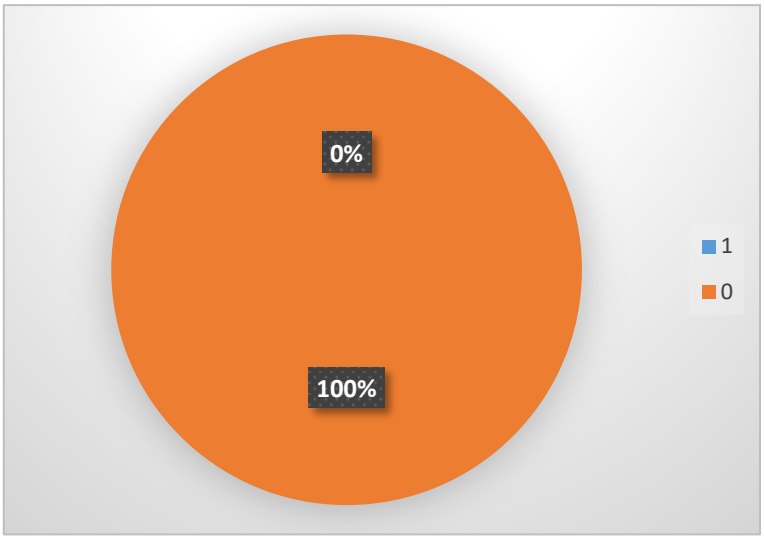


Ilustración 4-7: Confirmación de contraseña

Realizado por: Kevin G., 2023

A continuación, en la tabla 8 con relación a la integridad acerca de la notificación de cambio de datos se describen las respuestas a la interrogante 7, ¿El sistema envía alguna notificación al usuario cuando hay una modificación de datos?

Tabla 4-7: Notificación en cambio de datos

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	0	0%
FALSO	3	100%
TOTAL	3	100%

Realizado por: Kevin G., 2023

Con respecto a la posibilidad del envió de alguna notificación al usuario con respecto a la modificación de datos en el gráfico 8-4 el 100% de los evaluadores concuerda en que esta interrogación es falsa debido a que no envía dicha información pues no se puede modificar la información.

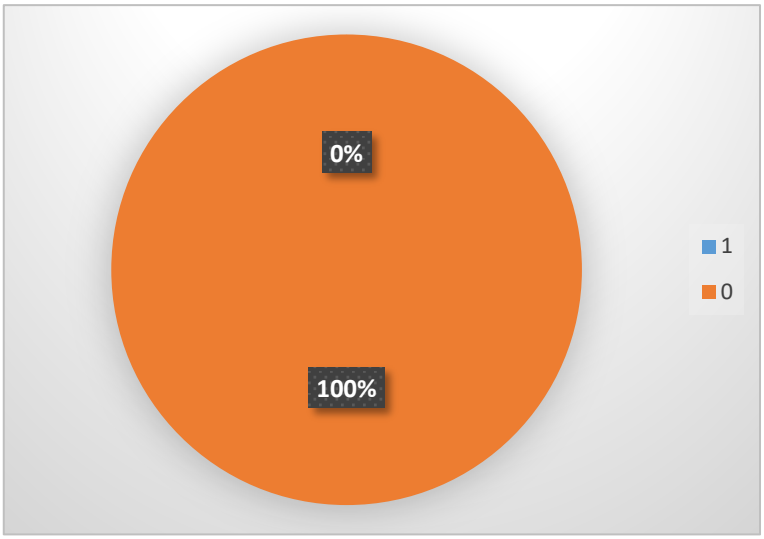


Ilustración 4-8: Notificación en cambio de datos

Realizado por: Kevin G., 2023

En la tabla 9 se muestra la respuesta por parte de los evaluadores con respecto a la pregunta 8, ¿El sistema considera una jerarquía en el acceso de varios datos entre los administradores del sitio?

Tabla 4-8: Jerarquía de datos en administradores

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	0	0%
FALSO	3	100%
TOTAL	3	100%

Realizado por: Kevin G., 2023.

Con relación a la identificación de jerarquía en el acceso de varios datos entre los administradores del sitio en el gráfico 9-4 el 100% de los evaluadores manifiestan que esta aseveración es falsa debido a que no existen jerarquías en la Dapps, además se cuenta con un contrato inteligente, pues está escrito de tal forma que todos los usuarios asociados a Ethereum con su billetera consigan interactuar con la Dapps.

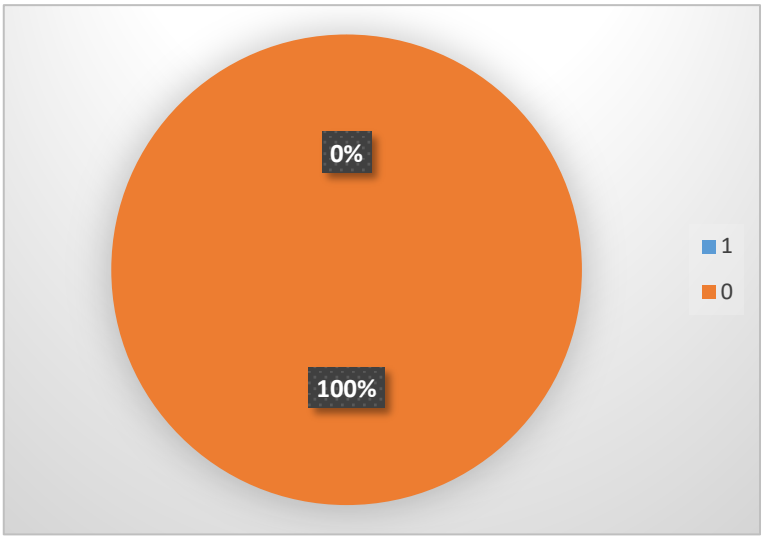


Ilustración 4-9: Jerarquía de datos en administradores

Realizado por: Kevin G., 2023

A continuación, en la tabla 10 se muestra el cálculo de la media de cada pregunta contestada por los evaluadores, además de la media general con relación a las preguntas que verifican la integridad que ofrece la Dapps.

Tabla 4-9: Media de evaluación de preguntas de integridad

EVALUADORES	PREGUNTA 1	PREGUNTA 2	PREGUNTA 3	PREGUNTA 4
1	1	2	2	2
2	1	2	2	2
3	1	2	2	2
SUMA	3	6	6	6
MEDIA	1	2	2	2
Media general				1,75
Verdad=1 ; Falso=2				

Realizado por: Kevin G., 2023

La obtención de la media con relación a cada pregunta y la media general se muestran en el gráfico 10-4 donde se obtuvo que el valor de la media general es de 1.75 sobre 2 acerca de las preguntas de identificación de integridad de la Dapps, lo que permite verificar que existe un porcentaje de 87.5% en integridad situado entre 60 % <= X < 90 % que se considera **admisible.**

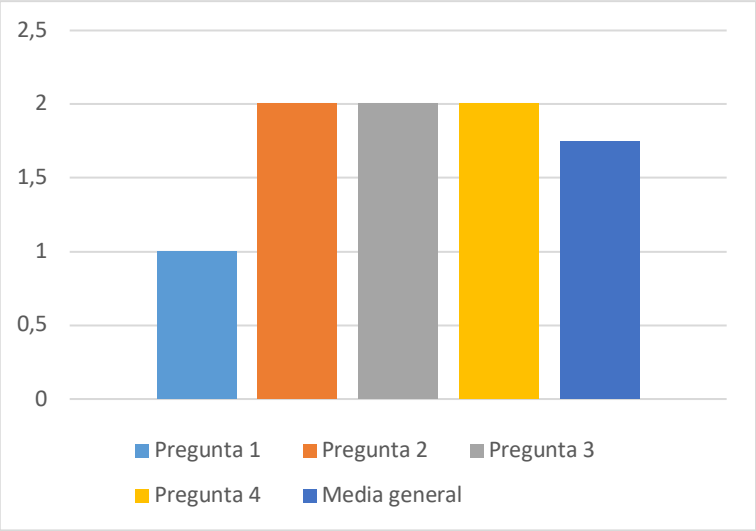


Ilustración 4-10: Media de evaluación de preguntas de integridad

Realizado por: Kevin G., 2023

4.1.3. Autenticidad

Con respecto a la autenticidad de la Dapps, a continuación, en la tabla 11 se muestran las respuestas con relación a la pregunta 9 ¿El sistema permite la conexión de un mismo usuario en dos instancias de acceso diferentes?

Tabla 4-10: Conexión en dos instancias

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	3	100%
FALSO	0	0%
TOTAL	3	100%

Realizado por: Kevin G., 2023

A continuación, en el gráfico 11-4 con relación a la interrogante acerca de que si el sistema permite la conexión de un mismo usuario en dos instancias de diferente acceso el 100% de los evaluadores mencionan que es verdadero, esto acontece siempre y cuando se pueda autenticar con su billetera, la cual contiene verificación por contraseña, por llave privada y por frase de recuperación.

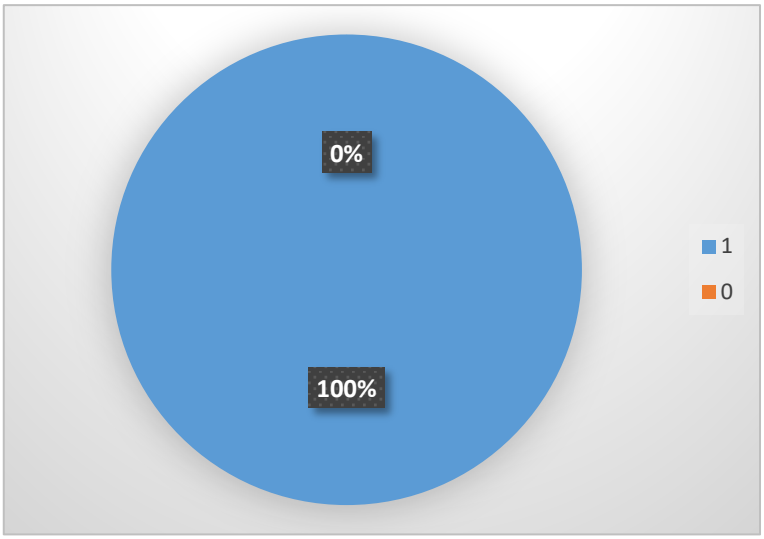


Ilustración 4-11: Conexión en dos instancias

Realizado por: Kevin G., 2023

En relación con la autenticidad de la Dapps con respecto a la pregunta 10, ¿El sistema cuenta con un asistente para el registro de nuevos usuarios?, en la tabla 12 se muestran los resultados expuestos por los evaluadores.

Tabla 4-11: Asistente de registro

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	3	100%
FALSO	0	0%
TOTAL	3	100%

Realizado por: Kevin G., 2023

En el gráfico 12-4 con respecto al asistente para el registro de nuevos usuarios se identifica que el 100% de los evaluadores mencionan que la Dapps si cuenta con dicho sistema, debido a que la Dapps detecta si no existe una billetera con cuenta asociada y redirige a la página de Metamask para poder hacer el vínculo.

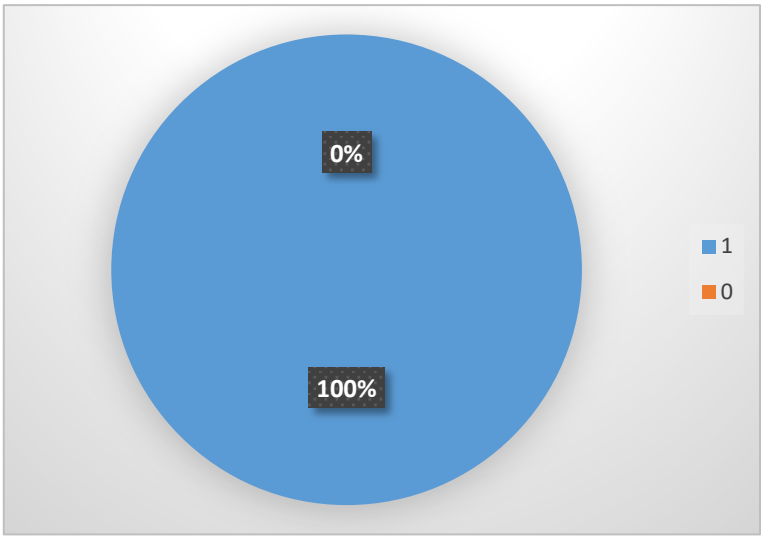


Ilustración 4-12: Asistente de registro

Realizado por: Kevin G., 2023

A continuación, en la tabla 26 se determinan los resultados de la Pregunta 11, ¿El sistema contempla que no puede haber dos cuentas con el mismo correo electrónico o nombre de usuario, pero datos diferentes?

Tabla 4-12: Dos cuentas con el mismo correo o usuario

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	3	100%
FALSO	0	0%
TOTAL	3	100%

Realizado por: Kevin G., 2023

Con respecto a si el sistema contempla si no puede haber dos cuentas con el mismo correo electrónico o nombre de usuario, pero datos diferentes, en el gráfico 13-4 se identifica que el 100% de los evaluadores concuerdan en que es verdadero debido a que en la red descentralizada Blockchain no existen direcciones de usuario similares, por lo tanto, es imposible la duplicidad.

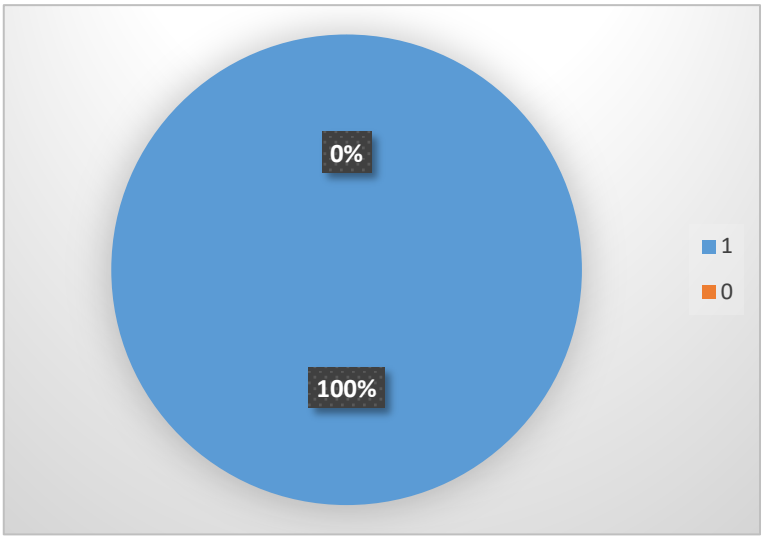


Ilustración 4-13: Dos cuentas con el mismo correo o usuario

Realizado por: Kevin G., 2023

A continuación, con respecto a la Pregunta 12 ¿El sistema contempla el paso de verificación de correo electrónico, cuando se genera un usuario?, en la tabla 14 se muestra el resultado que los evaluadores manifestaron.

Tabla 4-13: Verificación de correo al crear usuario

ITEM	FRECUENCIA	PORCENTAJE
VERDADERO	0	0%
FALSO	3	100%
TOTAL	3	100%

Realizado por: Kevin G., 2023

Con respecto a la interrogante el sistema contempla el paso de verificación de correo electrónico, cuando se genera un usuario los evaluadores en el gráfico 14-4 mencionan que esta aseveración es falsa debido a que no se asocia correo electrónico, la Dapps interactúa directamente con la cuenta de Ethereum contemplada en la billetera.

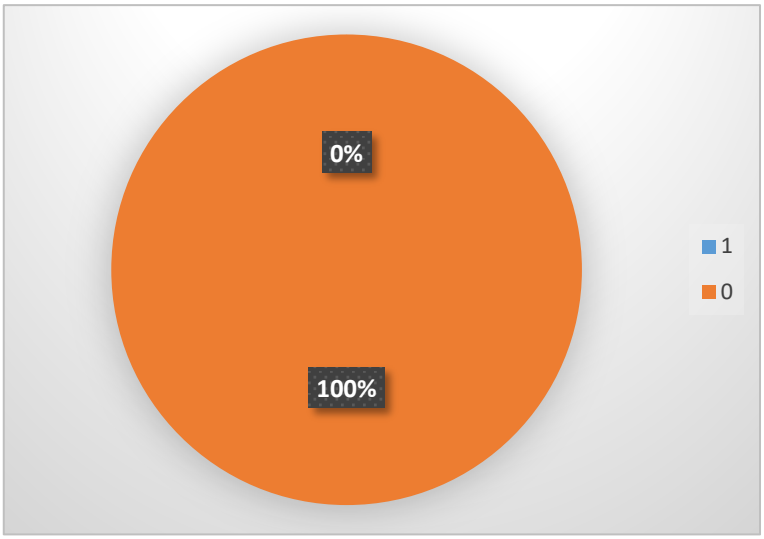


Ilustración 4-14: Verificación de correo al crear usuario

Realizado por: Kevin Gallardo, 2023.

A continuación, en la tabla 15 se detalla el cálculo de la media de cada pregunta de acuerdo con la respuesta de los evaluadores, además de la media general con relación a las preguntas que verifican la autenticidad de la Dapps.

Tabla 4-14: Media de evaluación de preguntas de autenticidad

EVALUADORES	PREGUNTA 1	PREGUNTA 2	PREGUNTA 3	PREGUNTA 4
1	1	1	1	2
2	1	1	1	2
3	1	1	1	2
SUMA	3	3	3	6
MEDIA	1	1	1	2
Media general				1,25
Verdad=1; Falso=2				

Realizado por: Kevin G., 2023

El resultado de la media de cada pregunta y la media general se muestran en el gráfico 15-4 donde se obtuvo que el valor de la media general es de 1.25 sobre 2 acerca de las preguntas de identificación de confidencialidad lo que representa que la autenticidad de la dapp es segura para el uso de esta encontrándose en un porcentaje de 60 % <= X < 90 % que constituye un nivel **admisible.**

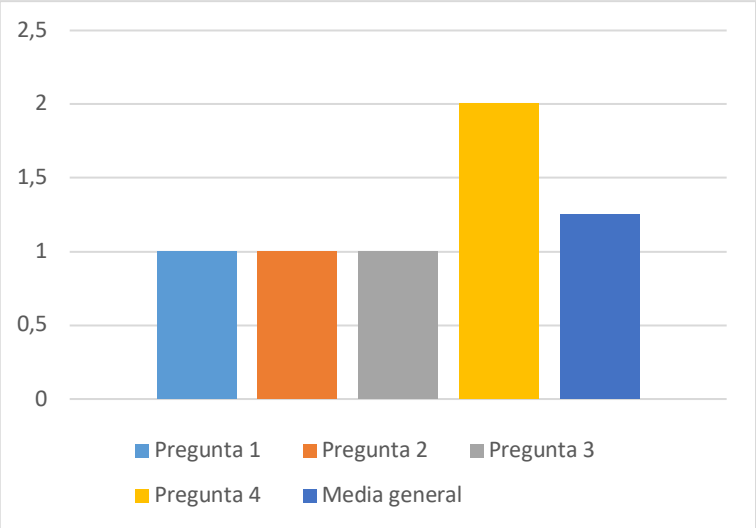


Ilustración 4-15: Media de evaluación de preguntas de autenticidad

Realizado por: Kevin Gallardo, 2023.

4.1.4. Resultados generales

La Tabla 4-16 presenta el grado de cumplimiento para cada Sub-características de la característica de seguridad evaluada en la DAPP desarrollada. Se utilizó la norma ISO 25010:2011 para establecer los criterios de evaluación y se obtuvo un grado de cumplimiento para cada subcategoría evaluada.

En este caso, se evaluaron tres subcategorías: confidencialidad, integridad y autenticidad. Para confidencialidad e integridad, se obtuvo un grado de cumplimiento admisible del 87.5%, lo que indica que la DAPP cumple con los criterios establecidos para estas subcategorías. Por otro lado, para autenticidad, se obtuvo un grado de cumplimiento admisible del 62.5%, lo que sugiere que hay margen de mejora en esta subcategoría más sin embargo está dentro del criterio.

Tabla 4-15: Grado de cumplimiento por cada Sub-características

Subcategoría para la característica de Seguridad	Criterio	Grado de cumplimiento
Confidencialidad	ADMISIBLE	87.5%
Integridad	ADMISIBLE	87.5%
Autenticidad	ADMISIBLE	62.5%

Realizado por: Kevin G., 2023

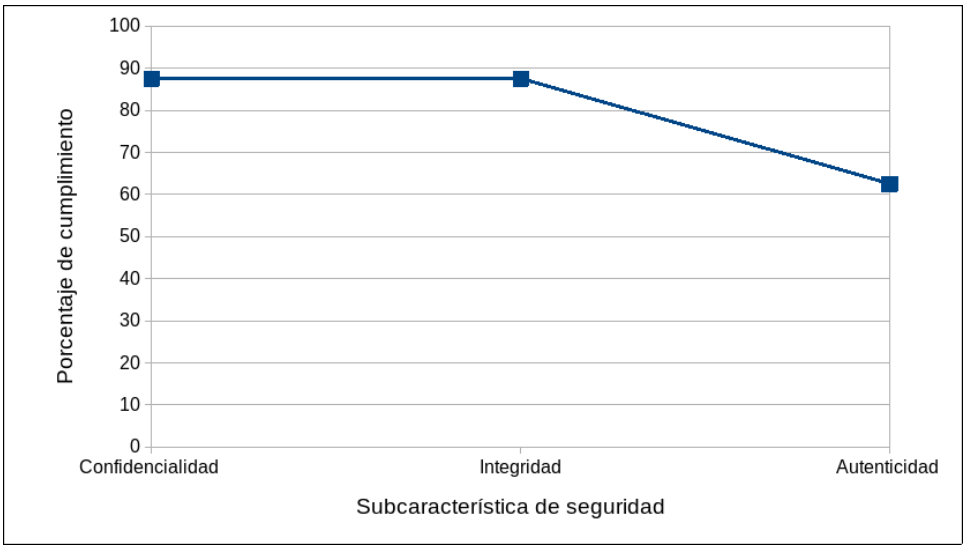


Ilustración 4-16: Porcentaje de cumplimiento por subcategoría

Realizado por: Kevin G., 2023

En el gráfico 4-16 podemos observar el cumplimiento por subcategoría en cuanto a la seguridad de la Dapps. Es importante tener en cuenta que estos resultados deben ser interpretados dentro del marco de referencia de la herramienta de medición utilizada, que establece diferentes rangos y criterios para clasificar la aceptación del porcentaje obtenido de los criterios positivos totales.

CONCLUSIONES

- Después de comparar las aplicaciones convencionales con las Dapps, se llegó a la conclusión de que las Dapps tienen varias ventajas significativas, incluyendo su seguridad, descentralización y disponibilidad. Estas características aseguran que la operatividad de las Dapps con tecnología Blockchain sean altamente confiables y confiables para los usuarios.

- Luego de comparar diferentes tipos de Blockchain para el desarrollo de la solución, se optó por una red Blockchain pública (Ethereum-Goerli) debido a que permite el acceso y verificación de información por parte de cualquier persona. Esta red es transparente y abierta, sin entidades centralizadas que regulen su funcionamiento, lo que la hace altamente confiable y adecuada para las necesidades del proyecto.

- La metodología ágil de desarrollo de software SCRUM es flexible y permite dimensionar mejor los proyectos para poder llevar a cabo su ejecución; aplicando esta metodología se tuvo como resultado una duración de 360 horas de desarrollo, lo que es el resultado de 7 historias de usuario y 4 historias técnicas, además de 11 tareas de ingeniería y 11 pruebas de aceptación

- Se empleó una metodología de evaluación de seguridad basada en la norma 25010:2011 para evaluar la seguridad de la DAPP en relación con las Sub-características de confidencialidad, integridad y autenticidad. Se utilizó un instrumento de evaluación y una tabla de criterios para realizar la evaluación, lo que arrojó resultados satisfactorios y clasificó la DAPP como "segura" con un nivel “admisible” en función de las Sub-características mencionadas.

- Se puede concluir, tras realizar la investigación, desarrollar la solución y evaluar la seguridad, que una aplicación descentralizada puede solucionar problemas como la alteración o pérdida de información dentro de la granja avícola. Además, esta información puede ser validada fácilmente por todos los usuarios que accedan a la DAPP. En consecuencia, la hipótesis inicial planteada se ha confirmado.

RECOMENDACIONES

- En el proceso de desarrollo de una Dapps, al momento de codificar los contratos inteligentes previo a su despliegue, se recomienda instalar ganache, con la finalidad de desplegar los contratos inteligentes localmente para realizar pruebas antes de ser desplegados en la red de Blockchain a través de Infura.

- Se recomienda continuar con el desarrollo de la Dapps, para integrar plataformas cómo IPFS, que permiten el almacenamiento y fácil recuperación de data en la Blockchain, lo cuál sería un valor adicional al proyecto.

- En cuanto a las billeteras virtuales cómo Metamask, al momento de registrarse se recomienda almacenar la clave secreta o bien sea la llave privada, para facilitar la recuperación o acceso a la Wallet al momento de cambiar de dispositivo.

- Para el desarrollo de Dapps se recomienda revisar la documentación oficial de las tecnologías involucradas, mirar videos tutoriales, explorar código en repositorios públicos, para que se facilite la interacción con la Blockchain.

BIBLIOGRAFÍA

ALHARBY, M., & MOORSEL, A. *Blockchain-based Smart Contracts: A Systematic Mapping Study.* Nuev York. Edicions l, 2017, p.15.

ALVAREZ, Diana; et al. *A methodology to evaluate the safety-based witch.* México, Edicions 7, 2021, pp.1-7.

AMIR, Rana; et al. *Retail level Blockchain transformation for product supply chain using truffle development platform.* California. Edicions l, 2021, p.26.

BURGWINKEL, D. *Blockchain Technology: Einuhrung fur Bussiness und IT Manager.* Boston : Edicions 26, 2016, p.18.

BUTERIN, V. *A Next Generation Smart Contract y Decentralized.* Chicago. Edicions l, 2019, p.40.

CUESTA, G. *Solidity, el lenguaje de programación más usado para crear Smart Contracts.* Edicions 1, 2021, p.32.

DIKA, A. *Ethereum Smart Contracts: Security.* California. Edicions l, 2017, p.52.

GALVEZ, Juan, et al. *Future challenges on the use of blockchain for food traceability analysis.*Virginia. Edicions 107, 2018, p.75.

GARCÍA, P. *Criptoderecho. La regulación de Blockchain.* Madrid. Edicions 7, 2018, pp.45-60.

GÓMEZ, D. *Aplicación descentralizada basada en sistema de incentivos.* Catalunya. Edicions l, 2021, p.101.

IBÁÑEZ, J. *Blockchain : primeras cuestiones en el ordenamiento español.* Madrid. Edicions 16, 2018, p.32.

LUQUE, R. *Blockchain: Estado del arte, tendencias y retos.* Ovieda. Edicions l, 2022, pp.15-25.

MAKHDOOM, Imran; et al. *PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities.* London. Edicions 88, 2020, p.30.

MANSOUR, Ali; et al. *Sistema de voto electrónico descentralizado basado en Smart Contract mediante el uso de tecnología Blockchain.* Georgia. Edicions 15, 2021, p.12.

MARTÍN, A. *BLOCKCHAIN: aplicación en el Registro de la Propiedad e implicaciones en materia probatoria.* Mssachussetts. Edicions 2, 2021. p.102.

MIN, H. *Blockchain technology for enhancing supply chain resilience.* Florida. Edicions 69, 2019, p.21.

MOUGAYAR, W. *Blockchain Trainings Corporate Brochure.* Florida. Edicions l, 2019. p.18.

MUZAMMAL, Muhammad; et al. *Renovating blockchain with distributed databases: An open source system.* California. Edicions 90, 2019, pp.15-31.

NAVARRO , Andrés; et al. *Revisión de metodologías ágiles para el desarrollo de software.* Caribe. Edicions 11, 2013, p.19.

OKTIAN, Y., & LEE, S. *BorderChain: Blockchain-Based Access Control Framework for the Internet of Things Endpoint.* California. Edicions l, 2021, p.10.

PECK, M. *Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem.* California. Edicions l, 2017, p.17.

PEYROTT, S. *An Introduction to Ethereum and Smart Contracts.* Virginia. Edicions l, 2017, p.9.

RADU, L. *Disruptive Technologies in Smart Cities: A Survey on Current Trends and Challenges.* Inglaterra. Edicions l, 2022, p.22.

REYNA, Ana; et al. *On blockchain and its integration with IoT. Challenges and opportunities.* Texas. Edicions 88, 2018, p.98.

ROSERO, L. *Propuesta de una aplicación basada en la tecnología blockchain para el registro de títulos académicos.* Quito. Edicions 2, 2019, p.23.

SINGH, M., & KIM, S. *Branch based blockchain technology in intelligent vehicle.* Florida. Edicions 145, 2018, p.4.

STRACQUADAINI, L.*Una guía para el cuerpo de conocimiento de Scrum.* Texas. Edicions 3, 2017, p.21.

SULLIVAN, C., & BURGER, E. *E-Residency and Blockchain.* Washington. Edicions 5, 2017, p.87.

VILALTA, A. *Smart legal contracts y blockchain: La contratación inteligente a través de la tecnología blockchain.* Madrid, Edicions 8, 2019, pp.45-47.

VIRIYASITAVAT, W., & HOONSOPON, D. *Blockchain characteristics and consensus in modern business processes.* California. Edicions 4, 2019, p.19.

WANG, Xiaonan; et al. *Contrato inteligente basado en blockchain para la gestión de la demanda de energía.* Georgía. Edicions 158, 2019, p.72.

WINDLEY, P. *The Live Web.* Boston. Edicions 4, 2014, p.16.

YAVARI, Mostafa; et al. *An Improved Blockchain-Based Authentication Protocol for IoT Network Management.* Nueva York. Edicions 5, 2020, p.40.

ZHENG, Zibin; et al. *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.* California. Edicions 3, 2017, p.8.

ANEXOS

ANEXO A: HISTORIAS TÉCNICAS

HT_01

Número de historia	**HT_01**
Historia Técnica	Como desarrollador deseo diseñar la arquitectura de la Dapps
Usuario	Desarrollador
Sprint asignada	1
Prioridad en el Negocio	Alta
Puntos Estimados	40
Riesgo en el desarrollo	Alta
Puntos Reales	40
Descripción	Como desarrollador, deseo diseñar la arquitectura de la Dapps y definir las herramientas a utilizar.
Observaciones	Se deberá crear un diagrama de arquitectura con las tecnologías a utilizar en el desarrollo de la Dapps.
Pruebas de Aceptación	Verificar que la arquitectura diseñada y las herramientas seleccionadas sean las adecuadas para el desarrollo de una Dapps.

HT_02

Número de historia	**HT_02**
Historia Técnica	Como desarrollador deseo registrarme en el proveedor Infura
Usuario	Desarrollador
Sprint asignada	1
Prioridad en el Negocio	Alta
Puntos Estimados	40
Riesgo en el desarrollo	Alta
Puntos Reales	40
Descripción	Como desarrollador, deseo registrarme en el proveedor Infura para obtener una clave API que me permita acceder a sus servicios.
Observaciones	La clave API obtenida será utilizada para conectarse a la red de Ethereum y enviar transacciones. Se deberá documentar el proceso de registro y la configuración necesaria para utilizar la clave API en el proyecto.
Pruebas de Aceptación	Verificar que la clave API obtenida funciona correctamente y que se puede utilizar para conectarse a la red de Ethereum y enviar transacciones.

HT_03

Número de historia	**HT_03**
Historia Técnica	Como desarrollador deseo configurar el entorno de desarrollo para el cliente Front-End
Usuario	Desarrollador
Sprint asignada	1
Prioridad en el Negocio	Alta
Puntos Estimados	20
Riesgo en el desarrollo	Alta
Puntos Reales	20
Descripción	Como desarrollador, deseo configurar el entorno de desarrollo para el cliente Front-End para permitir el desarrollo y despliegue de la Dapps.
Observaciones	Se deberán configurar las herramientas necesarias para el desarrollo de la interfaz de usuario, incluyendo el servidor de desarrollo local, los DreamWorks y librerías a utilizar, así como la integración con el proveedor de la red de Ethereum.
Pruebas de Aceptación	Verificar que se ha configurado correctamente el entorno de desarrollo para el cliente Front-End, y que se puede iniciar el servidor de desarrollo local y visualizar la interfaz de usuario de la Dapps. Además, se deberá comprobar que se ha establecido correctamente la conexión con la red de Ethereum y se pueden obtener datos de la misma.

HT_04

Número de historia	**HT_04**
Historia Técnica	Como desarrollador deseo configurar el entorno de desarrollo para los contratos inteligentes (Backend).
Usuario	Desarrollador
Sprint asignada	2
Prioridad en el Negocio	Media
Puntos Estimados	20
Riesgo en el desarrollo	Media
Puntos Reales	20
Descripción	Como desarrollador, deseo configurar el entorno de desarrollo para los contratos inteligentes (Backend) de la Dapps para permitir su desarrollo y despliegue

HT_05

Número de historia	**HT_05**
Historia Técnica	Como desarrollador deseo configurar el Endpoint dentro del proveedor de Blockchain
Usuario	Desarrollador
Sprint asignada	2
Prioridad en el Negocio	Alta
Puntos Estimados	40
Riesgo en el desarrollo	Alta
Puntos Reales	40
Descripción	Como desarrollador, deseo configurar el Endpoint dentro del proveedor de Blockchain para permitir la interacción con la red de Ethereum.
Observaciones	Se deberá configurar el Endpoint dentro del proveedor de Blockchain, incluyendo la conexión y autenticación a la red de Ethereum, y la configuración de la API para la interacción con los contratos inteligentes.
Pruebas de Aceptación	Verificar que se ha configurado correctamente el Endpoint dentro del proveedor de Blockchain y que se pueden interactuar con los contratos inteligentes en la red de Ethereum. Además, se deberá comprobar que se están almacenando y recuperando los datos correctamente.

HT_06

Número de historia	**HT_06**
Historia Técnica	Como desarrollador deseo configurar una cuenta con la billetera virtual para acceder a la Blockchain
Usuario	Desarrollador
Sprint asignada	2
Prioridad en el Negocio	Media
Puntos Estimados	20
Riesgo en el desarrollo	Media
Puntos Reales	20
Descripción	Como desarrollador, deseo configurar una cuenta con la billetera virtual para acceder a la Blockchain y poder realizar transacciones con los contratos inteligentes.
Observaciones	Se deberá configurar una cuenta en la billetera virtual seleccionada para el proyecto y se deberá asegurar que se pueden realizar transacciones en la red de Ethereum.
Pruebas de Aceptación	Verificar que se ha configurado correctamente la cuenta en la billetera virtual y que se pueden realizar transacciones con los contratos inteligentes en la red de Ethereum.

HT_07

Número de historia	**HT_07**
Historia Técnica	Como desarrollador necesito diseñar la interfaz de usuario para la dapp
Usuario	Desarrollador
Sprint asignada	2
Prioridad en el Negocio	Alta
Puntos Estimados	40
Riesgo en el desarrollo	Alta
Puntos Reales	40
Descripción	Como desarrollador, necesito diseñar la interfaz de usuario para la dapp para que los usuarios puedan interactuar con los contratos inteligentes de manera intuitiva y eficiente.
Observaciones	Se deberá diseñar la interfaz de usuario siguiendo las especificaciones del producto y se deberá asegurar que la misma es intuitiva, eficiente y fácil de usar para los usuarios finales.
Pruebas de Aceptación	Verificar que la interfaz de usuario diseñada cumple con las especificaciones del producto y es intuitiva, eficiente y fácil de usar para los usuarios finales. Además, se deberá comprobar que la interfaz permite interactuar correctamente con los contratos inteligentes.

ANEXO B: HISTORIAS DE USUARIO

HU_01:

Número	**HU_01**
Nombre	Codificar una función en el contrato inteligente para la carga de información en la Blockchain.
Usuario	Desarrollador
Iteración asignada	3
Prioridad en el negocio	Alta
Puntos estimados	40
Riesgo en el desarrollo	Alta
Puntos reales	40
Descripción	Como desarrollador, deseo codificar una función en el contrato inteligente para la carga de información en la Blockchain.
Observaciones	-
Pruebas de aceptación	Verificar que se pueda cargar información en la Blockchain a través del contrato inteligente.

HU_02

Número	**HU_02**
Nombre	Codificar una función en el contrato inteligente para traer información de la red Blockchain.
Usuario	Desarrollador
Iteración asignada	3
Prioridad en el negocio	Alta
Puntos estimados	40
Riesgo en el desarrollo	Alta
Puntos reales	40
Descripción	Como desarrollador, deseo codificar una función en el contrato inteligente para traer información de la red Blockchain.
Observaciones	-
Pruebas de aceptación	Verificar que se pueda traer información de la red Blockchain a través del contrato inteligente.

HU_03

Número	**HU_03**
Nombre	Desplegar el contrato inteligente en la red Blockchain.
Usuario	Desarrollador
Iteración asignada	3
Prioridad en el negocio	Alta
Puntos estimados	40
Riesgo en el desarrollo	Alta
Puntos reales	40
Descripción	Como desarrollador, deseo desplegar el contrato inteligente en la red Blockchain.
Observaciones	-
Pruebas de aceptación	Verificar que el contrato inteligente se despliegue correctamente en la red Blockchain.

HU_04

Número	**HU_04**
Nombre	Instalar las dependencias necesarias para interactuar con la web.
Usuario	Desarrollador
Iteración asignada	4
Prioridad en el negocio	Alta
Puntos estimados	40
Riesgo en el desarrollo	Alta
Puntos reales	40
Descripción	Como desarrollador, deseo instalar las dependencias necesarias para interactuar con la web.
Observaciones	-
Pruebas de aceptación	Verificar que las dependencias se hayan instalado correctamente y se puedan utilizar para interactuar con la web.

HU_05

Número	**HU_05**
Nombre	Iniciar sesión en la Dapps a través de Metamask
Usuario	Usuario público
Iteración asignada	4
Prioridad en el negocio	Media
Puntos estimados	20
Riesgo en el desarrollo	Media
Puntos reales	20
Descripción	Como usuario público deseo iniciar sesión en la Dapps a través de Metamask
Observaciones	Se debe permitir al usuario iniciar sesión con Metamask en la Dapps
Pruebas de Aceptación	Verificar que el usuario puede iniciar sesión en la Dapps mediante Metamask

HU_06

Número	**HU_06**
Nombre	Cargar un nuevo documento
Usuario	Usuario
Iteración asignada	4
Prioridad en el negocio	Alta
Puntos estimados	40
Riesgo en el desarrollo	Alta
Puntos reales	40
Descripción	Como usuario requiero cargar un nuevo documento
Observaciones	Se debe permitir al usuario cargar un archivo en la red Blockchain y almacenarlo en el contrato inteligente
Pruebas de Aceptación	Verificar que el documento se carga correctamente en la red Blockchain

HU_07

Número	**HU_07**
Nombre	Visualizar la información de documentos existentes en la red de Blockchain
Usuario	Usuario
Iteración asignada	4
Prioridad en el negocio	Media
Puntos estimados	20
Riesgo en el desarrollo	Media
Puntos reales	20
Descripción	Como usuario requiero visualizar la información de documentos existentes en la red de Blockchain
Observaciones	Se debe permitir al usuario ver la información de los documentos almacenados en el contrato inteligente
Pruebas de Aceptación	Verificar que se muestra la información de los documentos almacenados en el contrato inteligente

HU_08

Número	**HU_08**
Nombre	Cargar un documento en verificación de documentos
Usuario	Usuario
Iteración asignada	5
Prioridad en el negocio	Alta
Puntos estimados	40
Riesgo en el desarrollo	Alta
Puntos reales	40
Descripción	Como usuario requiero cargar un documento en verificación de documentos
Observaciones	Se debe permitir al usuario cargar un documento para su verificación en la red Blockchain
Pruebas de Aceptación	Verificar que el documento se carga correctamente en la red Blockchain

HU_09

Número	**HU_09**
Nombre	Validar la autenticidad de un documento
Usuario	Usuario
Iteración asignada	5
Prioridad en el negocio	Alta
Puntos estimados	40
Riesgo en el desarrollo	Alta
Puntos reales	40
Descripción	Como usuario requiero validar la autenticidad de un documento
Observaciones	Se debe permitir al usuario verificar si un documento es auténtico en la red Blockchain
Pruebas de Aceptación	Verificar que el sistema permita a los usuarios verificar la autenticidad de un documento en la red Blockchain.

HU_10:

Número	**HU_10**
Nombre	Recargar gas en los sitios Faucet de Ethereum
Usuario	Usuario
Iteración asignada	5
Prioridad en el negocio	Media
Puntos estimados	20
Riesgo en el desarrollo	Media
Puntos reales	20
Descripción	Como usuario requiero recargar gas en los sitios Faucet de Ethereum
Observaciones	Se debe proporcionar al usuario un enlace a un sitio Faucet de Ethereum donde pueda recargar gas para interactuar con el contrato inteligente
Pruebas de Aceptación	Verificar que el usuario puede recargar gas en el sitio faucet y utilizarlo para interactuar con el contrato inteligente.

ANEXO C: CUESTIONARIO DE EVALUACIÓN

EVALUACIÓN DE SEGURIDAD A UNA DAPP

Luego de haber socializado y presentado hacia ustedes la aplicación descentralizada con tecnología blockchain que permite la verificación de documentos, se procede con unas preguntas con la finalidad de evaluar su seguridad según la ISO 25010:2011 en cuanto a las subcaracterísticas de integridad, autenticidad y confidencialidad.

INTEGRIDAD

¿El sistema ofrece al usuario la opción de privacidad de datos? *

- Verdadero
- Falso

En el sistema, ¿hay alguna forma de que los usuarios no registrados accedan a los datos de los usuarios registrados? *

- Verdadero
- Falso

En el sistema, ¿hay alguna forma de que los administradores del sitio web puedan ver la información personal de los usuarios? *

- Verdadero
- Falso

¿El sistema almacena en la base de datos un control de acceso? *

- Verdadero
- Falso

AUTENTICIDAD

¿El sistema considera un paso de autenticidad? *

- Verdadero
- Falso

¿El sistema solicita una confirmación de contraseña al cambiar los datos del usuario? *

- Verdadero
- Falso

¿El sistema envía alguna notificación al usuario cuando hay una modificación de datos? *

- Verdadero
- Falso

¿El sistema considera una jerarquía en el acceso de varios datos entre los administradores del sitio? *

- Verdadero
- Falso

CONFIDENCIALIDAD

¿El sistema permite la conexión de un mismo usuario en dos instancias de acceso diferentes? *

- Verdadero
- Falso

¿El sistema cuenta con un asistente para el registro de nuevos usuarios? *

- Verdadero
- Falso

¿El sistema contempla que no puede haber dos cuentas con el mismo correo electrónico o nombre de usuario, pero datos diferentes? *

- Verdadero
- Falso

¿El sistema contempla el paso de verificación de correo electrónico, cuando se genera un usuario *

- Verdadero
- Falso

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 18/07/2023

INFORMACIÓN DEL AUTOR
Nombres – Apellidos: Kevin Andres Gallardo Espinoza
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Software
Título a optar: Ingeniero de Software
f. Analista de Biblioteca responsable: Ing. Fernanda Arévalo M.

1454-DBRAI-UPT-2023