



Universidad  
Nacional  
de Loja

# Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales No  
Renovables

Carrera de Ingeniería en Sistemas

Implementación de una DApp con tecnología blockchain para la  
trazabilidad de la producción de vinos Ambrosia

Trabajo de Titulación previo a la  
obtención del título de Ingeniero en  
Sistemas.

**AUTOR:**

Jimmy Leonel Vicente Guayanay

**DIRECTOR:**

Ing. Cristian Ramiro Narváz Guillen, Mg.Sc.

LOJA – ECUADOR

2023

*Educamos para Transformar*

## Certificación

Loja, 15 de marzo del 2023

Ing. Cristian Ramiro Narváez Guillen, Mg. Sc.

**DIRECTOR DEL TRABAJO DE TITULACIÓN**

### CERTIFICO:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Titulación denominado: **Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia**, previo a la obtención del título de **Ingeniero en Sistemas**, de la autoría del estudiante **Jimmy Leonel Vicente Guayanay** con cédula de identidad **Nro. 1105279044**. Una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto, autorizo la presentación para la respectiva sustentación y defensa.



Firmado electrónicamente por:  
CRISTIAN RAMIRO  
NARVAEZ GUILLEN

Ing. Cristian Ramiro Narváez Guillen, Mg.Sc.

**DIRECTOR DEL TRABAJO DE TITULACIÓN**

## **Autoría**

Yo, **Jimmy Leonel Vicente Guayanay**, declaro ser el autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi Trabajo de Titulación en el Repositorio Institucional - Biblioteca Virtual.



Firmado electrónicamente por:  
**JIMMY LEONEL  
VICENTE GUAYANAY**

**Firma:**

**Cédula de Identidad:** 1105279044

**Fecha:** 03 de Julio de 2023

**Correo Electrónico:** jimmy.vicente@unl.edu.ec

**Teléfono:** 0989309933

**Carta de autorización del Trabajo de Titulación por parte del autor, para la consulta de producción parcial o total, y publicación electrónica del texto completo**

Yo **Jimmy Leonel Vicente Guayanay**, declaró ser el autor del Trabajo de Titulación denominado: **Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia** como requisito para optar por el título de **Ingeniero en Sistemas**, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional: Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con los cuales tenga convenio la Universidad. La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de titulación que realice un tercero. Para constancia de esta autorización, en la ciudad de Loja, a los tres días del mes de julio de dos mil veintitrés.



Firmado electrónicamente por:  
**JIMMY LEONEL  
VICENTE GUAYANAY**

**Firma:**

**Autor:** Jimmy Leonel Vicente Guayanay

**Cédula:** 1105279044

**Dirección:** Pedro Vicente Maldonado y Francisco de Caldas

**Correo Electrónico:** jimmy.vicente@unl.edu.ec

**Teléfono:** 0989309933

**DATOS COMPLEMENTARIOS:**

**Director del Trabajo de Titulación:** Ing. Cristian Ramiro Narváez Guillen, Mg.Sc.

## **Dedicatoria**

Dedico este trabajo de manera especial a mis padres, quienes han sido mi inspiración y un pilar fundamental para lograr cumplir esta meta académica. También quiero expresar mi gratitud a mis hermanos, por su motivación y apoyo incondicional durante todo el proceso. Agradezco profundamente a cada uno de mis familiares por su constante apoyo y contribución para culminar esta etapa académica. Sus palabras de aliento y ánimo han sido un gran estímulo para seguir adelante. Finalmente, quisiera expresar mi agradecimiento a mis compañeros de carrera, quienes han sido esenciales en mi formación académica. A través de su colaboración y amistad dentro y fuera de las aulas, hemos forjado vínculos duraderos y enriquecedores que valoraré siempre.

*Jimmy Leonel Vicente Guayanay*

## **Agradecimiento**

Agradecer a Dios por haberme brindado la perseverancia necesaria para perseguir todas las metas y desafíos que se han presentado en mi vida. Estoy especialmente agradecido por haber contado con el apoyo constante de mi familia y amigos, quienes siempre han estado ahí para mí en los momentos más difíciles, animándome y ayudándome a crecer como persona. Sus palabras de aliento y su respaldo incondicional han sido fundamentales para mi éxito, y estoy muy agradecido por su presencia en mi vida.

Quiero expresar mi más sincero agradecimiento a la Universidad Nacional de Loja, en particular a la carrera de Ingeniería en Sistemas, por brindarme un sólido apoyo durante mi trayectoria académica. Estoy muy agradecido con todos los instructores que me impartieron clases, no solo por compartir su valioso conocimiento en el campo de la docencia, sino también por su dedicación y compromiso con nuestra formación integral.

Quiero expresar mi profundo agradecimiento al Ing. Cristian Ramiro Narváez Guillen, Mg.Sc mi director de Trabajo de Titulación. Su capacidad profesional y calidad humana siempre fueron una fuente de inspiración y admiración para mí, lo que me motivó a culminar exitosamente mi proyecto. Su guía y orientación fueron fundamentales para el logro de mis objetivos y estoy muy agradecido por haber contado con su apoyo.

Y finalmente quiero expresar mi gratitud a mis compañeros de clase por su ayuda colaborativa a lo largo de todos estos años. Agradezco su constante apoyo y motivación durante las horas más difíciles de estudio, lo que me permitió superar los retos académicos con éxito. El compartir el aula con ellos ha sido una experiencia enriquecedora, y estoy agradecido por haber tenido la oportunidad de aprender y crecer juntos.

***Jimmy Leonel Vicente Guayanay***

## Índice de Contenidos

<b>Portada</b> .....	<b>i</b>
<b>Certificación</b> .....	<b>ii</b>
<b>Autoría</b> .....	<b>iii</b>
<b>Carta de autorización</b> .....	<b>iv</b>
<b>Dedicatoria</b> .....	<b>v</b>
<b>Agradecimiento</b> .....	<b>vi</b>
<b>Índice de Contenidos</b> .....	<b>vii</b>
Índice de Tablas:.....	xi
Índice de Figuras: .....	xii
Índice de Anexos: .....	xiii
<b>1. Título</b> .....	<b>1</b>
<b>2. Resumen</b> .....	<b>2</b>
2.1. Abstract.....	3
<b>3. Introducción</b> .....	<b>4</b>
<b>4. Marco teórico</b> .....	<b>6</b>
4.1. Aplicación Descentralizada (DApp).....	6
4.1.1. Características .....	7
4.1.2. Usos.....	8
4.2. Blockchain en la trazabilidad .....	9
4.3. Algoritmo Proof of Work (PoW) para el consenso de Blockchain .....	10
4.4. Contratos inteligentes .....	11
4.4.1. Características .....	12
4.4.2. Proceso de contrato inteligente .....	12
4.4.3. Composición de un contrato inteligente.....	13
4.4.4. Gas y transacciones .....	13
4.4.5. Ethereum .....	14

4.5.	Ethereum Virtual Machine .....	15
4.6.	ABCDE (agile block chain DApp engineering) .....	16
4.7.	Solidity.....	22
4.8.	Truffle Suite.....	22
4.8.1.	Ganache .....	23
4.8.2.	Truffle.....	23
4.8.3.	Truffle Teams .....	23
4.9.	Node.js.....	24
4.10.	Vue JS .....	24
4.11.	Visual Studio Code (IDE) .....	24
4.12.	Funciones HASH .....	24
4.12.1.1.	SHA-256.....	25
4.13.	Trabajos relacionados .....	25
<b>5.</b>	<b>Metodología .....</b>	<b>28</b>
5.1.	Metodología de desarrollo de software .....	28
5.2.	Proceso.....	28
5.6.	Métodos .....	29
5.6.1.	Analítico .....	29
5.3.2.	Investigación-acción .....	29
5.6.2.	Experimentales Controlados .....	30
5.6.2.1.	Replicación .....	30
5.6.2.2.	Simulación .....	30
5.6.3.	Métodos Observacionales .....	30
5.6.3.1.	Análisis estático.....	30
5.6.3.2.	Caso de estudio.....	30
5.7.	Técnicas .....	31
<b>5.7.1.1.</b>	<b>Entrevista .....</b>	<b>31</b>



5.7.2.	Reuniones .....	31
5.8.	Estándares .....	31
5.8.1.	IEEE 830 .....	31
5.8.2.	ERC 20 .....	31
5.9.	Materiales .....	32
5.9.1.	Recurso Humano .....	32
5.9.2.	Recursos de Software y Hardware .....	32
5.9.3.	Insumos .....	33
<b>6.</b>	<b>Resultados .....</b>	<b>35</b>
6.1.	Objetivo 1 .....	35
6.1.1.	Determinar los procesos de producción de vinos Ambrosia .....	36
6.1.2.	Fase 1: Elicitar Requisitos .....	37
6.1.3.	Fase 2: Actores de la DApp .....	37
6.1.4.	Fase 3: Requerimientos e Historias de usuario de la DApp .....	38
6.1.5.	Requisitos funcionales .....	38
6.1.6.	Requisitos no funcionales .....	39
6.1.7.	Historias de usuario .....	39
6.1.8.	Caso de usos .....	40
6.1.9.	Fase 4: Diagrama de la arquitectura de la DApp .....	40
6.2.	Objetivo 2 .....	42
6.2.1.	Iteraciones (sprints) de la DApp .....	43
6.2.2.	Control de versiones de la DApp .....	44
6.2.3.	Configuración inicial .....	44
6.2.4.	Estructura de la DApp .....	45
6.2.4.1.	Esquema del sistema de contratos inteligentes .....	45
6.2.4.2.	Esquema del subsistema de aplicaciones backend .....	46
6.2.4.3.	Esquema del subsistema de aplicaciones frontend .....	47

6.2.5.	Fase 5: Diseño del subsistema de contratos inteligentes .....	49
6.2.6.	Fase 6: Codificación del subsistema de contratos inteligentes .....	50
6.2.7.	Fase 7: Codificación del subsistema de aplicaciones backend .....	51
6.2.8.	Fase 8: Diseño del subsistema de aplicaciones frontend.....	52
6.3.	Objetivo 3 .....	53
6.3.1.	Fase 9: Pruebas de integración de la DApp.....	54
6.3.1.1.	Integrar el sistema DApp .....	54
6.3.1.2.	Probar el sistema DApp .....	56
6.3.1.3.	Desplegar el sistema DApp .....	58
<b>7.</b>	<b>Discusión .....</b>	<b>63</b>
7.1.	Desarrollo de la propuesta alternativa .....	63
7.2.1.	Objetivo 1: Determinar los procesos de producción de vinos Ambrosia que permita delimitar y elicitar los requerimientos y la arquitectura de la DApp.....	63
7.2.2.	Objetivo 2: Desarrollar la DApp cumpliendo con la arquitectura y elicitación de los requerimientos.....	64
7.2.3.	Objetivo 3: Desplegar y probar la DApp sobre la testnet de blockchain donde se valide la trazabilidad de la elaboración de Vinos Ambrosia.....	65
<b>8.</b>	<b>Conclusiones .....</b>	<b>66</b>
<b>9.</b>	<b>Recomendaciones .....</b>	<b>67</b>
<b>10.</b>	<b>Bibliografía .....</b>	<b>69</b>
<b>11.</b>	<b>Anexos .....</b>	<b>73</b>

## Índice de Tablas:

<b>Tabla 1.</b> Equivalencias de las unidades WEI a ETH.....	14
<b>Tabla 2.</b> Trabajos relacionados.....	26
<b>Tabla 3.</b> Recurso Humano.....	32
<b>Tabla 4.</b> Recursos de Software.....	32
<b>Tabla 5.</b> Recursos de Hardware.....	33
<b>Tabla 6.</b> Insumos.....	34
<b>Tabla 7.</b> Roles de la DApp.....	37
<b>Tabla 8.</b> Requisitos funcionales.....	38
<b>Tabla 9.</b> Requisitos no funcionales.....	39
<b>Tabla 10.</b> Historias de usuario.....	39
<b>Tabla 11.</b> Iteraciones del subsistema de contratos inteligentes.....	43
<b>Tabla 12.</b> Iteraciones del subsistema de aplicaciones.....	43
<b>Tabla 13.</b> Ajustes iniciales.....	44
<b>Tabla 14.</b> Esquema del sistema de contratos inteligentes.....	45
<b>Tabla 15.</b> Esquema de subsistema de aplicaciones backend.....	46
<b>Tabla 16.</b> Esquema de subsistema de aplicaciones cliente.....	48
<b>Tabla 17.</b> Lista de API-REST.....	51
<b>Tabla 18.</b> Resultados de las Pruebas de Integración.....	54
<b>Tabla 19.</b> Escenarios para Pruebas Funcionales.....	56
<b>Tabla 20.</b> Resumen de Pruebas Aceptación.....	57
<b>Tabla 21.</b> Criterio para evaluar las Pruebas de Aceptación.....	57
<b>Tabla 22.</b> Resumen de costo total del despliegue en ETH.....	59
<b>Tabla 23.</b> Costo de registro de la TVA.....	62

## Índice de Figuras:

<b>Figura 1.</b> Estructura general de DApp [5].....	6
<b>Figura 2.</b> Estructura completa de una DApp [5]. .....	6
<b>Figura 3.</b> Trazabilidad de cadena de suministro con Blockchain [13].....	10
<b>Figura 4.</b> Proceso de un contrato inteligente [19]. .....	12
<b>Figura 5.</b> Procesos de la metodología ABCDE [23]. .....	21
<b>Figura 6.</b> Diagrama BPMN de las fases para el desarrollo del objetivo 1. ....	35
<b>Figura 7.</b> Procesos de producción de vinos Ambrosia .....	36
<b>Figura 8.</b> Diagrama de casos de uso de la DApp. ....	40
<b>Figura 9.</b> Arquitectura de la DApp con Ganache (testnet blockchain local) .....	41
<b>Figura 10.</b> Arquitectura de la DApp con Sepolia (testnet blockchain Ethereum).....	41
<b>Figura 11.</b> Diagrama BPMN de las fases para el desarrollo del objetivo 2. ....	42
<b>Figura 12.</b> Control de versiones de la DApp con GitHub. ....	44
<b>Figura 13.</b> Esquema del sistema de contratos inteligentes.....	45
<b>Figura 14.</b> Esquema del subsistema de aplicaciones backend. ....	46
<b>Figura 15.</b> Esquema del subsistema de aplicaciones cliente. ....	48
<b>Figura 16.</b> Diagrama de clases de la DApp para subsistema de smart contracts .....	50
<b>Figura 17.</b> Modelo Vista Controlador con la Blockchain. ....	52
<b>Figura 18.</b> Arquitectura física de la DApp. ....	53
<b>Figura 19.</b> Diagrama BPMN de las fases para el desarrollo del objetivo 3. ....	53
<b>Figura 20.</b> Colección de Postman con la administración de la TVA .....	54
<b>Figura 21.</b> Resultado de las Pruebas de Integración de la DApp. ....	55
<b>Figura 22.</b> Proyecto de Infura para desplegar en la testnet de Sepolia. ....	58
<b>Figura 23.</b> Comando para desplegar los contratos inteligentes.....	59
<b>Figura 24.</b> Historial de las transacciones en Etherscan. ....	60
<b>Figura 25.</b> Proyecto creado en Heroku.....	61
<b>Figura 26.</b> Esquema cliente-servidor.....	61
<b>Figura 27.</b> Costo total en ETH para crear una TVA en la testnet Sepolia. ....	62

## **Índice de Anexos:**

<b>Anexo 1.</b> Entrevista a representante de vinos Ambrosia .....	73
<b>Anexo 2.</b> Definición de los requerimientos de software.....	75
<b>Anexo 3.</b> Descripción de Historias de usuario .....	97
<b>Anexo 4.</b> Diagrama de clases subsistema de contratos inteligentes .....	97
<b>Anexo 5.</b> Diagrama de clases subsistema de aplicaciones.....	98
<b>Anexo 6.</b> Código para el subsistema de contratos inteligentes .....	99
<b>Anexo 7.</b> Código para el subsistema de aplicaciones .....	119
<b>Anexo 8.</b> Pruebas Unitarias del subsistema de aplicaciones.....	130
<b>Anexo 9.</b> Pruebas de Integración .....	129
<b>Anexo 10.</b> Pruebas Funcionales .....	139
<b>Anexo 11.</b> Pruebas de Aceptación .....	164
<b>Anexo 12.</b> Manual de Usuario .....	169
<b>Anexo 13.</b> Certificación de traducción de resumen .....	188

## **1. Título**

**Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia**

## 2. Resumen

El presente Trabajo de Titulación (TT) tiene como objetivo el estudio de cómo la implementación de una DApp basada en tecnología blockchain puede mejorar la trazabilidad de los vinos Ambrosia. En vista que actualmente existe la falta de un sistema eficiente y transparente en la gestión de los productos de los vinos y en la satisfacción de los consumidores. Por lo tanto, se busca explorar el potencial de la tecnología blockchain para mejorar la eficiencia en su elaboración y así mejorar la experiencia del cliente.

Con la metodología ABCDE y las tecnologías utilizadas (Truffle Suite, Vue.js, Solidity y Nodejs) se ha llevado a cabo un proceso sistemático y riguroso para asegurar que la DApp cumpla con los objetivos planteados y se pueda validar su funcionalidad. En el primer objetivo, se identificó los actores involucrados; se crearon las historias de usuario y se definieron los requerimientos; se realizó un diagrama de arquitectura y se dividió la DApp en dos subsistemas: contratos inteligentes y aplicaciones. En el segundo objetivo, se desarrollaron las fases de diseño, codificación y pruebas unitarias para cada subsistema para asegurar su correcta funcionalidad. Finalmente, en el tercer objetivo, se realizaron las pruebas de integración, funcionales y de aceptación y desplegaron el módulo de software en la testnet de Sepolia de Ethereum.

La DApp implementada permite registrar información crítica sobre la producción de los vinos, en este caso los procesos de: materia prima, extracción del mosto, pasteurización, fermentación, clarificación, trasiego y envasado. De esta manera, se mejora la transparencia en la cadena de suministro y se asegura que los consumidores tengan acceso a información precisa y confiable sobre el vino que están adquiriendo. Al utilizar la tecnología blockchain, se garantiza la inmutabilidad y la integridad de la información, lo que significa que los datos no pueden ser alterados o eliminados una vez registrados en comparación con la manera tradicional de registrar la información sobre la producción de vinos, donde la información puede ser vulnerada y alterada.

**Palabras claves:** *ABCDE, blockchain, DApp, contratos inteligentes, Ethereum, Vue, truffle.*

## 2.1. Abstract

The objective of this Degree Project (TT) is to study how the implementation of a DApp based on blockchain technology can improve the traceability of Ambrosia wines. Given that there is currently a lack of an efficient and transparent system in the management of Ambrosia wine products and in consumer satisfaction. Therefore, it seeks to explore the potential of blockchain technology to improve efficiency in the production of Ambrosia wines and thus improve the customer experience.

With the ABCDE methodology and the technologies used (Truffle Suite, Vue.js, Solidity and Nodejs), a systematic and rigorous process has been carried out to ensure that the DApp meets the objectives set and its functionality can be validated. In the first objective, stakeholders were identified; user stories were created and requirements were defined; an architecture diagram was created and the DApp was divided into two subsystems: smart contracts and applications. In the second objective, the design, coding and unit testing phases were developed for each subsystem to ensure its correct functionality. Finally, in the third objective, integration, functional and acceptance tests were performed and deployed the software module on Ethereum's Sepolia testnet.

The implemented DApp allows to record critical information about the production of wines, in this case the processes of: raw material, juice extraction, pasteurization, fermentation, clarification, racking and packaging. In this way, transparency in the supply chain is improved and it is ensured that consumers have access to accurate and reliable information about the wine they are purchasing. By using blockchain technology, the immutability and integrity of the information is guaranteed, which means that the data cannot be altered or deleted once recorded compared to the traditional way of recording information on wine production, where the Information can be violated and altered.

**Keywords:** *ABCDE, blockchain, DApp, smart contracts, Ethereum, Vue, truffle.*



### **3. Introducción**

La industria de producción de vino es una de las más antiguas del mundo y ha evolucionado a lo largo de los siglos. Sin embargo, a pesar de la tradición y el prestigio que rodea a esta industria, todavía existen problemas relacionados con la falta de transparencia y autenticidad de algunos productos [1]. Los consumidores a menudo tienen dificultades para conocer de manera precisa el proceso de producción de un vino, incluyendo el origen de la materia prima, el proceso de elaboración y el almacenamiento. Esto puede dificultar la toma de decisiones informadas y generar desconfianza en el producto.

La falta de transparencia en la producción de vinos puede tener diversas consecuencias negativas. Por un lado, puede afectar la imagen de la industria y la confianza de los consumidores en el producto. También, puede dificultar el cumplimiento de ciertas normativas y regulaciones, como las que se refieren al origen de la materia prima y el proceso de elaboración. En consecuencia, puede facilitar la aparición de fraudes y prácticas engañosas. Por ejemplo, puede darse el caso de que se etiqueten como vinos de alta calidad productos que no cumplen con los requisitos necesarios para ser considerados como tal, como el caso de Madrid España más de 1.500 botellas falsas fueron vendidas llegando los agentes a comprobar que se estaban vendiendo supuestas botellas de varias marcas a precios que superaban los 1.900 euros[2]. Esto puede afectar negativamente la imagen de la industria y la confianza de los consumidores en el producto.

En la actualidad de acuerdo con [3] todos los sistemas de trazabilidad no plantean una solución efectiva y segura que permita a los consumidores conocer de manera precisa y detallada el proceso de producción de vinos y evitar fraudes. Según [4] afirma que la transparencia en el sector del vino potenciará la comercialización, es por ello que esto representa una oportunidad para desarrollar una solución innovadora que ayude a garantizar la calidad y la transparencia del producto y prevenir prácticas engañosas.

Es aquí donde la tecnología blockchain puede jugar un papel importante al permitir la creación de una base de datos descentralizada y segura en la que se puedan registrar y verificar todos los datos relacionados con la producción de vinos. Una aplicación descentralizada (DApp) basada en blockchain puede ser una solución efectiva para garantizar la transparencia y la autenticidad del proceso de producción de vinos, al permitir que los consumidores accedan a información precisa y verificable sobre el origen y el proceso de producción de cada vino.

El trabajo de titulación denominado "Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia" tiene como objetivo principal desarrollar una solución basada en blockchain que permita a los consumidores conocer de manera precisa y detallada el proceso de producción del vino previamente mencionado. Para llevar a cabo este proyecto, se utilizará la plataforma Ethereum para desarrollar la DApp y se integrará con las personas administrativas que administran la información en tiempo real durante el proceso de producción. Además, se trabajará en la creación de una interfaz de usuario amigable y segura que permita a los consumidores acceder a esta información de manera sencilla y rápida.

La implementación de esta solución tendrá numerosos beneficios tanto para la empresa Ambrosia como para los consumidores. Por un lado, la DApp permitirá demostrar la calidad y la transparencia de su proceso de producción, lo que puede mejorar su imagen de marca y aumentar la demanda de sus productos. Además, los consumidores podrán acceder a información precisa y detallada sobre el vino que adquieren.

Una de las principales ventajas de utilizar blockchain para la trazabilidad de la producción de vinos es la inmutabilidad de los datos. Una vez que se han registrado en la cadena de bloques, los datos son imposibles de modificar o eliminar, lo que garantiza su integridad y autenticidad. Además, como la información está descentralizada, no depende de una sola fuente o autoridad, lo que la hace más resistente a posibles fraudes o manipulaciones.

En conclusión, La implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia tiene el potencial de mejorar la calidad y transparencia del producto, así como aumentar la confianza de los consumidores en la marca y en el proceso de producción

## 4. Marco teórico

### 4.1. Aplicación Descentralizada (DApp)

Una aplicación que está en gran parte o completamente descentralizada se conoce como DApp. En la Figura 1 y Figura 2, extraídas de [5], representan la estructura de una DApp. Para ello hay que tener en cuenta factores que se describen a continuación:

- Backend.
- Frontend.
- Comunicación.
- Almacenamiento.
- Resolución de nombre.

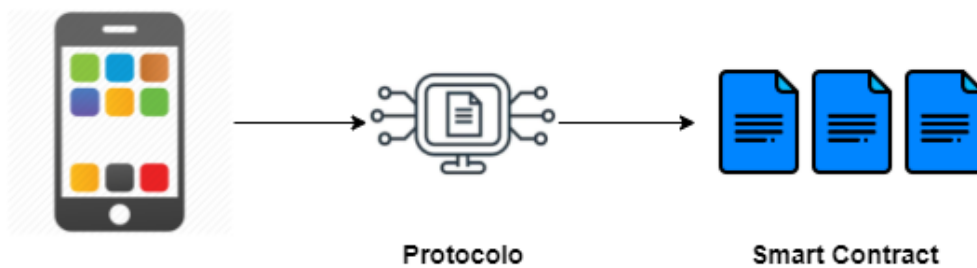


Figura 1. Estructura general de DApp [5].

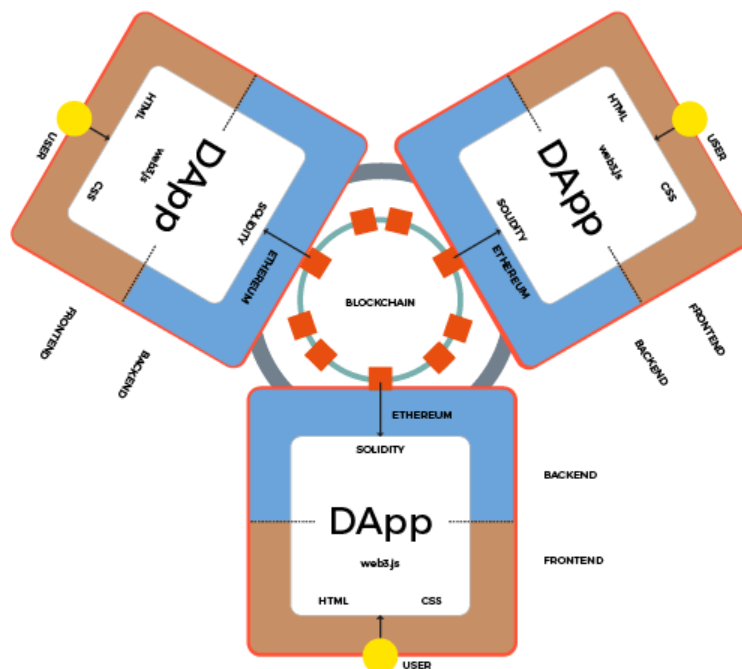


Figura 2. Estructura completa de una DApp [5].

Las DApps de acuerdo con [5], tienen que cumplir con tres características importantes descritas continuación:

## 1. Código abierto.

- a. Debe ejecutarse de manera independiente.
  - b. Ninguna entidad puede afirmar la propiedad de la gran mayoría de sus tokens.
  - c. Una aplicación descentralizada (DApp) tiene la capacidad de realizar cambios en su protocolo con el fin de responder a sugerencias y retroalimentación del mercado, aunque toda modificación debe contar con la aprobación unánime de los usuarios.
2. **Encriptación:** Con el fin de prevenir posibles interrupciones en la red, la información y los informes operativos de una DApp deben ser encriptados y almacenados en un espacio público, conocido como la cadena de bloques descentralizada.
3. **Token.** Cada contribución realizada por los mineros debe compensarse en tokens DApp, y un DApp debe requerir un token criptográfico (como bitcoin o el token utilizado para acceder a la aplicación original) para acceder a él.

### 4.1.1. Características

Los aspectos clave de una DApp es que tiene tecnología Blockchain con las siguientes características [6]:

- **Descentralización.** Un único nodo centralizado (sistema centralizado) no es de confianza en este momento. De lo contrario, todos los nodos que forman parte de la red blockchain controlan, colaboran y aprueban cada decisión (sistema descentralizado).
- **Trazabilidad.** El uso de la tecnología blockchain garantiza que los productos puedan rastrearse a lo largo de la cadena de suministro interna o externa, empaquetarse en un formato legible y prepararse para ser controlados por el propio software o en respuesta a una solicitud de servicio.
- **Transparencia.** La información recopilada por los sistemas que utilizan la tecnología Blockchain es inequívoca para cada nodo. Como un análogo a los libros mayores, donde cada acuerdo es registrado y visto por cualquier nodo.
- **Inmutabilidad.** Dado que las sistematizaciones utilizadas aquí son únicas e irreversibles, cualquier exploración se mantendrá para siempre. Las transacciones verificadas se ejecutan a través de un mecanismo criptográfico, lo que produce operaciones que son prácticamente imposibles de piratear.

- **Código abierto.** En términos generales, cualquier persona que quiera unirse a la red puede usar tecnologías de cadena de bloques. Esto representa cómo todos pueden acceder a la información de la red. Adicionalmente, los registros se pueden realizar de forma pública y se puede desarrollar cualquier aplicación requerida utilizando esta tecnología.
- **Autonomía.** Después de haber establecido una base de consenso, cada nodo presente en el sistema Blockchain tiene la capacidad de transmitir o actualizar información de manera segura y confiable. El propósito de esto es proporcionar confianza tanto en un individuo como en todo el sistema a las personas que interactúan con él.
- **Anonimidad.** El tema de la confianza entre nodos, o la transferencia de datos, se resolvió con la tecnología blockchain. Mientras que cada transacción puede mantenerse en secreto, todo lo que se requiere es comprender cómo la otra persona ve Blockchain.

#### 4.1.2. Usos

Prácticamente cualquier tipo de información que deba mantenerse intacta y accesible puede emplearse con esta tecnología. donde se mantiene de forma segura, descentralizada y menos costosa que a través de intermediarios. A continuación, se describen algunos usos [7]:

- **Uso de blockchain en la salud.** La cadena de bloques podría usarse para sincronizar y mantener registros de salud. De esta manera, independientemente del centro médico donde se atendió al paciente, el historial médico de cada paciente estaría seguro y al mismo tiempo accesible para todos los médicos autorizados. También se puede utilizar para validar medicamentos y detener el fraude de medicamentos en el sector farmacéutico.
- **Uso de blockchain para trazabilidad.** Al rastrear en tiempo real todos los movimientos y estados por los que pasan los artículos, de manera encriptada sin posibilidad de modificación o falsificación de la información, la tecnología blockchain en este contexto le permite obtener trazabilidad y seguridad en todas sus transacciones [8].
- **Otros usos del blockchain.** Es posible que se produzca una revolución en el campo del Internet de las cosas (IoT), el cual se caracteriza por tener una gran cantidad de dispositivos conectados a la red que requieren ser gestionados por proveedores de servicios. En un futuro cercano, el modelo centralizado puede no ser suficiente para manejar la gran cantidad de dispositivos y muchos de ellos pueden presentar problemas de seguridad. Para abordar estos desafíos, la tecnología blockchain puede permitir que

los dispositivos se conecten directamente entre sí de manera segura, confiable y descentralizada, sin necesidad de intermediarios. Esto podría significar un cambio significativo en la forma en que se gestionan y operan los dispositivos IoT.

#### **4.2. Blockchain en la trazabilidad**

La blockchain proporciona un registro descentralizado, seguro e inmutable de los datos de la cadena de suministro, lo que puede mejorar la transparencia y la eficiencia en la industria, y garantizar la autenticidad y calidad de los productos. En primer lugar, el estudio de Deloitte [9] destaca el potencial que tiene la blockchain para revolucionar el rastreo y seguimiento de los alimentos. Este estudio señala que la blockchain puede proporcionar un registro inmutable de los datos de la cadena de suministro, lo que puede mejorar la transparencia y la eficiencia en la industria alimentaria. Además, la blockchain puede ayudar a garantizar la seguridad alimentaria, al permitir una mayor trazabilidad de los productos y una rápida respuesta a los incidentes de seguridad.

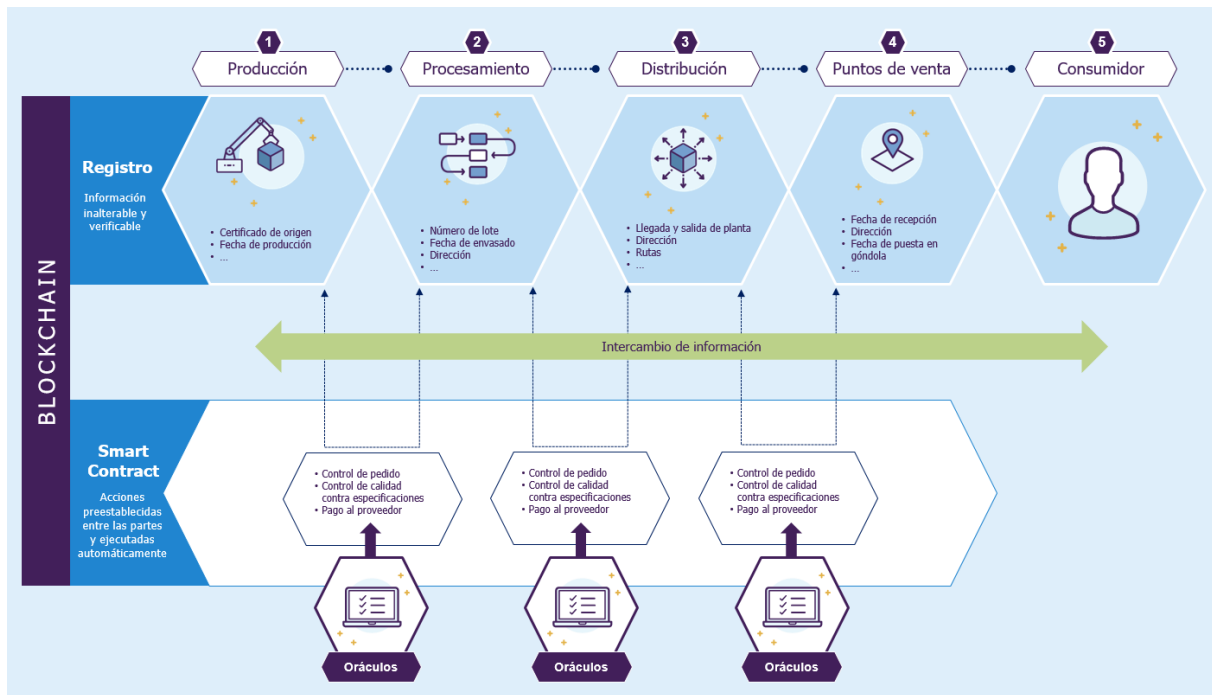
Por otro lado, el artículo de Nature [10] menciona que la blockchain puede ayudar a asegurar la trazabilidad y autenticidad de los medicamentos. Este artículo destaca que la falta de transparencia en la cadena de suministro de medicamentos puede tener graves consecuencias para la salud pública, y que la blockchain puede ser una solución para mejorar la trazabilidad y autenticidad de los medicamentos.

En tercer lugar, el estudio de la Universidad de Nicosia [11] destaca que la blockchain se considera una tecnología ideal para la trazabilidad en la cadena de suministro. Este estudio menciona que la blockchain puede proporcionar un registro descentralizado, seguro e inmutable de los datos de la cadena de suministro, lo que puede mejorar la transparencia y la eficiencia en la industria.

Es importante destacar que la blockchain puede mejorar la transparencia y la eficiencia en la cadena de suministro, lo que puede llevar a una reducción de costos y una mejora de la calidad del producto. Esto puede ser especialmente útil en la cadena de suministro de productos de alta gama, donde la autenticidad y calidad son especialmente importantes.

Dentro de la trazabilidad todos los participantes tienen la capacidad de enviar transacciones, y si son genuinas, serán adquiridas. Este tipo de cadena de bloques se conoce como cadena de bloques pública porque no hay restricciones sobre quién puede leer sus datos o visualizar sus transacciones para incluirlas en la cadena de bloques. a través de la cadena de bloques. Cada nodo tiene la oportunidad de participar en el proceso de consenso [12].

La Blockchain es considerada una arquitectura “totalmente descentralizada”. Por ejemplo, Bitcoin y Ethereum son Blockchain públicas [6]. En la Figura 3 se observa la arquitectura para la trazabilidad de la cadena de suministro de alimentos.



**Figura 3.** Trazabilidad de cadena de suministro con Blockchain [13]

#### 4.3. Algoritmo Proof of Work (PoW) para el consenso de Blockchain

En blockchain, es importante este algoritmo para obtener la colección de bloques. Para que la persistencia de la cadena funcione, todos los usuarios deben cumplir con un conjunto continuo de reglas bien establecidas. Los participantes deben estar de acuerdo sobre qué cadena es legítima antes de que esto pueda proceder contra las bifurcaciones (bifurcaciones) de la cadena. Además, se debe determinar quién es el encargado de encadenar los bloques y si pueden agregar bloques adicionales a la sucesión o no.

Los algoritmos de consenso más notorios son PoS (proof of stake) y PoW (proof of work) el cual se utilizó en este Trabajo de Titulación (TT).

Los nodos en Proof of Work (intento de trabajo) resuelven un problema matemático y crean como resultado un bloque, añadiéndolo a la cadena. La cadena es la encargada de confirmar que prevalecerán los bloques con más retenciones o contenidos. Si alguien intentara cambiarlo, se necesitaría mucha energía eléctrica y más potencia de procesamiento que todos los demás nodos de la red juntos [14].

Su uso masivo de recursos es el tema clave. También requiere actualizaciones continuas de hardware [14].

#### **4.4. Contratos inteligentes**

Los smart contracts, también conocidos como contratos inteligentes, ahora son un componente estándar de la tecnología blockchain. Son programas de computadora que operan en el bloque más grande. El procesamiento directo y la interacción con otros contratos inteligentes son posibles gracias a este tipo de programa, que también puede usarse para facilitar, confirmar o hacer cumplir las regulaciones entre las partes [15].

Los contratos inteligentes se escriben bajo código de programación, lo que los convierte en programas informáticos que ejecutan de forma autónoma y automática los términos de un contrato. Al igual que un contrato tradicional, pueden definir las reglas y sus estrictas repercusiones, pero a diferencia de un documento legal tradicional, también pueden tomar información como entrada, procesarla de acuerdo con las reglas del contrato y luego tomar las acciones necesarias como resultado. Todo sin necesidad de intervención humana [16].

Además, un contrato inteligente puede ser realizado e invocado tanto por personas naturales y/o jurídicas como por computadoras u otros softwares que se ejecutan de forma independiente. La capacidad de un contrato inteligente para funcionar independientemente de la autoridad es el resultado de la naturaleza de su código, que es accesible para todos y no puede modificarse porque se basa en la tecnología blockchain, lo que le otorga su naturaleza descentralizada, inmutable y transparente [17].

La relación entre los contratos inteligentes y la certificación digital se debe establecer porque, en la certificación digital, un contrato inteligente podría servir como una interfaz en la cadena de bloques que especifica las pautas para la administración y el almacenamiento de los atributos de identificación. Es crucial prestar atención a los detalles, como la forma en que se guardan los datos y los tipos de datos que se emplean [16].



#### 4.4.1. Características

Según [18], estos son las características principales que permiten la confianza en los contratos inteligentes:

- **Inmutabilidad:** Ser inmutable después de la creación significa que nunca puede ser alterado. Nadie puede cambiar maliciosamente el código escrito en los contratos inteligentes.
- **Distribuido:** Al igual que las transacciones de Bitcoin, la red también verifica los contratos.
- **Deterministas:** El código contenido en un contrato inteligente debe ser determinista, lo que significa que, todos los nodos devuelven el mismo resultado al realizar una entrada. Esto es necesario ya que el código se ejecuta simultáneamente en numerosos nodos distribuidos. Eso indica que no puede haber aleatorización en la codificación.
- **Verificables:** Un contrato inteligente recibirá una dirección distinta después de su implementación. Esto está libre para que cualquiera puedan ver y examinar el código de antemano para mayor seguridad.

#### 4.4.2. Proceso de contrato inteligente

La Figura 4, extraída de [19], muestra el proceso. Donde una cuenta de un usuario puede transmitir ether:

1. Dirección de usuario.
2. Dirección de contrato.
3. El contrato inteligente puede ejecutar funciones como, enviar ether a otro usuario o contratos mediante una transacción.

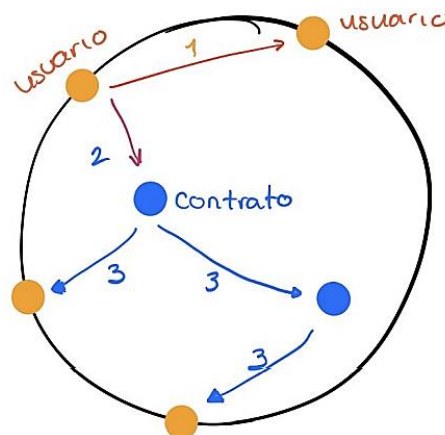


Figura 4. Proceso de un contrato inteligente [19].

Ahora hay muchos sistemas de cadena de bloques que permiten contratos inteligentes, pero Ethereum, que se basa en el Proyecto Preliminar, es el más grande y más flexible para el Proyecto de Trabajo de Grado. La funcionalidad de contrato inteligente también está disponible para Bitcoin, pero está mucho más limitada que para Ethereum.

#### 4.4.3. Composición de un contrato inteligente

De acuerdo con [20], el contrato incluye una cuenta relacionada que se compone de tres campos.

- **Saldo:** La cantidad de ether presente en dicha cuenta es esencial, ya que se empleará para la implementación de contratos inteligentes, los cuales implican un costo en ether, así como también para la modificación de otras cuentas, lo cual también conlleva un costo en ether. Por lo tanto, es indispensable contar con un saldo adecuado en la cuenta del contrato inteligente para poder realizar estas operaciones (transferencias).
- **Almacenamiento:** la información guardada para este contrato inteligente, incluida cualquier información requerida para su interfaz con otros sistemas o para su correcto funcionamiento.
- **Código:** Debido a que el código está compilado, una persona no podría ejecutarlo; pero, para la computadora, es como hablar su propio idioma.

#### 4.4.4. Gas y transacciones

En Ethereum, debe pagar por el cálculo al igual que el código se guarda en un servidor externo (realizar cálculos, modificar contratos o realizar transacciones). Los usuarios de la aplicación pagan los costes computacionales, a diferencia del propietario de la aplicación. Esto se debe a que se supone que no se requiere control administrativo sobre el programa porque Ethereum es una red descentralizada [20].

El costo de una transacción está determinado por el WEI, y su costo de transición es el más alto. Los equivalentes de las unidades WEI a ETH se muestran en la Tabla 1 a continuación, que se obtuvo de [20].

**Tabla 1.** Equivalencias de las unidades WEI a ETH

Unidad	Valor de Wei	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
miliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

#### 4.4.5. Ethereum

Ethereum es la segunda plataforma blockchain más reconocida, cuyo desarrollo estuvo a cargo del famoso programador y escritor ruso, Vitalik Buterin. Este también es reconocido por haber fundado Bitcoin Magazine y haber iniciado el desarrollo de Ethereum a finales del año 2014, según [18].

Según [18], la meta de Ethereum es establecer una plataforma que fomente y respalde la elaboración de aplicaciones descentralizadas basadas en contratos inteligentes (smart contracts) por parte de otros desarrolladores. Además, esta plataforma funciona a nivel global para la ejecución de dichas aplicaciones.

Ether (ETH), la fuente de energía de la plataforma, es la propia moneda de Ethereum. Los usuarios de la cadena de bloques Ethereum utilizan esta criptomoneda como su principal medio de intercambio [18]. Ether se usa en la creación de contratos inteligentes además de ser una moneda similar a Bitcoin que se puede usar para realizar pagos a otras personas. Ether actúa como un incentivo para que los programadores creen aplicaciones de alta calidad y sirve como recompensa que reciben los mineros por agregar nuevos bloques a la cadena.

Ethereum construye su infraestructura para la transición de aplicaciones y servicios centralizados a un mundo descentralizado utilizando las capacidades y la tecnología de la cadena de bloques. Al igual que Bitcoin, Ethereum también utiliza el proceso de Prueba de trabajo para agregar nuevos bloques a la cadena de bloques. Pero desde 2017, ha habido especulaciones de que Ethereum cambiará a un modelo de minería de Prueba de participación o Prueba de participación en uno de sus próximos lanzamientos [18].

Con Proof of Stake, se crea un nuevo bloque al azar, a diferencia de Proof of Work, donde el algoritmo paga a los mineros que resuelven acertijos matemáticos para validar transacciones y crear nuevos bloques.

La base Proof of Stake es un sorteo. Debe guardar tanto ether como desee para poder participar. El minero del bloque se seleccionará en función de la cantidad de éter bloqueado. Cada ether tiene una identificación única, por lo tanto, cuanto más ether esté bloqueado, más posibilidades hay de ser seleccionado, como si el ether bloqueado fuera una papeleta para una lotería. El ganador del sorteo se elegirá al azar utilizando uno de los valores aleatorios de un bloque [18].

#### **4.5. Ethereum Virtual Machine**

Una máquina virtual que es un componente del ecosistema blockchain de Ethereum se llama Ethereum Virtual Machine (EVM). Su función es habilitar la ejecución de programas o contratos inteligentes para que la funcionalidad adicional pueda implementarse en la cadena de bloques y ser utilizada por los usuarios.

Solidity es un lenguaje de alto nivel que EVM desarrolló por su cuenta. Este lenguaje de programación facilita la creación de contratos inteligentes. Después de eso, Solidity se convierte primero en códigos de operación (CÓDIGOS OP) y luego en código de bytes. En última instancia, EVM lo pone en práctica para llevar a cabo las tareas enumeradas en un contrato inteligente [21]. Como resultado, permite que la EVM lleve a cabo incluso los procesos más complicados. Las siguientes son las propiedades de EVM citadas en [21] :

- Las aplicaciones descentralizadas y los contratos inteligentes desarrollados en EVM se caracterizan por ser completamente distribuidos y descentralizados, con un enfoque en la seguridad y en la capacidad de ejecutar código en máquinas alrededor del mundo, incluso si no se confía en la fuente de dicho código. Como consecuencia de esto, no se requiere la intervención de terceros y, una vez creados, no pueden ser alterados ni modificados.
- El EVM permite la creación de más aplicaciones, que luego pueden ejecutarse en la misma red de cadena de bloques sin interferir con otros procesos. Los contratos inteligentes construidos por EVM son impermeables y capaces de ejecución y cumplimiento autónomos y automáticos. Esto elimina la burocracia, los gastos costosos y los largos períodos de espera incluidos en los contratos convencionales.
- La EVM funciona significativamente peor que otras máquinas virtuales comunes en términos de eficiencia. Esto se debe a que su diseño se orientó principalmente a la

utilidad actual más que al alto rendimiento. El EVM solo ha visto una pequeña cantidad de modificaciones y avances hasta el momento.

- El diseño de EVM no está diseñado para la movilidad, lo que restringe los entornos en los que se puede implementar una máquina virtual de este tipo y, como resultado, no está optimizada para la velocidad de muchas plataformas de hardware.

#### 4.6. ABCDE (agile block chain DApp engineering)

La metodología ABCDE divide las dos tareas porque reconoce la distinción significativa entre el desarrollo de software convencional (el sistema de aplicación) y la creación de contratos inteligentes. Debido a que los enfoques ágiles son apropiados para elaborar sistemas donde sus requisitos no se entienden completamente desde el principio o tienen tendencia a ser diferentes, así como las DApps, ABCDE utiliza un enfoque ágil para ambos proyectos. Esto no permite el empleo de métodos incrementales iterativos que dependen de iteraciones más largas, así como enfoques basados en programación como cascada. Debido a la popularidad, la simplicidad y el estatus de Scrum como la metodología de desarrollo de software más utilizada, junto con la experiencia personal de los autores en su investigación e implementación, ABCDE es una técnica ágil que se basa en Scrum [22].

La Figura 5 de [22] ilustra los pasos del método de desarrollo ABCDE con un enfoque en la cadena de bloques Ethereum y el lenguaje de programación Solidity. Debido a que el enfoque es iterativo y gradual, cabe señalar que la mayoría de los pasos se llevan a cabo más de una vez. Las reuniones de planificación de sprint (SPM) y las reuniones de revisión de sprint (SRM) representadas en la Figura 5 se llevan a cabo al inicio y al final de cada sprint, respectivamente. Las reuniones retrospectivas y los scrums diarios, que son reuniones de pie que se realizan todos los días, están ausentes.

El proceso de desarrollo que se observa en la Figura 5, es el siguiente tomado de [22]:

1. **Objetivo del sistema.** El objetivo debe resumirse entre 10 y 30 palabras, y debe publicarse donde todos los miembros del equipo puedan verlo. Se asemeja al "Objetivo Sprint" que la metodología Scrum instruye para identificar y hacer visible para el equipo al comienzo de cada iteración, excepto que este objetivo es para todo el sistema.
2. **Identificar los actores.** Se deben identificar los actores con los que interactuará el sistema de aplicación. Los actores en la DApp que se está construyendo son sistemas o dispositivos externos que intercambian información con ella, así como roles humanos.

3. **Historias de usuario.** De acuerdo con la metodología tradicional de gestión ágil de proyectos, los requisitos del sistema se definen como Historias de Usuario (HU). En este paso se debe tener en cuenta el sistema de aplicación completo que se está diseñando. No importa si se desarrolla utilizando una cadena de bloques, una granja de servidores, potencialmente en la nube u otra arquitectura en este caso. Es ventajoso, pero no necesario, utilizar un diagrama de casos de uso UML en esta fase para representar visualmente los vínculos entre los actores y las necesidades del sistema.
4. **Segmentación en subsistemas / división o partición.** En los siguientes:
  - a. Los contratos inteligentes basados en blockchain (Pasos (5) y (6)).
  - b. El sistema de aplicación, o sistema externo, interactúa con la cadena de bloques al transmitir y producir transacciones, así como al realizar un seguimiento de las actividades que tienen lugar cuando un contrato inteligente realiza una función (Pasos (7)–(8)).

Cree una arquitectura para todo el sistema en esta etapa, especificando qué datos pertenecen a la cadena y cuáles pertenecen fuera de ella. Para que los actores confíen en la DApp, los contratos inteligentes deben controlar los datos y el procesamiento de forma transparente e inmutable. La gestión de todos los demás datos, computación e interfaces de usuario debe ocurrir fuera de la cadena. El patrón de "almacenamiento de datos fuera de la cadena" se puede utilizar para proteger la privacidad de los datos en los que se debe confiar pero que no se pueden colocar en Blockchain debido a su transparencia en la cadena. Se pueden usar otras técnicas de ofuscación para evitar la fuga del volumen de transacciones y las partes participantes.

5. **Diseño de los contratos inteligentes.** Usando el lenguaje de programación Solidity, este paso implica la creación de contratos inteligentes. Esta actividad tiene una serie de características peculiares en comparación con el diseño de software estándar. La actividad se lleva a cabo mediante iteraciones, y cada iteración requiere la creación y entrega de contratos inteligentes incrementales. Se divide en pasos más pequeños que se ofrecen en una secuencia lógica y se tienen especialmente en cuenta (pero no es necesario que se realicen necesariamente en una secuencia en "cascada"). Estos pasos secundarios se decidieron después de conversaciones con muchos desarrolladores de DApp y experiencia en la creación de contratos inteligentes y DApps, al igual que todos los pasos secundarios en los siguientes pasos principales. Aquí están algunos ejemplos:
  - a. Repita los pasos (2) y (3) nuevamente, esta vez prestando especial atención a los actores que interactúan directamente con los contratos inteligentes (identificar

actores y HU). Los actores deben incluirse si los contratos inteligentes del sistema en desarrollo aprovechan los contratos inteligentes externos. Incluya la prueba de aceptación necesaria en la definición de cada narrativa de usuario que creó en esta (s) fase (s). el posterior:

- b. Defina ampliamente qué son los contratos inteligentes y cómo encajan en el subsistema de contratos inteligentes. Indique las funciones de almacenamiento de información, cálculo y coordinación con otros contratos inteligentes para cada contrato inteligente. Es probable que se requieran varios contratos inteligentes interconectados para sistemas no triviales. Piense en abstraer las funcionalidades comunes de los contratos inteligentes utilizando también la herencia. Identifique específicamente cualquier asociación con contratos inteligentes externos, incluidas las bibliotecas. Usaremos diagramas de clases UML y agregaremos las modificaciones necesarias.
- c. Especifique los canales de comunicación y las transferencias de Ether entre el sistema de aplicación, los contratos inteligentes externos y los contratos inteligentes. Para representar estas interacciones, utilice diagramas de secuencia UML mejorados. Defina los cambios de estado del contrato inteligente utilizando diagramas de estado UML según sea necesario.
- d. Cada estructura de datos de contrato inteligente, interfaz externa (interfaz binaria de aplicación o ABI) y los eventos importantes que puede desencadenar deben describirse en detalle.
- e. Especificar funciones concretas, como funciones internas y privadas y sus modificadores, que verifiquen con frecuencia los requisitos previos necesarios para que una función pueda ejecutarse de forma segura.
- f. Realizar procedimientos de evaluación de seguridad y definir pruebas. Esta es una etapa crucial ya que, como ya se dijo antes, la mayoría de los contratos inteligentes son realmente cruciales e involucran dinero.

**6. Codificación y prueba del sistema de contratos inteligentes:** El sistema de contrato inteligente se desarrolla y prueba poco a poco utilizando una metodología ágil. Escribir y probar contratos inteligentes de forma incremental son los procesos de codificación y prueba. Esta actividad no puede llevarse a cabo de forma estrictamente progresiva debido a los estrictos requisitos de seguridad. En cambio, la arquitectura general del contrato inteligente principal se crea y evalúa primero antes de pasar a la estructura de datos y las interfaces de los contratos inteligentes.

- a. Evalúe el código escrito para los incrementos de seguridad y uso de gas.
- b. Para los requisitos implementados y los contratos inteligentes, respectivamente, escriba pruebas unitarias automatizadas (PU) y pruebas de aceptación (PA). Incluya las nuevas pruebas en la colección de pruebas.
- c. El ambiente de ensayo más comúnmente empleado para Solidity es Truffle, el cual se utiliza para llevar a cabo una serie de pruebas exhaustivas que garanticen que las nuevas adiciones al sistema no lo alteren negativamente.

**7. Diseño del subsistema de interacción externa (Sistema de aplicaciones).** La creación del sistema de aplicación, que se comunica con los usuarios y el hardware, entrega mensajes a la cadena de bloques y puede administrar sus propios repositorios (bases de datos y/o documentos), es el paso final. Esta tarea es bastante comparable a la creación de una aplicación web típica. La cadena de bloques es el único actor nuevo y puede iniciar eventos y recibir mensajes, pero no enviarlos. Tenga en cuenta que las consideraciones de seguridad también deben tomarse muy en serio en esta situación. En realidad, en lugar de utilizar las vulnerabilidades de los contratos inteligentes, los piratas informáticos del sistema DApp suelen aprovechar las fallas en el sistema de la aplicación.

- a. Vuelva a escribir los actores y los requisitos previos para el sistema de aplicación en función de la información recopilada en los pasos (2) y (3), agregando los nuevos actores representados por los contratos inteligentes que se comunican con el sistema de aplicación. Definición de prueba de aceptabilidad del sistema de aplicación.
- b. Describa cómo acceder a la cadena de bloques configurando y ejecutando uno o más nodos, a través de un proveedor externo o utilizando una billetera normal, así como la arquitectura de alto nivel del sistema de aplicación, incluidos los niveles de servidor y cliente.
- c. Defina la interfaz de usuario del sistema de la aplicación, generalmente utilizando un método receptivo, para permitir que funcione tanto en PC como en terminales móviles. Para que el programa tenga éxito en el mercado, es crucial tener una interfaz de usuario visualmente atractiva.
- d. Describir los módulos del sistema de aplicación, sus interfaces y el flujo de mensajes que tiene lugar entre ellos. Si es necesario, especifique los diagramas de estado para los módulos y los procedimientos que siguen cuando los contratos inteligentes generan eventos. Describir el proceso de mantenimiento y



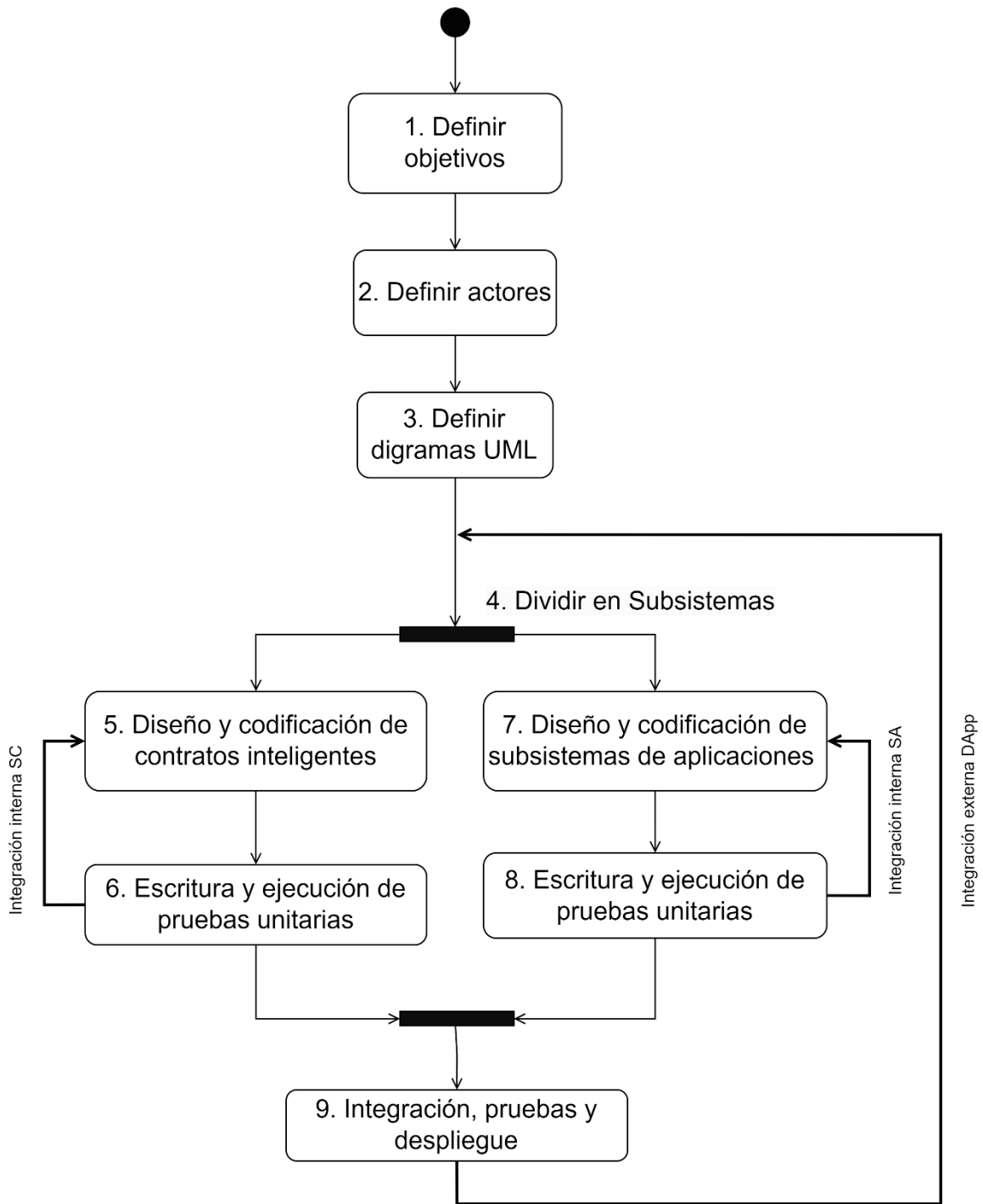
organización de datos permanentes. Puede elegir qué datos están anclados a la cadena de bloques certificando ante notario el hash de resumen de los datos utilizando el patrón "Almacenamiento de datos fuera de la cadena". Definir la estructura de datos o clases del sistema de aplicación, así como el control y flujo de información entre los módulos. El análisis del Paso 2 debe ir seguido de interacciones de contratos inteligentes (5). (C). Las iteraciones, que implican la codificación y la entrega de incrementos del sistema de aplicación, se utilizan para implementar los criterios de la actividad de diseño en lugar de

e. Llevar a cabo una evaluación de la seguridad del sistema externo.

**8. Codificación y prueba del sistema de aplicaciones.** El sistema de aplicación se desarrolla y prueba simultáneamente con el sistema de contrato inteligente utilizando el mismo método para desarrollar contratos inteligentes. Cada dos o tres iteraciones, como se indica en la Figura 5, los resultados de las dos ramas deben integrarse si la creación de contratos inteligentes y el sistema de aplicación se realizan de manera iterativa. Paralelamente se están desarrollando las siguientes iniciativas:

- a. Los requisitos del sistema de aplicación deben implementarse gradualmente. Esta etapa es idéntica a la creación de una aplicación web y es parte del "flujo adecuado" ABCDE (consulte la Figura 5). están:
- b. Ejecute un análisis de seguridad en el código creado para el incremento.
- c. Para las necesidades implementadas, cree PU y PA automatizados. El conjunto de pruebas debe incluir las nuevas pruebas. Ejecute todas las pruebas para asegurarse de que las adiciones no rompan el sistema.

**9. Integrar, probar y desplegar el Sistema DApp.** Los sistemas globales desarrollados previamente deben instalarse en una cadena de bloques o red de prueba local para combinar los contratos inteligentes y el sistema de aplicación. Se deben realizar pruebas de integración para garantizar que todas las partes funcionen juntas según lo previsto (por ejemplo). Los mensajes enviados por el Sistema de aplicaciones hacen que las transacciones de la cadena de bloques se validen y ejecuten correctamente, por ejemplo, y los eventos activados por contratos inteligentes son recogidos por el Sistema de aplicaciones.



**Figura 5.** Procesos de la metodología ABCDE [23].

#### **4.7. Solidity**

De acuerdo con [20] ,El lenguaje de programación denominado Solidity se compara frecuentemente con JavaScript debido a algunas de sus características. Sin embargo, tiene algunas diferencias muy significativas, como el hecho de que, a diferencia de JavaScript, Solidity está muy tipado, lo que nos obliga a declarar qué tipo se necesita para cada variable antes de asignarla.

Al escribir código en Solidity, compilarlo y luego ejecutarlo, hay dos resultados. El primero es el código Byte, que es simplemente un código escrito en un nivel muy básico para que una computadora pueda leerlo y utilizarlo para la implementación en la cadena de bloques. El otro componente que se creará como resultado es el ABI de la aplicación, que funciona como un traductor al comunicarse con el frontend de la web en relación con el código Byte que se ha distribuido en la cadena de bloques [20].

#### **4.8. Truffle Suite**

La Truffle Suite proporciona una amplia variedad de herramientas a los desarrolladores para crear, probar y emplear distintas soluciones de software en una Blockchain de Ethereum. Esta suite está diseñada específicamente para facilitar el proceso de desarrollo en Ethereum, ofreciendo una amplia gama de funcionalidades que incluyen, entre otras, un compilador para Solidity (el lenguaje de programación utilizado en Ethereum), un sistema de migración para gestionar el despliegue de contratos inteligentes, una consola interactiva para interactuar con la red de Ethereum y una serie de bibliotecas que facilitan el desarrollo y la implementación de aplicaciones descentralizadas en esta plataforma. Gracias a esta suite de herramientas, los desarrolladores pueden trabajar de manera más eficiente y productiva, logrando una mayor calidad en sus desarrollos y contribuyendo al crecimiento y evolución de la red de Ethereum

- Ganache.
- Truffle.
- Truffle Teams.

Ocurre porque la creación de DApps y la gestión de contratos inteligentes suele ser muy difícil de lograr cuando se carece de las habilidades y los recursos necesarios. Un conjunto de herramientas de código abierto efectivo para crear aplicaciones en Ethereum Blockchain es Truffle Suite [24].

#### **4.8.1. Ganache**

Se utiliza una cadena de bloques de Ethereum personal llamada Ganache para crear y probar innovaciones como DApps y contratos inteligentes. Se ofrece como un programa de línea de comandos y una aplicación de escritorio (anteriormente conocido como TestRPC). Hay versiones de Ganache para Windows, Mac y Linux. [25].

#### **4.8.2. Truffle**

Con el objetivo de simplificar la vida de los desarrolladores, Truffle es un entorno de desarrollo de primer nivel que ofrece un marco de prueba y una cartera de activos para Blockchain utilizando Ethereum Virtual Machine (EVM). Según [25], algunas de sus características más destacables son:

- Compilación, vinculación, implementación y gestión binaria de contratos inteligentes integrados.
- Automatización de pruebas de contrato para un desarrollo rápido.
- Marco de migración e implementación que es flexible y configurable.
- Se puede implementar cualquier cantidad de redes públicas y privadas mediante la administración de redes.

#### **4.8.3. Truffle Teams**

Una herramienta llamada Truffle Teams permite administrar y realizar un seguimiento del progreso de las aplicaciones que están habilitadas en una Blockchain. Según [25], algunas de sus características más destacables son:

- Datos y seguimiento de DApp: ofrece una descripción general conveniente y completa de los estados de las pruebas en varios proyectos.
- Configuración al ofrecer un entorno uniforme para la prueba continua de contratos inteligentes, la integración continua elimina las discrepancias ambientales.
- Implementaciones automatizadas: promueve la colaboración y lo hace tan simple como usar GitHub.
- Además, permite la ejecución automática de pruebas, liberando recursos del sistema y horas de trabajo de los desarrolladores.

#### **4.9. Node.js**

Un entorno para ejecutar JavaScript se conoce como Node.js. Donde el tiempo de ejecución en tiempo real incluye todo el tiempo necesario para ejecutar una aplicación JavaScript [26]. Además, de acuerdo con [27] Node.js es una plataforma creada sobre el tiempo de ejecución de javascript de Chrome que simplifica la creación de aplicaciones de red rápidas y escalables. Es liviano y efectivo, lo que lo hace ideal para aplicaciones en tiempo real que requieren una gran cantidad de datos porque utiliza un paradigma de E/S sin bloqueo y controlado por eventos.

#### **4.10. Vue JS**

Vue (pronunciado /vju:/, como "view") es un framework que permite la construcción progresiva de interfaces de usuario. A diferencia de otros frameworks monolíticos, Vue fue creado para ser utilizado de manera incremental desde su concepción. La librería central se enfoca en la capa de visualización y se puede integrar fácilmente con otras librerías o proyectos existentes. Asimismo, Vue es capaz de potenciar aplicaciones de página única avanzadas cuando se utiliza junto con herramientas modernas y otras librerías de apoyo [28].

#### **4.11. Visual Studio Code (IDE)**

La definición de Visual Studio Code es un editor de código fuente de escritorio que se considera potente pero ligero. Para los sistemas operativos Windows, macOS y Linux, es accesible. Incluye soporte incorporado para TypeScript, JavaScript y Node.js, el último de los cuales tiene un ecosistema considerable de extensiones para muchos lenguajes diferentes, incluidos C ++, C #, Java, Python, PHP y Go. También se incluyen tiempos de ejecución, como .NET y Unity [29].

#### **4.12. Funciones HASH**

La función hash es un tipo de operación que convierte cualquier cantidad de datos de entrada en una salida de tamaño fijo que se conoce como hash o hash. El tamaño de salida a menudo se expresa en bits de datos y con frecuencia se incluye en el nombre de la función hash. Las aplicaciones que incluyen autenticación, integridad de mensajes, huellas dactilares, detección de datos corruptos y firmas digitales utilizan funciones hash criptográficas. Dado que las funciones hash criptográficas deben ser unidireccionales, el hash criptográfico se diferencia claramente del cifrado. Por ejemplo, puede ingresar texto sin formato y obtener un resultado utilizando una función hash [30].

Dentro de este Trabajo de Titulación se utilizó SHA-256.

#### **4.12.1.1. SHA-256**

Una función hash criptográfica, el método SHA-256 se utiliza tanto para la integridad de los datos como para los certificados digitales. NIST es la empresa que creó SHA-256 (Instituto Nacional de Estándares y Tecnología). Se puede ingresar un mensaje de cualquier longitud inferior a 264 bits en el algoritmo SHA-256, que devuelve un resumen del mensaje de 256 bits de la entrada [31].

#### **4.13. Trabajos relacionados**

Actualmente no existe un proyecto o solución tecnológica en Ecuador que utilice la tecnología blockchain para verificar la trazabilidad de los vinos Ambrosia. Con el fin de descubrir iniciativas que empleen la tecnología Blockchain para validar documentos y brindar mayor confiabilidad y seguridad a los usuarios, se buscó a nivel latinoamericano. Estos proyectos se mencionan en la Tabla 2 junto con sus conclusiones específicas.

**Tabla 2.** Trabajos relacionados

<b>Título</b>	<b>Hallazgo</b>	<b>Referencia</b>
Ambrosus	<p>Ambrosus está desarrollando un ecosistema que, aunque se puede aplicar a alimentos y medicinas en general, se puede simplificar para compararlo con el sistema de trazabilidad confiable propuesto para el vino.</p> <p>Internet de las cosas: Los dispositivos que se pueden conectar en red y automatizar brindan seguridad y prueba de datos, lo que los convierte en la fuente de información veraz que se puede rastrear y utilizar adecuadamente.</p> <p>Almacenamiento seguro de datos: Los datos descentralizados, que se definen como inmutables e interoperables permiten una fácil autenticación y uso compartido, con contratos inteligentes automatizados que reducen la entrada manual. La prueba de conocimiento cero se utiliza para autenticar a los usuarios manteniendo una privacidad estricta.</p> <p>Trazabilidad de la cadena de suministro: Una red para rastrear cualquier producto desde el origen hasta el minorista, con rastreo de ubicación geográfica, autenticación de productos y control de calidad y condición, a través de datos que no se pueden manipular.</p> <p>Prueba de origen: Los informes de envío actualizados y otros documentos comerciales brindan información confiable sobre el fabricante y la logística. La prueba para cumplir se mantiene a través de informes automatizados por la cadena de bloques en una red descentralizada y transparente.</p>	[32]
Universidad Comillas pontifica	La universidad Comillas pontifica plantea el tema de Viabilidad de la trazabilidad basada en la tecnología Blockchain en productos de agroalimentación. Esto permite eliminar ambigüedades de la procedencia de los productos que	[33]

---

Revista publicada en China	producen de tal manera que evitan problemas en cuestión a seguridad alimentaria. En una revista publicada en China plantean In Vino Veritas Blockchain como una solución viable para combatir los vinos falsificados, esto les permite que el consumidor final pueda escanear el código QR que viene impreso en la etiqueta y comprobar la procedencia del producto y verificar si es el original	[34]
----------------------------	--	------

---



## 5. Metodología

El Trabajo de Titulación permitió una verificación precisa de la seguridad y trazabilidad del vino Ambrosia mediante la implementación de una DApp con tecnología blockchain. El proyecto se originó a partir de una pregunta de investigación: **¿Cómo validar la trazabilidad de vinos Ambrosia?** y se llevó a cabo desde su desarrollo hasta su finalización.

También, se desarrolló, definió y organizó un conjunto de metodologías, métodos, técnicas, estándares y materiales, creando una serie de pasos ordenados para el desarrollo del proyecto que se describen a continuación:

### 5.1. Metodología de desarrollo de software

En este Trabajo de Titulación se utilizó la metodología de desarrollo "Agile Blockchain DApp Engineering" (ABCDE), que proporcionó una serie de pasos adecuados para su implementación. Para obtener más información detallada sobre la metodología, se puede consultar la sección 4.6 del Marco Teórico.

### 5.2. Proceso

A continuación, se detalla cómo completar cada objetivo TT, con una descripción de cada objetivo y sus actividades asociadas:

#### 1. Objetivo 1

1.1. Definir la Dapp

1.2. La fase 1 del TT implica establecer el objetivo de la DApp utilizando la metodología de desarrollo de software ABCDE, tal y como se describe en la sección 6.1.1 del Objetivo 1 la sección Resultados.

1.3. La fase 2 de la metodología de desarrollo de software ABCDE implica la determinación de los actores involucrados en la DApp, según se indica en el punto 6.1.2 del Objetivo 1 la sección Resultados

1.4. La fase 3 de la metodología de desarrollo de software ABCDE implica la determinación de los requisitos de la DApp, lo cual incluye la elaboración del documento de especificación de requisitos de la IEEE 830, tal como se describe en el punto 6.1.3 del Objetivo 1 de los resultados obtenidos.

#### 2. Objetivo 2

2.1. La fase 4 de la metodología de desarrollo de software ABCDE consiste en dividir la DApp en componentes y determinar las tecnologías necesarias

para lograr el siguiente objetivo, como se describe en el punto 6.2.4 del Objetivo 2 la sección Resultados.

2.2.La creación de los sistemas de contratos inteligentes y aplicaciones está contemplada en las fases 5 y 7 del enfoque de desarrollo ABCDE, como se detalla en el apartado 6.2.5 del Objetivo 2 la sección Resultados

2.3.La implementación y evaluación individual de cada subsistema, incluyendo los contratos inteligentes y las aplicaciones, se lleva a cabo en las fases 6 y 8 del enfoque de desarrollo ABCDE. Los detalles se pueden encontrar en los puntos 6.2.6 y 6.2.7 del Objetivo 2 la sección Resultados.

2.4.Realizar pruebas en una testnet para evaluar la solución.

### **3. Objetivo 3**

**5.3.** La realización y ejecución de pruebas de integración forma parte de la fase 9 del enfoque de desarrollo ABCDE. Este proceso se describe con más detalle en el punto **6.3.1.1 del Objetivo 3 la sección Resultados.**

**5.4.** La creación y ejecución de pruebas funcionales y de aceptación forma parte de la fase 9 del enfoque de desarrollo ABCDE. Los detalles se pueden encontrar en el punto **6.3.1.2 del Objetivo 3 la sección Resultados.**

**5.5.** Desplegar el módulo en la testnet Sepolia y del servicio en la nube de Heroku se lleva a cabo en la fase 9 del enfoque de desarrollo ABCDE. Los detalles se pueden encontrar en el punto **6.3.1.3 del Objetivo 3 la sección Resultados.**

## **5.6. Métodos**

### **5.6.1. Analítico**

Esta técnica, que se utilizó para dividir el trabajo de graduación en fases conocidas como objetivos particulares con sus actividades relacionadas esto ayudo a plantear cada una de las actividades del **Objetivo 1, Objetivo 2 y Objetivo 3**, se basa en dividir todos los elementos o piezas para encontrar causas, características y efectos [35].

### **5.3.2. Investigación-acción**

El enfoque de investigación se estructura en ciclos y se caracteriza por su flexibilidad, ya que es un proceso activo que requiere ajustes a medida que avanza la investigación hasta lograr una solución al problema. La secuencia de pasos comprende la identificación del problema en primer lugar, la elaboración de un plan para abordarlo en segundo lugar, la implementación y

evaluación del plan en tercer lugar, y la presentación de una solución en cuarto lugar. Este enfoque resulta útil en las diversas etapas del Trabajo de Titulación en especial en el **Objetivo 2 y Objetivo 3**.

## **5.6.2. Experimentales Controlados**

### **5.6.2.1. Replicación**

Esto permite desarrollar muchos tipos de productos con versiones diferentes, en este caso la DApp, hasta que cumpla con los requisitos de IEEE 830. Se utilizo para la especificación de requisitos que se encuentran en la sección del **Objetivo 1**.

### **5.6.2.2. Simulación**

Este procedimiento posibilita la utilización de información ficticia para operar un producto [36]. De esta manera, se logra simular la DApp en una testnet de blockchain, lo que permite cumplir con **Objetivo 3** que consiste en probar la solución en una testnet de blockchain para la DApp encargada de verificar la trazabilidad de los vinos Ambrosia.

Este método le permite crear un producto con datos de diseño [36]. Por ende, permitirá que el desarrollo de la DApp se mantenga en la red de prueba de la cadena de bloques al completar con éxito al objetivo 3 denominado Desplegar y probar la DApp sobre la testnet de blockchain donde se valide la trazabilidad en la elaboración de Vinos Ambrosia.

## **5.6.3. Métodos Observacionales**

### **5.6.3.1. Análisis estático**

Con este método se puede llevar a cabo un análisis detallado de la estructura del producto, específicamente de la DApp que verifica la trazabilidad de los vinos Ambrosia, con el propósito de detectar posibles fallos, lo que permite cumplir con **Objetivo 3** que consiste en probar la solución en una testnet de blockchain para la DApp encargada de verificar la trazabilidad de los vinos Ambrosia.

### **5.6.3.2. Caso de estudio**

Este enfoque tiene como finalidad emplear herramientas para supervisar minuciosamente un proyecto, lo que contribuye a determinar la aceptación del Trabajo de Titulación y evaluar si las herramientas utilizadas son apropiadas, lo que permite cumplir con el **Objetivo 2 y Objetivo 3** que consisten en desarrollar los subsistemas, integrar, probar y desplegar.

## **5.7. Técnicas**

### **5.7.1.1. Entrevista**

La entrevista es un método clásico que se utiliza ampliamente en la investigación cualitativa para recolectar datos o requerimientos. Esta técnica es adecuada para abordar temas relacionados con el **Objetivo 1** ya que permite tomar la información de trazabilidad de vinos Ambrosia con el propósito de obtener requisitos.

### **5.7.2. Reuniones**

Este método permite que aquellos que estén interesados en el trabajo de títulos estudien los diversos avances en cada fase mientras brindan retroalimentación continuamente.

## **5.8. Estándares**

### **5.8.1. IEEE 830**

Es una lista de sugerencias para definir requisitos o especificaciones de software. Esto ayuda a lograr el primer objetivo particular de la ingeniería de requisitos del Trabajo de Titulación de definir el DApp para validar la trazabilidad de los vinos.

### **5.8.2. ERC 20**

Un marco que permite la creación de contratos inteligentes, que está conectado con el segundo objetivo específico del TT, para crear compatibilidad e interoperabilidad entre los diversos tokens de la red Ethereum y mejorar el ecosistema.

## 5.9. Materiales

### 5.9.1. Recurso Humano

Las personas involucradas para realizar el Trabajo de Titulación fueron en varios campos, como se puede ver en el Tabla 3.

**Tabla 3.** Recurso Humano

<b>Nombre</b>	<b>Descripción</b>
Jimmy Leonel Vicente Guayanay	Estudiante responsable de llevar a cabo el proyecto.
Ing. Cristian Ramiro Narváez Guillen, Mg.Sc.	Docente responsable de dirigir el Proyecto de Trabajo de Titulación.
Ing. Jaime Ramiro Santin Calva, Mg.Sc.	Socio y propietario de Vinos y Alimentos Ambrosia.
Darwin Alexander Sotomayor Mendoza	Socio y propietario de Vinos y Alimentos Ambrosia.

### 5.9.2. Recursos de Software y Hardware

El Trabajo de Titulación fue llevado a cabo mediante la utilización de diversos recursos de Software y Hardware, los cuales se encuentran detallados en la Tabla 4 y la Tabla 5. respectivamente. Estos recursos fueron necesarios para la implementación del proyecto y permitieron llevar a cabo diversas tareas, como la programación de la DApp para validar la trazabilidad de los vinos Ambrosia, el procesamiento de datos y la simulación de la DApp en una testnet de blockchain.

**Tabla 4.** Recursos de Software

<b>Recurso</b>	<b>Descripción</b>	<b>Acceso</b>
OneDrive	Sistema de almacenamiento para llevar un control de versiones del documento	<a href="https://www.microsoft.com/es-ww/microsoft-365/onedrive/online-cloud-storage">https://www.microsoft.com/es-ww/microsoft-365/onedrive/online-cloud-storage</a>
Diagrams.net	Plataforma de Google para realizar los diagramas	<a href="https://app.diagrams.net">https://app.diagrams.net</a>
Zoom	Plataforma de reuniones online para realizar entrevistas, e indicaciones generales	<a href="https://zoom.us">https://zoom.us</a>
Node js	Entorno para desarrollar el backend con javascript	<a href="https://nodejs.org/es">https://nodejs.org/es</a>
Ethereum	Plataforma de desarrollo basada en tecnología blockchain.	<a href="https://ethereum.org/es">https://ethereum.org/es</a>

Etherscan	Plataforma para observar el registro de transacciones previas (específicamente con la red de pruebas Sepolia).	<a href="https://sepolia.etherscan.io/">https://sepolia.etherscan.io/</a>
Sepolia	Testnet de Ethereum para el despliegue	<a href="https://sepolia.etherscan.io/#stats">https://sepolia.etherscan.io/#stats</a>
Infura	Suite que permite crear un proyecto donde ofrece las credenciales para la conexión con la testnet Sepolia	<a href="https://infura.io">https://infura.io</a>
Visual Studio Code	Editor de código fuente	<a href="https://code.visualstudio.com">https://code.visualstudio.com</a>
Truffle Suite	Herramienta con varias tecnologías que permitió el desarrollo de la DApp.	<a href="https://www.trufflesuite.com">https://www.trufflesuite.com</a>
GitHub	Repositorio online para almacenar y realizar el control de versiones de la DApp.	<a href="https://github.com">https://github.com</a>
Metamask	Software de Criptomoneda que es instalado como extensión de un navegador web para conexión con aplicaciones de Blockchain.	<a href="https://metamask.io">https://metamask.io</a>
web3.js	Se trata de un conjunto de librerías que posibilitan la interacción con un nodo Ethereum cercano o a distancia, a través de los protocolos HTTP, IPC o WebSocket.	<a href="https://web3js.readthedocs.io">https://web3js.readthedocs.io</a>
sha256.js	Función hash sencilla de SHA-256 para JavaScript, que es capaz de admitir la codificación UTF-8.	<a href="https://www.npmjs.com/package/sha256">https://www.npmjs.com/package/sha256</a>
Jest	Framework de pruebas para JavaScript.	<a href="https://jestjs.io">https://jestjs.io</a>
Selenium IDE	Es una herramienta para diversos tipos de pruebas.	<a href="https://www.selenium.dev/">https://www.selenium.dev/</a>
/@truffle/contract	Liberia que permite la conexión con los contratos inteligentes	<a href="https://www.npmjs.com/package/@truffle/contract">https://www.npmjs.com/package/@truffle/contract</a>
Heroku	El servicio de nube informática utilizado para realizar pruebas y desplegar la DApp.	<a href="https://www.heroku.com/">https://www.heroku.com/</a>

**Tabla 5.** Recursos de Hardware

<b>Recurso</b>	<b>Descripción</b>
Laptop	Dispositivo tecnológico fundamental para la elaboración del Trabajo de titulación.

### 5.9.3. Insumos

La Tabla 6. enumera los elementos necesarios para llevar a cabo el Proyecto de Trabajo de Titulación. Identificar estos insumos es un paso crucial en la planificación y ejecución del

proyecto, y su disponibilidad y acceso son aspectos críticos que deben ser considerados cuidadosamente.

**Tabla 6.** Insumos

<b>Insumos</b>	<b>Descripción</b>
Materiales de oficina	Utilizado en conjunto con la creación del trabajo de titulación.
Internet	Se utiliza para acceder a otras herramientas, realizar investigaciones y comunicarse.

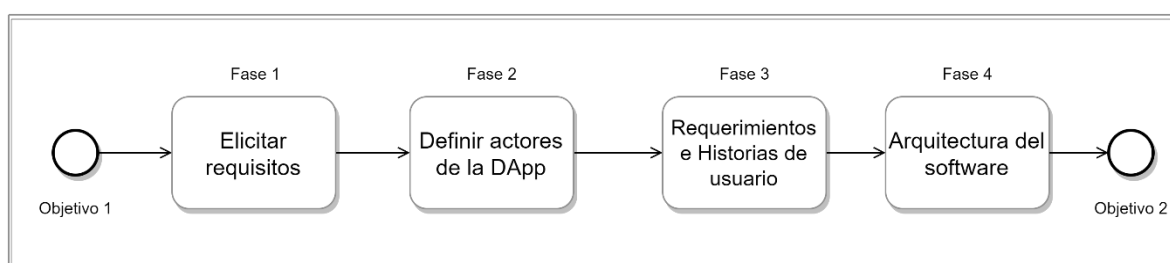
## 6. Resultados

En esta sección se exponen los resultados obtenidos durante la ejecución del Proyecto de Trabajo de Titulación, el cual se desarrolló siguiendo la metodología de desarrollo ABCDE y cumpliendo con los objetivos específicos establecidos.

### 6.1. Objetivo 1

**Determinar los procesos de producción de vinos Ambrosia que permita delimitar y elicitar los requerimientos y la arquitectura de la DApp**

En esta etapa, se realizan las siguientes fases descritas en la Figura 6 para la implementación de la DApp basada en tecnología blockchain para la trazabilidad de los vinos Ambrosia:



**Figura 6.** Diagrama BPMN de las fases para el desarrollo del objetivo 1.

Las fases propuestas en la Figura 6 se detallan de la siguiente manera:

- Elicitar requisitos (Fase 1): En esta fase se recopilan las necesidades y requerimientos de los diferentes stakeholders del proyecto.
- Definir actores de la DApp (Fase 2): se identifican los diferentes actores que interactuarán con la DApp.
- Historias de Usuario (Fase 3): se crean las historias de usuario, que describen las diferentes acciones que pueden realizar los actores de la DApp.
- Arquitectura (Fase 4): se diseña la arquitectura de la DApp, que incluye las fases de desarrollo de la DApp.

Para una explicación más detallada, se pueden consultar los puntos 1, 2, 3 y 4 de la sección **ABCDE (agile block chain DApp engineering)** del Marco teórico.



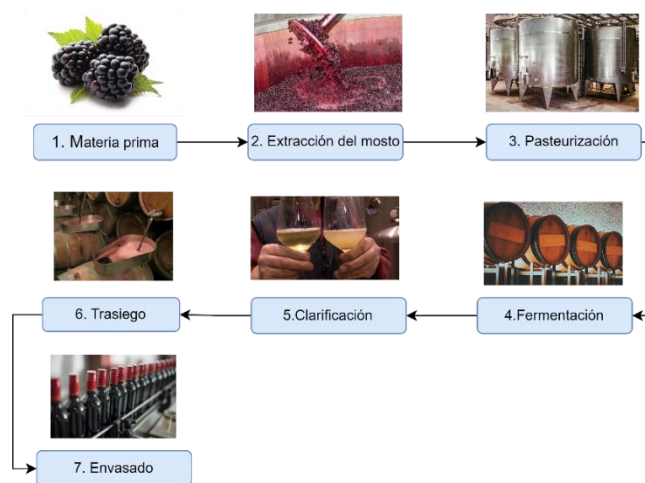
### 6.1.1. Determinar los procesos de producción de vinos Ambrosia

Según se detalla en la entrevista llevada a cabo (véase **Anexo 1. Entrevista a representante de vinos Ambrosia**) con los socios y propietarios de Vinos Ambrosia, cuyos perfiles se describen en la sección de **Recursos de Software y Hardware**, se logró identificar y definir los procesos clave que se ilustran en la **Figura 7**., El propósito de esta delimitación es determinar qué información se almacenará en la blockchain.

Durante la entrevista, se llevaron a cabo discusiones exhaustivas sobre las actividades comerciales y operativas de Vinos Ambrosia. Como resultado, se identificaron los procesos principales que son de vital importancia para la empresa. Estos procesos representan las etapas fundamentales que se deben seguir para llevar a cabo las distintas operaciones dentro de la organización.

La **Figura 7** representa una visualización gráfica de los procesos identificados, lo que proporciona una comprensión clara y concisa de cómo se interrelacionan y se desarrollan en la estructura general de Vinos Ambrosia. Estos procesos se han seleccionado cuidadosamente con el objetivo de determinar qué información será registrada y almacenada en la blockchain.

Al delimitar la información que se guardará en la blockchain, Vinos Ambrosia busca asegurar la integridad, la transparencia y la trazabilidad de los datos relacionados con sus procesos clave. Al aprovechar la tecnología de la cadena de bloques, la empresa puede garantizar que los registros sean inmutables y verificables, lo que fortalece la confianza tanto interna como externa en las actividades y transacciones de Vinos Ambrosia.



**Figura 7.** Procesos de producción de vinos Ambrosia

### 6.1.2. Fase 1: Elicitar Requisitos

Esta sección complementa el objetivo general del Trabajo de Titulación, el cual busca “Implementar una aplicación descentralizada (DApp) utilizando la tecnología blockchain que permita la trazabilidad de la producción de vinos Ambrosia”. Con el fin de lograr este objetivo, es fundamental recopilar las necesidades y requerimientos de los diferentes stakeholders del proyecto, en particular los productores de vinos.

Para garantizar que la DApp cumpla con las expectativas y necesidades de todos los actores involucrados, se emplean diversas metodologías de investigación, como entrevistas y encuestas. Estas técnicas permiten obtener una comprensión completa de los requisitos y deseos de los productores de vinos, así como de otros stakeholders relevantes en el proceso de producción.

La recopilación de requisitos a través de entrevistas y encuestas es un proceso crucial para el éxito del proyecto, ya que proporciona una base sólida para el diseño y desarrollo de la aplicación descentralizada. Al comprender a fondo las expectativas y necesidades de los stakeholders, se puede garantizar que la DApp sea diseñada de manera acorde y ofrezca las funcionalidades y características requeridas para lograr la trazabilidad deseada en la producción de vinos Ambrosia.

### 6.1.3. Fase 2: Actores de la DApp

La DApp define los siguientes actores que interactuarán con la DApp:

**Tabla 7.** Roles de la DApp

<b>Actores</b>	<b>Rol</b>
Usuario final	El usuario que requiere visualizar la trazabilidad del vino.
Usuario administrador	El usuario responsable de desplegar la trazabilidad correspondiente a cada botella producida.
SC-TVA (Smart Contract – Trazabilidad Vinos Ambrosia)	Uno o varios contratos inteligentes en la blockchain de Ethereum (ya sea en la red local de prueba o en Sepolia) que cuentan con la capacidad de registrar y verificar la trazabilidad del vino.

#### 6.1.4. Fase 3: Requerimientos e Historias de usuario de la DApp

En esta fase se detallan los requisitos funcionales y no funcionales (tomados del **Anexo 1**. Entrevista a representante de vinos Ambrosia) de acuerdo con el estándar IEEE 830. Estos requisitos se obtuvieron a partir de una entrevista con el representante legal de Vinos Ambrosia, quien describió los procesos de producción principales. Además, se incluyen las historias de usuario (**Anexo 3**. Descripción de Historias de usuario) y el diagrama de casos de uso.

#### 6.1.5. Requisitos funcionales

La especificación de requisitos funcionales de la DApp para verificar la trazabilidad de los vinos Ambrosia se muestra en la Tabla 8. Es importante señalar que la DApp utiliza la función SHA-256 ya que la cantidad de información es crucial porque a mayor tamaño, más costoso será la transacción. También tiene la mayor adopción y es más seguro que otros algoritmos de encriptación.

**Tabla 8.** Requisitos funcionales

<b>Código</b>	<b>Requisito</b>	<b>Descripción</b>
RF01	Gestionar registro de un proceso de TVA para generar HASH	La DApp gestionará un proceso de TVA para generar el HASH sha-256
RF02	Registrar HASH de TVA en la Blockchain	La DApp almacenará el hash de la TVA en la Blockchain de Ethereum, solo por la dirección de billetera que este autorizada
RF03	Generar código QR de la botella de vino	La DApp permitirá generar un código QR de la botella a partir del HASH de la TVA
RF04	Obtener HASH a partir del código QR en la botella de vino	La DApp permitirá obtener el HASH del código QR presente en la botella de vino mediante la cámara del dispositivo.
RF05	Obtener TVAs registradas	La DApp generará un HASH 256 de la TVA a validar a partir del código QR de la botella
RF06	Validar la trazabilidad de vino	La DApp verificará si hay una concordancia entre los TVAs obtenidos del RF05 y el generado en el RF02.
RF07	Presentar resultado	La DApp emitirá una notificación en el sitio web, donde se detallará el resultado correspondiente a la trazabilidad de la botella en cuestión.

### 6.1.6. Requisitos no funcionales

Para validar la trazabilidad de vinos Ambrosia dentro de la DApp se realizó varios requisitos no funcionales descritos en la Tabla 9.

**Tabla 9.** Requisitos no funcionales

<b>Código</b>	<b>Requisito</b>	<b>Descripción</b>
RNF01	Rendimiento	En una red de prueba de Ethereum, la transacción tarda entre 2 a 5 segundos; sin embargo, en un entorno real, puede tardar entre 15 segundos a 5 minutos.
RNF02	Usabilidad	La DApp debe tener una interfaz que sea fácil de usar y comprender, lo que hace que el procedimiento sea simple de completar. Además, debe permitir su uso en cualquier navegador web.
RNF03	Fiabilidad	La DApp debe implementar medidas de seguridad robustas para proteger la información sensible y los activos digitales relacionados con la producción de vinos.
RNF04	Seguridad	Se debe implementar un sistema de control de acceso para garantizar que solo los usuarios autorizados tengan permiso para realizar ciertas operaciones en la DApp. Esto incluye la gestión de roles y privilegios.

### 6.1.7. Historias de usuario

La Tabla 10 proporciona un resumen de las historias de usuario de la DApp que se utilizará para validar la trazabilidad de los vinos Ambrosia. La descripción completa de las historias de usuario se encuentra en el **Anexo 3**. Descripción de Historias de usuario.

**Tabla 10.** Historias de usuario

<b>Identificador de la historia</b>	<b>Rol</b>	<b>Característica / Funcionalidad</b>	<b>Razón / Resultado</b>
HU01	Como cliente	Quiero acceder a la información de TVA.	Con el objetivo de validar la trazabilidad de la TVA
HU02	Como administrador	Quiero registrar una TVA	Con el propósito de inscribir una TVA en la cadena de bloques.
HU03	Como Contrato inteligente (SM-TVA)	Quiero validar una TVA	Con el propósito de verificar si la TVA ha sido registrada en la cadena de bloques.
HU04	Como Contrato inteligente (SM-TVA)	Quiero registrar una TVA	Con el propósito de registrar una TVA en la cadena de bloques.
HU05	Como SPA-TVA	Quiero generar el SHA-256 del TVA	Con el propósito de crear el valor hash SHA-256 de la TVA.

### 6.1.8. Caso de usos

La Figura 8 muestra un diagrama que representa los distintos actores y sus correspondientes casos de uso.

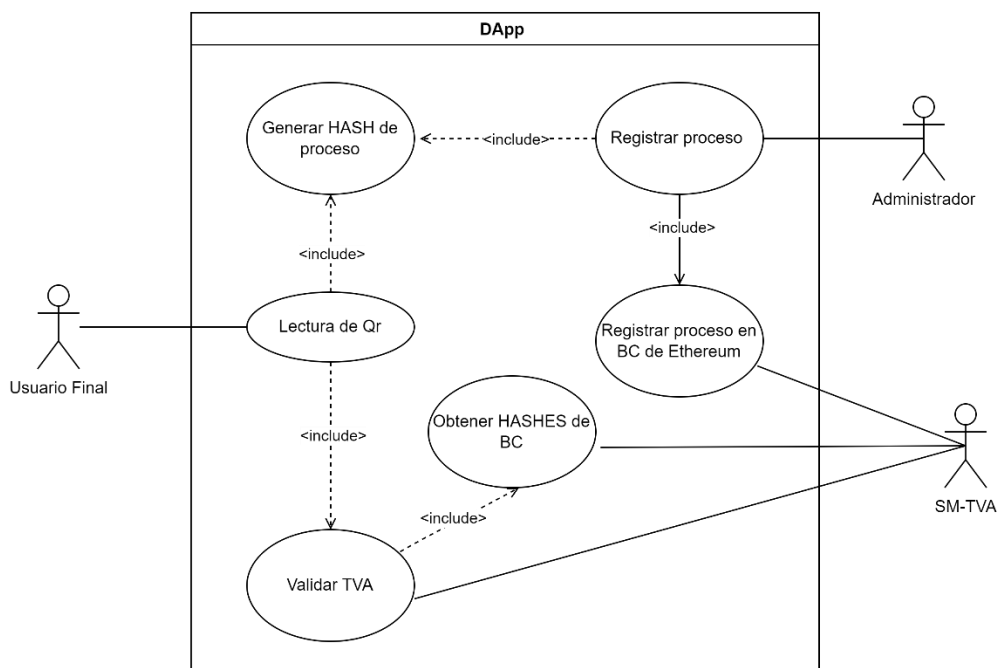
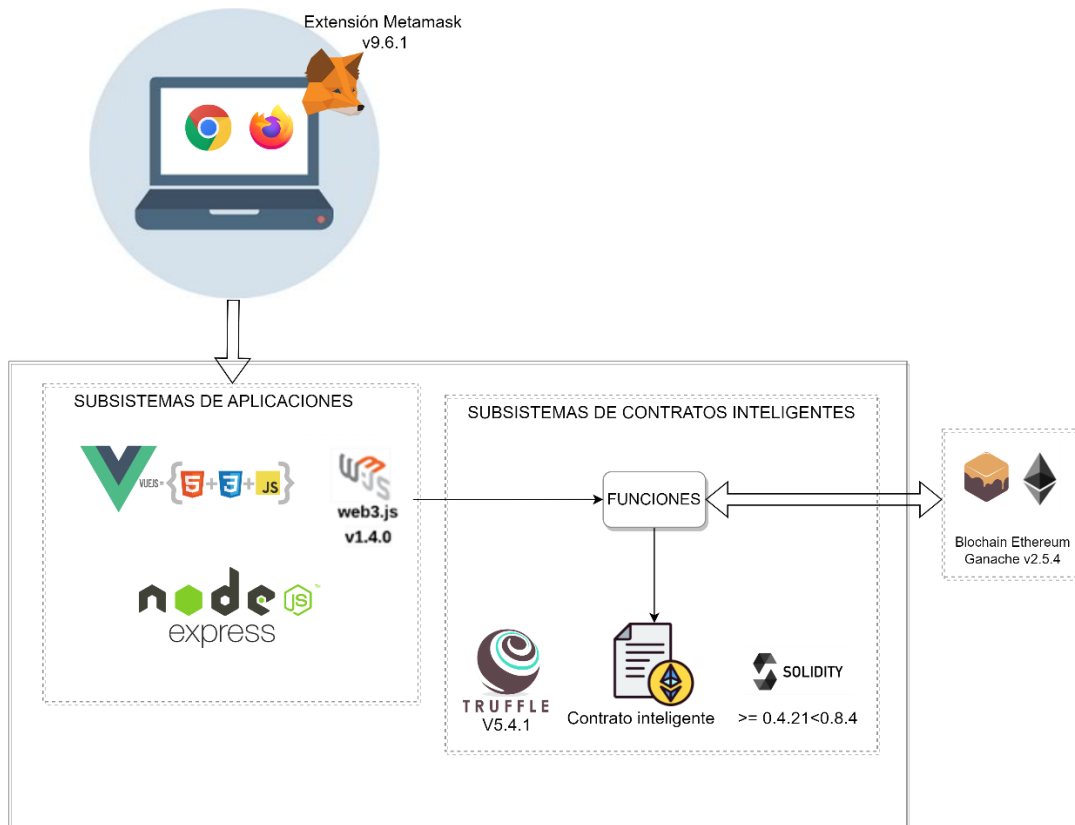


Figura 8. Diagrama de casos de uso de la DApp.

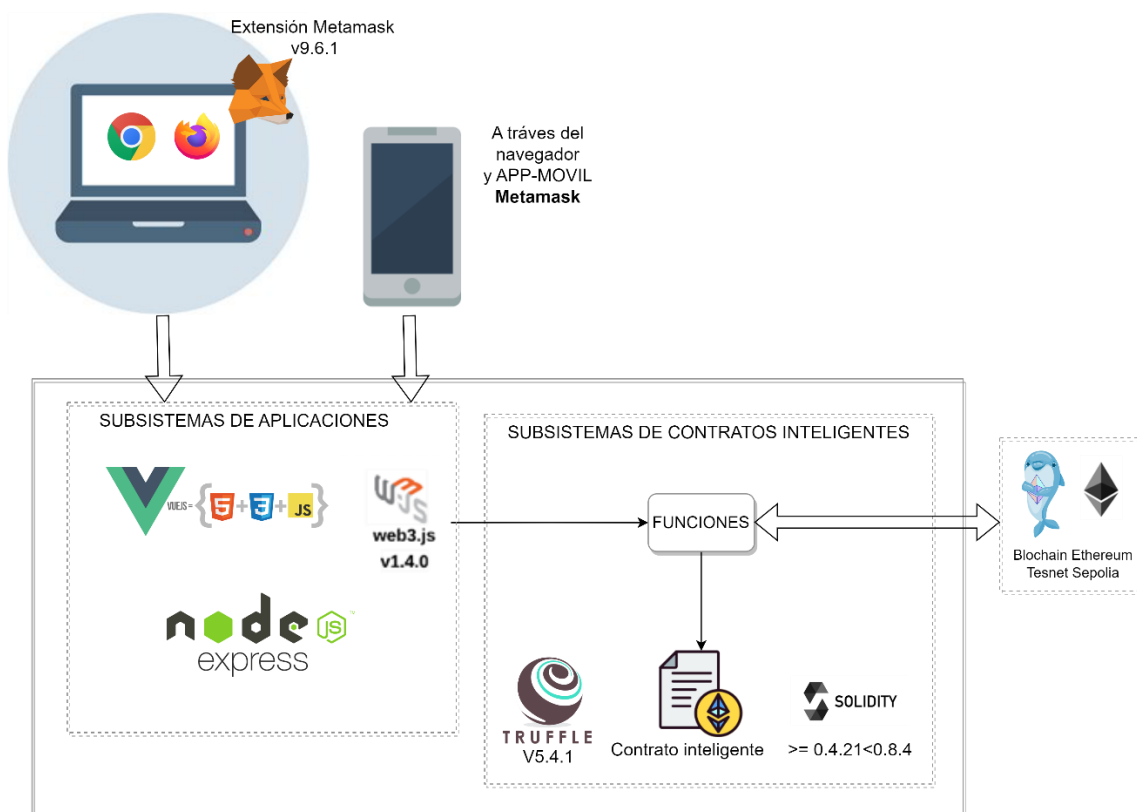
### 6.1.9. Fase 4: Diagrama de la arquitectura de la DApp

Durante esta etapa se propone el diagrama que representa la arquitectura de la DApp. En la Figura 9 y Figura 10 se presentan los diagramas que muestran la arquitectura de la DApp para la trazabilidad de vinos Ambrosia, y su conexión respectiva a la red de prueba local de Ganache y a la testnet Sepolia de Ethereum. Se emplean diversas tecnologías en cada uno de sus subsistemas.

Para interactuar con las funcionalidades de un contrato creado con la herramienta Truffle y el lenguaje de programación Solidity, el Frontend (Vue.js, HTML, CSS y JavaScript), Backend (Node.js, MongoDB), y web3.js; es necesario el complemento Metamask este instalado en el navegador. Esto hace posible crear un enlace a la cadena de bloques Ethereum de la red de prueba correspondiente. Además, ya se puede acceder a través del navegador de la aplicación móvil Metamask una vez que se haya instalado en la red de prueba de Sepolia para su implementación. Debe generar una billetera (Wallet) en Metamask de manera necesaria.



**Figura 9.** Arquitectura de la DApp con Ganache (testnet blockchain local)



**Figura 10.** Arquitectura de la DApp con Sepolia (testnet blockchain Ethereum).

## 6.2. Objetivo 2

### Desarrollar la DApp cumpliendo con la arquitectura y elicitación de los requerimientos.

Este objetivo es desarrollar la DApp que requiere varias fases importantes como se muestra en la Figura 11. Cada una de estas fases son importantes para garantizar el éxito de la DApp y su cumplimiento de los requisitos funcionales y no funcionales.

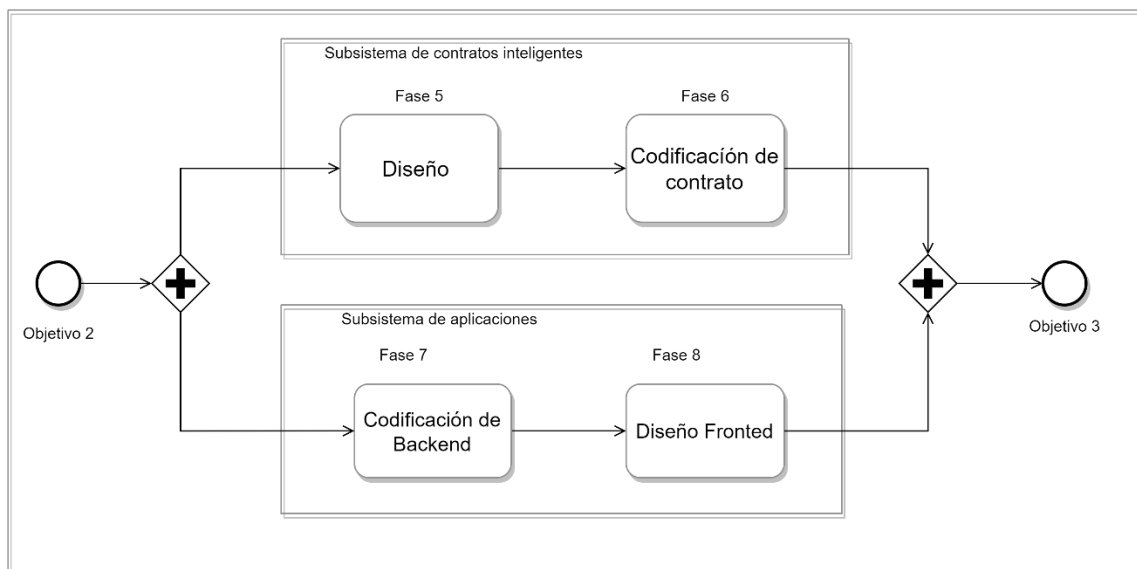


Figura 11. Diagrama BPMN de las fases para el desarrollo del objetivo 2.

Las fases de la Figura 11 se detallan a continuación:

- El subsistema de contratos inteligentes se compone de las etapas siguientes: diseño (fase 5) y codificación y prueba (fase 6) del subsistema
- El subsistema de aplicaciones comprende las etapas siguientes: programación del backend del subsistema de interacción externa (Sistema de aplicaciones) (fase 7) y diseño del frontend del subsistema de aplicaciones (fase 8).

Para una explicación más detallada, se pueden consultar los puntos 5, 6, 7 y 8 de la sección **ABCDE (agile block chain DApp engineering)** del Marco teórico.

### 6.2.1. Iteraciones (sprints) de la DApp

El enfoque ABCDE es iterativo e incremental en la mayoría de sus fases, con excepciones ocasionales en las fases 5 a 8 que corresponden al objetivo 2. Se propusieron sprints para cada subsistema que proporcionaban suficiente cumplimiento como se ve en la Tabla 11 y Tabla 12.

**Tabla 11.** Iteraciones del subsistema de contratos inteligentes

No. Sprints	Nombre	Duración en horas
1	Ajuste inicial	8
2	Elaboración del subsistema.	12
3	Desarrollar el contrato inteligente para proceso	50
4	Configuración del contrato ERC721	30
5	Compilación de los contratos	5
6	Migración del contrato	8
7	Pruebas unitarias	25

**Tabla 12.** Iteraciones del subsistema de aplicaciones

No. Sprints	Nombre	Duración en horas
1	Ajustes iniciales	10
2	Generar modelos en el Backend para el usuario y los 7 procesos de trazabilidad	20
3	Generar API-REST para administración de usuarios y procesos	30
4	Pruebas de API-REST mediante Postman	5
5	Diseño de interfaz con Vue de acuerdo a la temática de Vinos Ambrosia	20
6	Conexión al API-REST para administración de usuarios y procesos con librería Axios	30
7	Integración con web3	2
8	Integración con contratos inteligentes	5
9	Integración con las funciones del contrato inteligente.	18
10	Crear el hash SHA-256 del proceso de trazabilidad.	5
11	Generar tokens ERC721 de acuerdo al número de botellas producidas.	10
12	Asignar token ERC721 al usuario final.	10
13	Pruebas unitarias	22



## 6.2.2. Control de versiones de la DApp

Para el control de versiones se utilizó el software Visual Studio y Git. La Figura 12 muestra los compromisos que se realizaron en los diversos sprints que se llevaron a cabo a lo largo del desarrollo de los subsistemas utilizando la técnica ABCDE. Todo esto se puede encontrar en el siguiente repositorio de GitHub: <https://github.com/JimmyVicente/vinos-blockchain>.

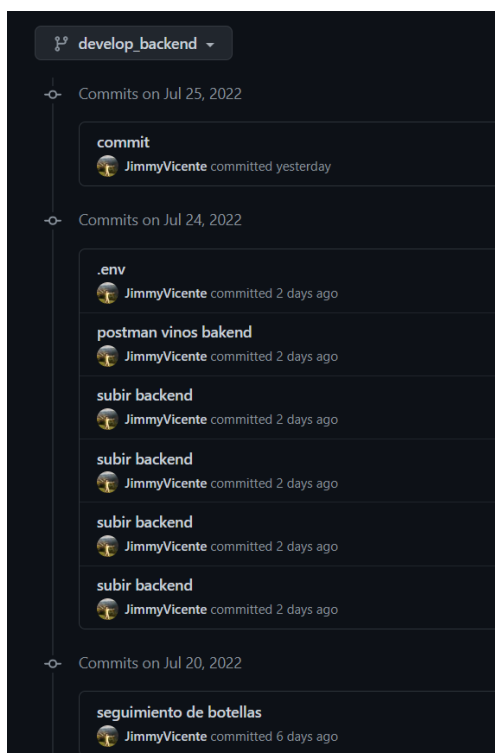


Figura 12. Control de versiones de la DApp con GitHub.

## 6.2.3. Configuración inicial

Para los dos subsistemas se realizó en conjunto la siguiente configuración inicial, que se observa en la Tabla 13:

Tabla 13. Ajustes iniciales

Tareas	Estado
Instalación y configuración de node.js.	✓
Instalación e integrar la librería web3.js	✓
Instalación Truffle y configurar Ganache	✓
Instalación y configurar GIT	✓
Instalación un Entorno de desarrollo integrado, en este caso Visual Studio Code, con dos plugin denominados:	✓
• “Solidity”	
• “Solidity Visual Developer”	
Instalación, configuración e introducir frase Metamask	✓

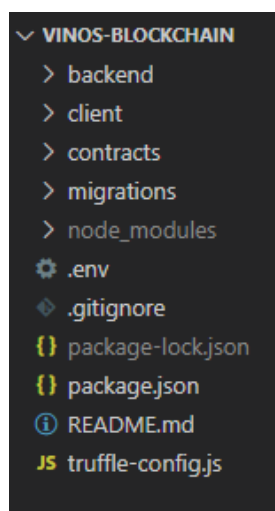
Instalación y configuración de servidor con express	✓
Instalación de las dependencias mongose, express y sha256 en el backend	✓
Instalación de la dependencia sha256 en la carpeta client	✓
Instalación de la dependencia vuetify en la carpeta client	✓
Instalación de la dependencia @truffle/contract en la carpeta client	✓
Instalación de la dependencia web3 en la carpeta client	✓

## 6.2.4. Estructura de la DApp

La DApp para la trazabilidad del vino Ambrosia contiene los tres subsistemas que se enumeran a continuación como su estructura. Los subsistemas están organizados en muchas carpetas.

### 6.2.4.1. Esquema del sistema de contratos inteligentes

En la Figura 13 proporciona una vista general de cómo están organizados los archivos y cómo están relacionados los diferentes componentes en el subsistema.



**Figura 13.** Esquema del sistema de contratos inteligentes.

En la Tabla 14 se proporciona una descripción detallada de la función principal de cada archivo dentro del subsistema de contratos inteligentes. Esta tabla incluye la función principal de cada archivo y su relación con otros archivos del subsistema.

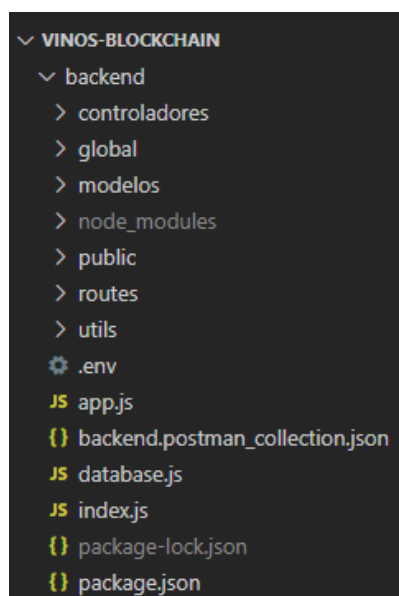
**Tabla 14.** Esquema del sistema de contratos inteligentes

Nombre	Descripción
<b>vinos-blockchain</b>	Directorio contenedor de la DApp para la TVA.
<b>backend</b>	<b>Subsistema de aplicaciones.</b>
<b>client</b>	<b>Subsistema de aplicaciones.</b>
<b>contract</b>	Directorio que guarda los distintos smart contracts.

<b>migrations</b>	Directorio que aloja los archivos JavaScript encargados de la migración de los distintos contratos inteligentes.
<b>node_modules</b>	Directorio que contiene los módulos utilizados por Node JS y donde se almacenan todas las dependencias para el subsistema.
<b>.env</b>	Archivo que almacena variables de entorno utilizadas en el subsistema
<b>.gitignore</b>	Archivo que lista los archivos o directorios que se deben excluir de la gestión de versiones.
<b>package-lock.json</b>	Archivo que contiene datos relevantes del subsistema y lista de paquetes o dependencias requeridas para su funcionamiento.
<b>package.json</b>	Archivo que guarda todas las dependencias del subsistema.
<b>README.md</b>	Archivo que contiene información acerca del subsistema.
<b>truffle-config.js</b>	Archivo js que almacena los ajustes de truffle.

#### 6.2.4.2. Esquema del subsistema de aplicaciones backend

La Figura 14 presenta una vista general de los archivos que conforman la estructura del subsistema de backend de aplicaciones.



**Figura 14.** Esquema del subsistema de aplicaciones backend.

En la Tabla 15 se proporciona una descripción detallada de la función principal de cada archivo dentro del subsistema de aplicaciones backend. Esta tabla incluye la función principal de cada archivo y su relación con otros archivos del subsistema.

**Tabla 15.** Esquema de subsistema de aplicaciones backend

Nombre	Descripción
--------	-------------

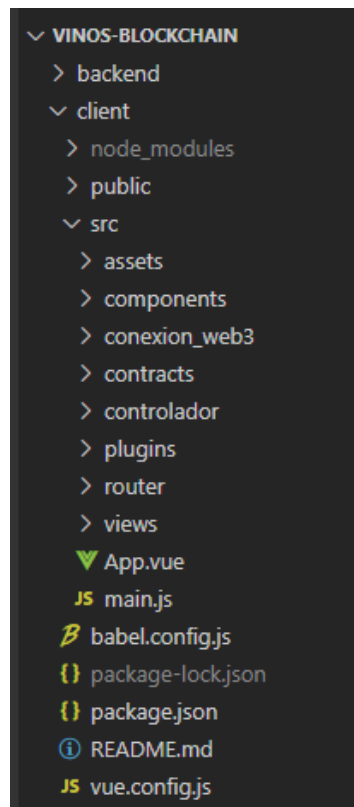
---

<b>controladores</b>	Directorio que almacena los controladores para agregar los procesos y usuarios.
<b>global</b>	Directorio que almacena variables globales del servidor
<b>modelos</b>	Directorio que almacena los modelos de usuarios y procesos.
<b>node_modules</b>	Directorio que contiene los módulos utilizados por Node JS y donde se almacenan todas las dependencias para el subsistema.
<b>public</b>	Directorio que contiene archivos públicos.
<b>routes</b>	Directorio que contiene las rutas del API-REST.
<b>utils</b>	Directorio que almacena funciones globales para validaciones y envío de peticiones del API-REST.
<b>.env</b>	Archivo que almacena variables de entorno utilizadas en el subsistema
<b>app.js</b>	Archivo que contiene la configuración del servidor
<b>backend.postman_collection.js</b>	Archivo de la colección de Postman de pruebas unitarias.
<b>database.js</b>	Archivo que contiene la configuración para conexión con la base de datos.
<b>index.js</b>	Archivo de ajustes para ejecutar el servidor.
<b>package-lock.json</b>	Archivo que contiene datos relevantes del subsistema y lista de paquetes o dependencias requeridas para su funcionamiento.
<b>package.json</b>	Archivo que guarda todas las dependencias del subsistema.

---

### 6.2.4.3. Esquema del subsistema de aplicaciones frontend

En la Figura 15 se observa la estructura del subsistema de aplicaciones frontend que incluye los diferentes componentes que componen la interfaz de usuario de la DApp. Además, proporciona una vista general de cómo se organiza la modelo vista controlador y cómo interactúan entre sí.



**Figura 15.** Esquema del subsistema de aplicaciones cliente.

La Tabla 16 proporciona una descripción detallada de cada archivo dentro del subsistema de aplicaciones frontend. Esta tabla incluye la función principal de cada archivo y su relación con otros archivos del subsistema. Esta información es esencial para comprender cómo se implementa la funcionalidad de la interfaz de usuario en la DApp y cómo interactúan entre sí los diferentes componentes para ofrecer diferentes funcionalidades.

**Tabla 16.** Esquema de subsistema de aplicaciones cliente

Nombre	Descripción
<b>public</b>	Directorio que contiene archivos públicos
<b>src</b>	Directorio que contiene la integración con el subsistema de contratos
<b>assets</b>	Directorio que contiene archivos como iconos, imágenes, etc.
<b>components</b>	Carpeta que almacena componentes de Vue para interfaz de usuario.
<b>conexion_web3</b>	Carpeta que almacena los archivos para la conexión a la web3 y conexión contratos inteligentes.
<b>node_modules</b>	Directorio que contiene los módulos utilizados por Node JS y donde se almacenan todas las dependencias para el subsistema.

---

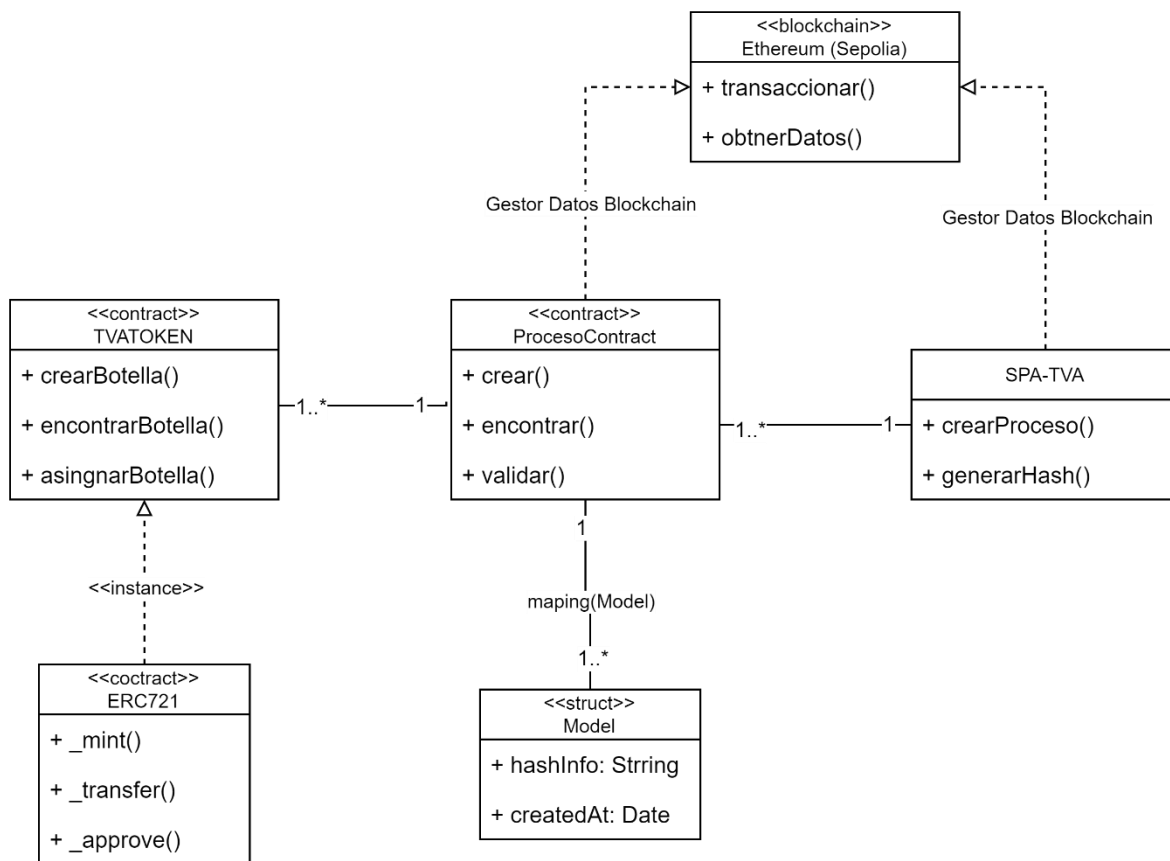
<b>contracts</b>	Directorio que contiene los contratos inteligentes compilados.
<b>controlador</b>	Directorio que contiene los controladores para la conexión al API-REST
<b>plugins</b>	Directorio que almacena el plugin utilizado en este caso vuetify
<b>router</b>	Directorio que almacena el archivo index.js para las rutas del cliente.
<b>views</b>	Directorio que contiene la interfaz del cliente y administrador
<b>App.vue</b>	Archivo que contiene la configuración de plugins utilizados en el frontend.
<b>main.js</b>	Archivo que contiene la configuración para inicializar el frontend.
<b>babel.config.js</b>	Archivo que nos va a permitir utilizar las funciones más actuales de JavaScript.
<b>package-lock.json</b>	Archivo que contiene datos relevantes del subsistema y lista de paquetes o dependencias requeridas para su funcionamiento.
<b>package.json</b>	Archivo que guarda todas las dependencias del subsistema.
<b>README.md</b>	Archivo que guarda información acerca del subsistema.
<b>vue.config.js</b>	Archivo que define la configuración de framework Vue.

---

A continuación, se describen las diversas etapas de la metodología ABCDE, junto con los resultados correspondientes, que forman parte del segundo objetivo.

#### **6.2.5. Fase 5: Diseño del subsistema de contratos inteligentes**

En esta fase se ha creado el **Diagrama de clases** con el objetivo de diseñar la estructura de la DApp, incluyendo las operaciones y relaciones correspondientes. La Figura 16 muestra el Diagrama de Clases completo, que se encuentra detallado en el **Anexo 4**. Diagrama de clases subsistema de contratos inteligentes.



**Figura 16.** Diagrama de clases de la DApp para subsistema de smart contracts

### 6.2.6. Fase 6: Codificación del subsistema de contratos inteligentes

Los contratos inteligentes codificados son "ProcesoContract.sol" y "TVAToken.sol", que se describen en detalle en el Anexo 5. Código de programación de subsistema de contratos inteligentes. A continuación, se detallan las funciones utilizadas en cada contrato.

Funciones del SC **ProcesoContract.sol** :

- La funcionalidad **crear()** está vinculada con el requisito funcional RF03 y tiene como objetivo recibir el valor hash SHA-256 del TVA (`_info`). Esta información se genera a partir de los 7 procesos previamente creados. Es importante destacar que esta funcionalidad es la única que conlleva un costo de transacción.
- La funcionalidad de validación, llamada **encontrar()**, está relacionada con el requisito funcional RF07. Esta función recibe como parámetro el valor hash SHA-256 del TVA y devuelve una estructura de datos "hash\_info" y "createdAt". Si el proceso no está registrado en la cadena de bloques, se devolverán valores vacíos, lo que permitirá validar si el proceso existe o no.

## Funciones del SC TVAToken.sol:

- La funcionalidad de **crear botella** que se denomina **crearBotella()**, recibe con información la cuenta del administrador dueño del contrato y el hash del proceso (SHA-256 del TVA), esto permite crear el token ERC721 con un id único perteneciente al proceso. Hay que tener en cuenta que este método está validado para que no se repitan las botellas ya que deben ser únicas y por ende esta funcionalidad tiene un costo.
- La funcionalidad de **encontrar botella** denominada **encontrarBotella()** recibe el parámetro `_hash` que hace referencia al id único generado en el método **crearBotella()**, esta función permite saber si el token ERC721 ya fue asignado a un cliente.
- La funcionalidad de **asignar botella** denominada **asignarBotella()** recibe los parámetros `address` y `tokenId` que hace referencia a la dirección de la billetera de usuario e id único de ERC721 para poder asignar el token. Hay que tener en cuenta que esta función va tener un costo de transacción que el usuario final debe pagar, el precio del fee va depender del valor de Ethereum.

### 6.2.7. Fase 7: Codificación del subsistema de aplicaciones backend

Esta fase se almacena la información de los 7 procesos (materia prima, extracción del mosto, pasteurización, fermentación, clarificación, trasiego, envasado) en base al diagrama de clases generado en el Anexo 5. Diagrama de clases subsistema de aplicaciones. Se desarrolló el API-REST para la administración de la TVA descritas en la Tabla 17 los métodos están descritos en el Anexo 7. Código para el subsistema de aplicaciones.

Tabla 17. Lista de API-REST

Ruta	Descripción
/proceso/listar_proceso	Permite listar los procesos generados
/proceso/listar_botella	Permite listar las botellas generadas por proceso
/proceso/aprobar_proceso	Sirve para aprobar un proceso
/proceso/encontrar_proceso_botella	Permite encontrar la botella cuando se lee el código QR
/proceso/cambiar_estado_botella	Permite cambiar el estado de la botella
/proceso/encontrar_proceso	Sirve para encontrar un proceso mediante el hash
/proceso/crear_editar_proceso	Permite crear y editar un proceso.
/usuario/crear_editar_usuario	Permite crear y editar un usuario
/usuario/eliminar_usuario	Sirve para eliminar un usuario
/usuario/listar_usuario	Permite listar los usuarios creados



## 6.2.8. Fase 8: Diseño del subsistema de aplicaciones frontend

Durante esta etapa, se relaciona el modelo de diseño del patrón Modelo-Vista-Controlador (MVC) con la DApp y se brindan detalles sobre cada uno de los puntos, tal como se puede observar en la Figura 17.

- **Modelo:** Se coloca en el bloque de génesis de la cadena y consistiría en la estructura de datos que estaría conectada al modelo de proceso de backend y el contrato inteligente en Blockchain.
- **Controlador:** es responsable de actualizar el modelo, está conectado a los métodos del contrato inteligente, en particular a los de la interfaz ABI, que se produjeron durante la compilación y migración del contrato.
- **Vista:** El frontend completo se creó como SPA (Single Page Application - Aplicaciones con una sola página, que permiten la gestión y validación de la TVA).

La biblioteca web3.js es el paquete que posibilita la interacción con Ethereum Blockchain y los contratos inteligentes, específicamente su sección web3.eth. De este modo, web3.eth puede ser considerado como la comunicación entre la vista y el controlador/modelo, ya que habilita la invocación de los métodos de la interfaz ABI del contrato inteligente.

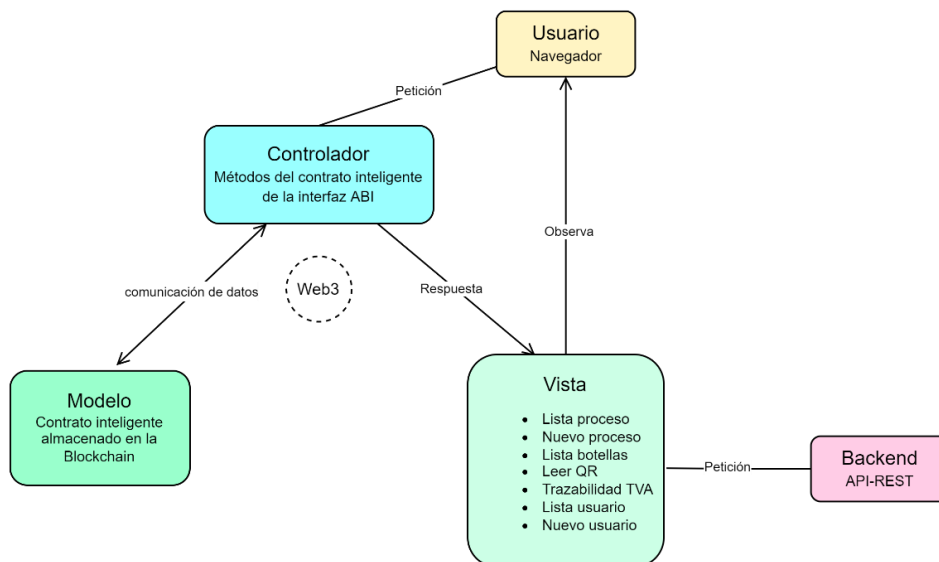


Figura 17. Modelo Vista Controlador con la Blockchain.

Del mismo modo, fue posible crear un diagrama de clase para el subsistema de la aplicación porque solo consta de la interfaz y el backend, se puede comparar con el subsistema de contrato inteligente para mayor claridad. que las tecnologías deseadas se pueden utilizar para el propio

backend del subsistema de la aplicación. El subsistema de aplicación se muestra en el punto 6.2.5 (Fase 5: Diseño del subsistema de contratos inteligentes), la Figura 16.

La Figura 18 muestra la vista de la arquitectura física que finalmente se desarrolló e incluye el subsistema de la aplicación y simula la disposición física de los nodos y componentes de la DApp.

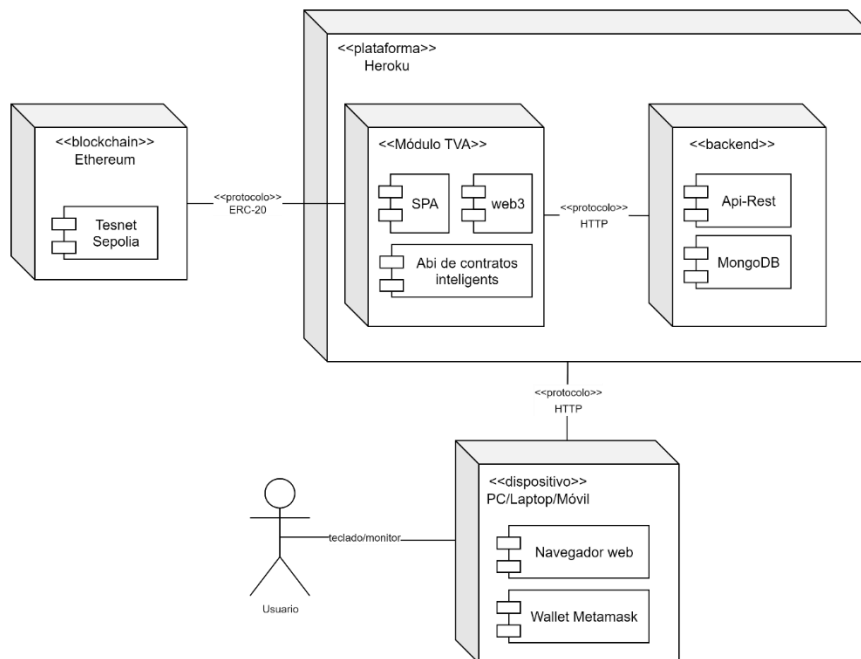


Figura 18. Arquitectura física de la DApp.

### 6.3. Objetivo 3

**Desplegar y probar la DApp sobre la testnet de blockchain donde se valide la trazabilidad de la elaboración de Vinos Ambrosia.**

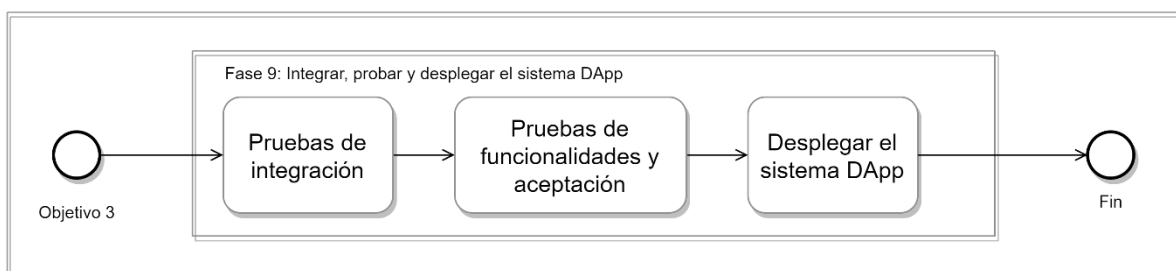


Figura 19. Diagrama BPMN de las fases para el desarrollo del objetivo 3.

En la Figura 19 la fase 9 que se encuentra denominada **Integrar, probar y desplegar el sistema DApp**, para mayor detalle se encuentran el punto 9 de la sección **ABCDE (agile block chain DApp engineering)** del Marco teórico

### 6.3.1. Fase 9: Pruebas de integración de la DApp

#### 6.3.1.1. Integrar el sistema DApp

En este punto se realizó las **Pruebas de Integración** que se complementan a las pruebas unitarias en el Anexo 8. Pruebas Unitarias del subsistema de aplicaciones, esto permite comprobar que todos los módulos de software funcionen correctamente de manera conjunta.

La Figura 20 muestra las pruebas realizadas a cada API-REST para validar el correcto funcionamiento (ver Anexo 10. Pruebas Funcionales).



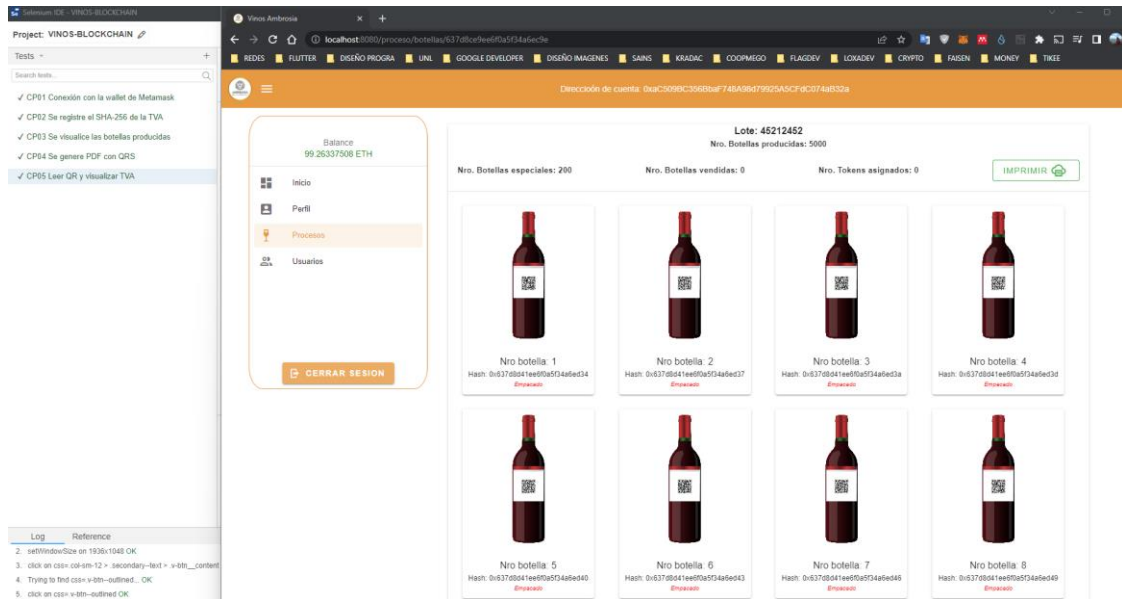
**Figura 20.** Colección de Postman con la administración de la TVA

La Tabla 18 muestra los casos de pruebas planificados y ejecutados bajo el framework de testing denominado **Selenium IDE**, el resultado se puede visualizar en la Figura 21.

**Tabla 18.** Resultados de las Pruebas de Integración

Nro. Caso de Prueba	Elemento	Descripción de lo que se probará	¿OK?	Observación
CP01	Wallet-Subsistema de aplicaciones	Conexión con la wallet de Metamask	✓	N/A
CP02	Subsistema de contratos inteligentes – Subsistema de aplicaciones	Se registre correctamente el SHA-256 de la TVA en la testnet de Blockchain	✓	N/A
CP03	Subsistema de aplicaciones-Blockchain	Se visualice correctamente las botellas producidas con la TVA	✓	N/A

		correspondiente al hacer clic en “BOTELLAS PRODUCIDAS”		
CP04	Subsistema de aplicaciones	Se genere correctamente el pdf con los QRS para imprimir al hacer clic en “IMPRIMIR”	✓	N/A
CP05	Subsistema de contratos inteligentes – Subsistema de aplicaciones	Al ingresar a LEER QR, se obtenga correctamente el SHA-256 de la TVA	✓	N/A



**Figura 21.** Resultado de las Pruebas de Integración de la DApp.

Revisar el **Anexo 9.** Pruebas de Integración, para examinar todo el plan de las pruebas de integración realizadas sobre la DApp.

### 6.3.1.2. Probar el sistema DApp

En este apartado se realizan las Pruebas Funcionales de la DApp utilizando tecnología blockchain (**Anexo 10. Pruebas Funcionales**). Los resultados se muestran en la Tabla 19. Todo esto se hace para garantizar que la DApp pueda cumplir con los requisitos predeterminados utilizando las características que se definieron inicialmente.

**Tabla 19.** Escenarios para Pruebas Funcionales

<b>Nro. Caso de prueba</b>	<b>Descripción del caso de prueba</b>	<b>RF relacionados</b>	<b>Resultado</b>	<b>Observación</b>
CP01	Se llevarán a cabo pruebas para verificar la respuesta de la DApp al momento de registrar los procesos correspondientes a la TVA.	RF01 RF02	SI	S/A
CP02	Se llevarán a cabo pruebas para evaluar la respuesta de la DApp al registrar el SHA-256 de la TVA en la blockchain.	RF01 RF02 RF03	SI	S/A
CP03	Se llevará a cabo una prueba para evaluar la respuesta de la DApp al momento de visualizar la trazabilidad de las botellas producidas.	RF03 RF04 RF05	SI	S/A
CP04	Se verificará la respuesta de la DApp al validar un código QR con un SHA-256 válido.	RF04 RF05 RF06 RF07	SI	S/A
CP05	Se evaluará el comportamiento de la DApp al validar un QR con un valor de sha-256 incorrecto.	RF04 RF05 RF06 RF07	SI	S/A

Las **Pruebas de Aceptación (Anexo 11. Pruebas de Aceptación)** están destinadas a comprobar la aceptación del producto, después de observar y manipular el sitio web por las personas seleccionadas se aplicó una encuesta, los parámetros y resultados se muestran en la Tabla 20. Se observa una alta tasa de aceptación, en muchos casos incluso más del 90%. Esto se realizó en una muestra de 83 personas administrativas y clientes de Vinos Ambrosia. Además de estos pasos, en la encuesta utilizada se solicitó su nombres, apellidos y correo electrónico para mayor veracidad de la información obtenida.

**Tabla 20.** Resumen de Pruebas Aceptación

No	Parámetros	Porcentaje (%)		
		Sí	Parcialmente	No
1	¿El lenguaje utilizado es fácil de entender?	89.2	9.6	1.2
2	¿Se otorga un tiempo adecuado para introducir la información mediante el teclado o la cámara?	91.6	7.8	0.6
3	¿Es comprensible tanto la interfaz como su contenido?	90.4	8.4	1.2
4	¿La interfaz está diseñada de manera que las tareas sean lo más fáciles posible de realizar?	92.8	7.12	0.08
5	¿Son adecuados los mensajes que muestra el sistema?	88	11.8	0.2
6	¿El sistema toma medidas para prevenir errores?	92.8	6	1.2
7	¿El sistema brinda una explicación clara sobre los errores que se presentan?	88	10.8	1.2
8	¿Facilita la navegación dentro del sistema y su salida de manera sencilla?	91.6	8.4	0
9	¿La información presentada al usuario es relevante y se enfoca solamente en lo que necesita saber?	89.2	10.8	0
	<b>PROMEDIO</b>	<b>90.4</b>	<b>8.97</b>	<b>0.63</b>

En los parámetros que tiene una respuesta negativa se debe a varias faltas ortográficas, unidades de medidas no correspondiente al tipo de dato que se estaba presentando, situación que no se había percibido hasta el momento, la cual fue corregida a tiempo.

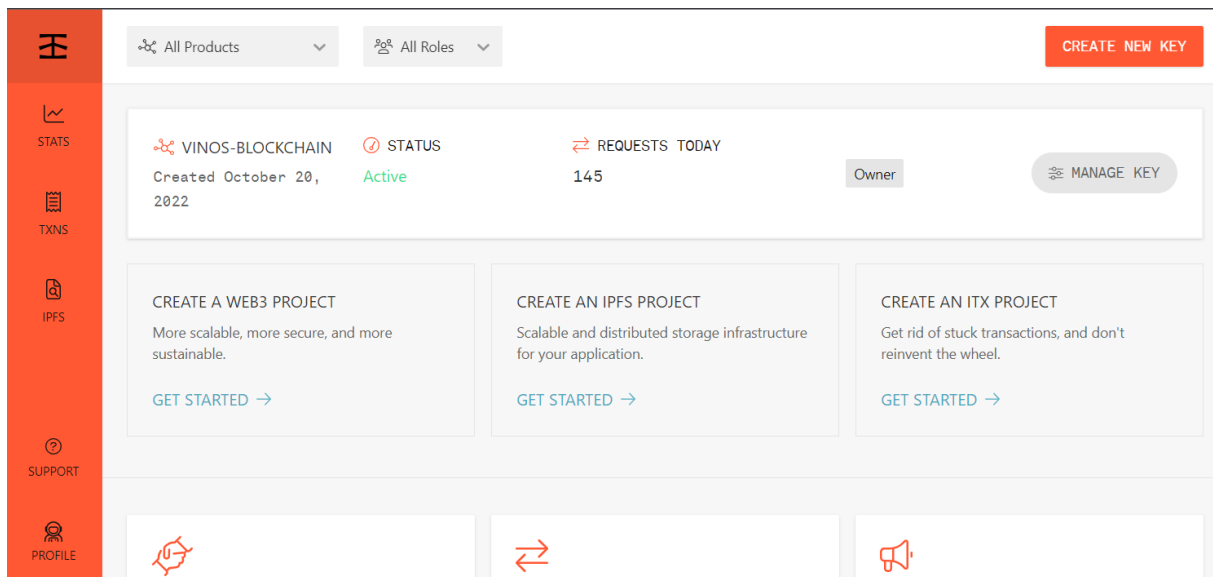
En la Tabla 20 se observa el resultado del criterio sí, parcialmente y no con un: 90.4; 8.97 y 0,63 por ciento respectivamente. Al combinar la información anterior con los valores de prueba de la Tabla 21, se concluye que las Pruebas de Aceptación son de calidad.

**Tabla 21.** Criterio para evaluar las Pruebas de Aceptación.

Estado de Pruebas de Aceptación	Criterio		
	Sí	Parcialmente	No
<b>Afirmativo</b>	$\geq 85\%$	$\leq 15\%$	$< 1\%$
<b>Negativo</b>	$< 85\%$	$> 15\%$	$> 1\%$

### 6.3.1.3. Desplegar el sistema DApp

En esta fase es importante poder elegir la testnet de blockchain que permitirá realizar las pruebas en este caso se utilizó la testnet de **Sepolia** debido a que es compatible con la versión 2.0 de Ethereum. Para poder desplegar en la testnet de Sepolia se utilizó el servicio Infura, que puede llamarse servicio de nodo o infraestructura. (IaaS) para crear un proyecto llamado "VINOS-BLOCKCHAIN" y así recibir credenciales para conectarse a la red de prueba, como se muestra en la Figura 22.



**Figura 22.** Proyecto de Infura para desplegar en la testnet de Sepolia.

En la Figura 23 se puede observar que el proceso de compilación y migración de los contratos inteligentes consta de tres pasos principales: la compilación del código fuente, la creación del archivo de migración y finalmente la migración de los contratos inteligentes en la red Sepolia. En el proceso de migración, se utiliza Truffle para desplegar y manejar el proceso de migración de los contratos inteligentes de manera segura y eficiente, lo que reduce la posibilidad de errores y problemas durante la migración.

```

PS E:\UNL\CICLO X\vinos-blockchain> truffle migrate --network sepolia --reset
Compiling your contracts...
=====
> Compiling @openzeppelin\contracts\token\ERC721\ERC721.sol
> Compiling @openzeppelin\contracts\token\ERC721\IERC721.sol
=====
> Network name: 'sepolia'
> Network id: 11155111
> Block gas limit: 30000000 (0x1c9c380)

1_migration.js
=====
Deploying 'ProcesoContract'
-----
> transaction hash: 0x0a194b77c22206d701140a09277091a0e938d929475727d632d66e8478ef93b9
> gas price: 2.500000007 gwei
> value sent: 0 ETH
> total cost: 0.000862330002414524 ETH
> Saving artifacts
-----
> Total cost: 0.000862330002414524 ETH

2_migration.js
=====
Deploying 'TVATOKEN'
-----
> transaction hash: 0xbcd1942255bf3329a821d0205cfad24d5ce18872757ea223deb835af7e6deb79
> Blocks: 2 Seconds: 20
> contract address: 0xD00FFdD650264c2EB04b1A065C1405f09afCba92
> block number: 2127885
> block timestamp: 1666300308
> account: 0xF4638D0534e993301e453227edF061CB03000DBE
> balance: 0.132374514950648642
> gas used: 1295635 (0x13c513)
> gas price: 2.500000007 gwei
> value sent: 0 ETH
> total cost: 0.003239087509069445 ETH
> Saving artifacts
-----
> Total cost: 0.003239087509069445 ETH

Summary
=====
> Total deployments: 2
> Final cost: 0.004101417511483969 ETH

```

**Figura 23.** Comando para desplegar los contratos inteligentes.

Es importante mencionar que el proceso de compilación y migración de los contratos inteligentes no es gratuito. Cada vez que se realiza una compilación y migración de los contratos inteligentes, se deben pagar ciertas tarifas en la red Ethereum. Estas tarifas son necesarias para compensar a los mineros de la red que verifican y ejecutan los contratos inteligentes. La Tabla 22 muestra el costo total de transacción del envío de contratos inteligentes a la red de prueba de Sepolia, que es 0.004101417511483969 ETH equivalente a 5.21 dólares estadounidenses. Recuerda que el valor para desplegar los contratos varía según la tasa de conversión ETH/USD.

**Tabla 22.** Resumen de costo total del despliegue en ETH.

Costo total (ETH)	Costo total (dólares estadounidenses)
0.004101417511483969	5.21
	Depende de la tasa de conversión ETH/USD



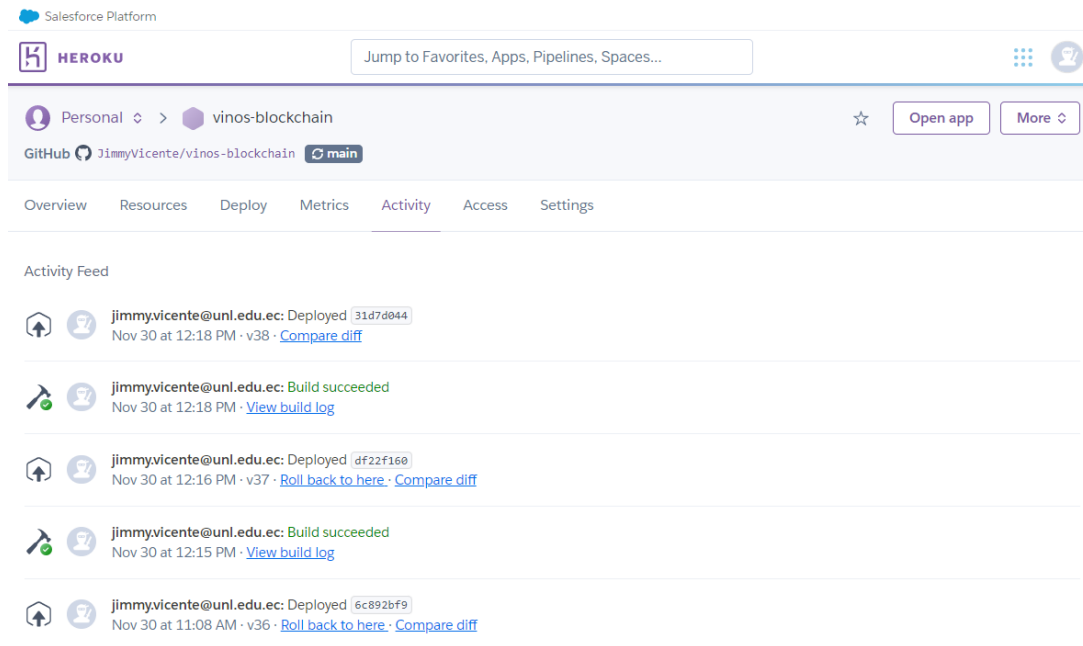
Por último, utilizando la herramienta **Etherscan** se pueden rastrear diversos métodos mediante el uso de un contrato inteligente, tal como se ilustra en la Figura 24.

The screenshot displays the Etherscan interface for a contract on the Sepolia Testnet. The contract address is 0xFfb9Cf59d4Ba086B48DA90EC497a5315Be09AEd2. The contract overview shows a balance of 0 Ether. The 'More Info' section indicates that the name tag is not available and the contract creator is 0xf4638d0534e993301e... at txn 0x0a194b77c22206d701... The 'Transactions' section shows the latest 5 transactions, all with a value of 0 Ether and a fee of 0.00028237.

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0xc6ec8219472e82acc2...	0x2d44dcdf9	2341616	44 mins ago	0xf4638d0534e993301e...	IN 0xfbb9cf59d4ba086b48d...	0 Ether	0.00028237
0xc0ac379de8a7ea8a30...	0x2d44dcdf9	2340714	4 hrs 9 mins ago	0xf4638d0534e993301e...	IN 0xfbb9cf59d4ba086b48d...	0 Ether	0.00028237
0xbaba5289d27988a073...	0x2d44dcdf9	2164946	27 days 15 hrs ago	0xb7216579a6b1dc25c8...	IN 0xfbb9cf59d4ba086b48d...	0 Ether	0.00028237
0x34f1402a4d97cc9a40...	0x2d44dcdf9	2128023	33 days 8 hrs ago	0xf4638d0534e993301e...	IN 0xfbb9cf59d4ba086b48d...	0 Ether	0.00028237
0x0a194b77c22206d701...	0x60886040	2127883	33 days 9 hrs ago	0xf4638d0534e993301e...	IN Contract Creation	0 Ether	0.00086233

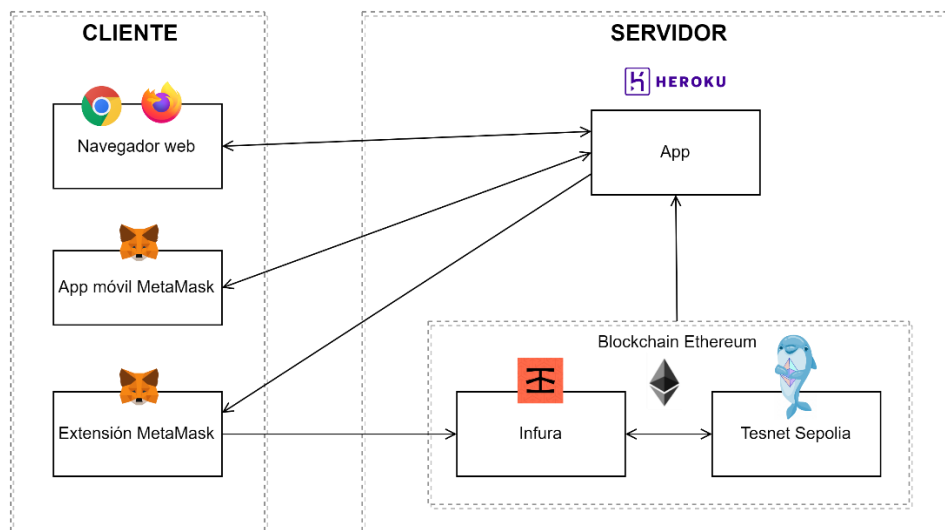
**Figura 24.** Historial de las transacciones en Etherscan.

También se llevó a cabo la implementación en el servidor de **Heroku**, tal como se evidencia en la Figura 25. Se creó un proyecto denominado "vinos-blockchain" y los resultados se pueden apreciar en la dirección web <https://vinos-blockchain.herokuapp.com>



**Figura 25.** Proyecto creado en Heroku.

En la Figura 26, se proporciona un diagrama esquemático que ilustra un modelo cliente-servidor asociado con las tecnologías descritas anteriormente. Cuando el cliente solicita los servicios de administración de un TVA y lectura de código QR se realiza a través del servicio en la nube de Heroku, y con la solicitud de la billetera Metamask e Infura (nodo para acceder a Ethereum-IaaS) realiza las solicitudes a la red de prueba de la cadena de bloques Sepolia Ethereum.



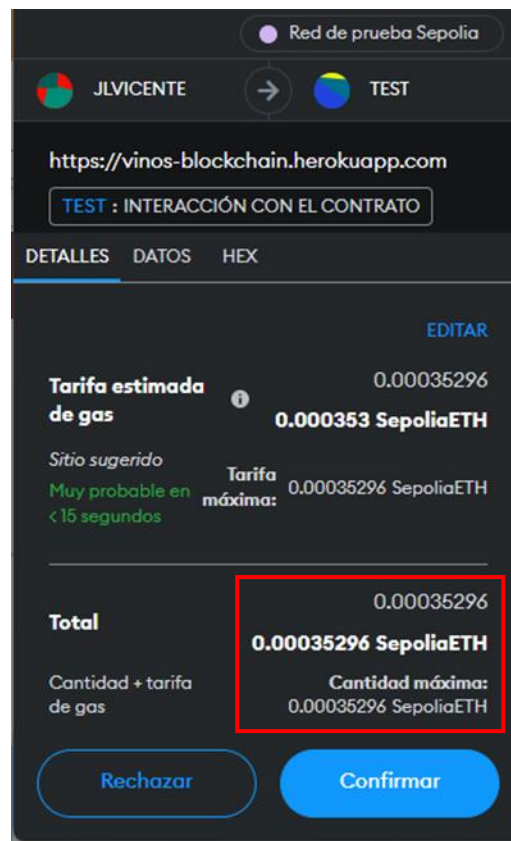
**Figura 26.** Esquema cliente-servidor.

La Tabla 23 muestra la cantidad de gas de 0.000353 ETH (\$0.44), que es la cantidad máxima que se puede pagar por el registro de TVA, todo esto se confirma en la Figura 27. Tenga en cuenta que esta cantidad puede variar según los requisitos computacionales. el precio e incluso

el tráfico web disponible, pero siempre rota a un valor fijo. Por lo tanto, el valor del dólar varía según el tipo de cambio ETH/USD.

**Tabla 23.** Costo de registro de la TVA

Gas máximo a usarse (ETH)	Costo (dólares estadounidenses)
0.000353	0.44
	Depende la tasa de conversión ETH/USD



**Figura 27.** Costo total en ETH para crear una TVA en la testnet Sepolia.

Al final, se elaboraron dos guías que son:

- Se ha creado un manual para programadores que se encuentra disponible en la siguiente dirección web: <https://github.com/JimmyVicente/vinos-blockchain> (README.md)
- **Manual de usuario** que se encuentra detallado en el **Anexo 12.** Manual de Usuario.

## 7. Discusión

### 7.1. Desarrollo de la propuesta alternativa

El Proyecto de Trabajo de Titulación denominado “Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia”, pretende implementar soluciones informáticas basadas en la trazabilidad de la cadena de suministro. Para lograr la solución se ha planteado los siguientes objetivos.

#### 7.2.1. **Objetivo 1: Determinar los procesos de producción de vinos Ambrosia que permita delimitar y elicitar los requerimientos y la arquitectura de la DApp**

Para poder cumplir el objetivo se realizó un análisis de los principales procesos de la producción de vino. Para ello, se consideró inicialmente la utilización de tecnología IOT para monitorear la siembra de la materia prima (mora y mandarina), sin embargo, esta opción presentó inconvenientes debido a la necesidad de utilizar equipos electrónicos, lo que podía generar dificultades en la implementación del proceso de trazabilidad. Eventualmente durante la entrevista (revisar **Anexo 1. Entrevista a representante de vinos Ambrosia**) con el CEO de Vinos Ambrosia se llegó a la conclusión que los procesos se tomarían a partir de la obtención de la materia prima, esto permitió definir 7 procesos (materia prima, extracción del mosto, pasteurización, fermentación, clarificación, trasiego, embazado) para la TVA (Trazabilidad Vinos Ambrosia). Además, se investigó una metodología que se enfoque al desarrollo de una DApp con tecnología blockchain, se encontró la metodología de desarrollo de software ABCDE (ver el punto **5.1 Metodología de desarrollo de software**) que permite diseñar, codificar y realizar pruebas de los contratos inteligentes. La metodología seleccionada permitió que la implementación de la DApp tenga una base sólida que le permite ejecutarse de manera correcta.

Las 4 primeras fases de la metodología de desarrollo de software ABCDE se realizó la elicitación de requisitos (ver **Anexo 2.**) que permitió delimitar el alcance de la DApp. En base a este documento se procedió a ejecutar la fase 3 correspondiente a las historias de usuarios para evitar conflictos en las fases posteriores, para mayor evidencia se adjunta el documento (ver **Anexo 3. Descripción de Historias de usuario**). Como punto final se realizó un diagrama de la arquitectura (ver **Fase 4: Diagrama de la arquitectura de la DApp**) para definir los dos Subsistemas para el desarrollo de la DApp.

## **7.2.2. Objetivo 2: Desarrollar la DApp cumpliendo con la arquitectura y elicitación de los requerimientos.**

En este objetivo, la DApp se divide en subsistemas: contratos inteligentes y aplicaciones para las que se realizó el diseño, codificación y ejecución de pruebas unitarias (según las fases 5 a 8 de la metodología de desarrollo de software ABCDE). La estructura de la DApp (ver el punto **6.2.4 de la sección de Resultados**) se generó en base a las tecnologías de Node js y Vue js. Aunque existen diferentes tecnologías que permiten el desarrollo de la DApp, se eligió estas porque son las más populares con amplia documentación para lograr el objetivo.

La fase de diseño en el subsistema de contratos inteligentes se completa con un diagrama de clases (ver el punto **6.2.5 de la sección de Resultados**), para ser un tipo de contrato inteligente, la metodología utilizada sugiere proporcionar identificadores únicos a los elementos. El proceso de programación se realiza en el lenguaje de programación Solidity (ver **Anexo 6.** ), un lenguaje de programación en el importante encontrar el tamaño correcto de las variables para evitar costes altos a futuro en las transacciones.

La fase de diseño en el subsistema de aplicaciones se realizó el diagrama de clases para la administración de la TVA (ver **Anexo 5.** Diagrama de clases subsistema de aplicaciones) lo que permitió realizar la codificación de la administración de la TVA mediante API-REST (ver **6.2.7** de la sección de Resultados). Por otro lado, se desarrolló la arquitectura/vista física y una relación con el MVC (ver **6.2.8** de la sección de Resultados), debido a que se desarrolló bajo la forma de una SPA (Single Page Application). La fase de codificación se desarrolló por medio de Nodejs, Vue js (ver **Anexo 7.** Código para el subsistema de aplicaciones), adicionalmente se instala la extensión MetaMask en el navegador y se crea una cuenta en la wallet (billetera). En la fase de Pruebas Unitarias se realizó mediante las tecnologías Jest y Enzyme (ver **Anexo 8.** Pruebas Unitarias del subsistema de aplicaciones).

Cada subsistema de la DApp se realizó mediante sprints (ver el punto **6.2.1** de la sección de resultados Iteraciones (sprints) de), descritos en la metodología de desarrollo de software ABCDE, dando como finalización a la última fase de este objetivo y poder continuar con el siguiente.

### **7.2.3. Objetivo 3: Desplegar y probar la DApp sobre la testnet de blockchain donde se valide la trazabilidad de la elaboración de Vinos Ambrosia.**

La fase 9 de la metodología de software ABCDE permitió completar este objetivo donde se identificó la testnet, se realizó pruebas de integración y despliego la DApp. Para identificar la testnet más conveniente se obtuvo credenciales a la conexión de Ethereum mediante la herramienta de Infura, entre las diferentes testnet existentes se eligió Sepolia Test Network porque después de la fusión de Ethereum 1.0 a la versión 2.0 es la única a la fecha actual que tiene mayor documentación y la facilidad de transferir fondos de prueba (Faucet) para realizar las funcionalidades de la DApp. Por medio de las Pruebas de Integración (ver **Anexo 9. Pruebas de Integración**) se simuló el uso de la aplicación en tiempo real y verificó la integración de los subsistemas, para ello se utilizó una herramienta denominada Selenium IDE la misma que completo los resultados exitosamente (ver el punto **6.3.1.1** de la sección de Resultados).

Los requisitos funcionales planteados se cumplieron exitosamente gracias a la ejecución de las Pruebas Funcionales (ver **Anexo 10. Pruebas Funcionales**) las cuales permitieron probar los diferentes escenarios de la DApp para validar la trazabilidad de la elaboración de Vinos Ambrosia. En base a la información de las personas Administrativas y Clientes de Vinos Ambrosia se realizaron las mejoras pertinentes a la DApp, misma información obtenida a partir de las Pruebas de Aceptación (ver **Anexo 11. Pruebas de Aceptación**) que se completaron con resultados positivos (ver el punto **6.3.1.2** de la sección de Resultados).

Además, se desplegó la DApp (ver el punto **6.3.1.3** de la sección de Resultados) mediante el servicio de computación Heroku porque su plan gratuito solventa las necesidades de la DApp. Para poder ejecutar las funcionalidades de la DApp en su totalidad está disponible dentro del navegador web que permita instalar la extensión de MetaMask y el navegador web dentro de la aplicación de Metamask disponibles para iOS y Android. Sin embargo, las personas que no dispongan de la wallet(billetera) estarán limitadas únicamente a realizar lectura de QR de la botella y ver la información de la Trazabilidad de la elaboración del Vino que es el principal objetivo de este Trabajo de Titulación.

## 8. Conclusiones

Una vez terminado el Trabajo de Titulación, se concluye que:

- La implementación de una aplicación descentralizada (DApp) utilizando la tecnología blockchain ha demostrado ser una solución eficaz para permitir la trazabilidad de la producción de vinos Ambrosia. Gracias a la inmutabilidad y transparencia de la blockchain, se ha logrado registrar de manera segura y confiable cada etapa del proceso de producción de los vinos, desde la materia prima hasta el embotellado y la distribución final.
- La fase para determinar los procesos de producción de vinos Ambrosia ha sido fundamental para delimitar y elicitar los requerimientos y la arquitectura de la DApp para la trazabilidad de la producción de los vinos. Gracias a la identificación y análisis de los procesos productivos, se han podido identificar los puntos críticos en los que se requiere una mayor trazabilidad. Lo cual permitió diseñar una arquitectura que cumpla con las necesidades específicas de la producción de los vinos Ambrosia.
- La identificación de los procesos críticos y la arquitectura específica diseñada para la producción de los vinos Ambrosia, han permitido el desarrollo de una solución que cumple con los requerimientos necesarios para registrar de manera segura y confiable cada etapa del, proceso productivo garantizando la integridad y confidencialidad de los datos registrados en la blockchain.
- El uso de códigos QR y contratos inteligentes en la tecnología blockchain para verificar el estado de una botella y documentar cada transacción ha permitido garantizar la transparencia en la red y disuadir a los usuarios de cometer fraude. Esto gracias a la tecnología blockchain que ofrece una solución segura y transparente para documentar y verificar transacciones.
- El despliegue y prueba de la DApp en la testnet de blockchain Sepolia ha sido fundamental para validar la trazabilidad de la producción de los Vinos Ambrosia debido que en la blockchain se puede observar cada transacción, lo que ha permitido garantizar la transparencia e integridad de los datos registrados en un entorno controlado.

## 9. Recomendaciones

Una vez terminado el Trabajo de Titulación, se recomienda que:

- Es fundamental estar al día en cuanto a las innovaciones y direcciones en la tecnología blockchain para poder utilizarlas con éxito en la creación de la DApp. De igual manera, se requiere llevar a cabo ensayos y confirmaciones constantes durante la etapa de ejecución para asegurar que la DApp sea eficiente y de alta calidad.
- Establecer una estrategia clara y detallada para el proyecto, incluyendo el alcance, los objetivos, el tiempo y los recursos necesarios. Esto ayudará a garantizar el cumplimiento de los plazos y a maximizar el impacto de la solución.
- Utilice la metodología ABCDE al crear sistemas descentralizados en los que se involucre la tecnología Blockchain porque las metodologías ágiles o tradicionales que se enseñan en la formación académica no cumplen lo que se requiere para crear una DApp, razón por la cual el término "contrato inteligente" no es aplicable de ninguna manera.
- Es recomendable fomentar la creación de DApps con tecnología Blockchain en la carrera de Ingeniería en Sistemas/Informática para estar al día con las nuevas tecnologías y brindar a los estudiantes las habilidades necesarias para tener éxito en el campo profesional y laboral en un futuro cercano. Para ello, se sugiere la inclusión de asignaturas y cursos especializados en la materia en el plan de estudios de la carrera, así como la promoción de proyectos y trabajos de investigación relacionados con la tecnología blockchain. De esta manera, se garantizará una formación académica completa y actualizada en los estudiantes, que les permitirá estar preparados para enfrentar los nuevos retos del mundo laboral y aprovechar al máximo las oportunidades que ofrece la tecnología blockchain en la actualidad.
- Considerar usar el Trabajo de Titulación como un recurso para desarrollar módulos o sistemas de software basados en blockchain que, entre otras cosas, se pueden usar para mantener la propiedad de los activos físicos o protegerse contra el fraude electoral. Dado que las diversas obras asociadas que se han descubierto son extremadamente poco comunes, y con frecuencia están cerca de cero a nivel local o nacional.



Se recomienda para trabajos a futuros:

- Dado el nivel cada vez mayor de digitalización y demanda de información e integridad del producto, el sector agroalimentario se encuentra en una posición única para explorar el potencial de Blockchain. Si bien la aplicación de blockchain en la industria agroalimentaria aún se encuentra en su etapa inicial, se puede esperar que cada vez más organizaciones tomen iniciativas.
- Desarrollo de un token (criptomoneda) para permitir operar en la gestión de Trazabilidad Vinos Ambrosia (TVA) sin depender de un tercer proyecto como Ethereum, esto proporcionaría menos gastos al momento de realizar las transacciones en la blockchain.
- Utilice el trabajo de Titulación como una guía para incorporar la trazabilidad en la cadena de suministro de cualquier otro producto alimenticio y, al mismo tiempo tomar en cuenta las diferencias en los detalles del procedimiento de fabricación. Por ejemplo, el mercado de la provincia de Loja se puede utilizar para rastrear el cacao, café y producciones agroalimentarias donde se pueda conocer la ubicación de procedencia, así como la trazabilidad y tiempos de permanencia en cada punto de la cadena de distribución es de gran interés.
- Considerar la adopción de estándares y protocolos comunes para la trazabilidad de productos alimenticios a nivel global, para así mejorar la interoperabilidad y la eficiencia en la cadena de suministro. Además, se recomienda fomentar la colaboración entre empresas y organizaciones de diferentes sectores para el intercambio de buenas prácticas y conocimientos en el uso de tecnologías blockchain para la trazabilidad de alimentos y bebidas. De esta manera, se podrán generar soluciones más integrales y efectivas que beneficien a toda la industria alimentaria y a los consumidores finales.

## 10. Bibliografía

- [1] J. Jiménez Godoy, “Trazabilidad fiable del vino: Blockchain,” Jul. 2018. <https://reunir.unir.net/bitstream/handle/123456789/6973/JIMENEZ%20GODOY%2c%20JOAQUIN.pdf?sequence=1&isAllowed=y> (accessed Jan. 04, 2023).
- [2] “Vinos falsificados a precio de lujo: desmantelada una organización dedicada al fraude de marcas exclusivas - Vida Sana Ecuador.” <https://www.vidasanaecuador.com/2018/07/vinos-falsificados-precio-de-lujo.html> (accessed Jan. 04, 2023).
- [3] “La tecnología blockchain aplicada a la trazabilidad de valor del vino.” <https://www.addvante.com/es/tecnologia-blockchain-aplicada-vino/> (accessed Jan. 04, 2023).
- [4] “Soriano afirma que la transparencia en el sector del vino potenciará la comercialización | Gobierno de Castilla-La Mancha.” <https://www.castillalamancha.es/actualidad/notasdeprensa/soriano-afirma-que-la-transparencia-en-el-sector-del-vino-potenciar%C3%A1-la-comercializaci%C3%B3n> (accessed Jan. 04, 2023).
- [5] Blockchain Academy México, “Blockchain 2.0 | Smart Contract | DAapp,” 2020. Accessed: Mar. 14, 2021. [Online]. Available: <https://blockchainacademy.mx/>
- [6] S. Moscoso, D. Suárez, and D. Martín, “Certificación digital de documentos académicos usando Blockchain Formato IEEE,” *Tecnología Investigación y Academia*, vol. 7, no. 2, pp. 21–27, 2020, [Online]. Available: <https://revistas.udistrital.edu.co/index.php/tia/article/view/12757>
- [7] C. Pastorino, “Blockchain: qué es, cómo funciona y cómo se está usando en el mercado | WeLiveSecurity.” Sep. 2018. Accessed: Feb. 28, 2021. [Online]. Available: <https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/>
- [8] “Tecnología blockchain en la trazabilidad de las cadenas de suministro.” <https://www.macsa.com/blog/beneficios-de-la-tecnologia-blockchain-en-la-trazabilidad-de-las-cadenas-de-suministro/> (accessed Jan. 04, 2023).

- [9] E. Piscini, D. Dalar, D. Mapgaonkar, and P. Santhana, “The symphonic enterprise,” 2018. [Online]. Available: [https://www2.deloitte.com/content/dam/insights/us/articles/Tech-Trends-2018/4109\\_TechTrends-2018\\_FINAL.pdf](https://www2.deloitte.com/content/dam/insights/us/articles/Tech-Trends-2018/4109_TechTrends-2018_FINAL.pdf).
- [10] P. Olsen and M. Borit, “The components of a food traceability system,” *Trends Food Sci Technol*, vol. 77, pp. 143–149, Jul. 2018, doi: 10.1016/J.TIFS.2018.05.004.
- [11] B. Ayan, E. Güner, and S. Son-Turan, “Blockchain Technology and Sustainability in Supply Chains and a Closer Look at Different Industries: A Mixed Method Approach,” *Logistics 2022, Vol. 6, Page 85*, vol. 6, no. 4, p. 85, Dec. 2022, doi: 10.3390/LOGISTICS6040085.
- [12] D. Plaza, “Diseño y desarrollo de diplomas académicos digitales mediante la tecnología blockchain,” Cali, 2019. [Online]. Available: [http://vitela.javerianacali.edu.co/bitstream/handle/11522/11222/Diplomas\\_académicos\\_digitales\\_Blockchain.pdf?sequence=1&isAllowed=y](http://vitela.javerianacali.edu.co/bitstream/handle/11522/11222/Diplomas_académicos_digitales_Blockchain.pdf?sequence=1&isAllowed=y)
- [13] “Trazabilidad de alimentos - Blockchain Federal Argentina.” <https://bfa.ar/blockchain/casos-de-uso/trazabilidad-de-alimentos> (accessed Feb. 21, 2023).
- [14] C. Piris, A. Cabellos, and J. Vilanova, “Design and implementation of the Transactional and Communication layer of a Blockchain to secure IP prefixes Autor,” 2018.
- [15] E. Piscini, D. Dalton, and L. Kehoe, “Panorama de Blockchain y Ciberseguridad Blockchain & Ciberseguridad,” 2018. [Online]. Available: <https://www.bloomberg.com/news/articles/2016>
- [16] J. Valencia, “Contrato inteligentes,” *Revista de Investigación en Tecnologías de la Información*, vol. 7, no. 14, pp. 1–10, 2019, doi: 10.36825/riti.07.14.001.
- [17] Universidad del Rosario, “SMART CONTRACTS.”
- [18] V. Palacios, “Explorando la Blockchain de Ethereum y el desarrollo de smart contracts,” Catalunya, Feb. 2018.
- [19] Blockchain Academy México, “OBJETIVO BLOCKCHAIN | 2.0 Smart Contract,” 2020, Accessed: Mar. 14, 2021. [Online]. Available: <https://blockchainacademy.mx/>

- [20] Escuela Crypto ES, *Programando Ethereum: Crea el futuro*, Kindle. 2021.
- [21] Bit2Me Academy, “¿Qué es la Ethereum Virtual Machine (EVM)? | Bit2Me Academy.” <https://academy.bit2me.com/que-es-ethereum-virtual-machine-evm/> (accessed Mar. 13, 2021).
- [22] L. Marchesi, M. Marchesi, and R. Tonelli, “ABCDE-agile block chain DApp engineering,” Cagliari, Nov. 2020. Accessed: Aug. 22, 2021. [Online]. Available: <https://reader.elsevier.com/reader/sd/pii/S2096720920300026?token=C7ABB69531EE9D9BF844D0FB4CD0972FC4845DABFA6CE14E39B70797AB33CC2194C8A67287483155BD184992500CF4BA&originRegion=us-east-1&originCreation=20210824012952>
- [23] “The proposed ABCDE process, shown as a UML activity diagram. | Download Scientific Diagram.” [https://www.researchgate.net/figure/The-proposed-ABCDE-process-shown-as-a-UML-activity-diagram\\_fig3\\_338064306](https://www.researchgate.net/figure/The-proposed-ABCDE-process-shown-as-a-UML-activity-diagram_fig3_338064306) (accessed Feb. 01, 2023).
- [24] “Home - Truffle Suite.” <https://trufflesuite.com/> (accessed Jan. 05, 2023).
- [25] Desde Linux, “Truffle Suite: Herramientas de código abierto para Blockchain.” <https://blog.desdelinux.net/truffle-framework-herramientas-codigo-abierto-blockchain/#Ganache> (accessed Mar. 13, 2021).
- [26] Jesús Lucas, “Qué es NodeJS y para qué sirve,” *OpenWebinars*, Sep. 04, 2019. <https://openwebinars.net/blog/que-es-nodejs/> (accessed Aug. 07, 2021).
- [27] A. Muñoz, “Introduccion-a-Nodejs.pdf,” Madrid, May 2013. Accessed: Aug. 07, 2021. [Online]. Available: [https://www.academia.edu/38559025/Introduccion\\_a\\_Nodejs\\_pdf](https://www.academia.edu/38559025/Introduccion_a_Nodejs_pdf)
- [28] “Introducción — Vue.js.” <https://es.vuejs.org/v2/guide/> (accessed Oct. 19, 2022).
- [29] Microsoft, “Documentation for Visual Studio Code.” <https://code.visualstudio.com/docs> (accessed Aug. 07, 2021).
- [30] R. Crespo, “Funciones Hash: MD5 y SHA-256,” 2020. <http://www.robertocrespo.net/kaizen/funciones-hash-md5-y-sha256/> (accessed Aug. 07, 2021).
- [31] D. Rachmawati, T. Tarigan, and A. B. C. Ginting, “A comparative study of Message Digest 5(MD5) and SHA256 algorithm,” 2017, doi: 10.1088/1742-6596/978/1/012116.

- [32] “Ambrosus anuncia el lanzamiento de sus kits de desarrollo de código fuente (SDKs) (1).” <https://www.europapress.es/comunicados/internacional-00907/noticia-comunicado-ambrosus-anuncia-lanzamiento-kits-desarrollo-codigo-fuente-sdks-20180612190535.html> (accessed Feb. 22, 2022).
- [33] C. de Ingeniería De Sistemas and I. de Sistemas, “UNIVERSIDAD POLITÉCNICA SALESIANA SEDE CUENCA Tesis previa a la obtención del Título de,” 2013.
- [34] J. I.-H. Hsiao, “In Vino Veritas: Blockchain as a Viable Solution for Combating Counterfeit Wines in China,” *Wine Law and Policy*, pp. 777–794, Nov. 2020, doi: 10.1163/9789004438316\_027.
- [35] G. Hernández, “METODO ANALITICO,” Pachuca , 2017. Accessed: May 24, 2021. [Online]. Available: [https://www.uaeh.edu.mx/docencia/P\\_Presentaciones/b\\_huejutla/2017/ Metodo\\_Analitico.pdf](https://www.uaeh.edu.mx/docencia/P_Presentaciones/b_huejutla/2017/ Metodo_Analitico.pdf)
- [36] G. Barchini, “Métodos ‘I + D’ de la Informática,” Santiago del Estero. Accessed: May 24, 2021. [Online]. Available: <http://laboratorios.fi.uba.ar/lie/Revista/Articulos/020205/A2ago2005.pdf>
- [37] *Optimización de la trazabilidad del aceite de palma por medio de blockchain y IoT*. Lima, 2019. Accessed: Dec. 07, 2022. [Online]. Available: [https://pirhua.udep.edu.pe/bitstream/handle/11042/4368/MDE\\_1950.pdf?sequence=2&isAllowed=y](https://pirhua.udep.edu.pe/bitstream/handle/11042/4368/MDE_1950.pdf?sequence=2&isAllowed=y)

## **11. Anexos**

### **Anexo 1. Entrevista a representante de vinos Ambrosia**

#### **Entrevista a representante de vinos Ambrosia**

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Versión: 1.0

Fecha: 05/05/2022

**1. ¿Para la producción de vino existe algún estándar técnico en el caso de existir qué estándar realiza la empresa Ambrosia?**

Realizan control de calidad de materias primas

**2. ¿Cuáles son los procesos que se llevan a cabo para la producción de vinos?**

- Selección de la materia prima
- Limpieza
- Extracción del mosto (Molturación)
- Estandarización (Formulación)
- Pasteurización del mosto
- Siembra del mosto
- Fermentación
- Clarificación
- Trasiego
- Filtrado
- Embazado

**3. ¿Cuáles procesos son automatizados, o se aplican técnicas de IoT(Internet de las cosas)?**

No hay procesos automatizados solo semiautomáticas

- Extracción del mosto
- Trasiego
- Embazado

**4. ¿Cuáles son los procesos que se encuentran bajo demanda de supervisión técnica-manual?**

Todos los procesos son de técnica manual.

**5. ¿Qué procesos considera usted que le sería fundamental conocer al cliente?**

- Procedencia de materia prima.

**6. ¿Cree que la trazabilidad en la producción aportará transparencia y confiabilidad en el usuario final?**

Si porque el consumidor final valora la producción artesanal y tener conocimiento de la procedencia como en Argentina tienen enumeradas las botellas, y saber que en la cosecha número n soy la persona que consumirá la botella 440 de 500, que si me gusta y cumple las expectativas de calidad y saber mediante un QR es muy importante con la fecha.

**7. ¿Si usted fuera consumidor de Vinos Ambrosía que información relevante quisiera que le muestre?**

- Selección de la materia prima
- Extracción del mosto (Molturación)
- Pasteurización del mosto
- Fermentación
- Clarificación
- Trasiego
- Embazado

**Anexo 2.** Definición de los requerimientos de software.

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Versión: 1.0

Fecha: 16/05/2022



## 1. Introducción

En este documento se presenta una especificación de requisitos de software (ERS) para la implementación de una DApp basada en blockchain para la trazabilidad de la producción de vino Ambrosia. El formato de este estándar fue determinado por ANSI/IEEE 830, 1998, Práctica recomendada del estándar IEEE para especificaciones de requisitos de software.

### 1.1. Propósito

El objetivo de este documento es delinear los requisitos funcionales y no funcionales para crear una DApp que permitirá que la tecnología blockchain valide la trazabilidad de los vinos Ambrosia.

### 1.2. Alcance

La especificación de requisitos transmite lo que el usuario final desea del software, que tiene como objetivo validar la trazabilidad de vinos Ambrosia por tecnología blockchain.

### 1.3. Personal involucrado

Tabla 1. Personal involucrado estudiante de la CIS

<b>Nombre</b>	Jimmy Leonel Vicente Guayanay
<b>Rol</b>	Analista y Desarrollador de Software
<b>Categoría Profesional</b>	Estudiante de la CIS
<b>Responsabilidad</b>	Análisis de información, diseño y programación de la DApp
<b>Información de contacto</b>	jimmy.vicente@unl.edu.ec

Tabla 2. Personal involucrado docente de la CIS

<b>Nombre</b>	Cristian Ramiro Narváez Guillen
<b>Rol</b>	Director del trabajo de titulación
<b>Categoría Profesional</b>	Docente de la de la CIS
<b>Responsabilidad</b>	Supervisar y asesorar en el desarrollo del Trabajo de Titulación
<b>Información de contacto</b>	cristian.narvaez@unl.edu.ec

## 1.4. Definiciones, acrónimos y abreviaturas

Tabla 3. Definiciones, acrónimos y abreviaturas

Nombre	Descripción
<b>BC</b>	Blockchain
<b>TVA</b>	Trazabilidad de vinos Ambrosia
<b>CIS</b>	Carrera de Ingeniería en Sistemas
<b>RF</b>	Requerimiento Funcional
<b>RNF</b>	Requerimiento No Funcional
<b>ERS</b>	Especificación de Requisitos Software
<b>SM-TVA</b>	Contrato Inteligente de trazabilidad vinos Ambrosia
<b>Usuario</b>	Individuo que empleará el sistema para ver la trazabilidad.
<b>SPA-TVA</b>	Subsistema de aplicaciones de trazabilidad vinos Ambrosia
<b>QR</b>	Código de barras de dos dimensiones con forma cuadrada capaz de guardar información codificada.

## 1.5. Referencias

Tabla 4. Referencias ERS

Título del Documento	Referencia
<b>IEEE Std 830-1998</b>	IEEE Recommended Practice for Software Requirements Specifications

## 1.6. Resumen

El documento está dividido en tres secciones. En la primera sección se introduce el tema y se presenta una visión general de la especificación de recursos del sistema. En la segunda sección, se describe en términos generales el sistema, incluyendo sus funciones principales, datos asociados, factores y restricciones. La tercera sección, por último, se centra en los requisitos específicos que debe cumplir el sistema y los detalles de su definición.

## 2. Descripción general

### 2.1. Perspectiva del producto

La DApp diseñada para validar la TVA se instalará para su uso en la web, lo que facilitará su aplicación de manera veloz y eficiente, a la vez que proporcionará atributos de transparencia, inmutabilidad, seguridad y trazabilidad.

## 2.2. Funcionalidad del producto

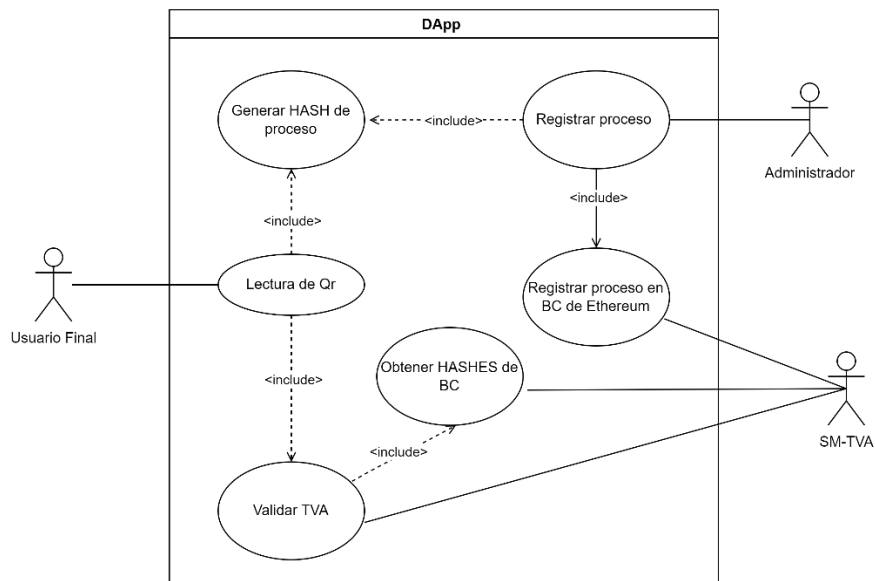


Figura 1. Roles y actividades.

## 2.3. Características de los usuarios

Tabla 5. Características usuario de usuario final

<b>Responsable</b>	Usuario final
<b>Formación</b>	N/A
<b>Actividades</b>	<ul style="list-style-type: none"> <li>• Leer QR.</li> <li>• Visualizar la información de la TVA.</li> </ul>

Tabla 6. Características usuario administrador

<b>Responsable</b>	Administrador
<b>Formación</b>	Personal autorizado de Vinos Ambrosia
<b>Actividades</b>	Registra la información de cada proceso de producción de vino.

Tabla 7. Características usuario SM-VC

<b>Responsable</b>	SM-VC
<b>Formación</b>	N/A
<b>Actividades</b>	El contrato inteligente que integra las funcionalidades para comunicarse con la red de prueba (testnet) de Blockchain.

## 2.4. Restricciones

- Interfaz para ser usada con internet.

- Se emplearán las herramientas de Truffle Suite.
- La DApp será compatible con los navegadores Chrome, Mozilla o Edge.
- Para que la DApp funcione adecuadamente es necesario contar con una conexión a internet.
- Se utilizan los siguientes lenguajes y tecnologías: HTML, CSS, Vue Js, JavaScript, Infura, Sepolia, Truffle Suite y Solidity.
- Los servidores deben tener la capacidad de manejar consultas de manera simultánea.
- El diseño y la implementación del sistema deberán ser simples y no depender de la plataforma o del lenguaje de programación utilizado.

### **2.5. Suposiciones y dependencias**

- Se considera que los requisitos descritos en este documento son estables.
- Para asegurar una ejecución adecuada del sistema, los equipos en los que se instale deben satisfacer los requisitos mencionados anteriormente.

## **3. Requisitos específicos**

### **3.1. Requisitos comunes de las interfaces**

#### **3.1. Interfaces de usuario**

La interfaz de usuario estará compuesta por un grupo de ventanas con botones, listas y campos de texto. Esta interfaz se desarrollará especialmente para el sistema propuesto y se podrá ver desde un navegador web.

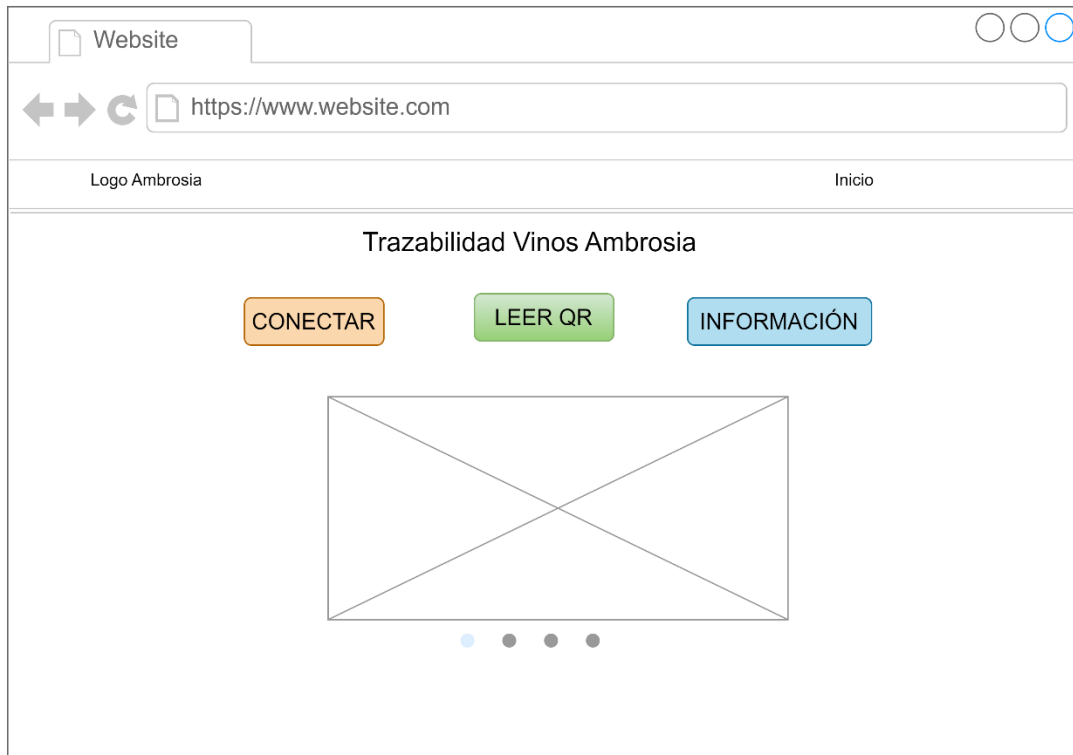


Figura 2. Diseño inicial.



Figura 3. Diseño para registrar el proceso de la TVA

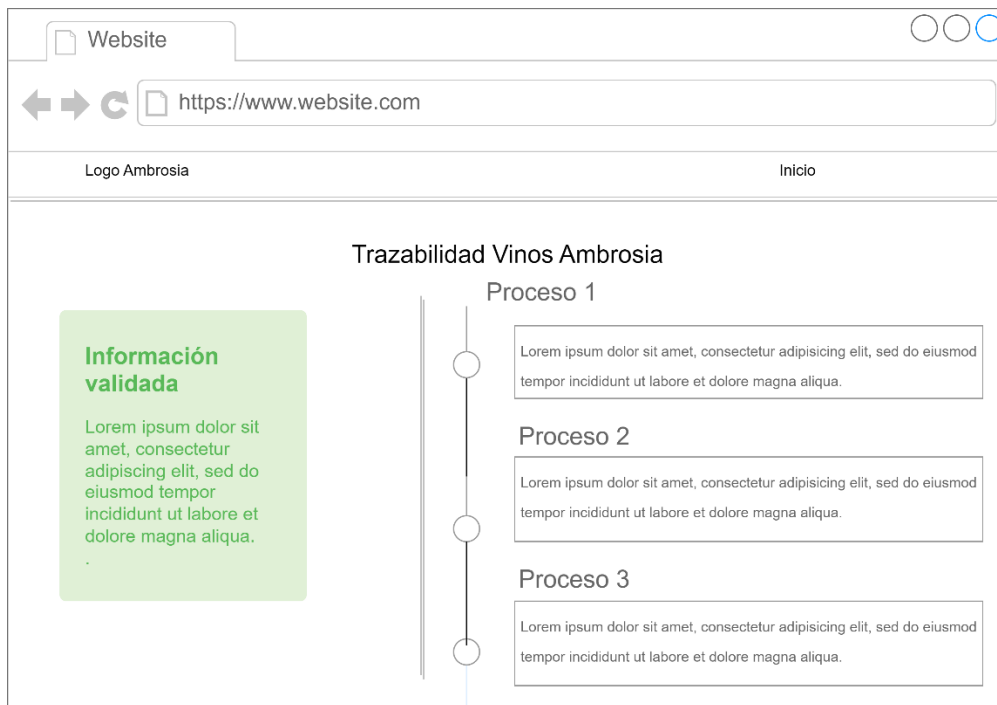


Figura 4. Diseño de la trazabilidad de una botella

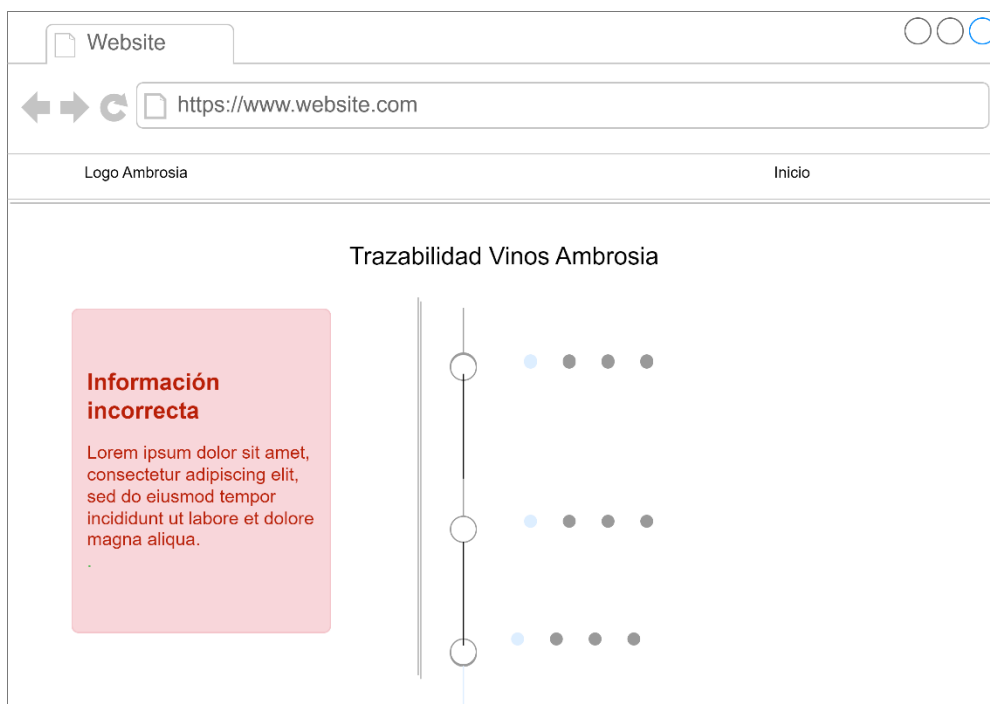


Figura 5. Diseño en el caso de no obtener resultado.

### 3.2. Interfaces de hardware

Será preciso contar con equipos informáticos en óptimas condiciones que posean las siguientes características:

- Ordenador:

- Pantalla con una dimensión mínima de 14 pulgadas y una resolución de 800 dpi.
- Al menos un procesador Core i3 o Pentium Dual Core.
- Un mínimo de 2 GB de memoria RAM.
- Dispositivos de entrada/salida.
- Conectividad:
  - Conexión de red a internet.

### **3.3. Interfaces de software**

- Sistema Operativo: Windows 7 o posterior.
- Navegador web: Mozilla o Chrome.

### 3.2. Requisitos funcionales

Tabla 8. Requisito funcional gestionar registro de un proceso TVA para generar HASH

<b>Identificación:</b>	RF01
<b>Nombre:</b>	Gestionar registro de un proceso de TVA para generar HASH
<b>Descripción:</b>	La DApp gestionará un proceso de TVA para generar el HASH sha-256
<b>Dependencias:</b>	El usuario administrador deberá tener permisos para gestionar la TVA
<b>Requisito NO funcional:</b>	RNF03 RNF04
<b>Prioridad:</b>	Alta

Tabla 9. Requisito funcional registrar HASH de la TVA en la blockchain

<b>Identificación:</b>	RF02
<b>Nombre:</b>	Registrar HASH de TVA en la Blockchain
<b>Descripción:</b>	La DApp el hash de la TVA en la Blockchain de Ethereum, solo por la dirección de billetera que este autorizada
<b>Dependencias:</b>	RF01
<b>Requisito NO funcional:</b>	RNF04
<b>Prioridad:</b>	Alta

Tabla 10. Requisito funcional generar código QR de la botella de vino

<b>Identificación:</b>	RF03
<b>Nombre:</b>	Generar código QR de la botella de vino
<b>Descripción:</b>	La DApp permitirá generar un código QR de la botella a partir del HASH de la TVA
<b>Dependencias:</b>	El usuario administrador debe haber registrado los procesos de la TVA
<b>Requisito NO funcional:</b>	RNF01 RNF04
<b>Prioridad:</b>	Alta

Tabla 11. Requisito funcional obtener HASH a partir del código QR en la botella de vino

<b>Identificación:</b>	RF04
<b>Nombre:</b>	Obtener HASH a partir del código QR en la botella de vino
<b>Descripción:</b>	La DApp permitirá obtener el HASH del código QR presente en la botella de vino mediante la cámara del dispositivo.
<b>Dependencias:</b>	RF03



<b>Requisito NO funcional:</b>	RNF04
<b>Prioridad:</b>	Alta

Tabla 12. Requisito funcional obtener TVAs registradas

<b>Identificación:</b>	RF05
<b>Nombre:</b>	Obtener TVAs registradas
<b>Descripción:</b>	La DApp por medio del contrato inteligente (smart contract) consultará el HASH o HASHES registrados
<b>Dependencias:</b>	RNF02
<b>Requisito NO funcional:</b>	RNF04
<b>Prioridad:</b>	Alta

Tabla 13. Requisito funcional validar la trazabilidad de vino

<b>Identificación:</b>	RF06
<b>Nombre:</b>	Validar la trazabilidad de vino
<b>Descripción:</b>	La DApp verificará si hay una concordancia entre los TVAs obtenidos del RF05 y el generado en el RF02.
<b>Dependencias:</b>	<ul style="list-style-type: none"> <li>• RF02</li> <li>• RF05</li> </ul>
<b>Requisito NO funcional:</b>	<ul style="list-style-type: none"> <li>• RNF03</li> <li>• RNF04</li> </ul>
<b>Prioridad:</b>	Alta

Tabla 14. Requisito funcional mostrar resultado

<b>Identificación:</b>	RF07
<b>Nombre:</b>	Presentar resultado
<b>Descripción:</b>	La DApp emitirá una notificación en el sitio web, donde se detallará el resultado correspondiente a la trazabilidad de la botella en cuestión.
<b>Dependencias:</b>	RF05
<b>Requisito NO funcional:</b>	<ul style="list-style-type: none"> <li>• RNF02</li> <li>• RNF04</li> </ul>
<b>Prioridad:</b>	Alta

### 3.3. Requisitos no funcionales

Tabla 15. Requisito no funcional rendimiento

<b>Identificación:</b>	RNF01
<b>Nombre:</b>	Rendimiento
<b>Descripción:</b>	En una red de prueba de Ethereum, la transacción tarda entre 2 a 5 segundos; sin embargo, en un entorno real, puede tardar entre 15 segundos a 5 minutos.
<b>Prioridad:</b>	Alta

Tabla 16. Requisito no funcional usabilidad

<b>Identificación:</b>	RNF02
<b>Nombre:</b>	Usabilidad
<b>Descripción:</b>	La DApp debe tener una interfaz que sea fácil de usar y comprender, lo que hace que el procedimiento sea simple de completar. Además, debe permitir su uso en cualquier navegador web.
<b>Prioridad:</b>	Alta

Tabla 17. Requisito no funcional fiabilidad

<b>Identificación:</b>	RNF03
<b>Nombre:</b>	Fiabilidad
<b>Descripción:</b>	La DApp debe implementar medidas de seguridad robustas para proteger la información sensible y los activos digitales relacionados con la producción de vinos.
<b>Prioridad:</b>	Alta

Tabla 18. Requisito no funcional seguridad

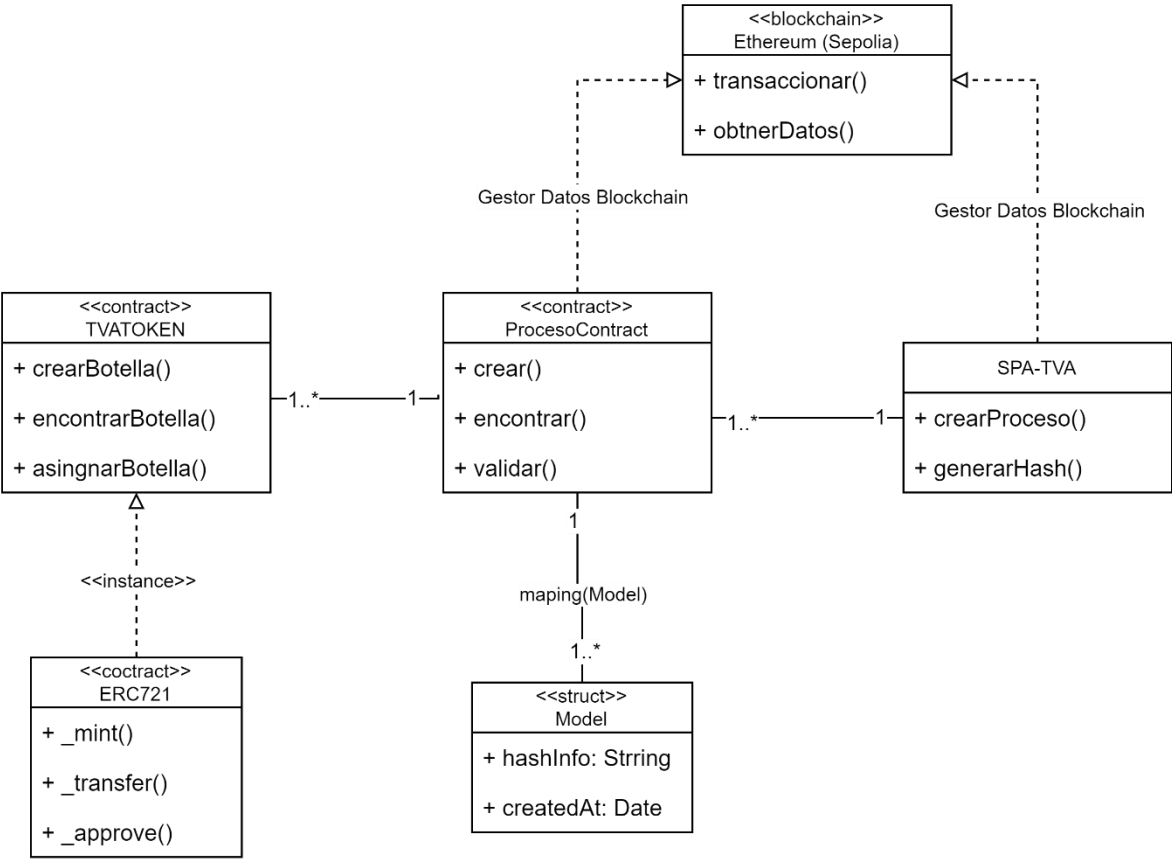
<b>Identificación:</b>	RNF04
<b>Nombre:</b>	Seguridad
<b>Descripción:</b>	Se debe implementar un sistema de control de acceso para garantizar que solo los usuarios autorizados tengan permiso para realizar ciertas operaciones en la DApp. Esto incluye la gestión de roles y privilegios.
<b>Prioridad:</b>	Alta

### Anexo 3. Descripción de Historias de usuario

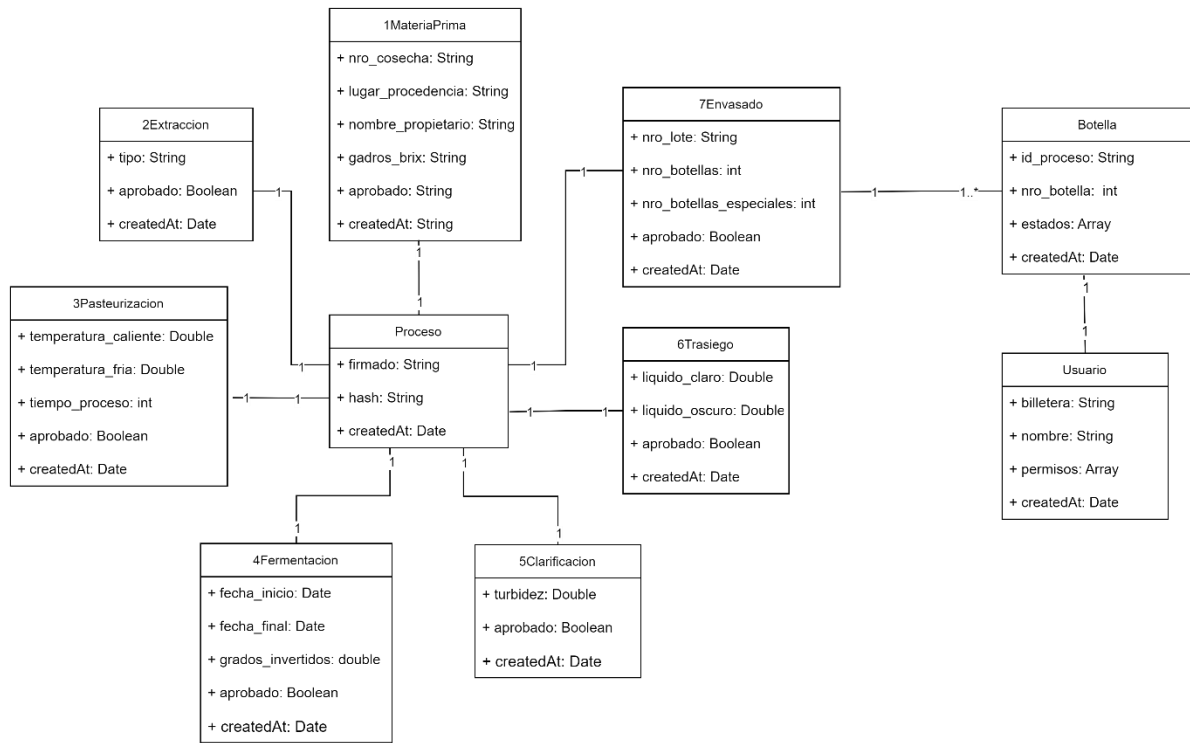
Identificador (ID) de la historia	Enunciado de la historia				Criterios de aceptación			
	Rol	Característica / Funcionalidad	Razón / Resultado	Número (#) de escenario	Criterio de aceptación (Título)	Contexto	Evento	Resultado / Comportamiento esperado
HU01	Como cliente	Quiero acceder a la información de TVA.	Con el objetivo de validar la trazabilidad de la TVA	1	Verificar si un QR de TVA es valida	En caso de validar una TVA registrada	Cuando se lea QR de botella	La DApp debe presentar una vista donde indique la información de la trazabilidad.
				2	Verificar si un QR de TVA no es valida	En caso de validar una TVA registrada	Cuando se lea QR de botella	La DApp debe mostrar una notificación que señale que la trazabilidad no es genuina.
				3	Verificar si un QR de TVA fue modificado	En caso de validar una TVA registrada	Cuando haga clic en el botón validar	La DApp debe mostrar una notificación que señale que la trazabilidad no es genuina.
HU02	Como administrador	Quiero registrar una TVA	Con el propósito de registrar una TVA en la Blockchain	1	Registrar una TVA	En caso de registrar un TVA	Al presionar el botón Firma contrato	La DApp debe desplegar una ventana de Metamask para verificar la transacción y mostrar un mensaje que confirme que la trazabilidad ha sido guardada exitosamente.
				2	Registrar un TVA existente	En caso de registrar una TVA	Al presionar el botón Firma contrato	La DApp debe mostrar un mensaje que señale que la TVA ya ha sido registrada previamente.

HU03	Como Contrato inteligente (SM-VC)	Quiero validar una TVA	Con el objetivo de validar si la TVA se encuentra registrado en la red Blockchain	1	Validar una TVA existente	En caso de validar si la TVA existe	Al ejecutar la función validarTVA del contrato inteligente	El contrato inteligente debe retornar valor sha-256
				2	Validar una TVA no existente	En caso de validar si la TVA no existe	Al ejecutar la función validarTVA del contrato inteligente	El contrato inteligente debe retornar valor indefinido
HU04	Como Contrato inteligente (SM-TVA)	Quiero registrar una TVA	Con el objetivo de validar si la TVA se encuentra registrado en la red Blockchain	1	Registrar una TVA	En caso de registrar una TVA	Al ejecutar la función registrarTVA del contrato inteligente	El contrato inteligente debe almacenar en la cadena de bloques el SHA-256 del TVA.
				2	Registrar una TVA ya existente	En caso de registrar una TVA	Al ejecutar la función registrarTVA del contrato inteligente	El contrato inteligente debe retornar un mensaje indicando que la TVA ya ha sido registrada previamente.
HU05	Como SPA-TVA	Quiero generar el SHA-256 del TVA	Con la finalidad de generar el SHA-256 del TVA	1	En caso de generar el SHA-256 de un TVA (QR que si se puede leer)	En caso de generar el SHA-256 de un QR	Al cargar el HASH del QR	La función Reader debe leer el QR para poder consultar la información de la trazabilidad
				2	En caso de generar el SHA-256 de un TVA (QR que no se puede leer)	En caso de generar el SHA-256 de un QR	Al cargar el HASH del QR	En caso de que falle la lectura del código QR, generar un mensaje de error.

**Anexo 4.** Diagrama de clases subsistema de contratos inteligentes



## Anexo 5. Diagrama de clases subsistema de aplicaciones



**Anexo 6.** Código para el subsistema de contratos inteligentes

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Fecha: 14/06/2022



## Índice de Contenidos

1. Código fuente del contrato inteligente ProcesoContract.sol..... 117
2. Código fuente del contrato inteligente TVAToken.sol ..... 117

## 1. Código fuente del contrato inteligente ProcesoContract.sol

El código fuente se observa en la Tabla 1.

Tabla 1.  
Código fuente del contrato ProcesoContract.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.11;

contract ProcesoContract {
    struct Model {
        string hash_info;
        uint256 createdAt;
    }
    mapping(string => Model) public lista;

    function crear(string memory _info) public returns (Model memory) {
        Model memory _model = Model(_info, block.timestamp);
        lista[_info] = _model;
        return _model;
    }

    function encontrar(string memory _id) public view returns (Model memory) {
        return lista[_id];
    }
}
```

## 2. Código fuente del contrato inteligente TVAToken.sol

El código fuente se observa en la Tabla 2.

Tabla 2.  
Código fuente del contrato TVAToken.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.4;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";

contract TVATOKEN is ERC721 {
    mapping(string => string) _botellas_ids;
    mapping(string => bool) _botellaExiste;
    uint256 contador = 0;

    constructor() ERC721("VINO", "TVANFT") {}

    function crearBotella(address cuenta, string memory _hash) public {
        require(!_botellaExiste[_hash]);
        _mint(cuenta, contador);
        _botellas_ids[_hash] = _hash;
        _botellaExiste[_hash] = true;
    }
}
```

```
    contador++;  
}  
  
function encontrarBotella(string memory _hash)  
    public  
    view  
    returns (string memory)  
{  
    return _botellas_ids[_hash];  
}  
  
function asignarBotella(address to, uint256 tokenId) public {  
    _transfer(msg.sender, to, tokenId);  
}  
}
```

## **Anexo 7.** Código para el subsistema de aplicaciones

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Fecha: 05/07/2022

## Índice de Contenidos

1. Subsistema de aplicaciones backend .....	121
2. Subsistema de aplicaciones frontend .....	126
3. Función de registrar y validar la TVA.....	128

## Subsistema de aplicaciones backend

Tabla 1.  
Controlador para administrar procesos de TVA

```
var sha256 = require('sha256');
//Models
var MateriaPrima = require('../modelos/1materia_prima');
var Extraccion = require('../modelos/2extraccion');
var Pasteurizacion = require('../modelos/3pasteurizacion');
var Fermentacion = require('../modelos/4fermentacion');
var Clarificacion = require('../modelos/5clarificacion');
var Trasiego = require('../modelos/6trasiego');
var Envasado = require('../modelos/7envasado');
var Proceso = require('../modelos/proceso');
var Botella = require('../modelos/botella');
//Modules
var GlobalApp = require('../global/global_app');
var UtilApi = require('../utils/util_api');

exports.listar_proceso = async function (req, res) {
  try {
    var procesos = await Proceso.find()
      .populate("materia_prima")
      .populate("extraccion")
      .populate("pasteurizacion")
      .populate("fermentacion")
      .populate("clarificacion")
      .populate("trasiego")
      .populate("envasado", "-botellas");
    UtilApi.succesServer(req, res, { procesos });
  } catch (error) {
    UtilApi.errorServer(req, res, error);
  }
};

exports.encontrar_proceso = async function (req, res) {
  try {
    let { id_proceso } = req.body;
    var proceso = await encontrar_proceso(id_proceso);
    UtilApi.succesServer(req, res, proceso);
  } catch (error) {
    UtilApi.errorServer(req, res, error);
  }
};
```

```

exports.crear_editar_proceso = async function (req, res) {
  try {
    let { proceso, id_proceso } = req.body;
    UtilApi.validarCampos({ proceso });
    switch (proceso) {
      case 1:
        let { nro_cosecha, lugar_procedencia, nombre_propietario, grados_brix } = req.body;
        UtilApi.validarCampos({ nro_cosecha, lugar_procedencia, nombre_propietario, grados_brix });
        if (id_proceso !== undefined) {
          var proceso_validar = await encontrar_proceso(id_proceso); //para validar si existe proceso
          var _id = proceso_validar.materia_prima?._id;
          await MateriaPrima.updateOne({ _id }, { nro_cosecha, lugar_procedencia, nombre_propietario,
gados_brix });
        } else {
          var materia_prima = await MateriaPrima.create({ nro_cosecha, lugar_procedencia,
nombre_propietario, gados_brix });
          var proceso_c = await Proceso.create({ materia_prima: materia_prima._id });
          id_proceso = proceso_c._id;
        }
        break;
      case 2:
        var proceso_validar = await encontrar_proceso(id_proceso); //para validar si existe proceso
        let { tipo } = req.body;
        UtilApi.validarCampos({ tipo });
        var _id = proceso_validar.extraccion?._id;
        if (_id !== undefined) {
          await Extraccion.updateOne({ _id }, { tipo });
        } else {
          var extraccion = await Extraccion.create({ tipo });
          await Proceso.updateOne({ _id: id_proceso }, { extraccion: extraccion._id });
        }
        break;
      case 3:
        var proceso_validar = await encontrar_proceso(id_proceso); //para validar si existe proceso
        let { temperatura_caliente, temperatura_fria, tiempo_proceso } = req.body;
        var data = { temperatura_caliente, temperatura_fria, tiempo_proceso };
        UtilApi.validarCampos(data);
        var _id = proceso_validar.pasteurizacion?._id;
        if (_id !== undefined) {
          await Pasteurizacion.updateOne({ _id }, data);
        } else {
          var pasteurizacion = await Pasteurizacion.create(data);
          await Proceso.updateOne({ _id: id_proceso }, { pasteurizacion: pasteurizacion._id });
        }
        break;
      case 4:
        var proceso_validar = await encontrar_proceso(id_proceso); //para validar si existe proceso
        let { fecha_inicio, fecha_final, grados_invertidos } = req.body;
        var data = { fecha_inicio, fecha_final, grados_invertidos };
        UtilApi.validarCampos(data);
        var _id = proceso_validar.fermentacion?._id;
        if (_id !== undefined) {

```

```

        await Fermentacion.updateOne({ _id }, data);
    } else {
        var fermentacion = await Fermentacion.create(data);
        await Proceso.updateOne({ _id: id_proceso }, { fermentacion: fermentacion._id });
    }
    break;
case 5:
    var proceso_validar = await encontrar_proceso(id_proceso); //para validar si existe proceso
    let { turbidez } = req.body;
    var data = { turbidez };
    UtilApi.validarCampos(data);
    var _id = proceso_validar.clarificacion?._id;
    if (_id !== undefined) {
        await Clarificacion.updateOne({ _id }, data);
    } else {
        var clarificacion = await Clarificacion.create(data);
        await Proceso.updateOne({ _id: id_proceso }, { clarificacion: clarificacion._id });
    }
    break;
case 6:
    var proceso_validar = await encontrar_proceso(id_proceso); //para validar si existe proceso
    let { liquido_claro, liquido_oscuero } = req.body;
    var data = { liquido_claro, liquido_oscuero };
    UtilApi.validarCampos(data);
    var _id = proceso_validar.trasiego?._id;
    if (_id !== undefined) {
        await Trasiego.updateOne({ _id }, data);
    } else {
        var trasiego = await Trasiego.create(data);
        await Proceso.updateOne({ _id: id_proceso }, { trasiego: trasiego._id });
    }
    break;
case 7:
    var proceso_validar = await encontrar_proceso(id_proceso); //para validar si existe proceso
    let { nro_lote, nro_botellas, nro_botellas_especiales } = req.body;
    var data = { nro_lote, nro_botellas, nro_botellas_especiales };
    UtilApi.validarCampos(data);
    if (nro_botellas_especiales > nro_botellas) throw { mensaje: GlobalApp.mensaje_botellas_max_error
}

    var _id = proceso_validar.envasado?._id;
    if (_id !== undefined) {
        await Envasado.updateOne({ _id }, data);
    } else {
        var envasado = await Envasado.create(data);
        await Proceso.updateOne({ _id: id_proceso }, { envasado: envasado._id });
    }
    break;
default:
    throw { mensaje: GlobalApp.mensaje_error_proceso };
}
UtilApi.succesServer(req, res, id_proceso, GlobalApp.mensaje_guardar_ok);

```



```

    } catch (error) {
      UtilApi.errorServer(req, res, error);
    }
  };

exports.aprobar_proceso = async function (req, res) {
  try {
    let { proceso, id_proceso } = req.body;
    UtilApi.validarCampos({ proceso, id_proceso });
    var proceso_validar = await encontrar_proceso(id_proceso);
    switch (proceso) {
      case 1:
        var _id = proceso_validar.materia_prima?._id;
        await MateriaPrima.updateOne({ _id }, { aprobado: true });
        break;
      case 2:
        var _id = proceso_validar.extraccion?._id;
        await Extraccion.updateOne({ _id }, { aprobado: true });
        break;
      case 3:
        var _id = proceso_validar.pasteurizacion?._id;
        await Pasteurizacion.updateOne({ _id }, { aprobado: true });
        break;
      case 4:
        var _id = proceso_validar.fermentacion?._id;
        await Fermentacion.updateOne({ _id }, { aprobado: true });
        break;
      case 5:
        var _id = proceso_validar.clarificacion?._id;
        await Clarificacion.updateOne({ _id }, { aprobado: true });
        break;
      case 6:
        var _id = proceso_validar.trasiego?._id;
        await Trasiego.updateOne({ _id }, { aprobado: true });
        break;
      case 7:
        var _id = proceso_validar.ensinado?._id;
        var ensinado = proceso_validar.ensinado;
        if (ensinado.botellas === undefined || ensinado.botellas.length === 0) {
          var botellas = [];
          for (let index = 0; index < ensinado.nro_botellas_especiales; index++) {
            var data = {
              nro_botella: index + 1,
              id_proceso: id_proceso,
              estados: [{ fecha: new Date(), estado: "Empacado" }]
            };
            var botella = await Botella.create(data);
            botellas.push({ botella: botella._id });
          }
          await Ensinado.updateOne({ _id }, { aprobado: true, botellas });
        }
    }
  }
}

```

```

        break;
      default:
        throw { mensaje: GlobalApp.mensaje_error_proceso };
      }
      UtilApi.succesServer(req, res, id_proceso, GlobalApp.mensaje_aprobar_proceso);
    } catch (error) {
      UtilApi.errorServer(req, res, error);
    }
  };

exports.firmar_proceso = async function (req, res) {
  try {
    let { id_proceso, hash } = req.body;
    UtilApi.validarCampos({ id_proceso, hash });
    await Proceso.updateOne({ _id: id_proceso }, { aprobado: true, hash });
    UtilApi.succesServer(req, res, id_proceso, GlobalApp.mensaje_aprobar_proceso);
  } catch (error) {
    UtilApi.errorServer(req, res, error);
  }
};

exports.encontrar_proceso_botella = async function (req, res) {
  try {
    let { hash_botella } = req.body;
    UtilApi.validarCampos({ hash_botella });
    var botella = await Botella.findOne({ _id: hash_botella });
    var proceso = await encontrar_proceso(botella.id_proceso);
    UtilApi.succesServer(req, res, { botella, proceso }, GlobalApp.mensaje_botella_encontrada);
  } catch (error) {
    UtilApi.errorServer(req, res, error, "Botella no encontrada");
  }
};

exports.cambiar_estado_botella = async function (req, res) {
  try {
    let { hash_botella } = req.body;
    UtilApi.validarCampos({ hash_botella });
    var botella = await Botella.findOne({ _id: hash_botella });
    var estados = botella.estados;
    var length = estados.length;
    if (length === 1) estados.push({ fecha: new Date(), estado: "Vendido" });
    if (length === 2) estados.push({ fecha: new Date(), estado: "Token Asignado" });
    await Botella.updateOne({ _id: botella._id }, { estados });
    UtilApi.succesServer(req, res, null, GlobalApp.mensaje_botella_actualizada);
  } catch (error) {
    UtilApi.errorServer(req, res, error, "Botella no encontrada");
  }
};

```

```

exports.listar_botella = async function (req, res) {
  try {
    let { id_proceso } = req.body;
    var proceso_validar = await encontrar_proceso(id_proceso);
    var _id = proceso_validar.envasado?._id;
    var envasado = await Envasado.findOne({ _id: _id })
      .populate("botellas.botella");
    var botellas = envasado.botellas;
    UtilApi.succesServer(req, res, { botellas }, GlobalApp.mensaje_botella_encontrada);
  } catch (error) {
    UtilApi.errorServer(req, res, error);
  }
};

async function encontrar_proceso(id_proceso) {
  UtilApi.validarCampos({ id_proceso });
  try {
    var proceso = await Proceso.findOne({ _id: id_proceso })
      .populate("materia_prima")
      .populate("extraccion")
      .populate("pasteurizacion")
      .populate("fermentacion")
      .populate("clarificacion")
      .populate("trasiego")
      .populate("envasado", "-botellas");
    if (proceso == undefined) throw { mensaje: GlobalApp.mensaje_error_proceso, error: error }
    return proceso;
  } catch (error) {
    throw { mensaje: GlobalApp.mensaje_error_proceso, error: error }
  }
}

```

## Subsistema de aplicaciones frontend

El código fuente se observa en la Tabla 1.

Tabla 2.  
Estados y conexión con web3, metamask, contrato y cuentas

```

import Web3 from 'web3';
var TruffleContract = require('@truffle/contract');

const getWeb3 = async () => {
  if (window.ethereum) {
    const web3 = new Web3(window.ethereum);
    await window.ethereum.request({ method: 'eth_requestAccounts' });
    return web3;
  }
}

```

```

} else if (window.web3) {
  const web3 = new Web3(window.web3.currentProvider);
  return web3;
} else {
  throw { mensaje: "Se detectó un navegador que no admitido. ¡Deberías considerar probar MetaMask!" };
}
}

export const infoCuenta = async () => {
  try {
    // Obtener el proveedor de red y la instancia web3.
    const web3 = await getWeb3();
    // Usar web3 para obtener las cuentas de los usuarios.
    const cuentas = await web3.eth.getAccounts();
    const cuenta = cuentas[0];
    web3.eth.defaultAccount = cuentas[0];
    //balance
    const balanceG = await web3.eth.getBalance(cuentas[0]);
    const balanceETHER = web3.utils.fromWei(balanceG, 'ether');
    return { web3, cuenta, balanceETHER };
  } catch (error) {
    console.log(error);
    var mensaje = error.mensaje ?? "Ocurrió un problema al conectarse con la blockchain";
    if (error.code === 4001) mensaje = "Rechazaste la solicitud para conectarte con metamask";
    if (error.code === -32002) mensaje = "Revisa la extensión de metamask y confirma la solicitud";
    throw { mensaje };
  }
};

export const cargarContrato = async (web3, contrato_json) => {
  const contrato_instancia = TruffleContract(contrato_json);
  contrato_instancia.setProvider(web3.eth.currentProvider);
  const contrato = await contrato_instancia.deployed();
  return contrato;
};

export const encontrarProceso = async (web3, contrato_json, _id) => {
  const contrato = await cargarContrato(web3, contrato_json);
  var model = await contrato.encontrar(_id);
  if (model.createdAt !== "0") {
    return model;
  } else {
    return undefined;
  }
};

export const escucharEvento = async (contrato_json, call) => {
  const { web3 } = await infoCuenta();
  const networkId = await web3.eth.net.getId();

```

```

const deployedNetwork = contrato_json.networks[networkId];
const contrato = new web3.eth.Contract(
  contrato_json.abi,
  deployedNetwork && deployedNetwork.address,
);
contrato.events.Id(function (error, result) {
  if (!error) {
    call(result.returnValues.id);
  }
});
};

```

## **Función de registrar y validar la TVA**

Tabla 3.  
Función de registrar y validar la TVA

```

import ProcesoContract from '../contracts/ProcesoContract.json';
import TVATOKEN from '../contracts/TVATOKEN.json';
import { infoCuenta, cargarContatrato } from './getWeb3';
var sha256 = require('sha256');

export const generarSha256Firma = async (proceso) => {
  var { materia_prima, extraccion, pasteurizacion, fermentacion, clarificacion, trasiego, envasado } = proceso;
  var data = { materia_prima, extraccion, pasteurizacion, fermentacion, clarificacion, trasiego, envasado };
  return sha256(JSON.stringify(data));
}

export const firmarProceso = async (proceso) => {
  var { web3, cuenta } = await infoCuenta();
  const config = { from: cuenta };
  var contratoProceso = await cargarContatrato(web3, ProcesoContract);
  var hashSend = await generarSha256Firma(proceso);
  await contratoProceso.crear(hashSend, config);
  return hashSend;
}

export const encontrarFirmaProceso = async (proceso) => {
  var { web3 } = await infoCuenta();
  var contratoProceso = await cargarContatrato(web3, ProcesoContract);
  var hashSend = await generarSha256Firma(proceso);
  var hash = await contratoProceso.encontrar(hashSend);
  return hash;
}

export const crearBotella = async (hash) => {
  var { web3, cuenta } = await infoCuenta();
  const config = { from: cuenta };

```

```
var contratoTVATOKEN = await cargarContrato(web3, TVATOKEN);
await contratoTVATOKEN.crearBotella(cuenta, hash, config);
}

export const encontrarBotella = async (hash) => {
  var { web3 } = await infoCuenta();
  var contratoTVATOKEN = await cargarContrato(web3, TVATOKEN);
  var encontrar = await contratoTVATOKEN.encontrarBotella(hash);
  console.log(encontrar);
}
```

## **Anexo 8.** Pruebas Unitarias del subsistema de aplicaciones

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Versión: 1.0

Fecha: 04/08/2022

## Hoja de control

---

<b>Organismo</b>	Universidad Nacional de Loja		
<b>Proyecto</b>	Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia		
<b>Entregable</b>	Pruebas Unitarias del subsistema de Aplicaciones		
<b>Autor</b>	Jimmy Vicente		
<b>Versión/Edición</b>	1.0	<b>Fecha Versión</b>	04/08/2022
<b>Aprobado por</b>	Cristian Ramiro Narváez Guillen, Mg.Sc.	<b>Fecha Aprobación</b>	05/08/20212
		<b>N° Total de Páginas</b>	7

---



## 1. Introducción

### Objeto

El objetivo de este documento es validar el correcto funcionamiento del subsistema de aplicaciones desglosando el código en sus componentes y confirmando que cada uno funciona según lo previsto.

### Propósito

Verificar y demostrar que el software está funcionando correctamente. La implementación de una DApp con tecnología blockchain permitirá rastrear la creación del vino Ambrosia, y lo hará de una manera que aborde cada función principal individualmente.

### Definición de los casos de pruebas

En este apartado se proporcionará una descripción detallada de cada uno de los casos de prueba que se han identificado previamente. Se explicará el objetivo de cada caso de prueba, los pasos que se deben seguir para llevarlo a cabo, los datos de entrada que se deben proporcionar y los resultados esperados. La descripción detallada de los casos de prueba es esencial para garantizar que se hayan cubierto todas las posibles situaciones y que el sistema funciona correctamente en cada una de ellas. Además, permite a los evaluadores y desarrolladores comprender mejor el comportamiento del sistema y asegurar que se ha cumplido con los requisitos y especificaciones establecidos.

Número del Caso de Prueba	Componente	Descripción de lo que se probará	Prerrequisitos
CP01	Sistema de aplicaciones	Verificar que la página se muestre correctamente sin vincular a web3, contratos o cuentas.	Navegador web
CP02	Sistema de aplicaciones	Verificar que cuando se conecte a web3, contratos o cuentas, la página se muestre correctamente.	Un navegador web compatible con la extensión de Metamask.
CP03	Sistema de aplicaciones	Verificar si el estado SHA-256 de TVA se está supervisando en el registro de TVA.	Formato JSON del contrato compilado y migrado al subsistema de aplicaciones.
CP04	Sistema de aplicaciones	Verificar que se redirija al estado correspondiente al momento de registrar un proceso TVA	Página correctamente renderizada

<b>CP05</b>	Sistema de aplicaciones	Verificar que el SHA-256 del TVA obtenida del QR existe en los registros de la blockchain.	Formato JSON del contrato compilado y migrado al subsistema de aplicaciones.
-------------	-------------------------	--	--

### CP01

Nº	Descripción	Método	Datos Entrada	¿OK?	Observaciones
1	Verificar que la página se muestre correctamente sin vincular a web3, contratos o cuentas.	test('Renderizar <App /> al no estar conectado a web3, cuentas, contrato o Metamask ')	N/A	ü	N/A

### CP02

Nº	Descripción	Método	Datos Entrada	¿OK?	Observaciones
1	Verificar que cuando se conecte a web3, contratos o cuentas, la página se muestre correctamente.	test('Renderizar <App /> correctamente si cumple con las condiciones')	N/A	ü	N/A
2	Verificar que se llamen las funciones que realizan solicitudes web3, de contrato y de cuenta	test('Llamar a infoCuenta()')	N/A	ü	N/A

### CP03

Nº	Descripción	Método	Datos Entrada	¿OK?	Observaciones
1	Mostrar adecuadamente los formularios para el registro de todos los procesos de la TVA	test('Mostrar formulario para registrar ')	N/A	ü	N/A
2	Verificar que se llama correctamente a la	test('Llamar a la función generarSha256Firma()')	N/A	ü	N/A

	función para generar SHA-256				
<b>3</b>	Verificar que se llama correctamente a la función de registrar en la blockchain	test('Llamar a la función firmarProceso()')	N/A	ü	N/A

---

**CP04**

---

<b>Nº</b>	<b>Descripción</b>	<b>Método</b>	<b>Datos Entrada</b>	<b>¿OK?</b>	<b>Observaciones</b>
<b>1</b>	Mostrar adecuadamente la TVA con el id de transacción	test('Mostrar id de transacción')	N/A	ü	N/A
<b>3</b>	Mostrar correctamente la gestión de la TVA (Imprimir QR, Visualizar botellas, etc)	test('Mostrar gestión de TVA')	N/A	ü	N/A

---

---

**CP05**

---

<b>Nº</b>	<b>Descripción</b>	<b>Método</b>	<b>Datos Entrada</b>	<b>¿OK?</b>	<b>Observaciones</b>
<b>1</b>	Mostrar adecuadamente la cámara para obtener información del SHA-256 de QR	test('Llamar a función onDecode()')	N/A	ü	N/A
<b>2</b>	Verificar que el SHA-256 se encuentre en el registro de la blockchain	test('Llamar a la función encontrarBotella()')	N/A	ü	N/A
<b>3</b>	Mostrar correctamente la TVA de la botella con los procesos correspondientes.	test('Mostrar TVA de la botella')	N/A	ü	N/A
<b>4</b>	Mostrar el mensaje adecuado si la TVA no existe en los registros de la blockchain.	test('Mostrar el mensaje adecuado cuando la TVA no existe')	N/A	ü	N/A

---

**Glosario**

En esta sección, se detallan y explican los términos técnicos, acrónimos o jerga utilizados en el documento con el fin de facilitar su comprensión. Esto es especialmente importante para aquellas personas que no tienen experiencia en el área o que no están familiarizadas con el lenguaje técnico.

---

<b>Término</b>	<b>Descripción</b>
TVA	Trazabilidad de Vinos Ambrosia
SHA-256	Algoritmo que permite encriptar información
QR	Código de barras bidimensional que permite guardar información
PTT	Proyecto de Trabajo de Titulación

---



## **Anexo 9.** Pruebas de Integración

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Versión: 1.0

Fecha: 11/08/2022

## Hoja de control

<b>Organismo</b>	Universidad Nacional de Loja		
<b>Proyecto</b>	Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia		
<b>Entregable</b>	Pruebas de Integración		
<b>Autor</b>	Jimmy Vicente		
<b>Versión/Edición</b>	1.0	<b>Fecha Versión</b>	11/08/2022
<b>Aprobado por</b>	Cristian Ramiro Narváez Guillen, Mg.Sc.	<b>Fecha Aprobación</b>	13/08/2022
		<b>N° Total de Páginas</b>	9

## Índice de Contenidos

1. Introducción .....	134
Objeto .....	134
Alcance.....	134
2. Definición de los casos de pruebas .....	134
3. Glosario.....	137
4. Bibliografía y referencias.....	138



## Introducción

### Objeto

El objetivo de este documento es ejecutar los casos de prueba que confirman que la DApp está funcionando de acuerdo con los requisitos funcionales. Una vez que las pruebas unitarias se han completado con éxito, se crean pruebas de integración para garantizar que se mantenga la naturaleza unitaria del software cuando se combinan elementos unitarios.

### Alcance

Los diferentes casos de prueba son validados por el profesor Ing. Cristián Narváez (director de la TT), quien enseña ingeniería de sistemas y computación en la Universidad Nacional de Loja. Por otro lado Jimmy Vicente, estudiante, es quien crea y graba los múltiples escenarios de prueba.

### Definición de los casos de pruebas

Este apartado se enfoca en proporcionar una descripción detallada de cada uno de los escenarios de prueba que han sido identificados para el sistema en cuestión. Aquí, se proporciona información completa sobre los casos de prueba, incluyendo los datos de entrada, la acción que se espera que se realice, la salida esperada y cualquier mensaje que pueda aparecer durante el proceso. Al proporcionar una descripción exhaustiva de cada escenario de prueba, se asegura de que se cubran todos los aspectos del sistema y se verifique su correcto funcionamiento en diferentes situaciones. Esto permitirá identificar cualquier problema o error en el sistema antes de su implementación y asegurará que el sistema esté listo para su uso por parte de los usuarios finales.

<b>Número del Caso de Prueba</b>	<b>Componentes</b>	<b>Descripción de lo que se probará</b>	<b>Prerrequisitos</b>
<b>CP01</b>	Wallet - Subsistema de aplicaciones	Conexión con la wallet de Metamask	<ul style="list-style-type: none"><li>• Acceder a la página</li><li>• Para acceder al sistema, será necesario contar con la frase de recuperación de la wallet o ingresar la contraseña si ya se ha iniciado sesión previamente.</li></ul>
<b>CP02</b>	Subsistema de contratos inteligentes –	Se registre correctamente el SHA-	<ul style="list-style-type: none"><li>• Acceder a la página.</li><li>• Ir a la billetera Metamask e inicie sesión.</li></ul>

---

	Subsistema de aplicaciones	256 de la TVA en la testnet de Blockchain	<ul style="list-style-type: none"> <li>• Tener acceso a la parte administrativa de la TVA.</li> </ul>
<b>CP03</b>	Subsistema de aplicaciones-Blockchain	Se visualice correctamente las botellas producidas con la TVA correspondiente al hacer clic en “BOTELLAS PRODUCIDAS”	<ul style="list-style-type: none"> <li>• Acceder a la página.</li> <li>• Ir a la billetera Metamask e inicie sesión.</li> <li>• Tener acceso a la parte administrativa de la TVA.</li> <li>• Estar dentro de la gestión de un TVA en específico</li> </ul>
<b>CP04</b>	Subsistema de aplicaciones	Se genere correctamente el pdf con los QRS para imprimir al hacer clic en “IMPRIMIR”	<ul style="list-style-type: none"> <li>• Acceder a la página.</li> <li>• Ir a la billetera Metamask e inicie sesión.</li> <li>• Tener acceso a la parte administrativa de la TVA.</li> <li>• Estar dentro de la gestión de un TVA en específico</li> </ul>
<b>CP05</b>	Subsistema de contratos inteligentes – Subsistema de aplicaciones	Al ingresar a LEER QR, se obtenga correctamente el SHA-256 de la TVA	<ul style="list-style-type: none"> <li>• Acceder a la página.</li> <li>• Ir a la billetera Metamask e inicie sesión.</li> <li>• Ingresar a la sección LEER QR.</li> <li>• Dar permiso al acceso de la cámara del dispositivo.</li> </ul>

---

---

**CP01**

---

<b>Paso</b>	<b>Descripción</b>	<b>Datos Entrada</b>	<b>Resultado esperado</b>	<b>¿OK?</b>	<b>Observaciones</b>
1	Ingresar a la página	Clic	Ventana de la wallet para ingresar la contraseña	✓	N/A
2	Completar el campo con la contraseña	String	Habilitar el botón de DESBLOQUEAR	✓	
3	Hacer clic en el botón CONECTAR	Clic	Un mensaje de alerta que se ha conectado correctamente y el sistema cargado completamente	✓	

---

---

**CP02**

---

<b>Paso</b>	<b>Descripción</b>	<b>Datos Entrada</b>	<b>Resultado esperado</b>	<b>¿OK?</b>	<b>Observaciones</b>
1	Presionar en el ítem “NUEVO PROCESO”.	Clic	Vista de validar	✓	N/A
2	Completar el registro de cada uno de los procesos del TVA	Object TVA	String Sha-256	✓	
3	Presionar el botón “FIRMAR CONTRATO”.	Clic	Una notificación que indique al usuario que debe confirmar la transacción.	✓	
4	Presionar el botón "Confirmar" en la ventana emergente de Metamask.	Clic	Respuesta indicando que el registro se ha completado satisfactoriamente.	✓	

---

---

**CP03**

---

<b>Paso</b>	<b>Descripción</b>	<b>Datos Entrada</b>	<b>Resultado esperado</b>	<b>¿OK?</b>	<b>Observaciones</b>
1	Presionar en el botón “BOTELLAS PRODUCIDAS”	Clic	Vista de una TVA	✓	N/A
4	Presionar en una de las botellas	Clic	Respuesta con el resultado de la TVA de la botella correspondiente	✓	

---

---

**CP04**

---

<b>Paso</b>	<b>Descripción</b>	<b>Datos Entrada</b>	<b>Resultado esperado</b>	<b>¿OK?</b>	<b>Observaciones</b>
1	Presionar en el botón “BOTELLAS PRODUCIDAS”	Clic	Vista de una TVA	✓	N/A
1	Presionar en el botón “IMPRIMIR”	Clic	Generar PDF con todos los QR de las botellas producidas	✓	

---

---

**CP05**

---

<b>Paso</b>	<b>Descripción</b>	<b>Datos Entrada</b>	<b>Salida Esperada</b>	<b>¿OK?</b>	<b>Observaciones</b>
1	Acceder a la página	Clic	Ventana de la wallet que solicita al usuario ingresar su contraseña.	✓	N/A
2	Presionar en el botón “LEER QR”	Clic	Una vista nueva con la TVA de la botella correspondiente	✓	

---

**Glosario**

En esta sección, se detallan y explican los términos técnicos, acrónimos o jerga utilizados en el documento con el fin de facilitar su comprensión. Esto es especialmente importante para aquellas personas que no tienen experiencia en el área o que no están familiarizadas con el lenguaje técnico.

---

<b>Término</b>	<b>Descripción</b>
TVA	Trazabilidad Vinos Ambrosia
SHA-256	Algoritmo que permite encriptar información

---

---

QR	Código de barras bidimensional que permite guardar información
PDF	Portable Document Format, «formato de documento portátil»
PTT	Proyecto de Trabajo de Titulación

---

### **Bibliografía y referencias**

---

<b>Referencia</b>	<b>Título</b>
Anexo 2 (del Documento del Trabajo de Titulación)	Definición de los requerimientos de software.

---

## **Anexo 10.** Pruebas Funcionales

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Versión: 1.0

Fecha: 17/10/2022

## Hoja de control

---

<b>Organismo</b>	Universidad Nacional de Loja		
<b>Proyecto</b>	Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia		
<b>Entregable</b>	Pruebas Funcionales		
<b>Autor</b>	Jimmy Vicente		
<b>Versión/Edición</b>	1.0	<b>Fecha Versión</b>	15/10/2022
<b>Aprobado por</b>	Cristian Ramiro Narváez Guillen, Mg.Sc.	<b>Fecha Aprobación</b>	17/10/2022
		<b>N° Total de Páginas</b>	19

---

## Índice de Contenidos

1. Introducción .....	153
Objeto .....	153
Alcance.....	153
2. Trazabilidad de casos de pruebas – requisitos .....	153
3. Definición de los casos de pruebas .....	153
5. Anexos .....	162
6. Glosario.....	163
7. Bibliografía y referencias.....	163



## Introducción

### Objetivo

El objetivo de este documento es generar casos de prueba que demuestren que el software del módulo cumple con los requisitos. Se requiere una descripción de los casos de prueba, una matriz que describa la relación entre los casos de prueba y los requisitos, y el plan de ejecución de la prueba.

### Alcance

El profesor Ing. Cristián Narváez (director de la TT) es el encargado de validar cada uno de los casos de prueba identificados. Él es un docente que imparte la materia de ingeniería de sistemas y computación en la Universidad Nacional de Loja. Por otro lado, los escenarios de prueba son creados y grabados por Jimmy Vicente, un estudiante del proyecto.

### Trazabilidad de casos de pruebas – requisitos

La relación entre los casos de prueba especificados y los requisitos funcionales de la especificación de requisitos se muestra en la siguiente MATRIZ. Las columnas contienen los requisitos funcionales y las filas cada uno de los casos de prueba definidos. La conexión actual se indica con una "x".

	RF01	RF02	RF03	RF04	RF05	RF06	RF07
CP01	x	x					
CP02	x	x	x				
CP03			x	x	x		
CP04				x	x	x	x
CP05				x	x	x	x

### Definición de los casos de pruebas

Cada caso de prueba que se identificó para confirmar la funcionalidad del sistema se describe en profundidad en esta sección. Además de enumerar las que se deben hacer para garantizar que la DApp se implemente correctamente.

Registrar un TVA	CP01	
	¿Prueba de despliegue?	Sí
<b>Descripción:</b> Se probará la respuesta de la DApp al registrar los procesos de la TVA		
<b>Prerrequisitos</b>		

- Acceder a la página.
- Inicio de sesión y conexión con la wallet de metamask
- Tener acceso a la administración de TVA.

**Pasos:**

1. Presionar en el botón denominado “NUEVO PROCESO”.
2. Completar los campos del proceso “Materia prima”.
3. Completar los campos del proceso “Extracción del mosto”.
4. Completar los campos del proceso “Pasteurización”.
5. Completar los campos del proceso “Fermentación”.
6. Completar los campos del proceso “Clarificación”.
7. Completar los campos del proceso “Trasiego”.
8. Completar los campos del proceso “Envasado”.
9. Esperar Visualizar Trazabilidad de vino Ambrosia (TVA).

**Resultado esperado:**

- Un mensaje de TVA genera correctamente.
- Una notificación indicando que el registro se ha realizado correctamente.

**Resultado obtenido:**

- Formulario para registro de materia prima

The screenshot shows a mobile application interface for a 'Nuevo proceso' (New process) registration. At the top, there is a balance of 99.26337508 ETH and a wallet address. The main title is 'Nuevo proceso' with an 'AGREGAR' button. Below the title is a progress bar with seven steps: 1. Materia Prima (active), 2. Extracción Del Mosto, 3. Pasteurización, 4. Fermentación, 5. Clarificación, 6. Trasiego, and 7. Envasado. The 'Materia Prima' form contains the following fields: 'Nº De Cosecha' (2), 'Lugar De Procedencia' (Majacatos-Loja), 'Nombre Del Propietario' (Pandro Calva), and 'Gastos Brn' (1.5). At the bottom are 'GUARDAR' and 'SALIR' buttons.

- Formulario para registro de extracción del mosto

The screenshot shows the 'Siguiete proceso: Extracción Del Mosto' (Next process: Extraction of the must) registration form. It features the same top navigation and progress bar as the previous form, with 'Extracción Del Mosto' now being the active step. The form contains a single dropdown menu for 'Tipo De Extracción' (Type of Extraction) with 'Pulpado' selected. At the bottom are 'GUARDAR' and 'SALIR' buttons.

- Formulario para registro de Pasteurización.

Balance: 99.26337508 ETH

Dirrección de cuenta: 0a6c508fc598baef740a98d79d25a5cf4c0746e32a

Siguiente proceso: Pasteurización

AGREGAR

Inicio

1 Materia Prima 2 Extracción Del Mosto 3 Pasteurización 4 Fermentación 5 Clarificación 6 Traseigo 7 Envasado

Temperatura Caliente (°C): 20

Temperatura Fría (°C): 12

Tiempo De Proceso (min): 7

GUARDAR SALIR

Fecha de creación: 23/11/2022, 00:17:34

- Formulario para registro de Fermentación.

Balance: 99.26337508 ETH

Dirrección de cuenta: 0a6c508fc598baef740a98d79d25a5cf4c0746e32a

Siguiente proceso: Fermentación

AGREGAR

Inicio

1 Materia Prima 2 Extracción Del Mosto 3 Pasteurización 4 Fermentación 5 Clarificación 6 Traseigo 7 Envasado

Fecha De Inicio De Fermentación: 23/11/2022 00:15

Fecha de Finalización De Fermentación: 04/12/2022 00:15

Grado Inicial(%): 20

GUARDAR SALIR

Fecha de creación: 23/11/2022, 00:17:34

1 Materia prima

No cosecha: 2

- Formulario para registro de Clarificación.

Balance: 99.26337508 ETH

Dirrección de cuenta: 0a6c508fc598baef740a98d79d25a5cf4c0746e32a

Siguiente proceso: Clarificación

AGREGAR

Inicio

1 Materia Prima 2 Extracción Del Mosto 3 Pasteurización 4 Fermentación 5 Clarificación 6 Traseigo 7 Envasado

Turbidez (ppm): 80

GUARDAR SALIR

Tiempo proceso: 7 min

Fecha de creación: 23/11/2022, 00:14:49

2 Extracción del mosto

- Formulario para registro de Traseigo.

Balance: 99.26337508 ETH

Inicio

Dirección de cuenta: 0x4C5098C356Baf748A98d79925A5Cf4d074e832a

### Siguiente proceso: Trasiego

AGREGAR

Materia Prima
  Extracción Del Mosto
  Pasteurización
  Fermentación
  Clarificación
  **Trasiego**
 Envasado

Líquido Claro (%)

Líquido Oscuro (%)

GUARDAR SALIR

Fecha de creación: 23/11/2022, 00:19:37

3 Pasteurización del mosto

Temperatura caliente: 20 °C

- **Formulario para registro de Envasado.**

Balance: 99.26337508 ETH

Inicio

Dirección de cuenta: 0x4C5098C356Baf748A98d79925A5Cf4d074e832a

### Siguiente proceso: Envasado

AGREGAR

Materia Prima
  Extracción Del Mosto
  Pasteurización
  Fermentación
  Clarificación
  Trasiego
  **Envasado**

Número De Lote

Total De Botellas Producidas

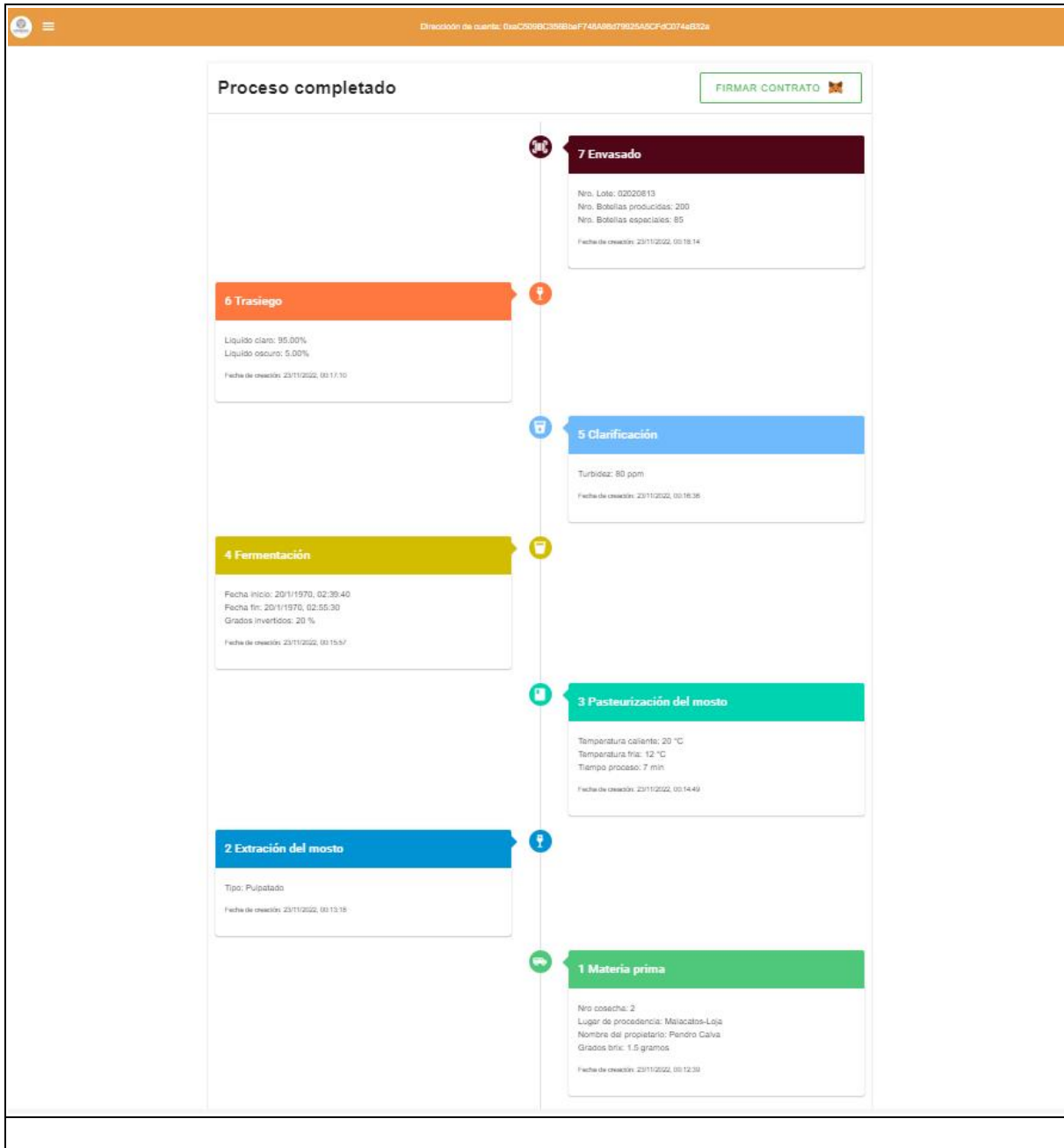
Botellas especiales

GUARDAR SALIR

4 Fermentación

Fecha inicio: 20/11/1970, 02:39:40  
 Fecha fin: 20/11/1970, 02:55:30  
 Grados alcoholicos: 20 %

- **Visualizar Trazabilidad de vino Ambrosia (TVA)**

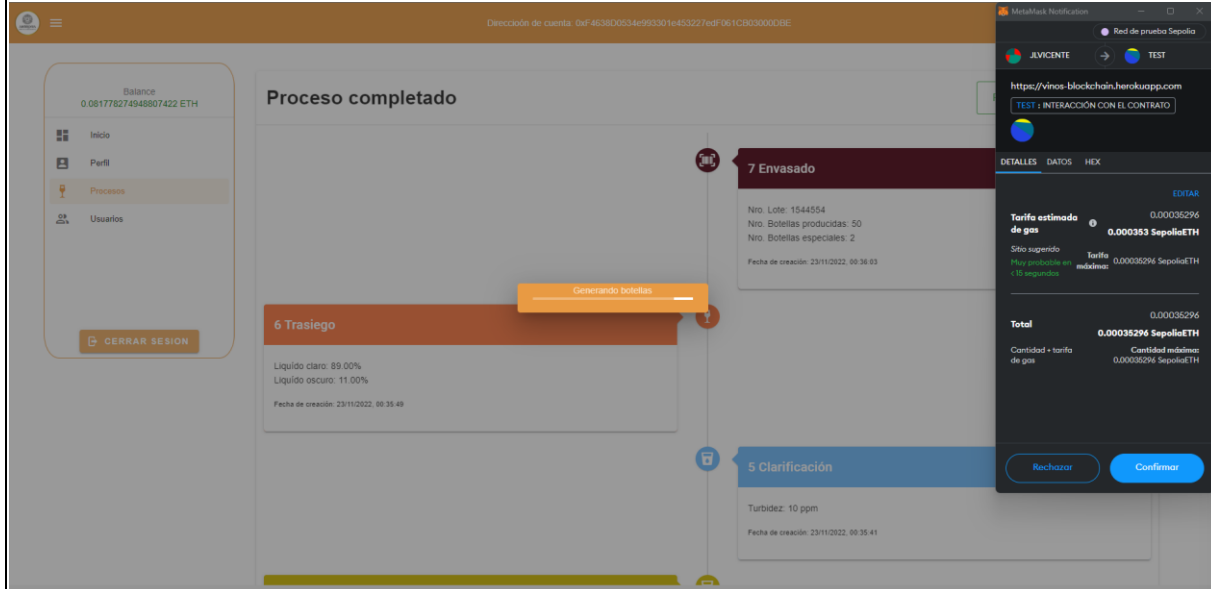


Registrar sha-256 en Blockchain	CP02	
	¿Prueba de despliegue?	Sí
<b>Descripción:</b> Se verificará la funcionalidad de la DApp al registrar el hash SHA-256 de TVA en la cadena de bloques y se evaluará la respuesta obtenida.		
<b>Prerrequisitos</b> <ul style="list-style-type: none"> <li>• Acceder a la página.</li> <li>• Inicio de sesión y conexión con la wallet de metamask</li> <li>• Tener acceso a la administración de TVA.</li> <li>• Tener registrados todos los procesos del TVA.</li> </ul>		
<b>Pasos:</b> <ol style="list-style-type: none"> <li>1. Presionar en el botón denominado “FIRMAR CONTRATO”.</li> <li>2. Validar la transacción en la ventana generada por metamask será el segundo paso a realizar.</li> <li>3. Esperar una notificación de confirmación.</li> </ol>		
<b>Resultado esperado:</b>		

- Ventana emergente de extensión metamask, para confirmar la transacción.
- Vista de espera.
- Una notificación de confirmación de registro con éxito.

**Resultado obtenido:**

- Ventana emergente de extensión metamask, para confirmar la transacción.



- Vista de espera.



- Una notificación de confirmación de registro con éxito..

Balance: 99.26337508 ETH

Inicio  
Perfil  
Procesos  
Usuarios

CERRAR SESION

Dirección de cuenta: 0xaC509BC356BbaF748A98d79925A5CFdC074aB32a

Proceso aprobado con éxito

### Proceso firmado

0x8c9a721f8bct2014932e9033e0764e486a65680ctc72729178806ed7d\_2

**BOTELLAS PRODUCIDAS**

**7 Envasado**

Nro. Lote: 10  
Nro. Botellas producidas: 10  
Nro. Botellas especiales: 1  
Fecha de creación: 22/11/2022, 21:43:32

**6 Trasiego**

Líquido claro: 80.00%  
Líquido oscuro: 20.00%  
Fecha de creación: 22/11/2022, 21:43:22

Visualizar botellas producidas	CP03	
	¿Prueba de despliegue?	Sí

**Descripción:**  
Se probará la respuesta de la DApp cuando se visualice la trazabilidad de las botellas producidas.

- Prerrequisitos**
- Acceder a la página.
  - Inicio de sesión y conexión con la wallet de metamask
  - Tener acceso a la administración de TVA.
  - Tener registrados todos los procesos del TVA.

- Pasos:**
1. Presionar en el botón “BOTELLAS PRODUCIDAS”.
  2. Presionar en el botón “IMPRIMIR”.

- Resultado esperado:**
- Vista de la TVA de las botellas producidas.
  - Vista de PDF con los QRS de la TVA de las botellas producidas.

- Resultado obtenido:**
- Vista de la TVA de las botellas producidas.

Balance: 99.26337508 ETH

Inicio  
Perfil  
Procesos  
Usuarios

CERRAR SESION

Dirección de cuenta: 0xaC509BC356BbaF748A98d79925A5CFdC074aB32a

Lote: 45212452  
Nro. Botellas producidas: 5000

Nro. Botellas especiales: 200      Nro. Botellas vendidas: 0      Nro. Tokens asignados: 0

IMPRIMIR

Nro botella: 1  
Hash: 0x6378b041ee90a5934a8ed34  
Empaquetado

Nro botella: 2  
Hash: 0x6378b041ee90a5934a8ed37  
Empaquetado

Nro botella: 3  
Hash: 0x6378b041ee90a5934a8ed3a  
Empaquetado

Nro botella: 4  
Hash: 0x6378b041ee90a5934a8ed3d  
Empaquetado

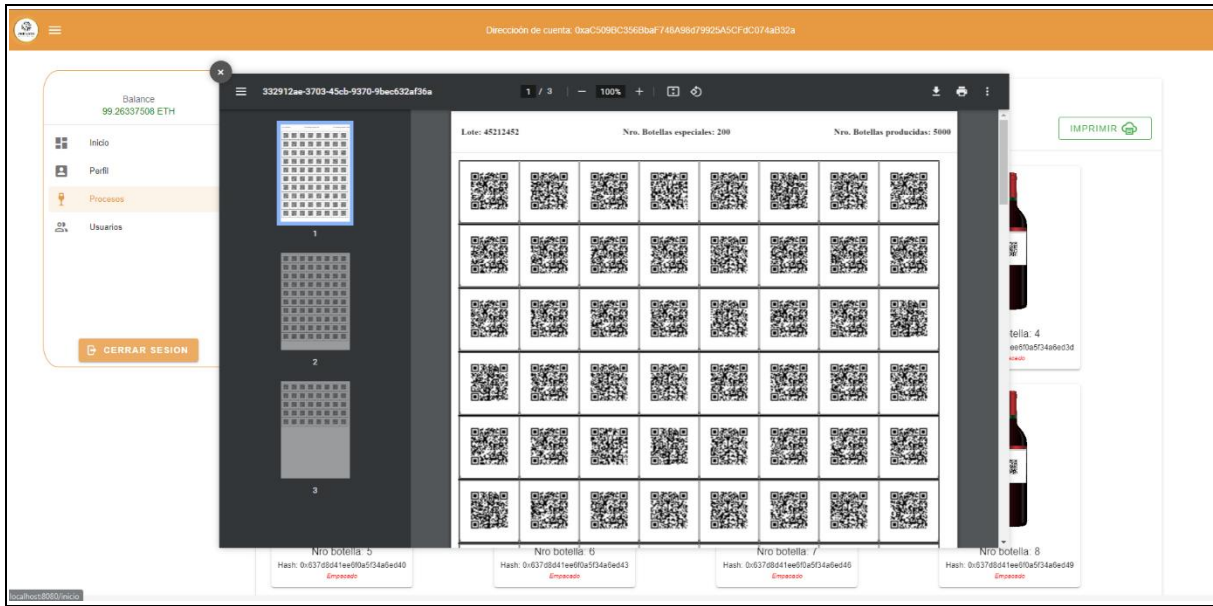
Nro botella: 5  
Hash: 0x6378b041ee90a5934a8ed40  
Empaquetado

Nro botella: 6  
Hash: 0x6378b041ee90a5934a8ed43  
Empaquetado

Nro botella: 7  
Hash: 0x6378b041ee90a5934a8ed46  
Empaquetado

Nro botella: 8  
Hash: 0x6378b041ee90a5934a8ed49  
Empaquetado

- Vista de PDF con los QRS de la TVA de las botellas producidas.



Validar con un QR válido	CP04	
	¿Prueba de despliegue?	Sí
<b>Descripción:</b> Se probará la respuesta de la DAPP al validar un QR con un sha-256 correcto		
<b>Prerrequisitos</b> <ul style="list-style-type: none"> <li>• Acceder a la página.</li> <li>• Inicio de sesión y conexión con la wallet de metamask</li> <li>• Tener un código QR para leer.</li> </ul>		
<b>Pasos:</b> <ol style="list-style-type: none"> <li>1. Hacer clic en el botón “LEER QR” disponible en la página principal.</li> <li>2. Leer código QR con la cámara.</li> </ol>		
<b>Resultado esperado:</b> <ul style="list-style-type: none"> <li>• Visualizar una notificación indicando que la botella fue encontrada.</li> <li>• Visualizar información de TVA de la botella correspondiente.</li> </ul>		
<b>Resultado obtenido:</b>		




Trazabilidad Vinos Ambrosia

✔ Botella encontrada

### Información

Trazabilidad de la botella Nro: 1



Información botella

Transaccion Hash:  
[0xa35729ad92f2e4524f6dc24b711b36aefc5573499a6535c479b9ee26047036](#)  
[26047036](#)

Firma de proceso:  
 0081b0f450135c509e207192df31e70f0ed19bd8408f020c9ff4180620265e

Nro Lote: 02020813

Nro botella: 1

Hash: 0xb37dad190b2f8ea37be3fe3c

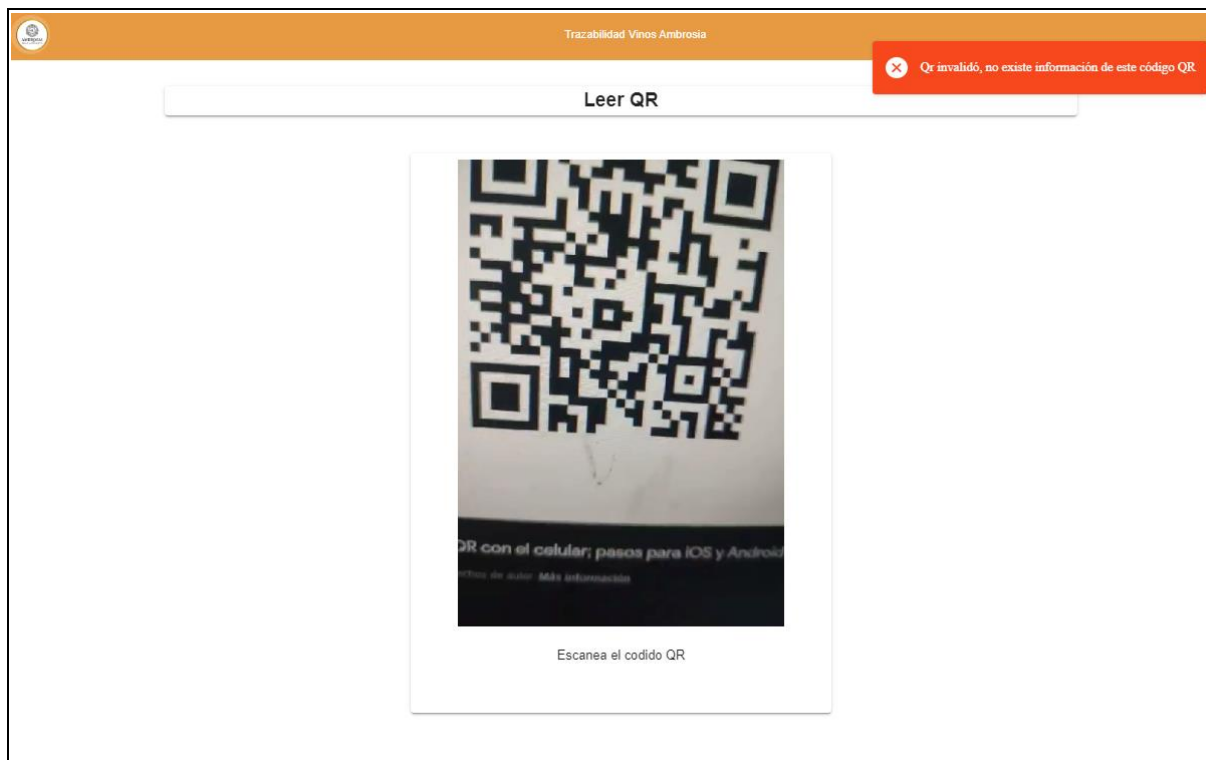
Estado de botella

Empacado:  
 0xa9c909bc3598ba748a98d70025a5cfd007494b32a  
 23/11/2022, 00:18:17

Acciones

CONECTAR

<b>Validar con un QR incorrecto</b>	<b>CP05</b>	
	<b>¿Prueba de despliegue?</b>	<b>Sí</b>
<b>Descripción:</b>		
Se probará la respuesta de la DApp al validar un QR con un sha-256 incorrecto		
<b>Prerrequisitos</b>		
<ul style="list-style-type: none"> <li>Acceder a la página.</li> <li>Inicio de sesión y conexión con la wallet de metamask</li> <li>Tener un código QR para leer.</li> </ul>		
<b>Pasos:</b>		
<ol style="list-style-type: none"> <li>3. Hacer clic en el botón “LEER QR” disponible en la página principal.</li> <li>1. Leer código QR con la cámara.</li> </ol>		
<b>Resultado esperado:</b>		
<ul style="list-style-type: none"> <li>Visualizar notificación indicando que el QR es invalido.</li> </ul>		
<b>Resultado obtenido:</b>		



## Anexos

La Figura 1 muestra varias transacciones realizadas en la red de prueba, cada una de las cuales incluye información detallada, como el número de bloque, la dirección del remitente y del destinatario, la cantidad de ethers transferidos y la tarifa de gas utilizada. Estos detalles permiten a los usuarios realizar un seguimiento completo de las transacciones y garantizar la transparencia y la seguridad de la plataforma.

**Etherscan**  
Sepolia Testnet Network

Contract: `0xFfb9cF59d4Ba086B48DA90EC497a5315Be09AEd2`

Balance: 0 Ether

More Info: My Name Tag: Not Available; Contract Creator: `0xf4638d0534e993301e...` at tx `0x0a194b77c22206d701...`

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
<a href="#">0xc6ec8219472e82acc2...</a>	<code>0x2d4adc9</code>	2341616	44 mins ago	<code>0xf4638d0534e993301e...</code>	<code>0xfbb9cf59d4ba086b48d...</code>	0 Ether	0.00028237
<a href="#">0xc0ac379de8a7ea8a30...</a>	<code>0x2d4adc9</code>	2340714	4 hrs 9 mins ago	<code>0xf4638d0534e993301e...</code>	<code>0xfbb9cf59d4ba086b48d...</code>	0 Ether	0.00028237
<a href="#">0xbaba5289d27988a073...</a>	<code>0x2d4adc9</code>	2164946	27 days 15 hrs ago	<code>0xb7216579a6b1dc25c8...</code>	<code>0xfbb9cf59d4ba086b48d...</code>	0 Ether	0.00028237
<a href="#">0x34f1402a4d97cc9a40...</a>	<code>0x2d4adc9</code>	2128023	33 days 8 hrs ago	<code>0xf4638d0534e993301e...</code>	<code>0xfbb9cf59d4ba086b48d...</code>	0 Ether	0.00028237
<a href="#">0x0a194b77c22206d701...</a>	<code>0x60806040</code>	2127883	33 days 9 hrs ago	<code>0xf4638d0534e993301e...</code>	Contract Creation	0 Ether	0.00066233

[Download CSV Export]

Figura 1. Trazabilidad del contrato inteligente en Etherscan Sepolia.

La Figura 2 presentada muestra información estadística sobre el uso de la testnet de Sepolia en Infura. En esta gráfica se puede visualizar claramente la cantidad de transacciones realizadas en la red durante un periodo de tiempo determinado. Es importante destacar que dicha información puede ser de gran utilidad para los desarrolladores, ya que les permite conocer el comportamiento de la red y ajustar sus aplicaciones en consecuencia.

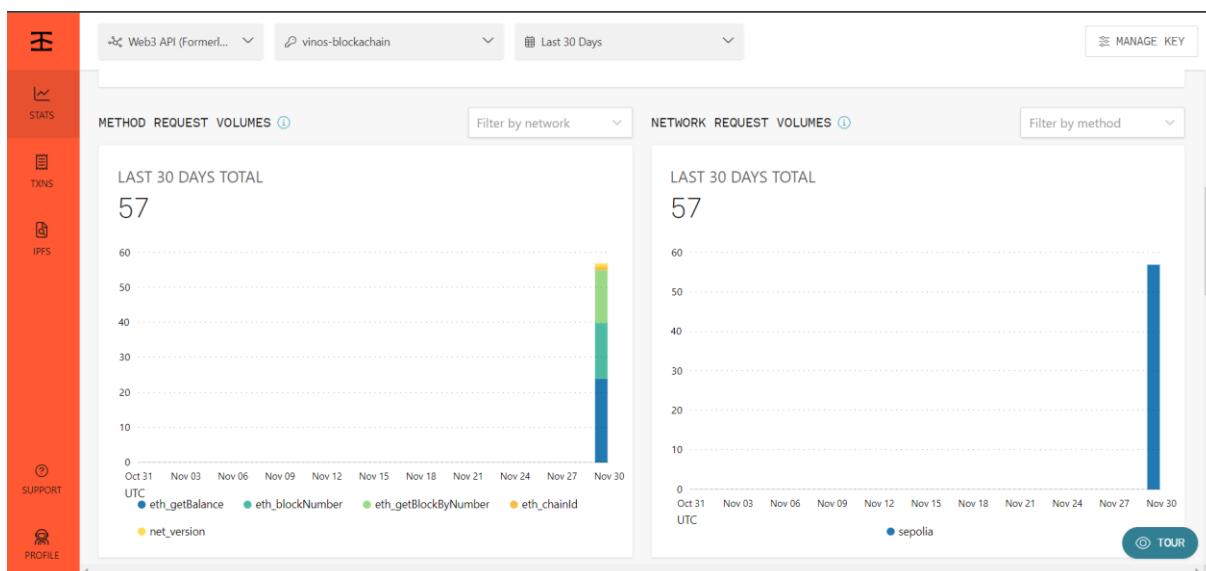


Figura 2. Estadística del uso de la testnet en Infura en el testnet de Sepolia.

## Glosario

En esta sección, se detallan y explican los términos técnicos, acrónimos o jerga utilizados en el documento con el fin de facilitar su comprensión. Esto es especialmente importante para aquellas personas que no tienen experiencia en el área o que no están familiarizadas con el lenguaje técnico.

Término	Descripción
TVA	Trazabilidad Vinos Ambrosia
SHA-256	Algoritmo que permite encriptar información
QR	Código de barras bidimensional que permite guardar información
PDF	Portable Document Format, «formato de documento portátil»
PTT	Proyecto de Trabajo de Titulación

## Bibliografía y referencias

Referencia	Título
Ref. 1	Anexo 2 Especificación de Requisitos del Sistema
Ref. 2	Anexo 9 Plan de pruebas de integración

## **Anexo 11. Pruebas de Aceptación**

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Versión: 1.0

Fecha: 02/11/2022

## Hoja de control

<b>Organismo</b>	Universidad Nacional de Loja		
<b>Proyecto</b>	Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia		
<b>Entregable</b>	Pruebas de Aceptación		
<b>Autor</b>	Jimmy Vicente		
<b>Versión/Edición</b>	1.0	<b>Fecha Versión</b>	01/11/2022
<b>Aprobado por</b>	Cristian Ramiro Narváez Guillen, Mg.Sc.	<b>Fecha Aprobación</b>	02/11/2022
		<b>N° Total de Páginas</b>	11

## Índice de Contenidos

1. Introducción .....	164
Objeto .....	164
Propósito.....	164
2. Parámetros de evaluación .....	164
3. Encuesta .....	165
4. Bibliografía y referencias.....	168

## Introducción

### Objetivo

El objetivo de este documento es recopilar datos (a través de una encuesta) que confirmen el funcionamiento y los requisitos de la DApp mediante la aceptación de una muestra de su personal administrativo y clientes de Vinos Ambrosia.

### Propósito

Mediante el uso de encuestas, una muestra de empleados y clientes de Vinos Ambrosia puede confirmar que la DApp que utiliza la tecnología blockchain para la trazabilidad de la producción de vino tiene la aceptación necesaria.

### Parámetros de evaluación

Nro.	Pregunta
1	¿El lenguaje utilizado es fácil de entender?
2	¿Se otorga un tiempo adecuado para introducir la información mediante el teclado o la cámara?
3	¿Es comprensible tanto la interfaz como su contenido?
4	¿La interfaz está diseñada de manera que las tareas sean lo más fáciles posible de realizar?
5	¿Son adecuados los mensajes que muestra el sistema?
6	¿El sistema toma medidas para prevenir errores?
7	¿El sistema brinda una explicación clara sobre los errores que se presentan?
8	¿Facilita la navegación dentro del sistema y su salida de manera sencilla?
9	¿La información presentada al usuario es relevante y se enfoca solamente en lo que necesita saber?

Así mismo, se plantea una tabla para determinar el estado de las Pruebas de Aceptación:

Estado de las Pruebas de Aceptación	Criterio		
	Sí	Parcialmente	No
Afirmativo	$\geq 85\%$	$\leq 15\%$	$< 1\%$
Negativo	$< 85\%$	$> 15\%$	$> 1\%$

## Encuesta

El propósito de la encuesta es determinar si la DApp basada en tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia cumple con los requisitos y el funcionamiento aceptable para una muestra de 83 personas, entre administrativos y clientes de Vinos Ambrosia. Se utilizó un formulario de Google para recopilar los datos y se presentaron los resultados en gráficos generados automáticamente.

¿El lenguaje utilizado es fácil de entender?

83 respuestas

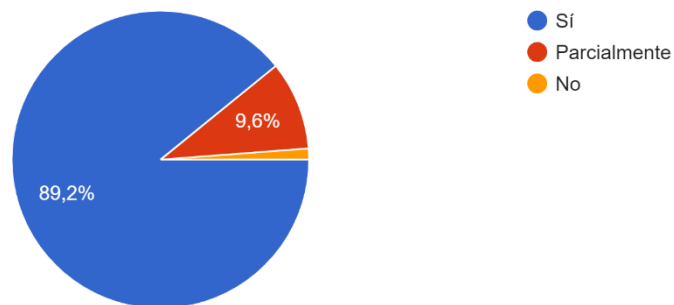


Figura 1. Resultado de pregunta número 1.

¿Se otorga un tiempo adecuado para introducir la información mediante el teclado o la cámara?

83 respuestas

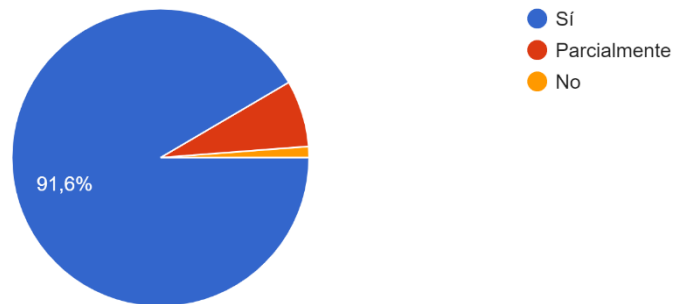


Figura 2. Resultado de pregunta número 2.



¿Es comprensible tanto la interfaz como su contenido?

83 respuestas

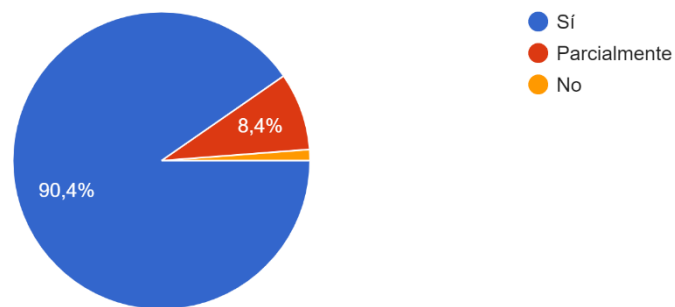


Figura 3. Resultado de pregunta número 3.

¿La interfaz está diseñada de manera que las tareas sean lo más fáciles posible de realizar?

83 respuestas

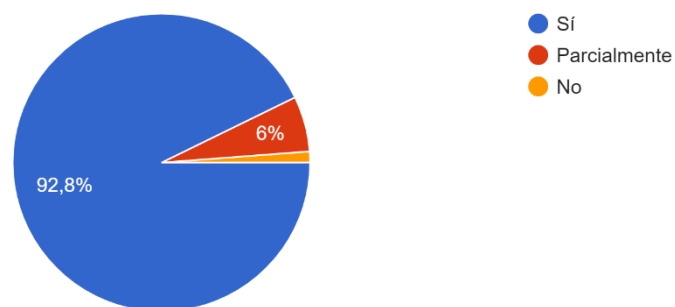


Figura 4. Resultado de pregunta número 4.

¿Son adecuados los mensajes que muestra el sistema?

83 respuestas

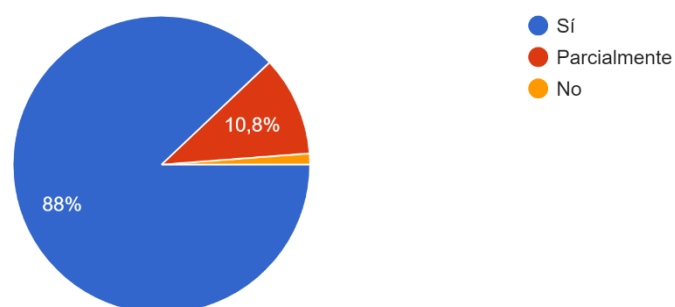


Figura 5. Resultado de pregunta número 5.

¿El sistema toma medidas para prevenir errores?  
83 respuestas

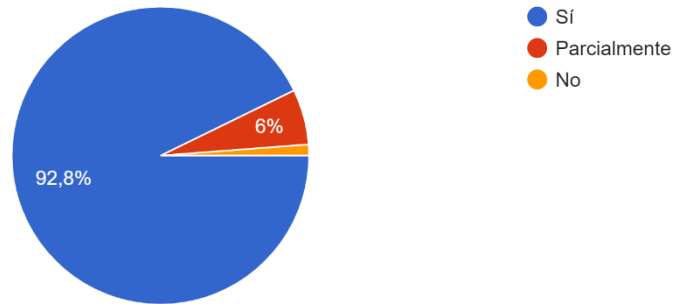


Figura 6. Resultado de pregunta número 6.

¿El sistema brinda una explicación clara sobre los errores que se presentan?  
83 respuestas

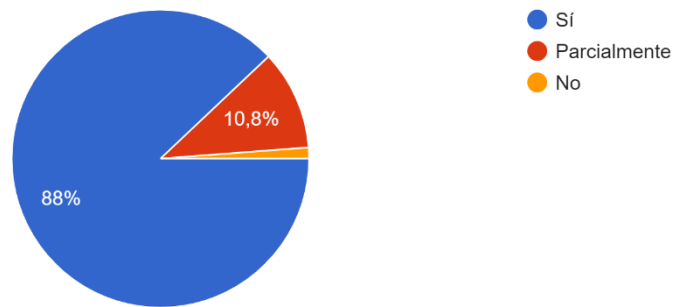


Figura 7. Resultado de pregunta número 7.

¿Facilita la navegación dentro del sistema y su salida de manera sencilla?  
83 respuestas

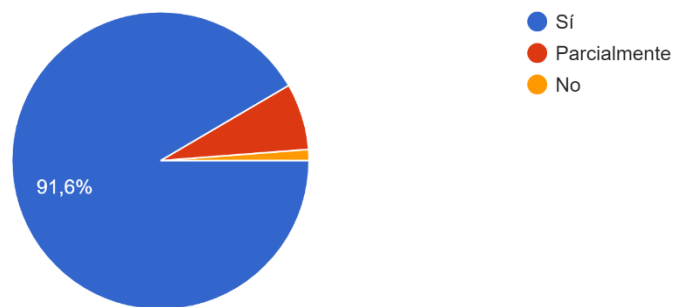


Figura 8. Resultado de pregunta número 8.

¿La información presentada al usuario es relevante y se enfoca solamente en lo que necesita saber?

83 respuestas

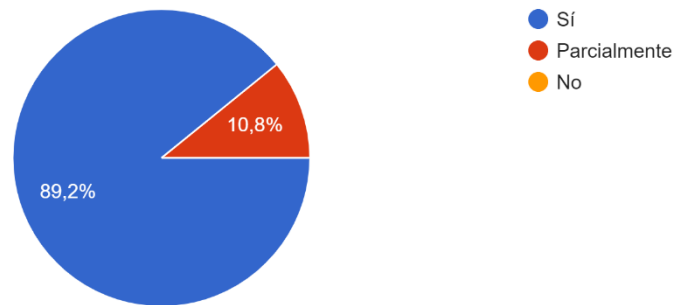


Figura 9. Resultado de pregunta número 9.

## Bibliografía y referencias

---

Referencia	Título
Anexo 2 (del Documento del Trabajo de Titulación)	Definición de los requerimientos de software.

---

## **Anexo 12.** Manual de Usuario

**Proyecto:** Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia

Versión: 1.0

Fecha: 24/11/2022

## Hoja de control

<b>Organismo</b>	Universidad Nacional de Loja		
<b>Proyecto</b>	Implementación de una DApp con tecnología blockchain para la trazabilidad de la producción de vinos Ambrosia.		
<b>Entregable</b>	Manual de Usuario		
<b>Autor</b>	Jimmy Vicente		
<b>Versión/Edición</b>	2.0	<b>Fecha Versión</b>	23/11/2022
<b>Aprobado por</b>	Cristian Ramiro Narváez Guillen, Mg.Sc.	<b>Fecha Aprobación</b>	24/11/2022
		<b>N° Total de Páginas</b>	16

## Índice de Contenidos

<b>Introducción.....</b>	<b>172</b>
<b>Requisitos.....</b>	<b>172</b>
<b>Ingreso al Sistema .....</b>	<b>172</b>
<b>Ingresar a la Administración de TVA (Trazabilidad Vinos Ambrosia) .....</b>	<b>178</b>
<b>Registrar un TVA (Trazabilidad Vinos Ambrosia) .....</b>	<b>179</b>
<b>Generar PDF de los códigos QR .....</b>	<b>184</b>
<b>Agregar un usuario .....</b>	<b>185</b>
<b>Leer código QR de una botella.....</b>	<b>186</b>

## **Introducción**

El manual de usuario es una guía detallada que tiene como objetivo explicar a los usuarios cómo utilizar la DApp de trazabilidad de la producción de vinos Ambrosia. Dado que la DApp se basa en la tecnología blockchain, el manual también proporciona una breve introducción sobre la blockchain y cómo funciona.

El manual comienza con una descripción general de la DApp, incluyendo sus características y funciones. Luego, se proporcionan instrucciones detalladas sobre cómo utilizar la DApp en el navegador web, y cómo conectarse a la red blockchain testnet. Además, el manual también aborda la utilización de la wallet de Metamask para realizar transacciones en la blockchain, así como la importancia de la seguridad y la privacidad al utilizar la DApp.

## **Requisitos**

La DApp de trazabilidad de la producción de vinos Ambrosia, desarrollada con tecnología blockchain, es compatible con diferentes navegadores:

- Chrome.
- Brave.
- Navegador de la aplicación móvil Metamask.

Para utilizar la DApp de trazabilidad de producción de vinos Ambrosia en los navegadores Chrome, Mozilla Firefox y Brave, es necesario instalar la extensión MetaMask y crear o iniciar sesión en una cuenta. También se debe obtener fondos a través de una Ethereum Sepolia Faucet, la cual se puede encontrar en la página web mediante la pregunta 4 en el siguiente enlace: <https://vinos-blockchain.herokuapp.com/informacion> o acceder directamente a la página de Sepolia Faucet en <https://faucet.sepolia.dev>

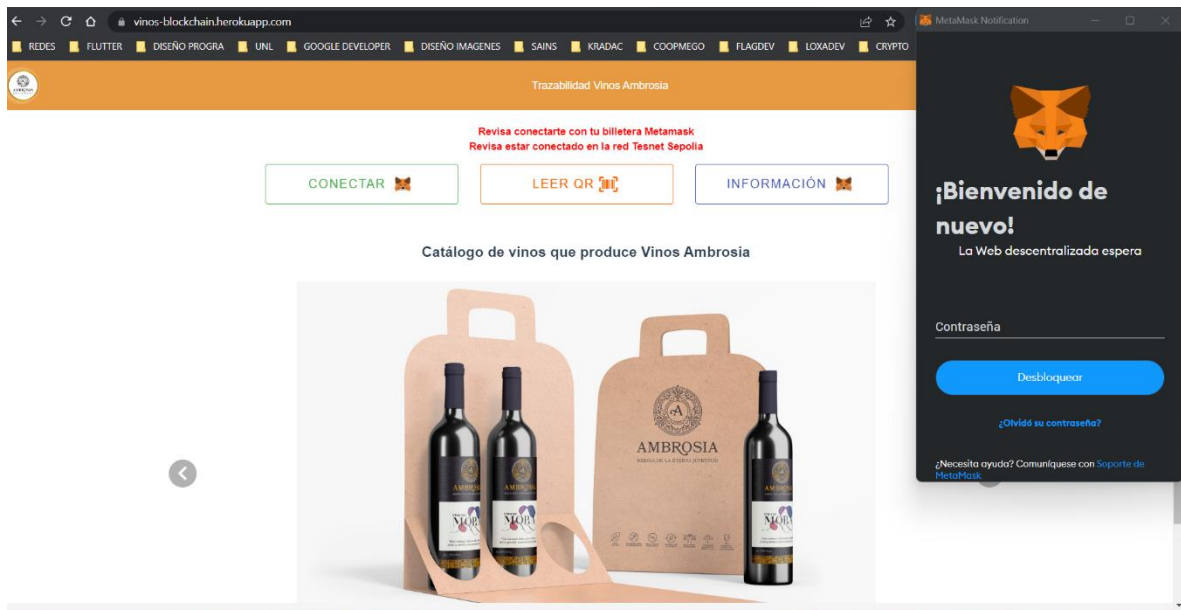
**NOTA:** Disponer de fondos es esencial para llevar a cabo las transacciones.

## **Ingreso al Sistema**

### **A través de un navegador web:**

1. Se debe acceder a la dirección web <https://vinos-blockchain.herokuapp.com> después de haber instalado la extensión correspondiente en el navegador seleccionado.
2. La extensión MetaMask generará una ventana automáticamente al cargar la página, tal

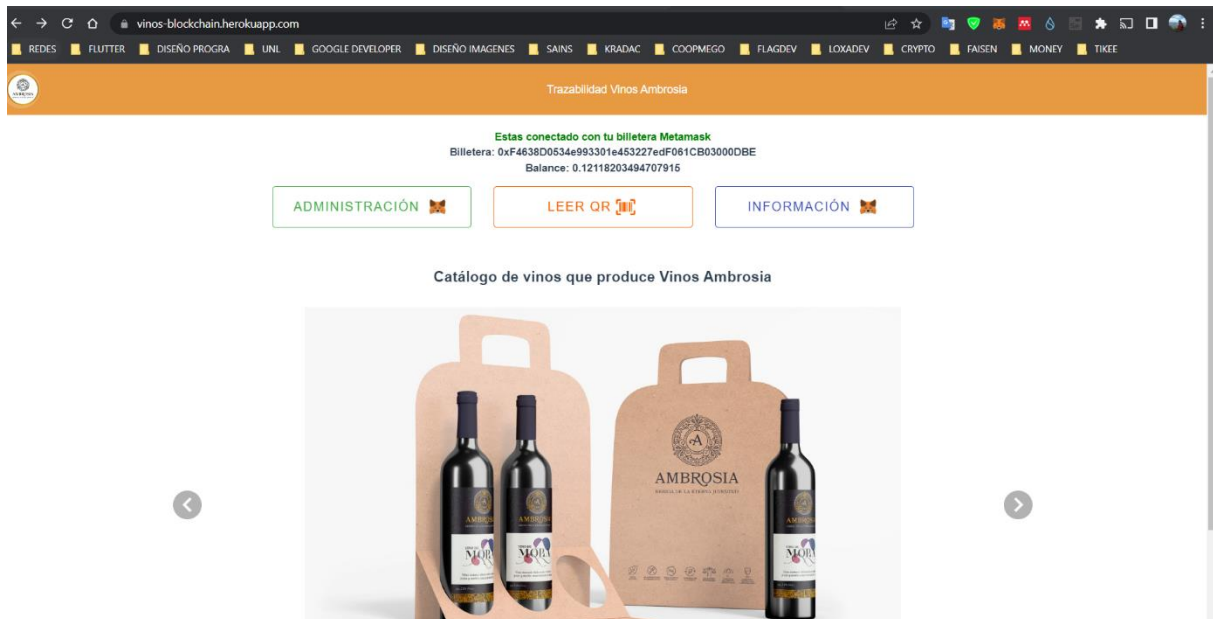
como se muestra en la siguiente imagen.



Se debe introducir la contraseña correspondiente en la ventana de la extensión de MetaMask o importar la frase de recuperación si es necesario.

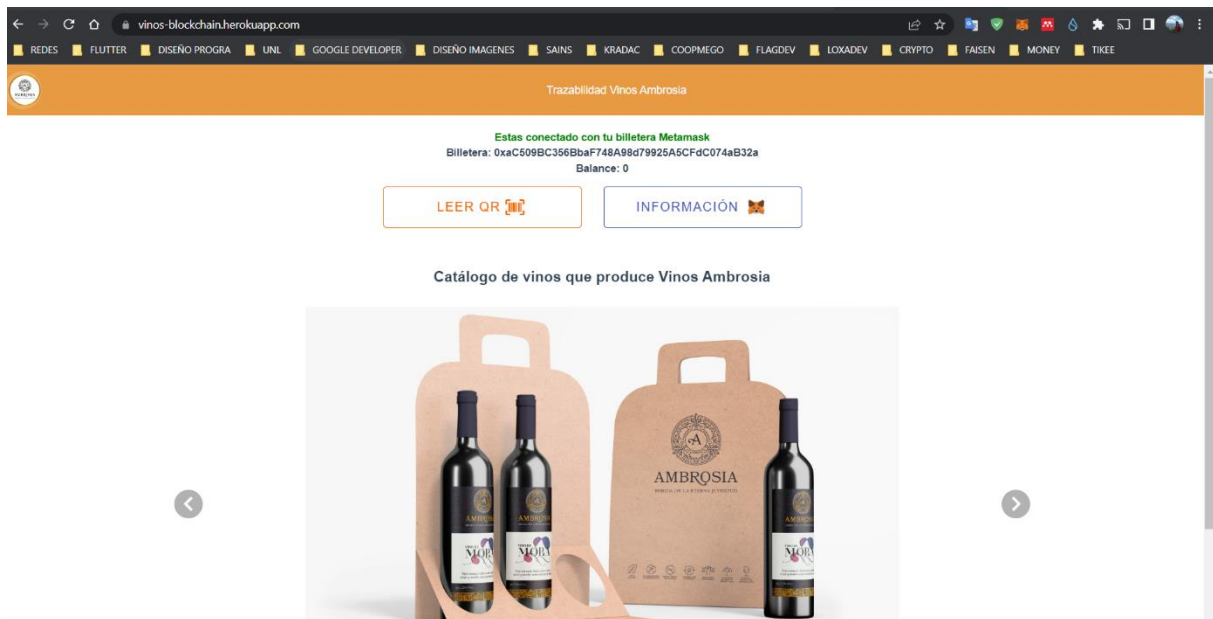
3. Después de ingresar la contraseña correctamente, la DApp presentará dos tipos de vistas que permitirán la gestión de: ADMINISTRAR, LEER QR, INFORMACIÓN según los permisos que tenga la cuenta:
  - 3.1. Si puede registrar y administrar la TVA (Trazabilidad Vinos Ambrosia), se mostrará la siguiente vista:



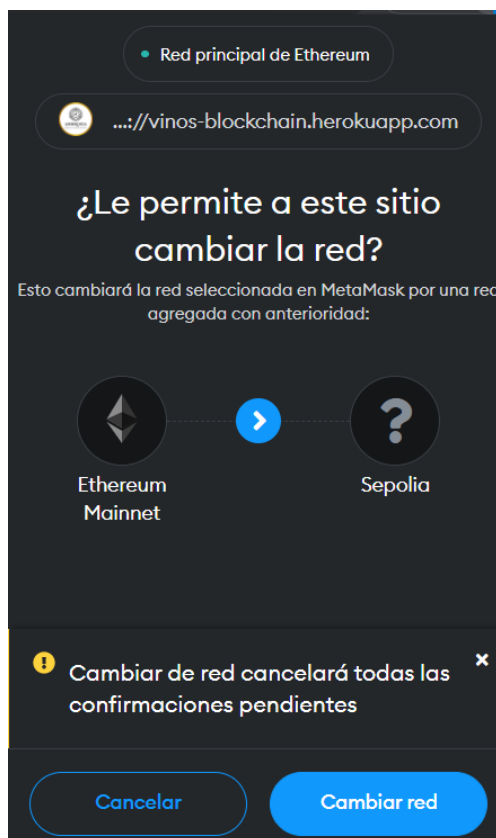


Se observará un botón de administración que le permitirá administrar la TVA (Trazabilidad Vinos Ambrosia).

3.2. Si no tiene permiso o no está conectado con una wallet solo le permitirá LEER QR y obtener información de la página:



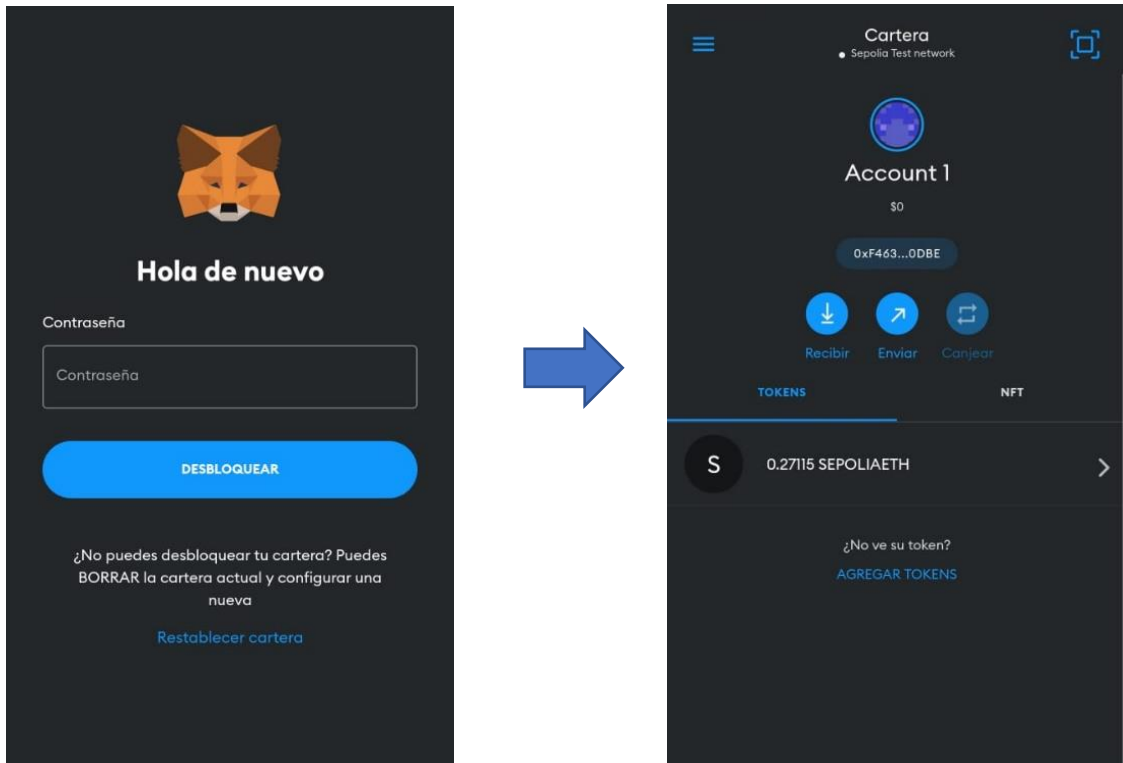
**NOTA:** Es fundamental que en ambas situaciones, la extensión de MetaMask se encuentre conectada a la red de pruebas **Sepolia Testnet** o si no se mostrará una notificación de MetaMask donde le permita confirmar cambiar de red como se muestra a continuación.




Debe confirmar que está conectado a la red de Sepolia caso contrario no le permitirá realizar las acciones de Administración

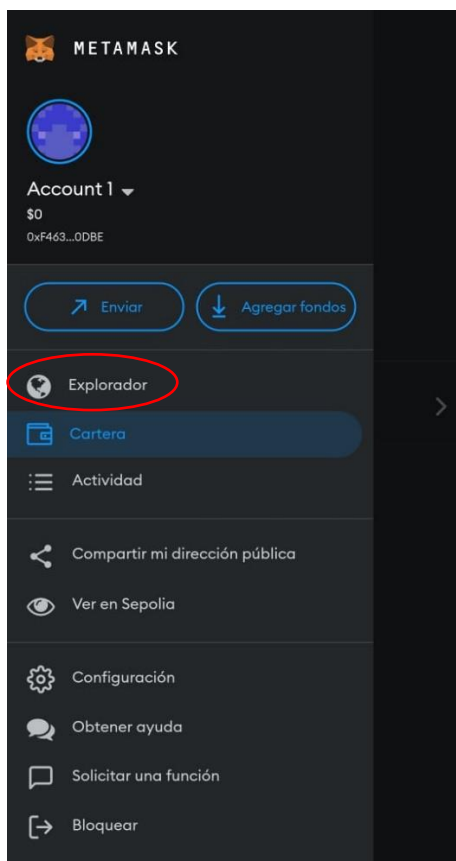
#### **A través de la app móvil de MetaMask:**

1. Abra la aplicación móvil e inicie sesión con su huella digital (si esta opción está activa) o su contraseña, como se muestra en la imagen.

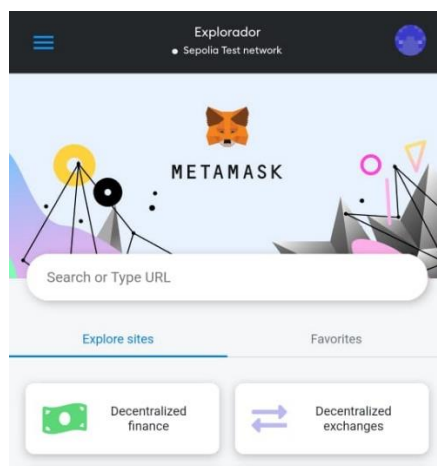


**NOTA:** Se recomienda comprobar que la red de **Sepolia Test Network** esté seleccionada en la parte superior de la sección de Cartera, para evitar problemas en el futuro.

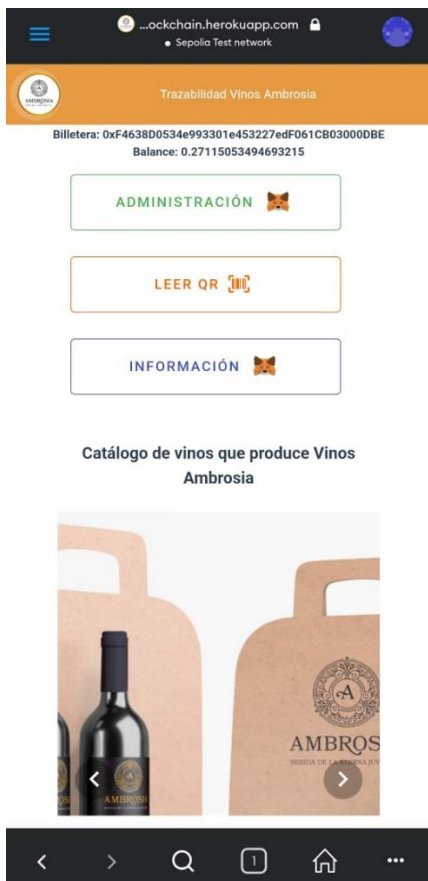
2. Pulsar sobre  se muestra un menú con diferentes opciones, ahí se debe pulsar la opción **“Explorador”**:



3. Se debe ingresar la dirección web <https://vinos-blockchain.herokuapp.com> en la barra de búsqueda "Search or Type URL" para acceder al sitio web correspondiente.




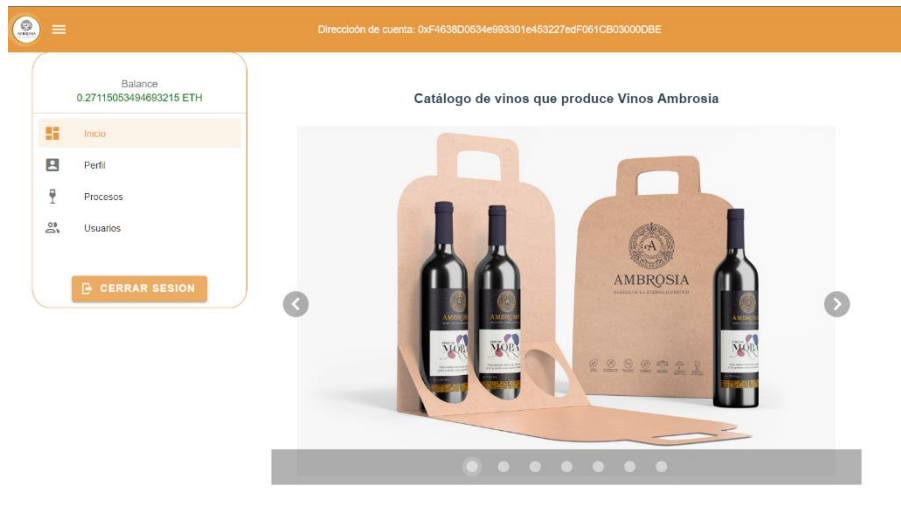
4. Al presentar la página se presentará dos tipos de vistas que le permitirá ADMINISTRAR, LEER QR, INFORMACIÓN según los permisos que tenga la cuenta:  
Si puede administrar un TVA, la vista de la izquierda se observa tres botones que le permiten navegar. Si solo puede LEER QR se muestra en la vista de la derecha:



**NOTA:** Los siguientes pasos explicarán cómo administrar un TVA y cómo leer un código QR. A partir de este punto, las instrucciones se presentarán en un navegador web, pero el proceso es el mismo en la aplicación móvil.


### Ingresar a la Administración de TVA (Trazabilidad Vinos Ambrosia)

1. Hacer clic sobre  y se observa la siguiente interfaz de administración:




### Registrar un TVA (Trazabilidad Vinos Ambrosia)

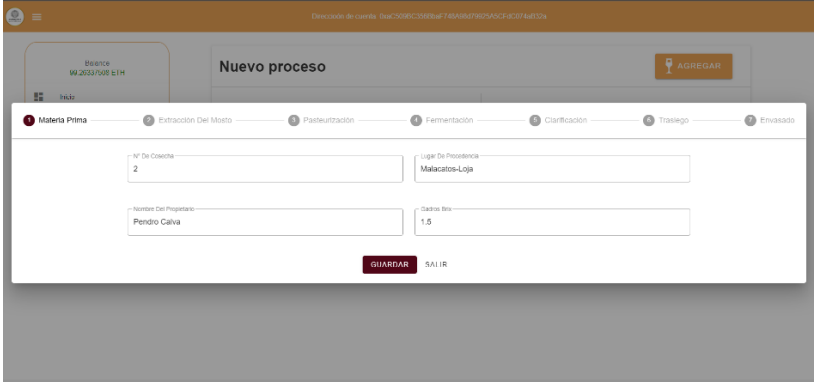
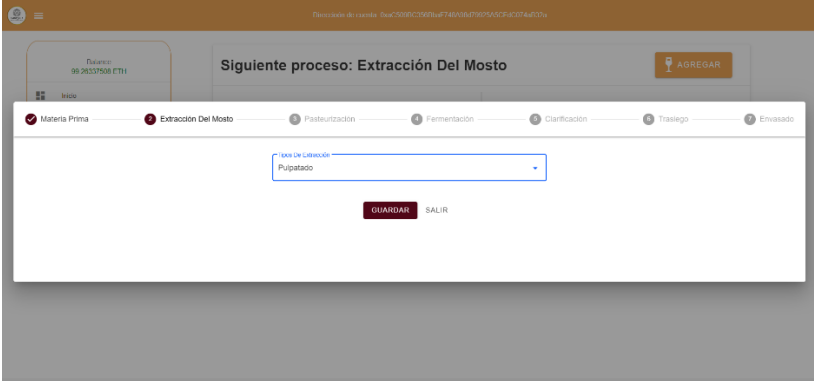
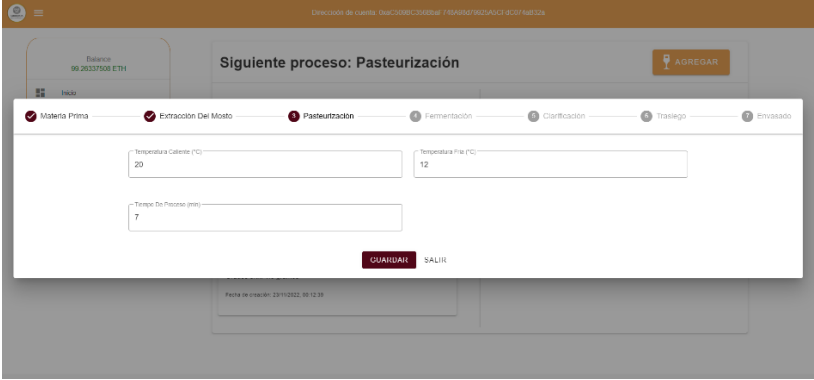
La funcionalidad que se presenta permite el registro de procesos en la red Blockchain de Ethereum en la Sepolia Test Network.

1. Hacer clic sobre  **Procesos** y se observa la siguiente interfaz de lista de procesos:

Procesos		NUEVO PROCESO		Buscar			
Materia Prima (Nro Cosecha)	Extracción Del Mosto (tipo)	Pasteurización (Tem Caliente)	Fermentación (Grados invertidos)	Clarificación (Turbidez)	Trasiego (Rendimineto)	Envasado (Nro botellas)	Estado
1 ✓	Licuada ✓	45 °C ✓	10 % ✓	10 ppm ✓	45.00 % ✓	10 ✓	Aprobado ✓
7868001185026 ✓	Pulpatado ✓	20 °C ✓	20 % ✓	80 ppm ✓	95.00 % ✓	4 ✓	Aprobado ✓
123456 ✓	Pulpatado ✓	45 °C ✓	10 % ✓	10 ppm ✓	80.00 % ✓	5000 ✓	Aprobado ✓
1123456 ✓	Licuada ✓	10 °C ✓	10 % ✓	10 ppm ✓	89.00 % ✓	50 ✓	Aprobado ✓
3 ✓	Pulpatado ✓	45 °C ✓	10 % ✓	10 ppm ✓	98.00 % ✓	200 ✓	Aprobado ✓

Rows per page: 10 1-5 of 5

2. Hacer clic sobre  **NUEVO PROCESO** y a continuación debe agregar cada uno de los procesos del TVA como se muestra a continuación:

Proceso	Interfaz
Formulario para registro de materia prima	
Formulario para registro de extracción del mosto	
Formulario para registro de Pasteurización.	

Formulario para registro de Fermentación.

Balance: 99.26337508 ETH

Siguiente proceso: Fermentación

Materia Prima

Extracción Del Mosto

Pasteurización

Fermentación

Clarificación

Trasego

Envasado

Fecha de Inicio De Fermentación: 23/11/2022 00:15

Fecha de Finalización De Fermentación: 04/12/2022 00:15

Grados alcoholícos: 20

GUARDAR SALIR

1 Materia prima

Formulario para registro de Clarificación.

Balance: 99.26337508 ETH

Siguiente proceso: Clarificación

Materia Prima

Extracción Del Mosto

Pasteurización

Fermentación

Clarificación

Trasego

Envasado

Turbador (ppm): 60

GUARDAR SALIR

2 Extracción del mosto

Formulario para registro de Trasego.

Balance: 99.26337508 ETH

Siguiente proceso: Trasego

Materia Prima

Extracción Del Mosto

Pasteurización

Fermentación

Clarificación

Trasego

Envasado

Líquido Claro (%): 95

Líquido Oscuro (%): 5

GUARDAR SALIR

3 Pasteurización del mosto

Formulario para registro de Envasado.

Balance: 99.26337508 ETH

Siguiente proceso: Envasado

Materia Prima

Extracción Del Mosto

Pasteurización

Fermentación

Clarificación

Trasego

Envasado

Número De Lot: 02020813

Total De Botellas Producidas: 200

Botellas especiales: 50

GUARDAR SALIR

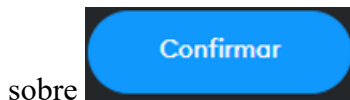
4 Fermentación



3. Presionar sobre **FIRMAR CONTRATO** y presenta lo siguiente:



4. En la ventana emergente de la extensión de MetaMask leer la información y presionar



**NOTA:** Es necesario que la cuenta tenga un balance de fondos suficiente, de lo contrario, el botón correspondiente no estará disponible para su uso.



**Proceso firmado**


Al presionar sobre [0xaC509BC356BbaF74BA98c79925A5CFdC074aB32a](https://vino-blockchain.herokuapp.com/tx/0xaC509BC356BbaF74BA98c79925A5CFdC074aB32a) se le redirigirá a una ventana en su navegador

donde podrá visualizar todos los detalles de la transacción.

The screenshot displays the Etherscan interface for a contract on the Sepolia Testnet Network. The contract address is 0xFb9cF59d4Ba086B48DA90EC497a5315Be09AEd2. The contract overview shows a balance of 0 Ether. The 'More Info' section indicates that the My Name Tag is 'Not Available' and the Contract Creator is 0xf4638d0534e993301e... at transaction 0x0a194b77c22206d701... The 'Transactions' tab is active, showing a list of 5 transactions. The table below provides details for each transaction, including the Txn Hash, Method, Block, Age, From, To, Value, and Txn Fee.


Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0xc6ec8219472e82acc2...	0x294abcd9	2341616	44 mins ago	0xf4638d0534e993301e...	0xfbf9cf59d4ba086b48d...	0 Ether	0.00028237
0xc0ac379de8a7ea8a30...	0x294abcd9	2340714	4 hrs 9 mins ago	0xf4638d0534e993301e...	0xfbf9cf59d4ba086b48d...	0 Ether	0.00028237
0xbaba5289d27988a073...	0x294abcd9	2164946	27 days 15 hrs ago	0xb7216579a6b1dc25c8...	0xfbf9cf59d4ba086b48d...	0 Ether	0.00028237
0x34f1402a4d97cc9a40...	0x294abcd9	2128023	33 days 8 hrs ago	0xf4638d0534e993301e...	0xfbf9cf59d4ba086b48d...	0 Ether	0.00028237
0x0a194b77c22206d701...	0x60006040	2127883	33 days 9 hrs ago	0xf4638d0534e993301e...	Contract Creation	0 Ether	0.00086233

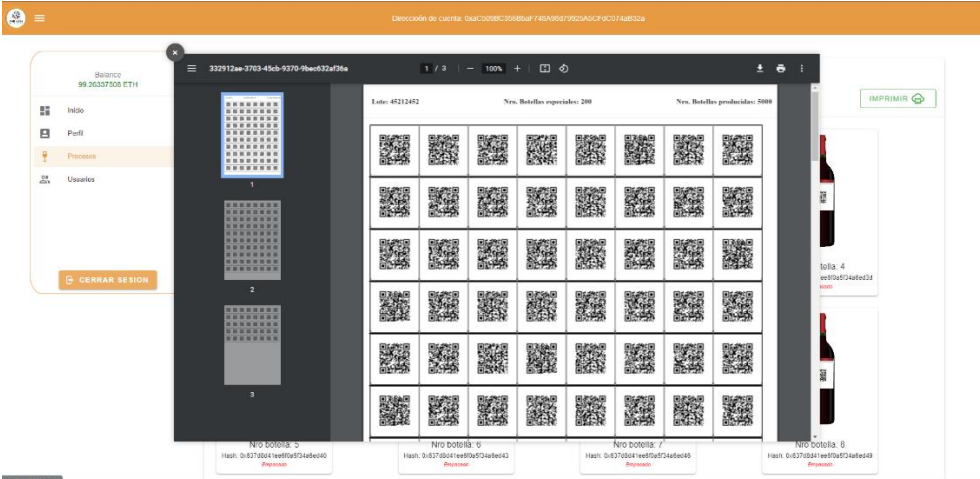
## Generar PDF de los códigos QR

1. Presionar sobre  Botellas como se muestra en la interfaz de la lista de procesos

Procesos		NUEVO PROCESO		Buscar				
Materia Prima (Nro Cosecha)	Extracción Del Mosto (tipo)	Pasteurización (Tem Caliente)	Fermentación (Grados Invertidos)	Clarificación (Turbidez)	Trasiego (Rendimiento)	Envasado (Nro botellas)	Estado	Acción
1 ✓	Licuada ✓	45 °C ✓	10 % ✓	10 ppm ✓	45.00 % ✓	10 ✓	Aprobado ✓	 Visualizar
7868001185026 ✓	Pulpatado ✓	20 °C ✓	20 % ✓	80 ppm ✓	95.00 % ✓	4 ✓	Aprobado ✓	 Botellas
123456 ✓	Pulpatado ✓	45 °C ✓	10 % ✓	10 ppm ✓	80.00 % ✓	5000 ✓	Aprobado ✓	
1123456 ✓	Licuada ✓	10 °C ✓	10 % ✓	10 ppm ✓	89.00 % ✓	50 ✓	Aprobado ✓	
3 ✓	Pulpatado ✓	45 °C ✓	10 % ✓	10 ppm ✓	98.00 % ✓	200 ✓	Aprobado ✓	


Rows per page: 10 1-5 of 5

2. Presionar sobre  como se muestra en la interfaz de la lista de botellas



3. Presionar sobre  para descargar PDF con códigos QR.

## Agregar un usuario

1. Presionar sobre  Usuarios donde se mostrará la interfaz de la lista de usuarios.

**Usuarios** + NUEVO USUARIO

Fecha	Nombres	Billetera	Rol	Permisos	Acción
20/10/2022	Jimmy Leonel Vicente Guayanay	0xF4638D0534e993301e453227edF061CB03000DBE	Administración	Materia prima, Extracción del mosto, Pasteurización, Fermentación, Clarificación, Trasiego, Envasado, Vendedor	⋮
25/10/2022	Cristian Narvaez	0xF3eD9A6dCEf2f2840119D1D3652660dCF547Cf13	Administración	Materia prima, Extracción del mosto, Pasteurización, Fermentación, Vendedor, Envasado, Trasiego, Clarificación	⋮

Rows per page: 10 1-2 of 2 < >

2. Presionar sobre + NUEVO USUARIO donde se mostrará el formulario para registrar usuario.

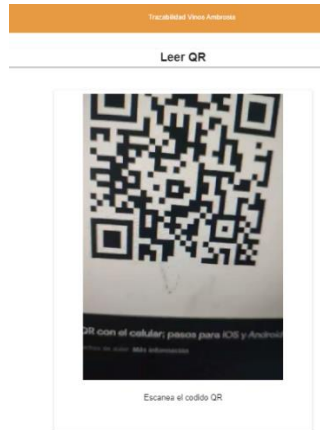
Materia prima  Extracción del mosto  Pasteurización  Fermentación  
 Clarificación  Trasiego  Envasado  Vendedor

3. Llenar el formulario y hacer clic sobre GUARDAR y a continuación se presentara el nuevo usuario agregado.

## Leer código QR de una botella

Con esta funcionalidad, es posible verificar la trazabilidad de una botella utilizando la red Blockchain de Ethereum en Sepolia Test Network.

1. En la página principal presionar sobre  donde se mostrará la interfaz con la cámara para leer el código QR.



**NOTA:** Se debe dar permiso al acceso de la cámara para leer el código QR


2. Una vez que se leyó el código QR le presentará el resultado de acuerdo a los siguientes escenarios:
  - Si existe la TVA mostrará la siguiente información:

Trazabilidad Vinos Ambrosia

Botella encontrada

### Información

Trazabilidad de la botella Nro: 1




Información botella	Estado de botella	Acciones
Transaction Hash: <a href="#">0xa30728-d67c3-ed524fba24b711b36e6d6d7349eb630a4789a</a> <a href="#">263d7038</a> Firma de proceso: 0081e10f450135c508e6297182df31e70f0e519e2d409f020c9fd 1886282e5e Nro Lote: 02020813 Nro botella: 1 Hash: 0x537dad196c2f8ea37be3fa3c	Empacado: 0xaC609BC3558baF749A98d70625A8FCaC074a832a 23/11/2022, 00:18:17	<input type="button" value="CONECTAR"/>

- Si NO es validó se muestra la siguiente notificación:

Trazabilidad Vinos Ambrosia

Qr invalido, no existe información de este código QR

### Leer QR



Escanea el código QR

## Anexo 13. Certificación de traducción de resumen

Loja, 03 de julio de 2023

Magister  
KARINA CELI JARAMILLO  
CATEDRÁTICA DE LA CARRERA DE PEDAGOGÍA DE LOS IDIOMAS  
NACIONALES Y EXTRANJEROS - UNL

### CERTIFICO:

Que el resumen del Trabajo de Integración Curricular del aspirante, Jimmy Leonel Vicente Guayanay con C.I. 1105279044 perteneciente a la Carrera de Ingeniería en Sistemas; traducido al inglés cumple con las características propias del idioma extranjero.

### Resumen:

El presente Trabajo de Titulación (TT) tiene como objetivo el estudio de cómo la implementación de una DApp basada en tecnología blockchain puede mejorar la trazabilidad de los vinos Ambrosia. En vista que actualmente existe la falta de un sistema eficiente y transparente en la gestión de los productos de los vinos y en la satisfacción de los consumidores. Por lo tanto, se busca explorar el potencial de la tecnología blockchain para mejorar la eficiencia en su elaboración y así mejorar la experiencia del cliente.

Con la metodología ABCDE y las tecnologías utilizadas (Truffle Suite, Vue.js, Solidity y Nodejs) se ha llevado a cabo un proceso sistemático y riguroso para asegurar que la DApp cumpla con los objetivos planteados y se pueda validar su funcionalidad. En el primer objetivo, se identificó los actores involucrados; se crearon las historias de usuario y se definieron los requerimientos; se realizó un diagrama de arquitectura y se dividió la DApp en dos subsistemas: contratos inteligentes y aplicaciones. En el segundo objetivo, se desarrollaron las fases de diseño, codificación y pruebas unitarias para cada subsistema para asegurar su correcta funcionalidad. Finalmente, en el tercer objetivo, se realizaron las pruebas de integración, funcionales y de aceptación y desplegaron el módulo de software en la testnet de Sepolia de Ethereum.

La DApp implementada permite registrar información crítica sobre la producción de los vinos, en este caso los procesos de: materia prima, extracción del mosto, pasteurización, fermentación, clarificación, trasiego y envasado. De esta manera, se mejora la transparencia en la cadena de suministro y se asegura que los consumidores tengan acceso a información precisa y confiable sobre el vino que están adquiriendo. Al utilizar la tecnología blockchain, se garantiza la inmutabilidad y la

integridad de la información, lo que significa que los datos no pueden ser alterados o eliminados una vez registrados en comparación con la manera tradicional de registrar la información sobre la producción de vinos, donde la información puede ser vulnerada y alterada.

Palabras claves: *ABCDE, blockchain, DApp, contratos inteligentes, Ethereum, Vue, truffle.*

#### **Abstract:**

The objective of this Degree Project (TT) is to study how the implementation of a DApp based on blockchain technology can improve the traceability of Ambrosia wines. Given that there is currently a lack of an efficient and transparent system in the management of Ambrosia wine products and in consumer satisfaction. Therefore, it seeks to explore the potential of blockchain technology to improve efficiency in the production of Ambrosia wines and thus improve the customer experience.

With the ABCDE methodology and the technologies used (Truffle Suite, Vue.js, Solidity and Nodejs), a systematic and rigorous process has been carried out to ensure that the DApp meets the objectives set and its functionality can be validated. In the first objective, stakeholders were identified; user stories were created and requirements were defined; an architecture diagram was created and the DApp was divided into two subsystems: smart contracts and applications. In the second objective, the design, coding and unit testing phases were developed for each subsystem to ensure its correct functionality. Finally, in the third objective, integration, functional and acceptance tests were performed and deployed the software module on Ethereum's Sepolia testnet.

The implemented DApp allows to record critical information about the production of wines, in this case the processes of: raw material, juice extraction, pasteurization, fermentation, clarification, racking and packaging. In this way, transparency in the supply chain is improved and it is ensured that consumers have access to accurate and reliable information about the wine they are purchasing. By using blockchain technology, the immutability and integrity of the information is guaranteed, which means that the data cannot be altered or deleted once recorded compared to the traditional way of recording information on wine production, where the Information can be violated and altered.

**Keywords:** *ABCDE, blockchain, DApp, smart contracts, Ethereum, Vue, truffle.*



Lo certifico.



Firmado digitalmente por:  
KARINA ALEXANDRA  
CELI JARAMILLO

KARINA CELI JARAMILLO M Ed.

**CATEDRÁTICA DE LA CARRERA DE PEDAGOGÍA DE LOS IDIOMAS  
NACIONALES Y EXTRANJEROS - UNL**