



UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE COMPUTACIÓN

TEMA:

**IMPLEMENTACIÓN DE UN PROTOTIPO DE UNA BILLETERA VIRTUAL PARA
TRANSACCIONES CON NFT (NON-FUNGIBLE TOKEN) EN UN SERVIDOR LOCAL**

Trabajo de titulación previo a la obtención del

Título de Ingeniero en Ciencias de la Computación

AUTORES: ALVARO JHAYR LOMAS PAREDES

STEVEN JOEL SARMIENTO SALAZAR

TUTOR: JULIO RICARDO PROAÑO ORELLANA

Quito – Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Alvaro Jhayr Lomas Paredes con documento de identificación N° 1725479032 y Steven Joel Sarmiento Salazar con documento de identificación N° 1725441461; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 18 de agosto de 2023

Atentamente,



Alvaro Jhayr Lomas Paredes

1725479032



Steven Joel Sarmiento Salazar

1725441461

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Alvaro Jhayr Lomas Paredes con documento de identificación No.1725479032 y Steven Joel Sarmiento Salazar con documento de identificación No.1725441461, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico: “Implementación de un prototipo de una billetera virtual para transacciones con NFT (non-fungible token) en un servidor local”, el cual ha sido desarrollado para optar por el título de: Ingenieros en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 18 de agosto de 2023

Atentamente,



Alvaro Jhayr Lomas Paredes

1725479032



Steven Joel Sarmiento Salazar

1725441461

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Julio Ricardo Proaño Orellana con documento de identificación N° 0103909412, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: IMPLEMENTACIÓN DE UN PROTOTIPO DE UNA BILLETERA VIRTUAL PARA TRANSACCIONES CON NFT (NON-FUNGIBLE TOKEN) EN UN SERVIDOR LOCAL, realizado por Alvaro Jhayr Lomas Paredes con documento de identificación N° 1725479032 y por y Steven Joel Sarmiento Salazar con documento de identificación N° 1725441461, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 18 de agosto de 2023

Atentamente,



Ing. Julio Ricardo Proaño Orellana, PhD
0103909412

DEDICATORIA

Este trabajo primero lo dedico a mi madre, Patricia Paredes, que siempre me ha apoyado en mis sueños y ha logrado dirigirme en cada uno de los pasos que doy desde muy pequeño, eres la fuente de mi inspiración y fortaleza para seguir adelante, te amo más de lo que las palabras podrían expresar, también a mi padre que, aunque no se encuentra en este mundo, sé que me cuidó en cada escalón que subía hasta llegar a la cima te extraño y amo demasiado.

También a todos mis amigos, en especial Nicolás Cabezas y Mateo Carrera, que varias veces me han apoyado y acompañado en mis momentos más difíciles y momentos clave para seguir adelante, sus palabras de aliento y disposición para escucharme y han sido incondicionales.

Steven Sarmiento este trabajo también es para ti y para nosotros, que ha sido una pieza fundamental para su elaboración, gracias por tu colaboración, ayuda y enseñarme lo que es ser un buen equipo.

Por su inquebrantable apoyo durante todo el proceso de mi tesis, a pesar de no estar en el país, quiero agradecer a Camila Zapata, tu constante aliento, además de paciencia y sabiduría han sido fundamentales para superar los desafíos y lograr este importante hito en mi vida académica y profesional. Agradezco infinitamente tu amor incondicional y el respaldo que desde que te conozco me has brindado.

“Ninguno de ellos es responsable de los errores que contengan estas páginas” (Cassany 2012, 19).

Alvaro Jhayr Lomas Paredes

DEDICATORIA

A mis padres: Irma Teresa Salazar Alarcón y Guido Benjamín Sarmiento, quienes con su inmenso amor, apoyo incondicional y sabias enseñanzas, me han brindado las bases sólidas para alcanzar mis sueños; su constante aliento y sacrificio han sido mi mayor inspiración en este arduo camino hacia la culminación de esta hermosa etapa de mi vida, gracias a los momentos de duda, altibajos y las adversidades que afronté me han ayudado a forjar mi carácter y determinación, éstas han sido lecciones valiosas que me han impulsado a levantarme, persistir y crecer como persona.

A mis hermanos de vida: Heiner Segura y Jerry Robalino, aquellos seres especiales con quienes he compartido risas, lágrimas y momentos inolvidables a lo largo de esta travesía, su amistad ha sido el soporte que ha aliviado los obstáculos y lo han convertido los retos, en oportunidades de crecimiento y sobre todo aprendizaje.

A mi grupo de compañeros universitarios: Daniel Mariño, Jhony Pillajo y Alvaro Lomas, quienes han sido mi apoyo y fuente de colaboración en cada paso de esta ardua jornada de aventura académica, juntos hemos enfrentado desafíos, superado barreras y celebrados logros, formando así un lazo de confianza que siempre perdurará y lo recordaré con cariño

A mis familiares , personas que me dieron su amor incondicional como si de su propio hijo se tratase y a quienes amo y respeto: Roberto García, Nixon Salazar, Georgina Peña y Grimaneza Salazar, aquellos seres queridos que han compartido mis alegrías y desafíos a lo largo de estos años, a ellos doy mi eterno agradecimiento por su respaldo inquebrantable cual faro de esperanza en los momentos más difíciles.

A todos ustedes, en quienes se entrelazan los hilos de mi vida, les dedico esta tesis; es el resultado de todos estos años de esfuerzo, dedicación y pasión, pero también de su influencia positiva y el apoyo constante que me han brindado.

“Nunca dejaste de esforzarte y eso es admirable” (E6, 2023).

Steven Joel Sarmiento Salazar

AGRADECIMIENTOS

Primero le damos gracias a Dios por permitirnos llevar a cabo esta nueva etapa de vida, a nuestros padres que aconsejaron y cuidaron en las noches de desvelo y situaciones difíciles.

A nuestro tutor de tesis, Ingeniero Julio Proaño quien supo confiar en nosotros y por brindarnos una parte de sus conocimientos, tiempo, apoyo y experiencia.

Por último, a todos nuestros docentes de la UNIVERSIDAD POLITÉCNICA SALESIANA, que a lo largo de nuestra vida estudiantil nos han capacitado, educado y formado para ser unos profesionales competitivos en el entorno laboral y personal.

Alvaro Jhayr Lomas Paredes

Steven Joel Sarmiento Salazar

INDICE

I	INTRODUCCIÓN.....	1
II	CAPITULO 1	2
2.1	DESCRIPCIÓN DEL PROBLEMA.....	2
2.2	OBJETIVOS.....	6
2.2.1	OBJETIVO GENERAL.....	6
2.2.2	OBJETIVOS ESPECÍFICOS.....	6
2.3	ALCANCE	7
2.4	JUSTIFICACIÓN	8
2.5	ANTECEDENTES O TRABAJOS RELACIONADOS	9
III	CAPITULO 2	15
3.1	METODOLOGÍA	15
3.2	MARCO TEÓRICO.....	16
IV	CAPÍTULO 3	16
4.1	REQUERIMIENTOS.....	22
4.1.1	REQUERIMIENTOS FUNCIONALES.....	22
4.1.2	REQUERIMIENTOS NO FUNCIONALES.....	23
4.2	MODELADO DEL SISTEMA.....	26
4.2.1	MÓDULO GENERAL DE LA APLICACIÓN.....	26
4.3	MÓDULO ESPECIFICO DE LA APLICACIÓN	27
4.3.1	Caso de Uso específico 1: Conectar con MetaMask	27
4.3.2	Caso de Uso específico 2: Diseñar colección de NFT	28
4.3.3	Caso de Uso específico 3: Agregar nuevo NFT	29
4.3.4	Caso de Uso específico 4: Comprar NFT	30
4.3.5	Caso de Uso específico 5: Pagar NFT con MetaMask.....	31
4.4	MÓDULO DE ACTIVIDAD DE LA APLICACIÓN	33
4.4.1	Diagrama de actividad 1: Conexión con MetaMask.....	33
4.4.2	Diagrama de actividad 2: Diseñar colección de NFT	34
4.4.3	Diagrama de actividad 3: Agregar nuevo NFT.....	35
4.4.4	Diagrama de actividad 4: Comprar NFT	36
4.4.5	Diagrama de actividad 5: Pagar NFT	37

4.5	ARQUETIPO DE LA APLICACIÓN	38
4.6	DIAGRAMA DE DESPLIEGUE	39
4.7	PROTOTIPADO DEL SISTEMA.....	40
4.8	FUNCIONALIDAD DEL SISTEMA.....	43
V	CAPITULO 4	46
5.1	PRUEBAS DE FUNCIONAMIENTO	46
5.1.1	INFORME DE PRUEBAS DE FUNCIONAMIENTO EN SONARCLOUD	46
5.1.2	COMPARACIÓN DE RESULTADOS.....	52
5.2	PRUEBAS DE CAJA NEGRA.....	56
5.3	PRUEBAS DE ACEPTACIÓN	59
VI	CONCLUSIONES.....	64
VII	RECOMENDACIONES.....	66
VIII	REFERENCIAS BIBLIOGRÁFICAS	67

INDICE DE FIGURAS

Figura 1. Caso de uso funcionalidad general de la aplicación.....	26
Figura 2. Caso de uso específico, conexión con MetaMask.....	27
Figura 3. Caso de uso específico, Diseñar colección NFT.....	28
Figura 4. Caso de uso específico, Agregar nuevo NFT.....	30
Figura 5. Caso de uso específico, Comprar NFT.....	31
Figura 6. Caso de uso específico, Pagar NFT con MetaMask.....	32
Figura 7. Diagrama de actividad para la conexión con MetaMask.....	33
Figura 8. Diagrama de actividad para el diseño de NFT.....	34
Figura 9. Diagrama de actividad para la adición de NFT.....	35
Figura 10. Diagrama de actividad para la compra de NFT.....	36
Figura 11. Diagrama de actividad para el pago de NFT.....	37
Figura 12 Diagrama de clases.....	38
Figura 14 Prototipo 1 de la Aplicación.....	40
Figura 15 Prototipo 2 de la Aplicación.....	41
Figura 16 Prototipo 3 de la Aplicación.....	42
Figura 17 Pantalla Inicio de la Aplicación.....	43
Figura 18 Dirección de Billetera.....	44
Figura 19 Imágenes en la Base de Datos Digital.....	44
Figura 20 Agregación de NFT al prototipo.....	45
Figura 21 Compra de NFT.....	46
Figura 22. Resumen de las pruebas en SonarCloud con código corregido.....	47
Figura 23. Apartado de bugs encontrados para Fiabilidad.....	48
Figura 24. Ejemplo de bug encontrado para Fiabilidad.....	48
Figura 25. Apartado de Seguridad.....	49
Figura 26. Apartado de code smells encontradas para Mantenibilidad.....	50
Figura 27. Ejemplo de code smells encontrado para Mantenibilidad.....	50
Figura 28. Apartado de Revisión de Seguridad.....	51
Figura 29. Ejemplo de problema encontrado para el apartado de Revisión de Seguridad.....	52
Figura 30. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código antiguo (derecha).....	52

Figura 31. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Fiabilidad	53
Figura 32. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Seguridad.....	54
Figura 33. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Mantenibilidad	55
Figura 34. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Revisión de Seguridad	56
Figura 35. Evidencia para Prueba de aceptación – Conexión.....	59
Figura 36. Evidencia para Prueba de aceptación – Agregar	61
Figura 37. Evidencia para Prueba de aceptación – Galería	61
Figura 38. Evidencia para Prueba de aceptación – Comprar.....	63
Figura 39. Evidencia para Prueba de aceptación – Débito de ETH en Ganache.....	63

INDICE DE TABLAS

Tabla 1 Requerimiento Funcional 1	22
Tabla 2 Requerimiento Funcional 2	22
Tabla 3 Requerimiento Funcional 3	22
Tabla 4 Requerimiento Funcional 4	23
Tabla 5 Requerimiento Funcional 5	23
Tabla 6 Requerimiento No Funcional 1.....	23
Tabla 7 Requerimiento No Funcional 2.....	24
Tabla 8 Requerimiento No Funcional 3.....	24
Tabla 9 Requerimiento No Funcional 4.....	24
Tabla 10 Requerimiento No Funcional 5.....	25
Tabla 11 Requerimiento No Funcional 6.....	25
Tabla 12 Caso de uso - Funcionalidad general de la aplicación	26
Tabla 13 Caso de uso específico - Funcionalidad general de la aplicación	28
Tabla 14 Caso de uso específico - Diseñar colección de NFT.....	29
Tabla 15 Caso de uso específico – Agregar nuevo NFT	30
Tabla 16 Caso de uso específico - Comprar NFT	31
Tabla 17 Caso de uso específico – Pagar NFT con MetaMask.....	32
Tabla 18 Pruebas de caja negra – Crear colección NFT.....	57
Tabla 19 Pruebas de caja negra – Conexión con MetaMask.....	57
Tabla 20 Pruebas de caja negra – Agregar NFT.....	58
Tabla 21 Pruebas de caja negra – Comprar NFT	59
Tabla 22 Pruebas de aceptación– MetaMask	59
Tabla 23 Pruebas de aceptación– Agregar.....	60
Tabla 24 Pruebas de aceptación– Galería	61
Tabla 25 Pruebas de aceptación – Comprar.....	62

RESUMEN

El proyecto técnico se centra en la implementación de un prototipo de billetera virtual para transacciones con NFTs en un servidor local. Aunque esta tecnología se encuentra en una etapa temprana de desarrollo y no hay cifras precisas sobre las transacciones realizadas con NFTs, el prototipo actualmente sirve como una herramienta experimental para aprender sobre la tecnología y la gestión de estos activos.

El prototipo se desarrolló en NodeJS, React y en lenguaje Solidity del cual se destacan los beneficios de incorporar los contratos inteligentes ERC721 y ERC165, que es son estándares utilizados en la red Ethereum para tokenizar activos no fungibles.

En el proyecto se cumple con la meta de acortar la brecha existente en el desconocimiento y el miedo de ingresar al mercado de los NFTs, las transacciones realizadas de compra y venta difieren de los sistemas de pago tradicionales, ya que se realizan directamente a través de la blockchain consumiendo ETH, sin el uso de tarjetas de crédito o transferencias bancarias convencionales, asegurando la anonimidad del usuario y resguardando los datos de este.

ABSTRACT

The technical project focuses on the implementation of a prototype virtual wallet for NFT transactions on a local server. Although this technology is in an early stage of development and there are no precise figures on transactions made with NFTs, the prototype currently serves as an experimental tool to learn about the technology and the management of these assets.

The prototype was developed in NodeJS, React and Solidity language from which the benefits of incorporating ERC721 and ERC165 smart contracts, which are standards used in the Ethereum network to tokenize non-fungible assets, stand out.

The project meets the goal of bridging the existing gap in the lack of knowledge and fear of entering the NFTs market, the purchase and sale transactions differ from traditional payment systems, as they are made directly through the blockchain consuming ETH, without the use of credit cards or conventional bank transfers, ensuring user anonymity and safeguarding the user's data.

I INTRODUCCIÓN

En los últimos años, especialmente alrededor de 2021, los Tokens No Fungibles (NFTs) surgieron como una nueva idea de revolución del mercado, estos han ocupado el panorama digital como una innovación disruptiva en el mercado digital. Estos activos digitales únicos han revolucionado la forma en que los artistas, creadores y propietarios de contenido pueden interactuar y comercializar sus obras en el entorno digital. Además, la adopción de otra tecnología emergente como lo son las billeteras virtuales ha tomado un papel muy importante en esta revuelta.

Al desarrollar una plataforma que sea segura, confiable y accesible se garantiza una solidez y protección de datos de personas que quieran incursionar en esta nueva ciencia aplicada. En este proyecto, se dará una revisión a los NFTs e implementará una billetera virtual dedicada a este tipo de activo digital, documentando todo el proceso y haciendo uso de tecnologías avanzadas para su pronto desarrollo y funcionamiento.

II CAPITULO 1

2.1 DESCRIPCIÓN DEL PROBLEMA

Las transacciones con NFTs (Non-Fungible Tokens) es un tema reciente y el cual ha ido aumentando su popularidad en los últimos años. Este tipo de activos digitales son únicos y hacen uso de la tecnología “blockchain” para reconocer su autenticidad y propiedad. Los tokens no fungibles (NFT) son identificadores digitales únicos que se utilizan para representar la propiedad de varios criptoactivos, como música, obras de arte, coleccionables, activos de juegos, además que permiten una cadena inalterable y probable de creación y propiedad (White et al., 2022). Las billeteras proporcionan a los clientes la capacidad de enviar y recibir monedas virtuales o tokens y ajustar su saldo a través de la interacción con blockchain (Suratkar S et al., 2020). Durante los últimos años, ha habido un creciente impulso en el mercado global para incorporar activos no convencionales en las carteras de inversión. Ejemplos notables de estos activos son las criptomonedas y los NFTs, los cuales han ganado popularidad significativa. Esta tendencia ha experimentado un aumento considerable, ya que cada vez más inversores buscan diversificar sus estrategias y aprovechar nuevas oportunidades de inversión. El interés en estas formas de activos ha generado un ambiente dinámico y emocionante en el mercado financiero, con un enfoque renovado en la innovación y la adopción de tecnologías disruptivas. (Fang et al., 2022). Las billeteras virtuales son aquellas que se van a utilizar para almacenar y gestionar este tipo de activos, esta es muy similar a una billetera de criptomonedas, la diferencia es que esta se especializa en token no fungibles.

Durante el año 2021, se registró un significativo número de usuarios a nivel mundial, aproximadamente 300.000, que participaron en transacciones de tokens no fungibles (NFTs), generando un volumen total de transacciones de alrededor de 23.000 millones de dólares. Dentro

de este volumen, la mayoría de las transacciones correspondieron a NFTs coleccionables. Aunque China ha impuesto restricciones en relación con las criptomonedas, no ha quedado excluida de esta tendencia. De hecho, el 25 de enero de 2022, anunciaron la puesta en marcha de su propia plataforma llamada Blockchain Services Network (BSN), la cual ofrece blockchain adaptadas que no están vinculadas a criptomonedas (las cuales están prohibidas en China). Esta plataforma permite la creación de NFTs chinos, lo que demuestra el interés y la adaptación del país a esta tecnología emergente.(La et al., 2022). El tipo de NFT a crear está basado en una pequeña colección de imágenes, la tratarse de un prototipo usaremos algunas platillas y a partir de estas crearemos este nuevo arte digital.

Se ha hecho un estudio sobre los NFTs en Estados Unidos, en el cual se quería conocer si las personas ya habían realizado alguna compra de este tipo de activos y las respuestas fueron clasificadas por sí y no. También se clasificaron las respuestas por edad y género para eliminar el sesgo de la muestra. En resumen, se obtuvo que los “non-fungible tokens” se han adaptado más rápido que los bitcoins y muchas personas han invertido en este tipo de activos, pero algunas personas tienen miedo de realizar inversiones por algunas licencias y contratos inteligentes que estos manejan. (Seigneur & Mesquita Borba Maranhao M, 2023). Según informa NonFungible.com, el mercado de NFT experimentó un crecimiento del 299% en términos de volumen de transacciones en América en el primer trimestre de 2021. El informe también señala que el continente americano es aquel que representa el 24% del volumen total de transacciones de NFT en todo el mundo. (BlueWeave Consulting and Research Pvt Ltd, 2022).

Ecuador muestra un rezago en comparación con otros países en términos de inversión en activos poco convencionales. La adquisición de estos activos implica un proceso que incluye la compra de criptomonedas, la creación de una billetera virtual, la selección de NFTs, la compra u

oferta de estos, su listado y posterior venta. Si se desea incluir estos activos digitales en una cartera de inversión, se sugiere colocarlos en la parte más arriesgada de los criptoactivos, donde la mayoría del negocio se encuentra en criptomonedas. Para fomentar la cultura de inversión en la sociedad ecuatoriana y mejorar la aceptación de los tokens digitales no fungibles, se recomienda promover su inclusión en diferentes tipos de portafolios de inversión.(Valencia Chávez et al., 2022). En Ecuador no hay datos específicos de tipo cuantitativos, sin embargo, se puede señalar que existe un interés creciente en el mercado, por lo que es posible que los inversores y coleccionistas de arte en el país estén interesados en el mercado de NFTs debido a su capacidad para autenticar y garantizar la propiedad de obras de arte digitales.

El siguiente proyecto técnico responderá a la problemática: ¿Existe la implementación de un prototipo de una billetera virtual para transacciones con NFT (non-fungible token) en un servidor local? En relación con la implementación de un prototipo de billetera virtual en un servidor local, es importante destacar que no existen cifras relevantes sobre transacciones realizadas con NFTs, ya que esta tecnología se encuentra en una etapa temprana de desarrollo. Entre los aportes que podemos brindar con la creación de este modelo, primero es que puede ser utilizada como una herramienta de tipo experimental, ya que mediante esta se puede aprender sobre la tecnología utilizada y la gestión de estos activos. Además, de incorporar el contrato inteligente ERC721 el cual es un estándar de token no fungible en la red de Ethereum, que garantiza la seguridad de cada token debido a su unicidad y no repetibilidad, lo que se logra a través del registro de cada token en la cadena de bloques de Ethereum. Los contratos inteligentes de ERC721 incluyen funciones de transferencia y aprobación para proteger a los usuarios de transacciones fraudulentas. Los usuarios pueden verificar la autenticidad de un token a través de la exploración de la cadena de bloques y la verificación de su contrato inteligente. Es importante tener en cuenta que la

seguridad de ERC721 depende de la correcta implementación de los contratos inteligentes por parte de los desarrolladores, quienes deben seguir las mejores prácticas de seguridad y realizar auditorías para identificar y abordar cualquier vulnerabilidad potencial.

En el proyecto técnico se busca terminar con el desconocimiento sobre las transacciones con NFTs, existen varias causas para que las personas no inviertan en este mercado. i) El desconocimiento llega principalmente de los adultos y adultos mayores, ya que al ser una nueva propuesta de mercado tecnológico puede resultar confuso para ellos. ii) Como es de conocimiento general los NFTs utilizan transacciones de pago que no son tradicionales, estas son realizadas directamente con la blockchain a diferencia de los tipos de sistemas de pagos tradicionales como tarjetas de crédito o transferencias bancarias. iii) Al ubicarnos en un país tercermundista las personas se cierran a la idea de hacer inversiones en este tipo de activos digitales. Con la buena gestión, determinación y creación del prototipo de la billetera virtual se busca cerrar con la brecha existente en el desconocimiento y el miedo de ingresar a este mercado.

Entre los efectos que más se pueden mencionar están: i) Escasa apertura a transacciones con NFTs debido al desconocimiento. ii) Riesgos de algún tipo de estafa monetaria al momento de usar tarjetas de crédito para la compra de otros activos o bienes, la implementación de una billetera virtual puede traer eficiencia en las transacciones ya que no se requiere de intermediarios. iii) El escaso mercado virtual en el Ecuador, ya que es de nuestro conocimiento que existen pocas personas y compañías que han invertido en este activo.

En cuanto a la implementación de este prototipo, se requerirán algunos componentes clave. Sin embargo, se trabajará en su ejecución que permitiría el almacenamiento y la gestión de NFT en un servidor local. Este prototipo incluirá elementos necesarios para el funcionamiento de una

billetera virtual, como la capacidad de enviar y recibir tokens, así como la gestión de las claves privadas necesarias para acceder a los distintos activos digitales. Se espera que esta iniciativa pueda sentar las bases para futuros desarrollos en el ámbito de las tecnologías blockchain y NFT, así brindando una oportunidad para que nuevos interesados se involucren en el mundo de los activos digitales y les permita experimentar con la compra, venta y transferencia de activos únicos. Es indispensable conocer que la billetera virtual contemplará el uso de un software donde se mostrarán los activos digitales a la venta, además de poder realizar la compra de cada uno de ellos a través de transacciones con la blockchain, pero no olvidar que al ser un prototipo se utilizarán herramientas como “Ganache” y “Metamask” para el correcto funcionamiento de la billetera.

2.2 OBJETIVOS

2.2.1 OBJETIVO GENERAL

Diseñar e implementar de un prototipo de una billetera virtual fría de software para NFT (non-fungible token) en un servidor local.

2.2.2 OBJETIVOS ESPECÍFICOS

- Recopilar información acerca de la implementación de billeteras virtuales y el uso de blockchain con la red Ethereum para NFT.
- Desarrollar el prototipo de una billetera virtual para transacciones con NFT en un servidor local.
- Realizar pruebas de funcionamiento del prototipo y evaluación de la calidad del código.

2.3 ALCANCE

Para el objetivo A: “Recopilar información acerca de la implementación de billeteras virtuales y el uso de blockchain con la red Ethereum para NFT.” Se recopilará información sobre la implementación de billeteras virtuales y el uso de la red blockchain descentralizada Ethereum para la gestión de NFT.

Para el objetivo B: “Desarrollar el prototipo de una billetera virtual para transacciones con NFT en un servidor local.” Una vez establecidos los requerimientos del prototipo de billetera virtual para realizar transacciones con NFT, se procederá al desarrollo en el lenguaje de programación Solidity, el cual se especializa en la construcción de contratos inteligentes utilizando estándares como ERC 165 – 721 y back-end. Además, el manejo del entorno de ejecución Node JS, React y Bootstrap para realizar la construcción del front-end del software. Este sistema estará alojado en un servidor local de una computadora de uso personal de parte de los desarrolladores del proyecto por lo que desarrolla en un entorno seguro trabajando además con Metamask. Las transacciones se gestionarán mediante compatibilidad cross-chain, permitiendo la comunicación de los protocolos y transferencia de activos y datos.

Para el objetivo C: “Realizar pruebas de funcionamiento del prototipo y evaluación de la calidad del código.” Se verificará el funcionamiento del prototipo de billetera virtual. El método por utilizar será mediante la realización de una matriz con sus respectivos checklist, con esta se generará un informe detallado de las pruebas de funcionamiento realizadas. Además, se evaluará el código fuente creado mediante métricas de desarrollo de software y se generará de igual forma su respectivo informe.

2.4 JUSTIFICACIÓN

En el contexto actual de rápida evolución tecnológica, la adopción de nuevas tecnologías vanguardistas está experimentando un crecimiento sin precedentes, así es como se destaca la red tecnológica blockchain, esta es una base de datos descentralizada la cual permite realizar transacciones de manera segura e inmutable, ya que al ser una tecnología con mayor seguridad y transparencia permite hacer uso en diferentes ámbitos de las aplicaciones. Entre estas redes, las más populares son Bitcoin, Ethereum, Litecoin, entre otras. Cada una de estas tienen sus propias características y aplicaciones; después de realizar una búsqueda corroboramos que la red Ethereum es la que mejor se adapta a nuestro proyecto ya que maneja una mejor documentación sobre el uso de NFT y billeteras virtuales. Así como se define en su propia página web los NFT son tokens que se utiliza para representar la propiedad de objetos únicos e irrepetibles en la web, esto nos permite representar arte, música, videos, contratos, trabajos académicos, dominios e incluso fragmentar el mercado de bienes y raíces como archivos digitales y tokenizarlos (Tókenes No Fungibles (NFT) | Ethereum.Org, n.d.). Además, las billeteras virtuales permiten a los usuarios almacenar, administrar y transferir dinero u otros activos digitales con la finalidad de dar mayor seguridad y tranquilidad al usuario, permitiendo una rápida transacción.

Estas redes han sido adoptadas por empresas como OpenSea o Polygon las cuales surgieron en el año 2021 con el crecimiento de las compras en línea a raíz de la pandemia dada por el Covid19, estas empresas son abiertas para el público en general y tienen sus sedes en Estados Unidos e Inglaterra respectivamente. Al ver este tipo de empresas que cada vez tiene más oportunidades, indagando en este tipo de tecnologías en Latinoamérica más específicamente en Ecuador, no se encuentra desarrollado este tipo de mercado ni aplicaciones debido a su poca documentación y alto impacto en su nivel de producción, por lo que su construcción será

innovadora y permitirá una expansión del mercado digital en diferentes regiones actualmente no contempladas.

El presente proyecto proporciona la creación e implementación de una billetera virtual para la gestión de NFT, el cual pretende ayudar al personal a confiar en las nuevas tecnologías y familiarizarse con las compras seguras en línea. Para la elaboración de esta billetera virtual es esencial el uso de tecnologías modernas, ya que estas nos brindaran una mejor gestión en el ambiente transaccional, así como mejorar su seguridad a través de contratos inteligentes y salvaguardar la información confidencial del usuario.

Se tiene como finalidad expandir las fronteras del mercado virtual a los consumidores interesados para que se gestione una compra segura en línea, realice trasferencias en el menor tiempo posible y que esta tecnología llegué al país a grandes empresas que puedan integrar esta forma de comercio innovador de forma segura.

2.5 ANTECEDENTES O TRABAJOS RELACIONADOS

(Darius G. et al, 2022) se enfocó en generar un software para validar la propiedad de NFT en una dirección blockchain determinada, con el objetivo de facilitar la venta, compra y comercio de obras de arte y bienes inmuebles de manera accesible. Para ello, como metodología utilizó una API para extraer metadatos de la billetera y, posteriormente, en Python se devolvió una respuesta “. json" donde se extrajeron solo los parámetros necesarios.

El resultado obtenido fue la dirección del NFT proporcionada directamente por la blockchain. Los NFT tienen metadatos que permiten agregar información adicional, como descripciones e imágenes. No se obtuvieron datos precisamente cuantitativos ya que al desarrollar este software la investigación se direccionó más a los requerimientos que este debería tener.

El trabajo destaca la importancia de la tecnología blockchain para asegurar la información relacionada con las transacciones y eliminar la necesidad de terceros, lo que hace que el mundo sea menos vulnerable al fraude. El estudio concluye que, gracias al software creado, es posible extraer los medios de los servidores de OpenSea que están alojados en granjas de servidores de Google y recuperar los NFT para cualquier dirección de cartera de blockchain de Ethereum.

(Sánchez M., 2019) tuvo como objetivo de estudio analizar la posible implementación de pagos móviles en Argentina. Se utilizó una metodología mixta combinando datos cuantitativos y cualitativos para analizar la situación de los pagos móviles en el mundo y los factores de éxito en su implantación.

Se encontró que Argentina tiene un entorno favorable para la capacitación en tecnología electrónica con 61 millones de conexiones móviles y algunas billeteras digitales en el mercado. Entre los resultados se encontró que las billeteras virtuales son fáciles, rápidas y seguras de usar, con ventajas como transacciones instantáneas y privacidad. En América Latina, el segmento de pagos y remesas es el principal negocio (24%), seguido por préstamos (18%) y gestión de finanzas empresariales (15%). En Argentina, el nivel de bancarización no ha aumentado en los últimos años, pero las billeteras digitales han crecido un 373% en los últimos 3 años, con 7,2 millones de usuarios empleando “home banking” y 7,1 millones utilizando banca móvil.

Se concluye que Argentina tiene una gran oportunidad para progresar en su desarrollo implementando tecnologías actuales en los servicios financieros, pero es necesario analizar los cuatro vectores que afectan la migración hacia un entorno digital: el gobierno, las políticas, la tecnología y la cultura. Es importante destacar que la implementación de pagos móviles en

Argentina podría mejorar la inclusión financiera y la eficiencia en el sistema de pagos, así como aumentar la competencia y la innovación en el sector.

(Wang Q. et al, 2021) en su trabajo realizado en conjunto con personas de la universidad de South África, Inglaterra y China tuvo como objetivo el desarrollo de las aplicaciones en base a NFT debe superar una cadena de barreras que se da en todas las tecnologías que están emprendiendo. Se empleó una metodología de tipo cualitativa-cuantitativa para el artículo, recopilando información en su mayoría cuantitativa, evaluando las diferentes fluctuaciones del mercado en base a aumento de inversión y pérdidas de estas. También se realiza el análisis de algunas variables como son la seguridad y la extensibilidad abarcando tanto los problemas a nivel de sistema causados por las plataformas basadas en blockchain. Los resultados obtenidos con los Non-Fungible Token es que al ser una tecnología emergente que prevalece en el blockchain, se obtuvieron soluciones NFT de vanguardia que ponen el mercado de activos digitales/virtuales, en primer lugar, se realizó un análisis exhaustivo de los aspectos técnicos y se proporcionaron modelos de diseño y características de los NFT. Posteriormente, se llevó a cabo una evaluación de la seguridad de los sistemas de NFT actuales, al tiempo que se continúa debatiendo sobre las oportunidades y posibles aplicaciones que pueden surgir a partir de este tipo de activos. Por último, se destacaron los desafíos de investigación que deben abordarse antes de lograr una adopción masiva en el mercado.

Los datos cualitativos recopilados revelaron que, en los últimos años, los NFT han ganado una atención considerable tanto en la comunidad industrial como en la científica. El mercado de NFT ha experimentado un incremento notable, con un volumen de operaciones promedio diario de 4.5 billones de dólares, representando aproximadamente el 1.3% del mercado de criptomonedas en tan solo 5 meses. Los primeros inversores han obtenido ganancias sorprendentes, y en mayo de

2021, el mercado de NFT ha experimentado un crecimiento significativo en comparación con enero de 2020, con un total de 25,729 ventas completadas y un gasto de 34,530,649.86 dólares.

Además, el número de billeteras activas sigue aumentando a un ritmo acelerado. La venta de NFT se estimó en 12 millones en diciembre de 2020, pero experimentó un aumento explosivo a 340 millones en tan solo dos meses (febrero de 2021), lo que lleva a algunos a considerar los NFT como el futuro de los activos digitales. En resumen, los inversores tempranos han obtenido ganancias significativas y este crecimiento ha llevado a una percepción generalizada de que los NFT representan el futuro de los activos digitales, mostrando un aumento notorio desde enero de 2020.

(Valencia C. et al., 2022) con su estudio declara que Ecuador se encuentra rezagado en términos de inversión en activos poco convencionales como los NFTs. El objetivo de este estudio fue evaluar el funcionamiento de estos activos digitales y su incorporación en los portafolios de inversión en el país. Se empleó una metodología cualitativa de múltiples métodos, que incluyó entrevistas con expertos y análisis de resultados preliminares.

Los resultados obtenidos indicaron que los NFTs son considerados criptoactivos de alto riesgo debido a su naturaleza especulativa. Se observó que muchas colecciones de NFTs, valoradas en millones de dólares, han experimentado una disminución en su valor recientemente. En el mercado ecuatoriano, el crecimiento de los NFTs está ocurriendo de manera orgánica y gradual. Se recomienda invertir en NFTs con montos entre 10 y 50 USD para minimizar posibles pérdidas económicas.

En términos cuantitativos, se utilizó el software QDA Miner para procesar las entrevistas, permitiendo la transcripción y codificación de la información. Se realizó un análisis descriptivo

basado en la frecuencia de los códigos para identificar relaciones en las respuestas obtenidas. En cuanto al tratamiento tributario, en el extranjero, Estados Unidos considera los NFTs como propiedad y se aplica un impuesto del 30% sobre las ganancias al gobierno. En cambio, en Ecuador, se considera una revalorización de activos y se paga un impuesto del 5% sobre las ganancias al estado.

En conclusión, la decisión de invertir en NFTs depende del perfil del inversionista. Sin embargo, invertir en NFTs dentro de un portafolio de inversión en Ecuador conlleva riesgos, ya que la mayoría de los criptoactivos se centran en la inversión en criptomonedas, las cuales tienen una mayor validez a mediano y largo plazo.

(Morocho N., & Mosquera R., 2020) el propósito de este estudio es examinar el uso de la tecnología blockchain en la provincia de El Oro. Se empleó una metodología mixta, combinando enfoques cualitativos y cuantitativos, para investigar la implementación de blockchain en medianas empresas ubicadas en la ciudad de Machala.

Los resultados revelan que existe un bajo nivel de conocimiento y utilización de la tecnología blockchain en las empresas estudiadas. Sin embargo, se reconoce que su adopción podría ser beneficiosa para el desarrollo empresarial, al aumentar la seguridad y la confianza en los procesos. Se enviaron un total de 169 formularios, de los cuales 33 empresas respondieron (18,39%). Se encontró que el 72,73% de las empresas encuestadas desconocen por completo la tecnología blockchain. Además, se observó que las empresas no familiares tienen un mayor nivel de conocimiento de la blockchain (15,15%) en comparación con las empresas familiares (12,12%).

Se concluye que se requiere la capacitación de más expertos en el campo de la blockchain para difundir el conocimiento sobre esta tecnología y su potencial. La falta de confianza en el mercado es un factor limitante que dificulta la adopción de esta nueva oportunidad de negocios.

(Gabela R., 2019) en su trabajo asumió como objetivo de estudio enfocarse en examinar las propiedades y composición de las criptomonedas, así como también los métodos que los criminales utilizan para llevar a cabo actividades delictivas mediante el uso de estas monedas digitales. Se empleó una metodología cualitativa-descriptiva a través de una investigación en fiscalías de Ecuador.

Las criptomonedas son bienes inmateriales recientes que han generado debates en torno a sus consecuencias legales. Su carácter anónimo, descentralizado e independiente de intermediarios tradicionales ha permitido que se utilicen para la perpetración de actividades delictivas, lo que ha generado preocupación sobre el uso que se les puede dar. Los resultados de este estudio fueron alarmantes, ya que se pudo demostrar que los delincuentes han logrado realizar transacciones sin dejar rastro, utilizando las criptomonedas para cometer delitos perfectos.

Entre los datos cuantitativos encontrados por los investigadores también hallaron más de 25,000 sitios web que ofrecen servicios de mezcladoras de cripto-divisas para lavar activos a través de criptomonedas. Concluyen que los riesgos que plantean las criptomonedas han llevado a los países a adoptar tres posturas diferentes: inacción, prohibición y regulación. Solo la regulación puede prevenir el uso ilícito de las criptomonedas. Se recomienda la creación de una Fiscalía especializada en Cibercrimen en Ecuador, dotada del personal adecuado y el cumplimiento de la normativa internacional, para la adopción de criptomonedas y la prevención de su uso delictivo.

3.1 METODOLOGÍA

Los NFTs (Tokens No Fungibles) son activos digitales únicos registrados en una blockchain, como Ethereum. Utilizan el estándar ERC721, el mismo que puede lograr establecer reglas y funciones para su comportamiento y funcionalidad adecuada. Los “Smart Contracts” son programas autónomos que se ejecutan en la EVM (Ethereum Virtual Machine). Estos son codificados en un lenguaje de programación denominado Solidity.

Los NFT Marketplaces, como por ejemplo OpenSea, son plataformas donde los usuarios pueden comercializar los “No fungible tokens”, realizando el proceso de compra, venta y comercialización, para ello se puede tener precios fijos o subastarse. Metamask es una billetera de criptomonedas donde se almacenarán las monedas virtuales, en este caso “Ethereum” permitiendo interactuar con aplicaciones descentralizadas.

Para lograr desarrollar los diferentes contratos inteligentes y crear el prototipo de billetera virtual fría para NFTs, se utiliza “Truffle”, el cual consta de un conjunto de instrumentos que permite a cualquier desarrollador crear aplicaciones en la blockchain. Mediante la EVM se permite crear contratos y aplicaciones inteligentes que Ethereum Blockchain puede entender. Para ello se debe configurar el entorno de trabajo, se escriben contratos inteligentes en lenguaje Solidity con su despliegue utilizando una red local como lo es Ganache.

Cabe recalcar que la creación de NFTs no se llevará a cabo de manera completa, sino que se toman como punto de partida imágenes que ejemplifiquen este proceso, aun así, se investigó sobre su realización y se creó una colección de imágenes utilizando JavaScript y Photoshop, estas

imágenes representan personajes novedosos que han sido generados mediante la combinación de fragmentos de otros personajes preexistentes.

Después se debe crear un archivo `package.json` para administrar las dependencias del proyecto y se inicia el archivo `index`. Se instalan las dependencias necesarias y se configuran los archivos de Truffle para la inicialización del proyecto.

Se debe hacer uso del estándar ERC721, este nos va a ayudar con la creación de tokens únicos y no intercambiables, además hay que implementar funciones como “Minting” y transferencia de NFTs. También se examinan e implementan otro tipo de estándares como ERC165, el cual permite verificar interfaces implementadas por los contratos.

Se deben realizar pruebas unitarias respectivas utilizando Truffle para asegurar el correcto funcionamiento de los contratos inteligentes. Luego, se crea una interfaz de usuario utilizando “React” con lenguajes de programación “JavaScript”, “HTML” y “CSS” donde se va a lograr la interacción entre los “Smart Contracts” y “Metamask”. Una vez establecida la conexión se realizan solicitudes para interactuar con la blockchain Ethereum. Para mostrar y almacenar los NFTs se usa una base de datos virtual llamada “Img-BB”

Por último, se exploran pruebas y análisis estáticos en SonarCloud para mejorar la calidad del código y detectar posibles problemas o vulnerabilidades.

3.2 MARCO TEÓRICO

El blockchain es una base de datos distribuida que permite almacenar y compartir información de manera segura, transparente e inmutable, en el artículo “ArtChain: Blockchain-enabled platform for art Marketplace.” se explica que la Blockchain es una tecnología en auge que tiene el potencial de revolucionar la industria mundial y crear una relación de confianza en una red

empresarial multipar tita. Existen varios casos prácticos en los que se ha aplicado blockchain. La blockchain es una tecnología que proporciona una solución segura y descentralizada para la gestión de transacciones y registros de diferentes tipos de datos, lo que puede tener un gran impacto en diversos sectores empresariales y en la forma en que se realizan las transacciones en línea (Wang et al., 2019). Cuenta con características tales como que su tecnología blockchain puede ser utilizada para crear cadenas de bloques con distintas características. Una de estas variantes son las blockchain privadas, que están diseñadas para limitar el acceso a los datos registrados en la cadena. Estas pueden ser de tipo cerradas y con usuarios identificados, permitiendo ser utilizadas en sectores regulados donde se requiere mantener la confidencialidad de sus bases de datos, pueden ser distribuidas y anónimas, dependiendo del nivel de acceso y privacidad requerido. La fortaleza de una blockchain privada depende de la cantidad de nodos que la protegen, los cuales son mantenidos por los participantes del sistema (Preukschat et al., 2017).

Blockchain además cuenta con herramientas como monederos digitales o CriptoWallet el cual se define como una herramienta fundamental para el uso de la tecnología blockchain, ya que permiten a los usuarios realizar transacciones de forma segura y fácil. Además de almacenar las claves privadas, algunas billeteras también ofrecen características avanzadas como la integración con otros servicios, la creación de contraseñas seguras y la capacidad de almacenar múltiples criptomonedas (Villameriel, 2019). Las CriptoWallet se utiliza para almacenar, enviar y recibir criptomonedas, las características típicas de una CriptoWallet incluyen la generación y almacenamiento de claves privadas y públicas, la compatibilidad con diferentes criptomonedas, la posibilidad de realizar transacciones seguras y la integración con otras aplicaciones o servicios de blockchain. Las CriptoWallet pueden ser de diferentes tipos, como hardware, software, móviles o

en línea, cada uno con sus propias ventajas y desventajas en términos de seguridad y facilidad de uso (Introduction | MetaMask docs, n.d.).

Estas billeteras están equipadas con un software que se puede instalar en un dispositivo informático o utilizar a través de un proveedor en línea que brinde este servicio. Estas carteras aprovechan la tecnología blockchain para facilitar el envío y la recepción de criptomonedas. Entre las opciones disponibles, la alternativa de utilizar un proveedor tiene la ventaja de permitir el acceso a la cartera desde cualquier ordenador y ubicación en el mundo (Introduction | MetaMask docs, n.d.). Así es el caso de la billetera digital MetaMask que en su propia página web se define como una billetera digital de criptomonedas y una extensión del navegador web que permite a los usuarios interactuar con aplicaciones descentralizadas (dApps) en la blockchain de Ethereum. Fue desarrollado por ConsenSys en 2016 y es una de las billeteras más populares utilizadas por los usuarios de Ethereum. (Introduction | MetaMask Docs, n.d.), además de que cuenta con características propias de la billetera como: Billetera de criptomonedas que permite a los usuarios almacenar, enviar y recibir Ethereum y tokens ERC-20, Integración con dApps para que los usuarios puedan interactuar con dApps directamente desde MetaMask sin tener que enviar transacciones manualmente desde otra billetera, Protección de seguridad en la cual MetaMask tiene medidas de seguridad incorporadas para proteger la privacidad y seguridad de los usuarios, incluyendo la protección de contraseñas y frases de recuperación, la autenticación de dos factores y la prevención de phishing.(Introduction | MetaMask Docs, n.d.)

Esta billetera utiliza Ethereum como energía o gas para poder realizar transacciones, debido a su costo actual en el mercado (3800\$ cada Ethereum) optamos por utilizar un software llamado Ganache Truffle Suite que está desarrollado por la compañía Truffle para el progreso, prueba y despliegue de aplicaciones blockchain. Incluye varias herramientas útiles, como Truffle que es un

marco que brinda un entorno de desarrollo para la creación de contratos inteligentes en Ethereum. Ofrece a los desarrolladores la capacidad de escribir, probar y desplegar contratos inteligentes de forma segura y eficiente. Truffle proporciona herramientas para la gestión de dependencias, la migración de contratos y la integración con otras herramientas de desarrollo (Preukschat et al., 2017). Igualmente nos brinda de una red de prueba privada llamada Ganache que se ejecuta localmente en tu máquina que permite a los desarrolladores probar y depurar sus contratos inteligentes en un entorno seguro y aislado antes de desplegarlos en una red pública. Ganache simula una red Ethereum completa, lo que significa que se puede utilizar para probar todas las características de un contrato inteligente, incluyendo la emisión de tokens y la interacción con otros contratos inteligentes (Ganache | Overview - Truffle Suite, n.d.).

Ethereum se enfoca en permitir la ejecución de contratos inteligentes y aplicaciones descentralizadas en su red blockchain. La criptomoneda nativa de Ethereum es el Ether (ETH), que se utiliza para costear las tarifas de transacción en la red y como estímulo para los mineros que mantienen la red. Las billeteras Ethereum en realidad solo se conectan a la blockchain y almacenan las claves privadas del usuario o facilitan la transmisión de transacciones firmadas. Las billeteras virtuales son una herramienta fundamental para el uso de la tecnología blockchain, ya que permiten a los usuarios realizar transacciones de forma segura y fácil (Informačních Technologí, F. s.f.).

En Ethereum, el Gas es una unidad que mide el costo computacional necesario para ejecutar operaciones y transacciones en la red. Cada operación o transacción tiene un costo de gas asociado y el usuario es aquel que establece un límite de gas antes de realizar la operación. Si la cantidad de gas supera el límite establecido, la operación se cancela y el gas se pierde. El precio de este es determinado por el usuario y se utiliza para calcular la tarifa total que se paga por la operación,

multiplicando la cantidad de gas utilizada por el precio del gas. (Ganache | Overview - Truffle Suite, n.d.) Para el costo de Gas en una transacción de Ether el usuario es aquel que debe indicar el límite, que es lo máximo que se debe emplear, si esta se supera la transacción se cancela y precio de este, que es el precio en Ethereum por unidad de gas que se pagará. Cuando se forma un nuevo bloque en la blockchain los mineros suelen usar aquellas transacciones con mayor precio de Gas para ganar más dinero. (Ganache | Overview - Truffle Suite, n.d.)

Los contratos inteligentes son programas informáticos que se activan automáticamente cuando se cumplen ciertas condiciones. Estos contratos tienen una amplia gama de aplicaciones, como la gestión de identidad, la cadena de suministro y los juegos en línea, entre otros. Estos contratos inteligentes están escritos en Solidity, un lenguaje de programación específico para contratos inteligentes en la blockchain de Ethereum. Solidity fue desarrollado por el equipo de Ethereum y es el lenguaje más utilizado para programar contratos inteligentes en la plataforma. Solidity es un lenguaje de programación de alto nivel que permite a los desarrolladores escribir contratos inteligentes utilizando una sintaxis similar a la de otros lenguajes de programación populares, como JavaScript y Python. Su diseño está orientado específicamente a la ejecución segura y eficiente de contratos en la blockchain de Ethereum. (Solidity — Solidity 0.8.20 Documentation, n.d.). De estos contratos tenemos el contrato ERC165 es un estándar de interfaz de contrato inteligente en la red blockchain de Ethereum. Este estándar se creó para permitir a los desarrolladores de contratos inteligentes de Ethereum verificar si un contrato inteligente determinado implementa una interfaz específica o no. ERC165 define una función en los contratos inteligentes llamada "supportsInterface" que permite a los desarrolladores de contratos inteligentes verificar si un contrato implementa una determinada interfaz. Esto permite a los desarrolladores de aplicaciones descentralizadas verificar si un contrato inteligente en la red Ethereum tiene las

funcionalidades necesarias para interactuar con su aplicación de manera eficiente y el contrato ERC721 que es un estándar de token no fungible (NFT) en la red blockchain de Ethereum. Los tokens no fungibles son tokens digitales que son únicos e indivisibles, lo que significa que cada uno tiene un valor único y no puede ser intercambiado por otro token de igual valor. ERC721 fue creado en 2018 como un estándar para la creación de tokens no fungibles en la red Ethereum, y se utiliza principalmente para la creación y comercio de arte digital, juegos en línea, coleccionables y otros activos digitales únicos o también llamados NFT.

La exploración de los NFTs tuvo sus inicios con la aparición de los "Colored Coins" en la red Bitcoin en la década de 2010. Los "Rare Pepes", que son ilustraciones del personaje "Pepe the Frog" creadas en el sistema de Bitcoin, fueron uno de los primeros experimentos en este campo. Algunos de estos "Rare Pepes" se vendieron en eBay, y un conjunto de ellos incluso se subastó en vivo en la ciudad de Nueva York. Sin embargo, la fecha exacta de origen de los NFTs es un tanto difícil de precisar, ya que el concepto ha evolucionado con el paso de los años. Según un artículo encontrado en CoinDesk, se puede ubicar el inicio de estos activos en la creación de los "CryptoPunks", que es una colección de Tokens no fungibles lanzados en junio de 2017. El concepto como tal sobre los NFTs (tokens no fungibles) se originó en 2017 con la creación del protocolo ERC-721 en la red Ethereum por el desarrollador de software Dieter Shirley. Este estándar permite la creación de tokens únicos e irrepetibles en la blockchain, lo que los convierte en un tipo de activo digital no fungible. Sin embargo, el término "NFT" no fue acuñado hasta algunos años después por el empresario y desarrollador de software estadounidense Anil Dash quien popularizó el término en un artículo de blog en 2018, donde hablaba sobre el potencial de los tokens no fungibles para la propiedad y la autenticación de activos digitales únicos (Finzer, 2020)

4.1 REQUERIMIENTOS

4.1.1 REQUERIMIENTOS FUNCIONALES

Id:	RF01
Nombre:	Conectar a MetaMask
Características:	Los usuarios deberán estar conectados a MetaMask para poder realizar las diferentes transacciones
Descripción:	<u>Conectar a MetaMask:</u> Los usuarios deberán estar conectados a MetaMask para poder comprar o añadir los NFTs
Prioridad:	Alta

Tabla 1 Requerimiento Funcional 1

Id:	RF02
Nombre:	Agregar NFT
Características:	El sistema permitirá añadir NFTs a la web.
Descripción:	<u>Agregar NFT :</u> El sistema permitirá al usuario agregar NFTs a la web, esta operación se completará mediante una transacción en una moneda virtual llamada “Ethereum”.
Prioridad:	Alta

Tabla 2 Requerimiento Funcional 2

Id:	RF03
Nombre:	Visualizar Galería de NFT
Características:	El sistema permitirá la visualización de todos los NFTs.
Descripción:	<u>Visualizar Galería de NFT:</u> El sistema permitirá la visualización de los NFTs agregados a la billetera virtual en forma de galería.
Prioridad:	Alta

Tabla 3 Requerimiento Funcional 3

Id:	RF04
Nombre:	Comprar NFT
Características:	El sistema permitirá comprar cualquier NFT disponible en la página
Descripción:	Comprar NFT: El sistema ofrecerá al usuario la posibilidad de realizar la compra de cualquier NFT disponible en la galería.
Prioridad:	Alta

Tabla 4 Requerimiento Funcional 4

Id:	RF05
Nombre:	Pagar NFT
Características:	El sistema ofrecerá al usuario realizar el pago del NFT.
Descripción:	Gestionar usuario: El sistema permitirá al usuario realizar el pago del NFT a través de MetaMask.
Prioridad:	Alta

Tabla 5 Requerimiento Funcional 5

4.1.2 REQUERIMIENTOS NO FUNCIONALES

Id:	RNF01
Nombre:	Interfaz del sistema.
Características:	El sistema presentará una interfaz gráfica de fácil de manejar.
Descripción:	El sistema ofrecerá una interfaz de usuario amigable e intuitiva para facilitar la navegación y el uso del sistema por parte de los usuarios.
Prioridad:	Alta

Tabla 6 Requerimiento No Funcional 1

Id:	RNF02
Nombre:	Mantenimiento.
Características:	El sistema contará con una guía del proceso de creación del sistema, que ayudará al mantenimiento del sistema.
Descripción:	El sistema requerirá de una interfaz que sea fácilmente actualizable, lo cual permitirá llevar a cabo tareas de mantenimiento de manera eficiente y con el menor esfuerzo necesario.
Prioridad:	Alta

Tabla 7 Requerimiento No Funcional 2

Id:	RNF03
Nombre:	Conexión a una base de datos digital
Características:	El sistema deber conectarse a una base de datos en la web.
Descripción:	La interfaz de usuario debe ser diseñada específicamente para adaptarse a las funcionalidades necesarias en un sistema de adquisición y compra de NFTs.
Prioridad:	Media

Tabla 8 Requerimiento No Funcional 3

Id:	RNF04
Nombre:	Seguridad en información
Características:	El sistema garantizara en todo momento la seguridad de la información procesada.
Descripción:	Garantizar la seguridad del sistema gracias a los contratos ERC 721 y ERC 165.
Prioridad:	Alta

Tabla 9 Requerimiento No Funcional 4

Id:	RNF05
Nombre:	Portabilidad
Características:	El sistema podrá ser llevado a cabo en diferentes ordenadores.
Descripción:	El sistema necesita de las siguientes características para un óptimo funcionamiento: RAM de 2 GB, Procesador de 1.66GHz o superior, ratón y teclado.
Prioridad:	
Alta	

Tabla 10 Requerimiento No Funcional 5

Id:	RNF06
Nombre:	Estructura Web
Características:	El prototipo de billetera virtual será llevado a cabo en lenguaje Solidity embebido con React.
Descripción:	El aplicativo se desarrollará con React, con ello también se utiliza un lenguaje llamado Solidity para los contratos inteligentes, Web 3.0, Node.js y Truffle.
Prioridad:	
Alta	

Tabla 11 Requerimiento No Funcional 6

4.2 MODELADO DEL SISTEMA

4.2.1 MÓDULO GENERAL DE LA APLICACIÓN

En la Figura 1 se observa el diagrama de caso de uso general donde se describen los dos módulos de gestión, tanto para la adición como para la compra de NFTs.

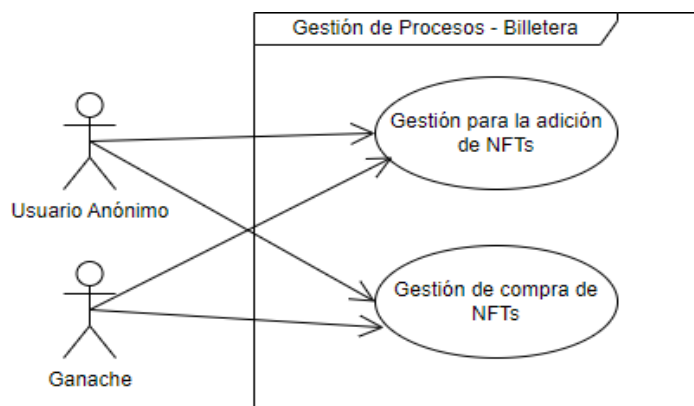


Figura 1. Caso de uso funcionalidad general de la aplicación.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Caso de uso # 1 Funcionalidad general de la aplicación	
Actores	Usuario Anónimo, Ganache
Camino Principal	Gestión para la adición de NFTs Gestión para la compra de NFTs
Precondiciones	Tener conexión con MetaMask y contar con una cuenta activa de Ethereum de Ganache. Conexión a internet para extraer las imágenes de la base de datos digital.
Postcondiciones	Cargar NFTs al prototipo de la billetera virtual. Comprar NFTs mediante MetaMask.

Tabla 12 Caso de uso - Funcionalidad general de la aplicación

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.3 MÓDULO ESPECIFICO DE LA APLICACIÓN

4.3.1 Caso de Uso específico 1: Conectar con MetaMask

En la Figura 2 se observa el diagrama de caso de uso específico donde se describen la conexión con MetaMask, generando un entorno de pruebas con Ethereum en la aplicación Ganache.

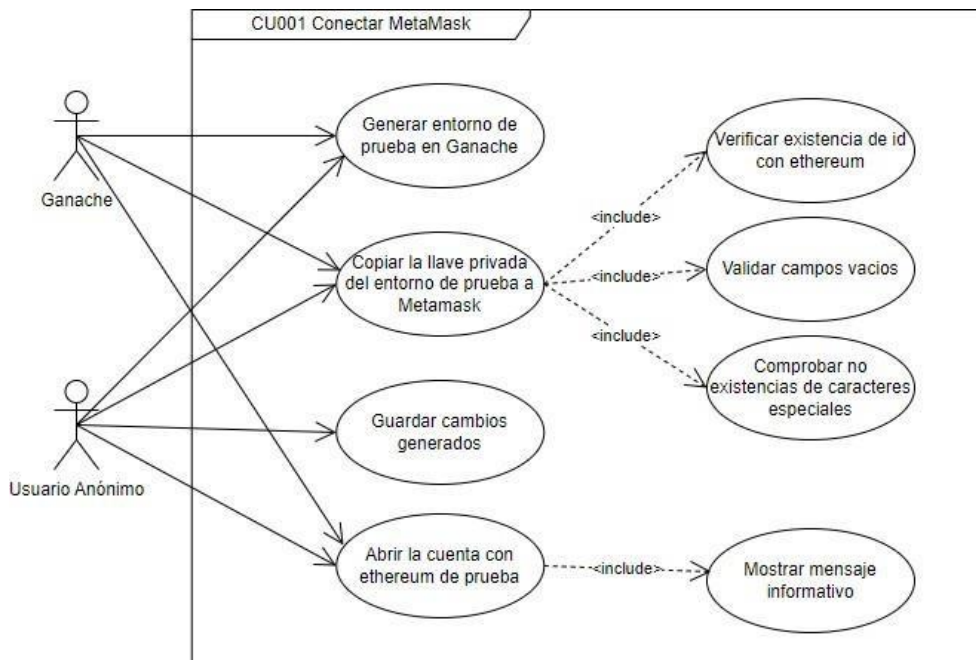


Figura 2. Caso de uso específico, conexión con MetaMask.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Caso de uso específico # 1 Conectar con MetaMask	
Actores	Usuario Anónimo, Ganache
Camino Principal	Generar entorno de prueba en Ganache. Copiar la llave privada del entorno de prueba a MetaMask. Abrir la cuenta con Ethereum de prueba.

Precondiciones	Abrir el entorno de prueba creado para poder utilizar el Ethereum.
Postcondiciones	Poseer una cuenta con Ethereum ficticio para realizar pruebas de adición y compra.

Tabla 13 Caso de uso específico - Funcionalidad general de la aplicación

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.3.2 Caso de Uso específico 2: Diseñar colección de NFT

En la Figura 3 se observa el diagrama de caso de uso específico donde se describen la creación de una colección propia de NFTs donde se combinan layers diseñados en Photoshop mediante un programa diseñado en Visual Studio Code que genera imágenes y archivos .json.

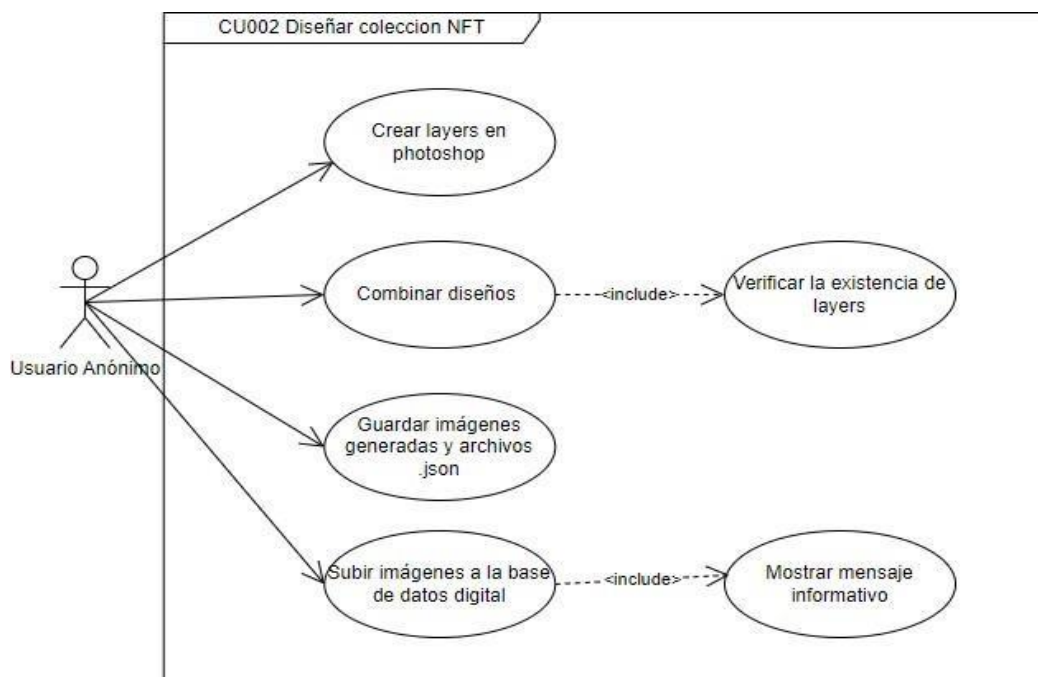


Figura 3. Caso de uso específico, Diseñar colección NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Caso de uso específico # 2 Diseñar colección de NFT	
Actores	Usuario Anónimo
Camino Principal	Crear layers en Photoshop Combinar diseños Guardar imágenes generadas y archivos .json Subir imágenes a la base de datos digital
Precondiciones	Tener el programa Photoshop y ciertas habilidades en creación y edición de imágenes.
Postcondiciones	Colección de imágenes y archivos json que respaldan la autenticidad y diseño único del NFT.

Tabla 14 Caso de uso específico - Diseñar colección de NFT

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.3.3 Caso de Uso específico 3: Agregar nuevo NFT

En la Figura 4 se observa el diagrama de caso de uso específico donde se describen la adición de un nuevo NFT al prototipo de billetera virtual, así como el débito de Ethereum de la cuenta conectada.

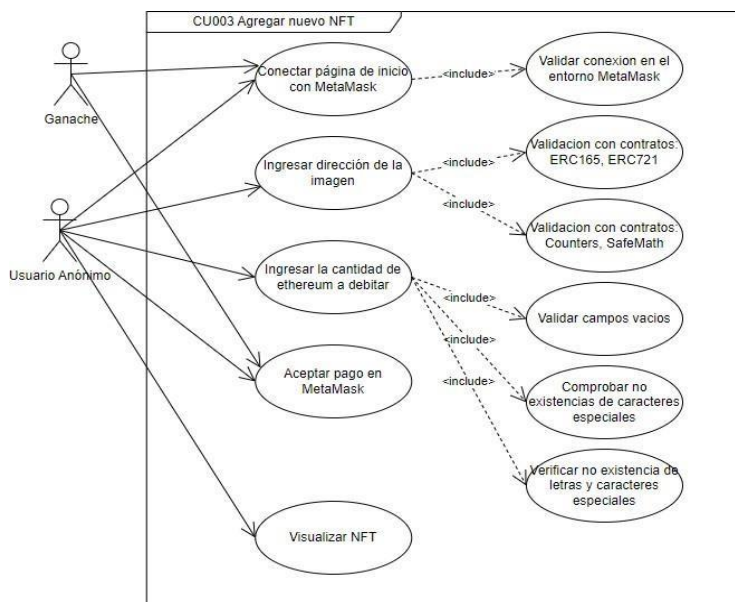


Figura 4. Caso de uso específico, Agregar nuevo NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Caso de uso específico # 3 Agregar nuevo NFT	
Actores	Usuario Anónimo
Camino Principal	<p>Conectar página de inicio con MetaMask.</p> <p>Ingresar dirección de la imagen.</p> <p>Ingresar la cantidad de Ethereum a debitar.</p> <p>Aceptar pago en MetaMask.</p> <p>Visualizar NFT.</p>
Precondiciones	<p>Tener conectada la página de inicio con la billetera MetaMask.</p> <p>Contar con Ethereum en la cuenta para realizar las transacciones.</p> <p>Contar con las imágenes en la base de datos digital.</p>
Postcondiciones	Galería de NFT única alojada en el prototipo de billetera.

Tabla 15 Caso de uso específico – Agregar nuevo NFT

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.3.4 Caso de Uso específico 4: Comprar NFT

En la Figura 5 se observa el diagrama de caso de uso específico donde se describen la compra de un NFT alojado en la galería del prototipo de billetera, esta transacción se realiza con Ethereum alojado en una cuenta de prueba de MetaMask.

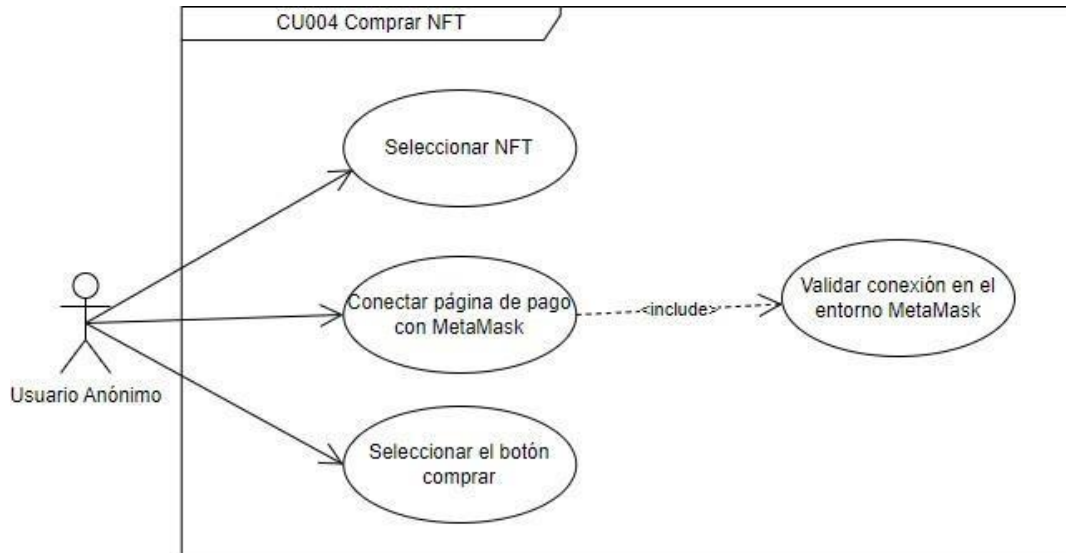


Figura 5. Caso de uso específico, Comprar NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Caso de uso específico # 4 Comprar NFT	
Actores	Usuario Anónimo
Camino Principal	Seleccionar NFT. Conectar página de pago con MetaMask. Seleccionar el botón comprar.
Precondiciones	Tener conectada la página de compra con la billetera MetaMask.
Postcondiciones	Página secundaria para realizar la transacción de débito en la compra de NFT.

Tabla 16 Caso de uso específico - Comprar NFT

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.3.5 Caso de Uso específico 5: Pagar NFT con MetaMask

En la Figura 6 se observa el diagrama de caso de uso específico donde se describe el pago mediante MetaMask y comprobar los parámetros detallados de la cuenta.

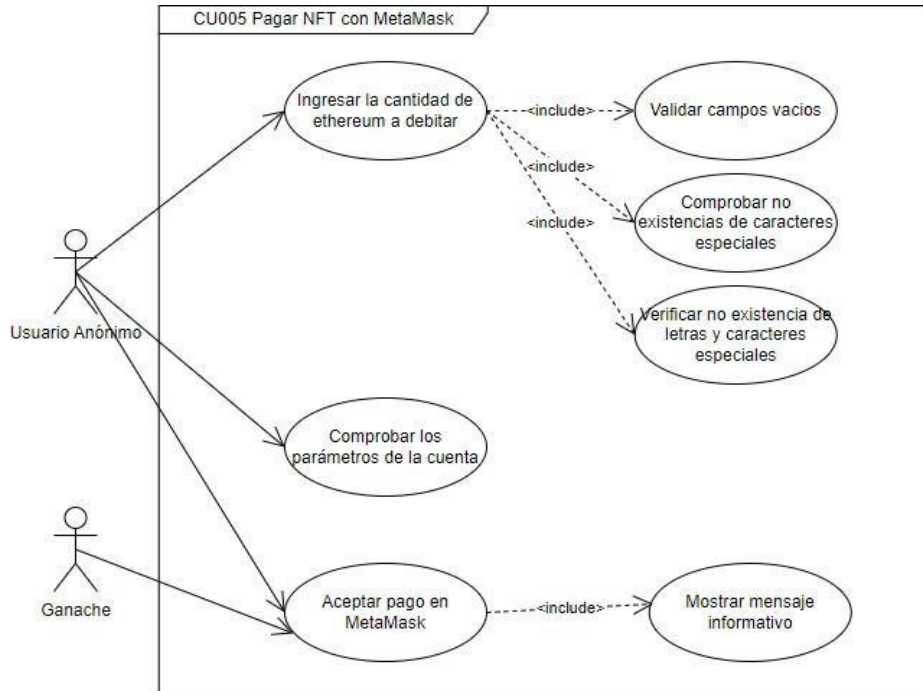


Figura 6. Caso de uso específico, Pagar NFT con MetaMask.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Caso de uso específico # 5 Pagar NFT con MetaMask	
Actores	Usuario Anónimo
Camino Principal	Ingresar la cantidad de Ethereum a debitar. Comprobar los parámetros de la cuenta Aceptar pago en MetaMask.
Precondiciones	Tener conectada la página de compra con la billetera MetaMask. Contar con Ethereum en la cuenta para realizar las transacciones.
Postcondiciones	Débito de Ethereum al comprar un NFT. Mensaje informativo de transacción exitosa.

Tabla 17 Caso de uso específico – Pagar NFT con MetaMask

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.4 MÓDULO DE ACTIVIDAD DE LA APLICACIÓN

4.4.1 Diagrama de actividad 1: Conexión con MetaMask

La figura 7 muestra las opciones del Usuario y de la aplicación Ganache, en donde se genera la conexión con la billetera virtual de Ethereum MetaMask.

En el caso de este módulo se genera el entorno de prueba en la aplicación Ganache, para poder obtener su respectiva clave privada y colocarla en el entorno de la billetera virtual de MetaMask, además de contar con sus respectivas validaciones para poder contar con Ethereum y realizar sus respectivas transacciones tanto de compra como de adición.

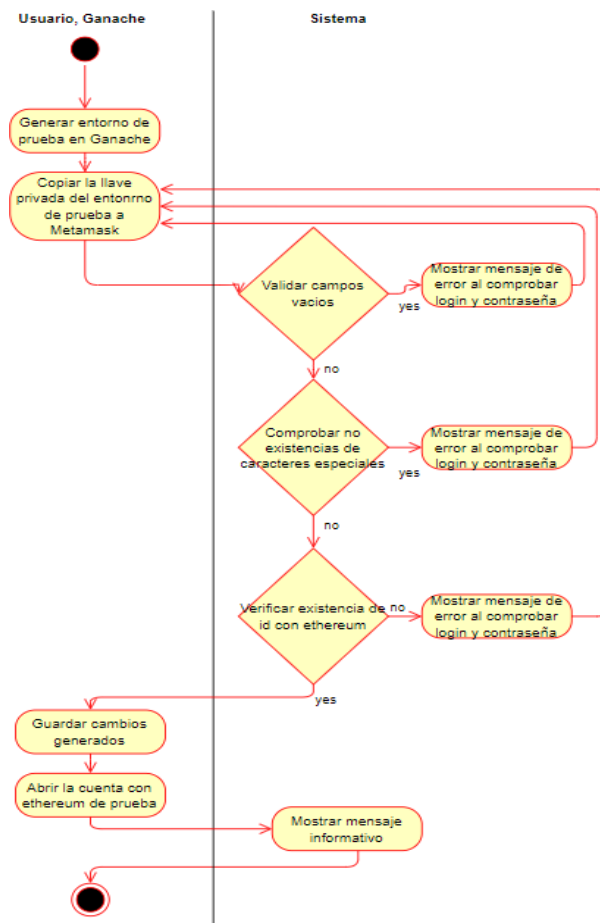


Figura 7. Diagrama de actividad para la conexión con MetaMask.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.4.2 Diagrama de actividad 2: Diseñar colección de NFT

La figura 8 muestra las opciones del Usuario, en donde se diseña una colección propia de NFT para ser publicada en el prototipo de billetera virtual.

En el caso de este módulo se diseñan distintos layers o diseños únicos, los cuales posteriormente van a ser combinados en un programa diseñado por el equipo de trabajo, el mismo hace sus respectivas validaciones y guarda las imágenes únicas creadas y sus archivos .json, los cuales dan fiabilidad y confianza al usuario ya que detalla la combinación de los elementos en la imagen y su identidad en la Web 3.0.

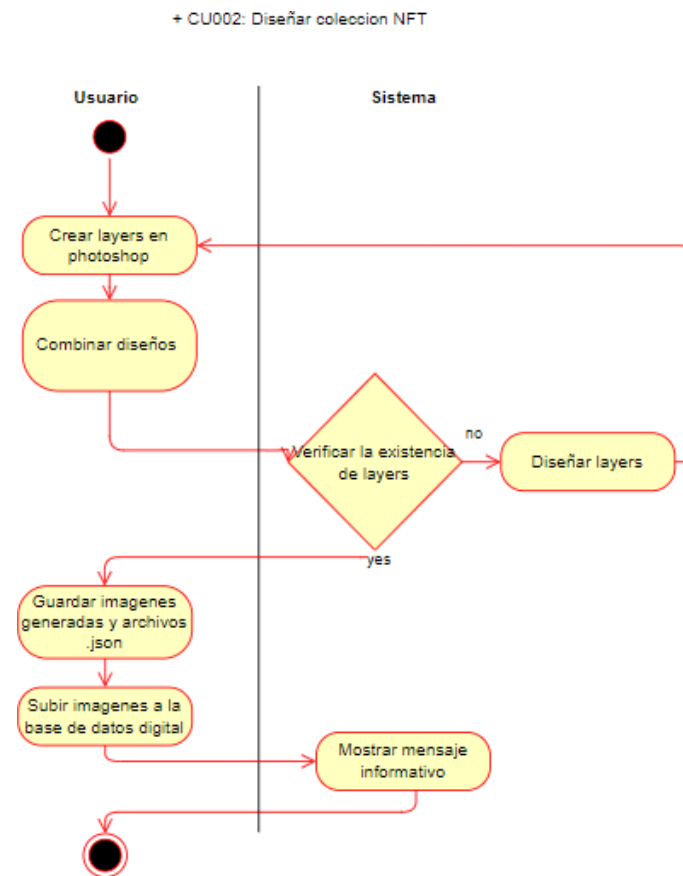


Figura 8. Diagrama de actividad para el diseño de NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.4.3 Diagrama de actividad 3: Agregar nuevo NFT

La figura 9 muestra las opciones del Usuario y de la aplicación Ganache, en donde se permite la adición al prototipo de billetera virtual.

En el caso de este módulo se ingresa la dirección de la imagen localizada en la base de datos digital para ser validada por los distintos contratos creados bajo el lenguaje Solidity, seguido se ingresa la cantidad necesaria de Ethereum a debitar de la cuenta en MetaMask, por último, se visualiza el NFT en la galería del prototipo de billetera virtual.

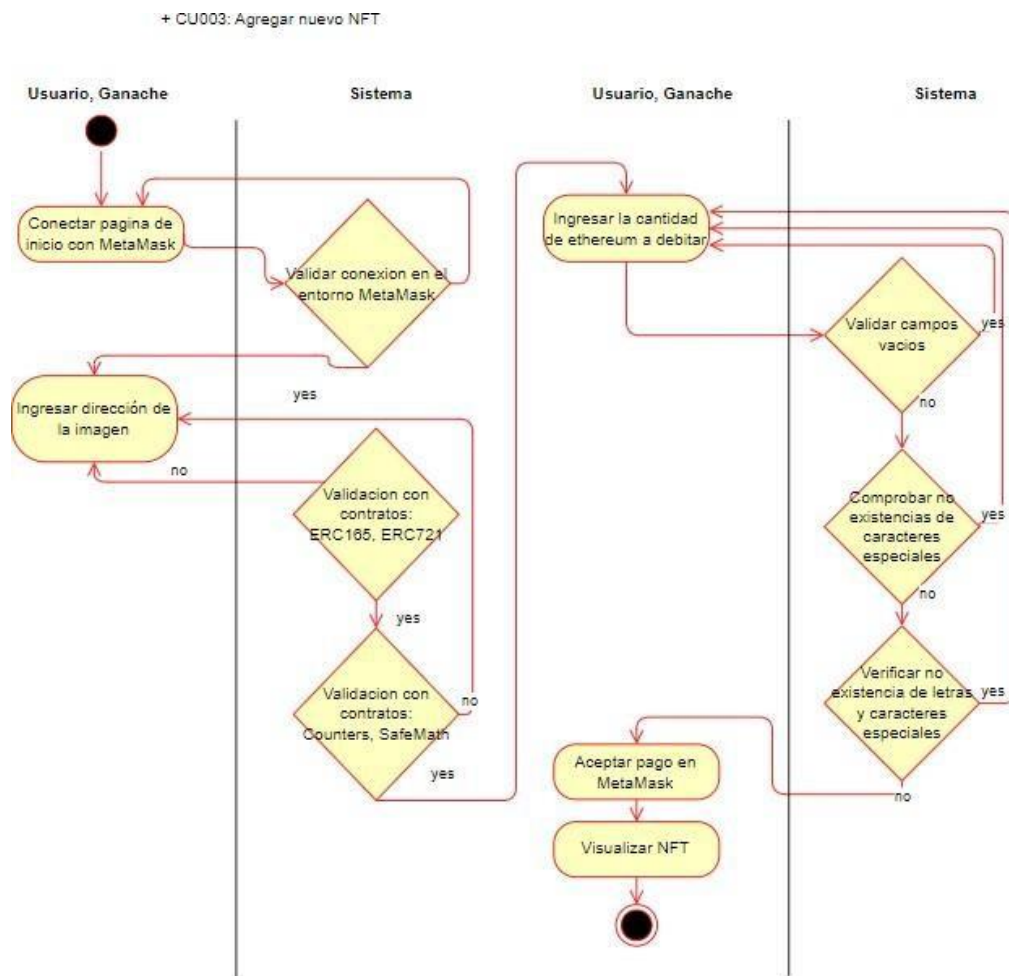


Figura 9. Diagrama de actividad para la adición de NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.4.4 Diagrama de actividad 4: Comprar NFT

La figura 10 muestra las opciones del Usuario, en donde se permite la compra de NFT mediante MetaMask.

En el caso de este módulo se selecciona el NFT ha ser comprado, seguido de esto nos lleva a otra página en donde brinda un agradecimiento por haber elegido ese diseño y un botón con una conexión a MetaMask.

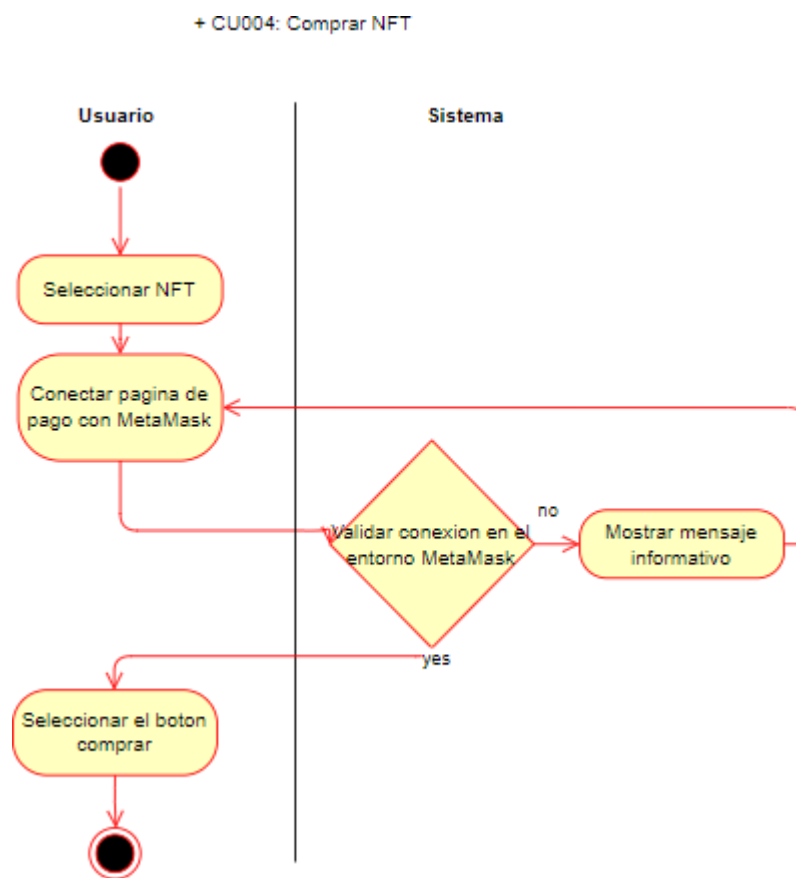


Figura 10. Diagrama de actividad para la compra de NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.4.5 Diagrama de actividad 5: Pagar NFT

La figura 11 muestra las opciones del Usuario y de la aplicación Ganache, en donde se permite el pago de NFT mediante MetaMask.

En el caso de este módulo se ingresa la cantidad de Ethereum a debitar, además se revisan los detalles de la transacción, se realizan las respectivas validaciones en el sistema, aceptamos el pago para ver un mensaje informativo de transacción exitosa.

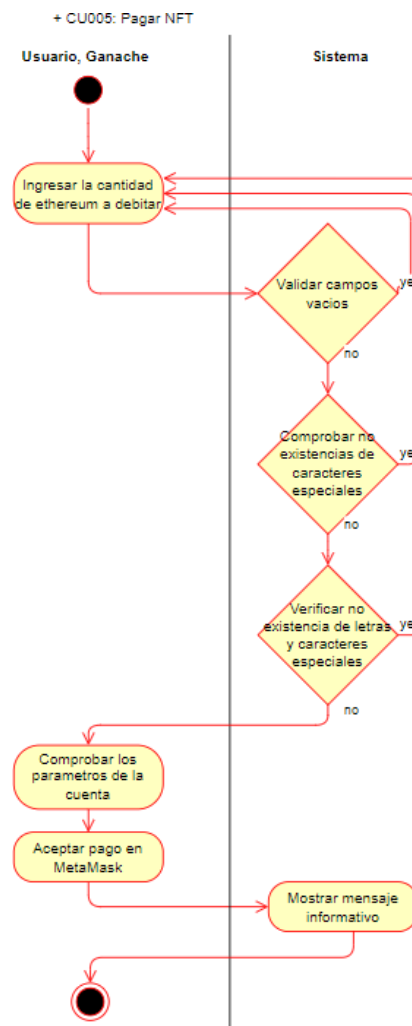


Figura 11. Diagrama de actividad para el pago de NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

4.5 ARQUETIPO DE LA APLICACIÓN

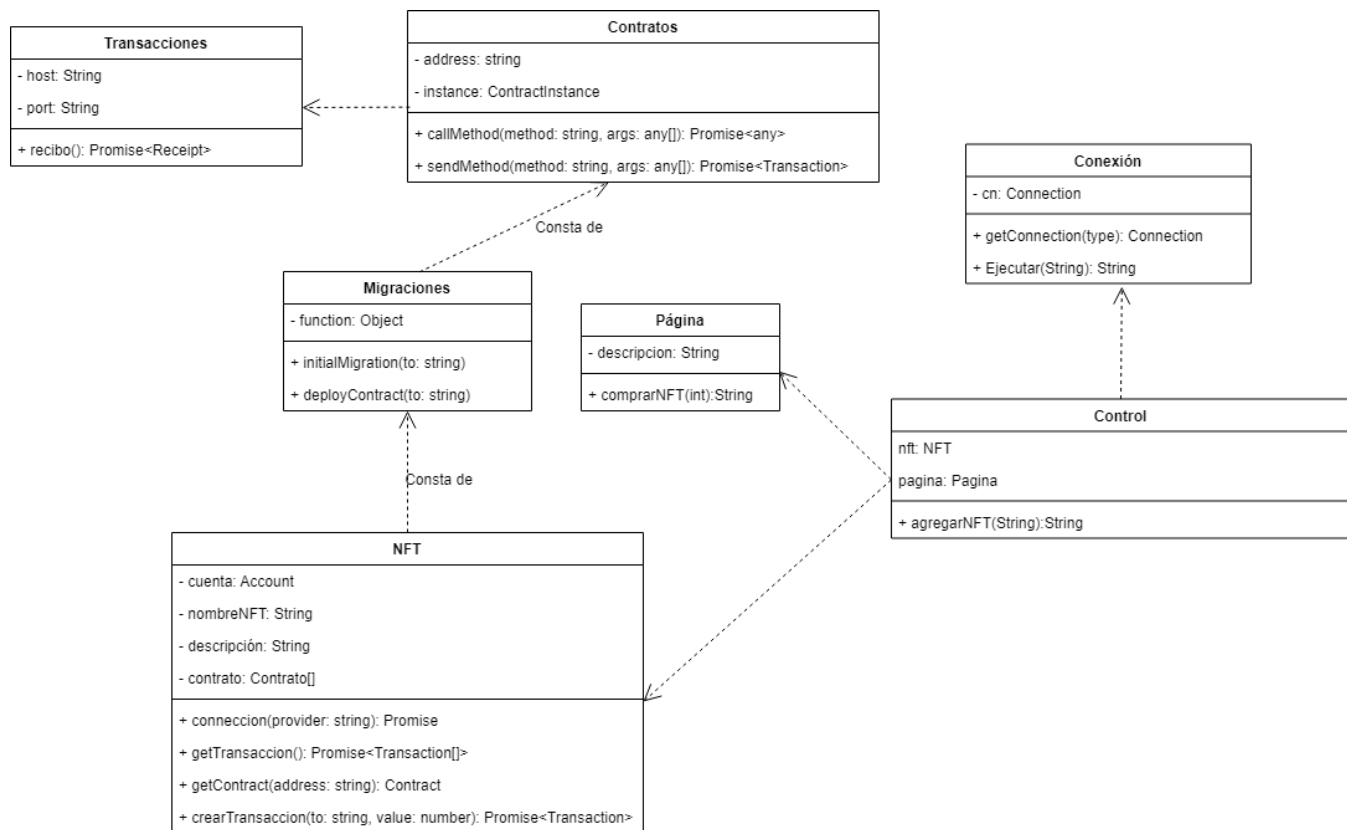


Figura 12 Diagrama de clases

Elaborado por: Steven Sarmiento y Alvaro Lomas.

La figura 12. En el diagrama de clases se representa un sistema que gestiona las transacciones de NFT (tokens no fungibles) entre diferentes usuarios. La clase "Conexión" es aquella que representa la conexión de la "Metamask" y contiene los métodos necesarios para establecer y cerrar la conexión. La clase "Control" representa el controlador principal del sistema, en este se encuentra el sistema necesario para agregar los activos digitales y se relaciona con la clase "NFT" a través de una relación de asociación. La clase "NFT" representa los tokens no fungibles y contiene los métodos necesarios para crear, actualizar y eliminar los tokens. Esta clase

también se relaciona con la clase "Migraciones" a través de una relación de composición, lo que significa que la clase "Migraciones" es parte de la clase "NFT" y solo existe mientras esta exista. La clase "Migraciones" representa el historial de migraciones y a través de esto se pueden ejecutar los diferentes “contratos inteligentes”, también contiene los métodos necesarios para ejecutar y revertir las migraciones. La clase "Contratos" se relaciona con la clase "Migraciones" a través de una relación de composición, este contiene los métodos necesarios para realizar las transacciones relacionándose con la clase "Transacciones". En resumen, este diagrama de clases representa un sistema que gestiona las transacciones de NFT entre diferentes usuarios, y muestra las clases involucradas y sus relaciones.

4.6 DIAGRAMA DE DESPLIEGUE

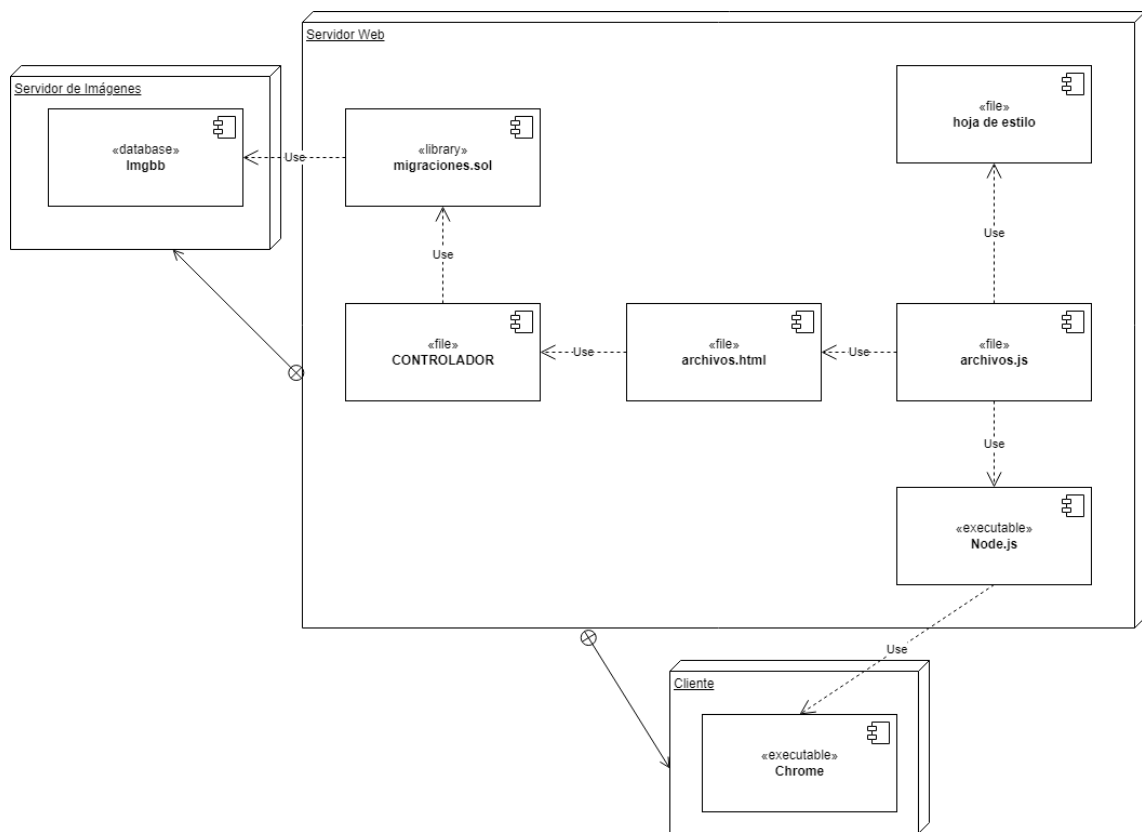


Figura 13 Diagrama de despliegue

Elaborado por: Steven Sarmiento y Alvaro Lomas.

El diagrama de despliegue que se visualiza en la figura 13 representa la arquitectura de un sistema web donde se visualiza el funcionamiento del sistema de billetera virtual de NFTs. El componente "Cliente" representa el software que se ejecuta en el navegador del usuario. El componente "Servidor web" representa el servidor que aloja la aplicación web y contiene archivos que ayudan al funcionamiento del programa, tales como: "Archivos JS", "Archivos HTML", "Hojas de Estilo", "Controladores" y "Migraciones". Estos almacenan los archivos que se utilizan para implementar la lógica de la aplicación, se define la apariencia visual de la aplicación, también se define la estructura y el contenido de la página web además de la lógica de control del servidor y terminan todas las tablas relacionándose con la tabla "Migraciones", que almacena el historial de migraciones realizadas en la web. La parte de imágenes y su base de datos se relaciona en general con el Servidor Web para permitir el acceso y la gestión de las imágenes compartidas por los usuarios.

4.7 PROTOTIPADO DEL SISTEMA

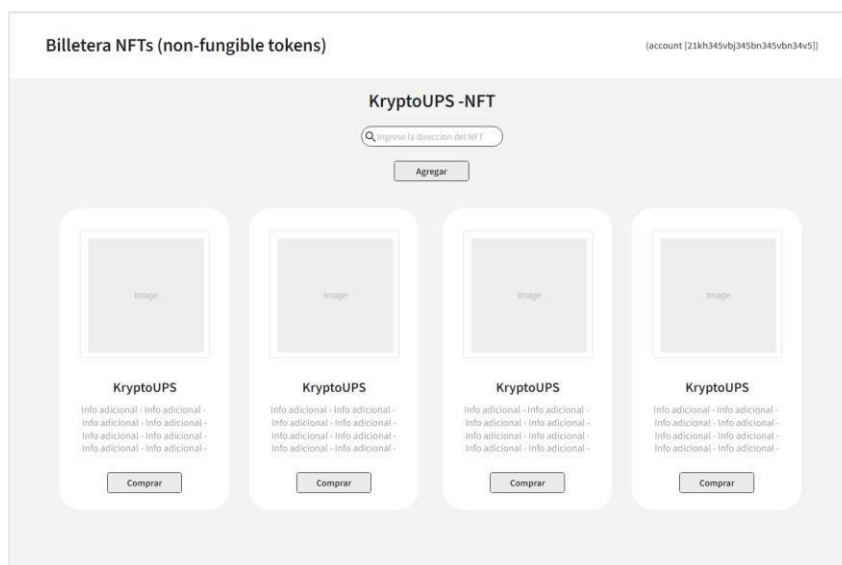


Figura 14 Prototipo 1 de la Aplicación

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Como se evidencia en la figura 14 la billetera cuenta con un módulo para ingresar la dirección de NFTs y luego visualizarla en la página, aquí se van a escoger entre varias opciones de este tipo de activos digitales para poder comprarlos. También en la parte superior derecha tendremos la cuenta con la cual se conecta a Metamask, además que como toque adicional se añadirá una transición en el fondo de la web.

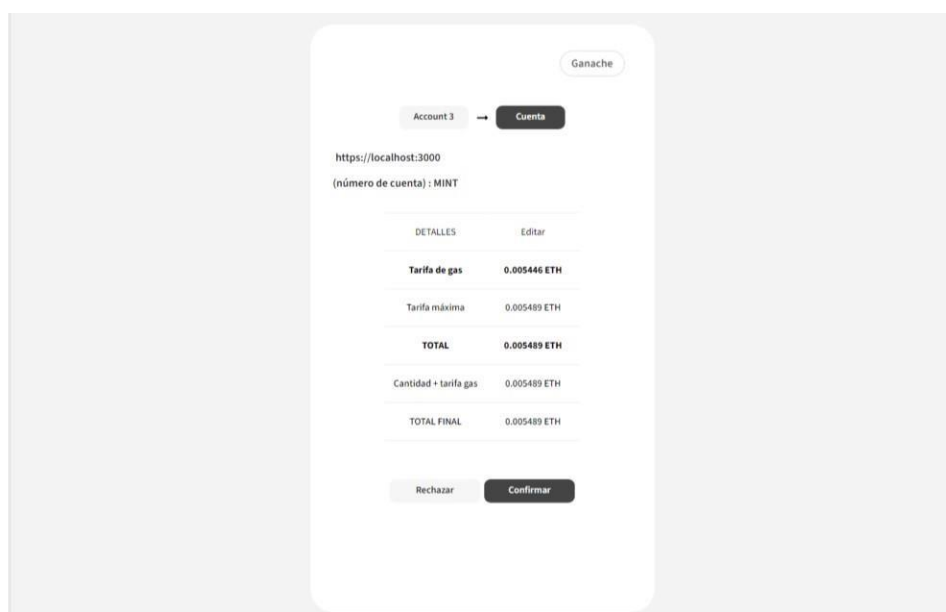


Figura 15 Prototipo 2 de la Aplicación

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la figura 15, al hacer clic en “comprar” podremos visualizar el monto de la transacción que se va a realizar para adquirir un NFT, esta pantalla es proporcionada por la misma MetaMask, previo a esto es indispensable tener la moneda digital con la cual se puedan realizar transacciones en la blockchain, en este caso Ethereum (ETH), cabe recalcar que al ser un prototipo nos ayudamos del software llamado “Ganache” el cual proporciona un entorno donde se tienen ETH para pruebas.



Figura 16 Prototipo 3 de la Aplicación

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Por último, en la figura 16, podremos evidenciar un mensaje de compra por parte de la página web.

4.8 FUNCIONALIDAD DEL SISTEMA

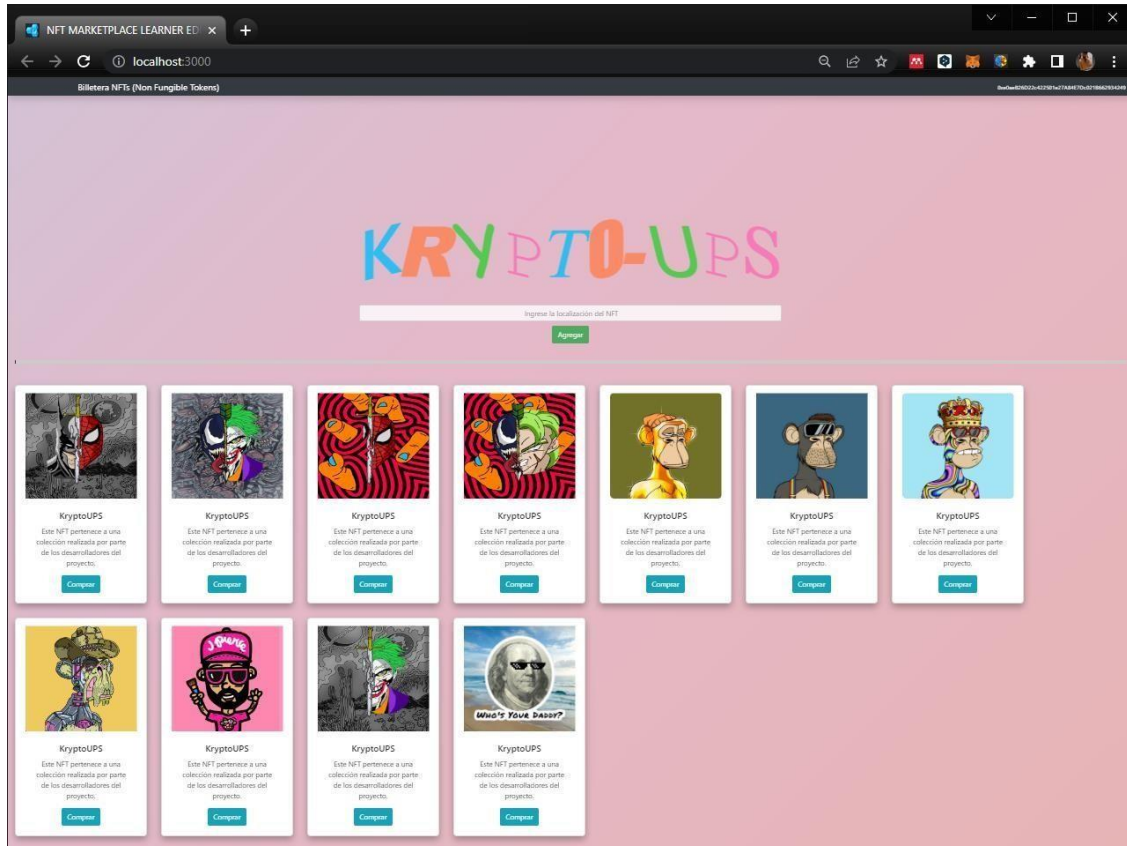


Figura 17 Pantalla Inicio de la Aplicación

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la figura 17, se evidencia el cumplimiento del prototipado de la página principal, en la cual se observa su barra de agregación para NFT, además de contar con la galería de colecciones de NFT cargadas por los usuarios.

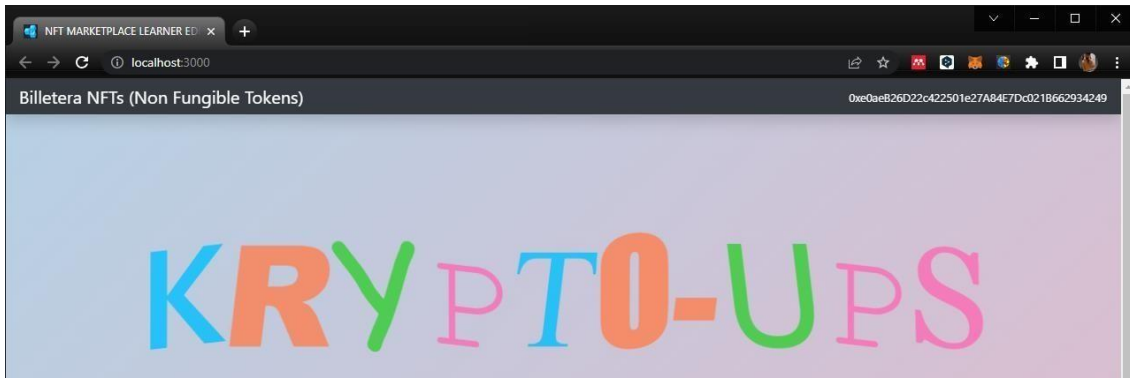


Figura 18 Dirección de Billetera

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la parte superior derecha de la figura 18, se presenta la dirección de la billetera en la cual extraemos el Ethereum de prueba para realizar las transacciones.

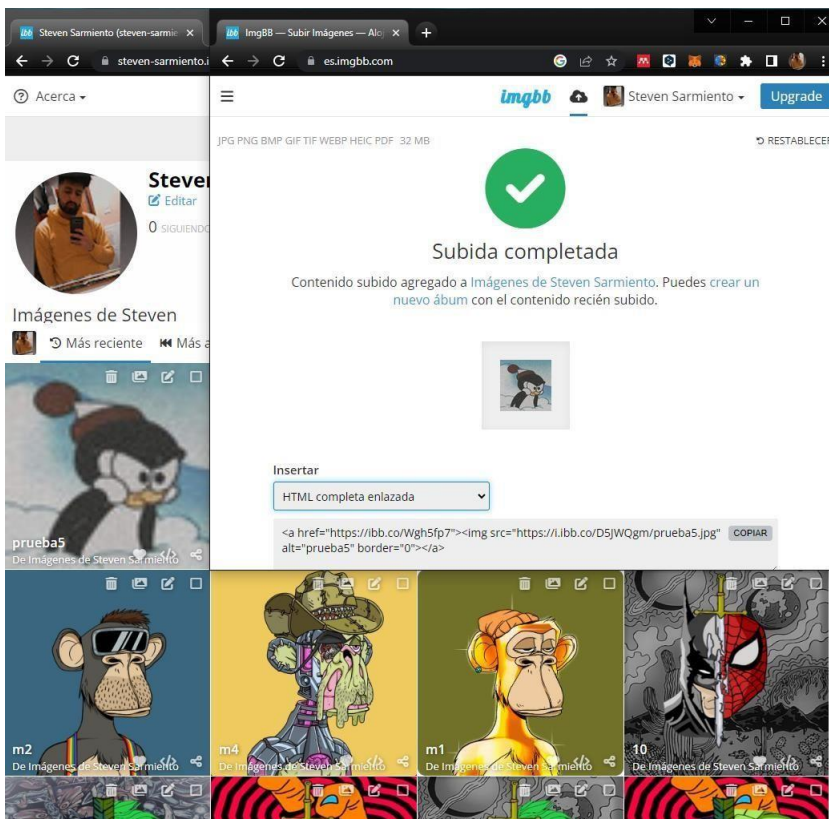


Figura 19 Imágenes en la Base de Datos Digital.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la figura 19, tenemos nuestra base de datos digital en la cual colocamos nuestros NFT, posterior a esto situamos en insertar “HTML completo enlazado” para que nuestro NFT se coloque con un tamaño determinado en nuestro prototipo y se ajuste a la galería principal.

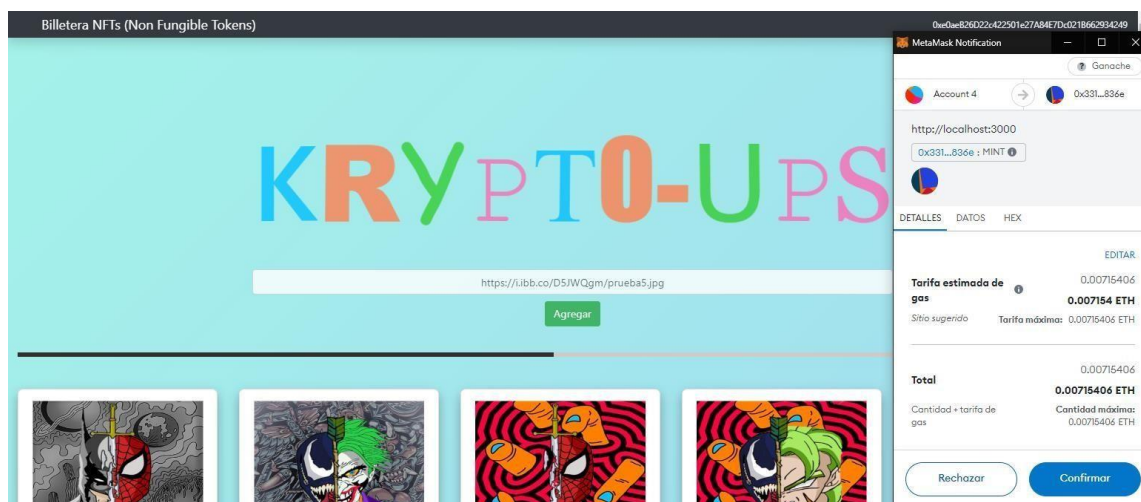


Figura 20 Agregación de NFT al prototipo.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la figura 20 se indica los pasos a seguir para agregar un nuevo NFT en nuestro prototipo de billetera, para ello se coloca la dirección web de nuestra imagen subida en nuestra base de datos digital, posterior a esto al dar clic en agregar nos redirecciona a una ventana flotante de MetaMask en la cual observamos el consumo de Ethereum que tendrá esta transacción, confirmamos y recargamos nuestra página para poder visualizar nuestro nuevo NFT en la galería de la billetera.

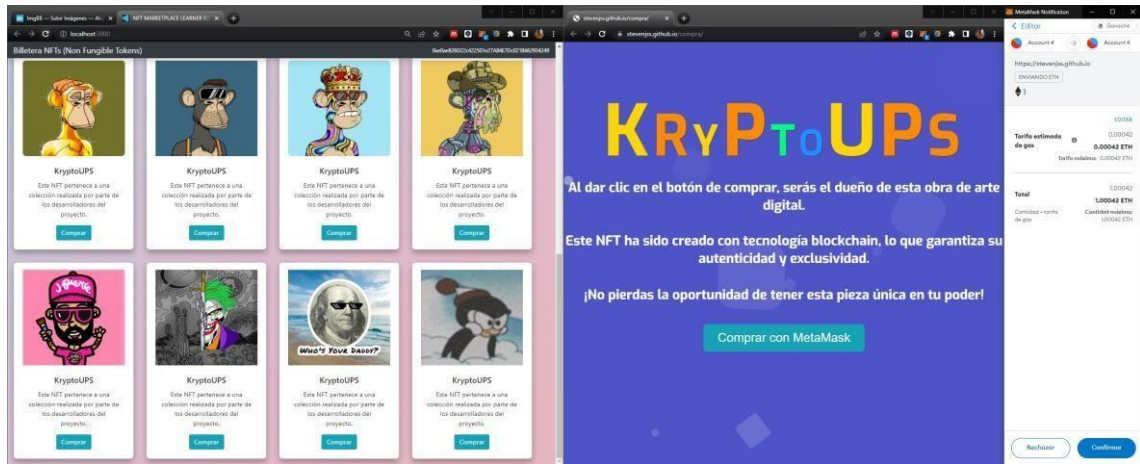


Figura 21 Compra de NFT.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Al dar clic en el botón comprar, como se observa en la figura 21, nos redireccionara a una nueva ventana donde podemos realizar la compra del NFT con nuestro Ethereum de prueba, confirmamos y automáticamente nos debita la cantidad acordada de nuestra moneda virtual.

V CAPITULO 4

5.1 PRUEBAS DE FUNCIONAMIENTO

5.1.1 INFORME DE PRUEBAS DE FUNCIONAMIENTO EN SONARCLOUD

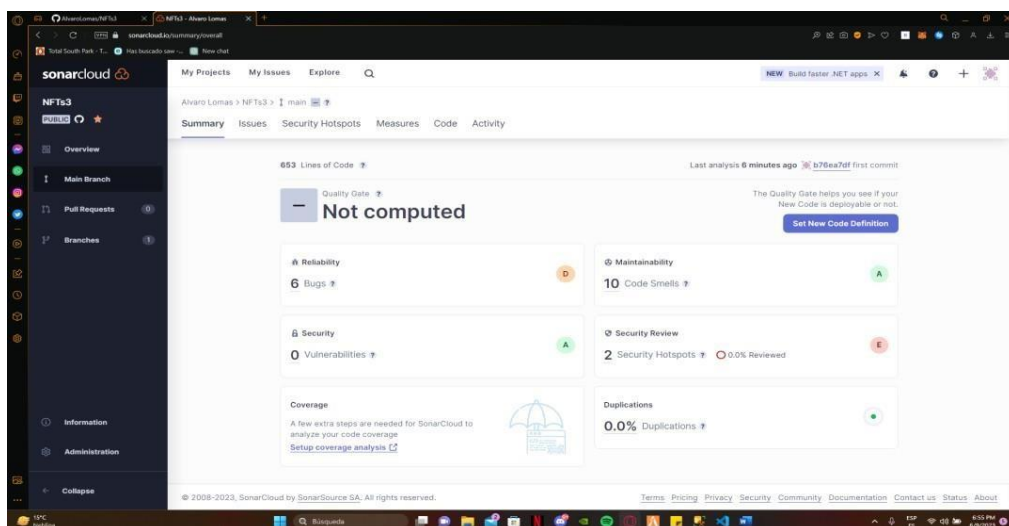


Figura 22. Resumen de las pruebas en SonarCloud con código corregido.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Fiabilidad:

El cambio que se han realizado para contar con una mejor calificación en la plataforma de SonarCloud está:

Reparación de 3 bugs en las líneas especificadas, entre estas resaltan la adición de del "tipo_de_documento" siendo la utilizada: HTML5

Entre algunos cambios que no se han realizado para contar con una mejor calificación en la plataforma de SonarCloud son los siguientes:

El uso de console.log en SonarCloud puede advertir sobre el código de producción, ya que se considera una práctica no deseada o insegura. Es por lo que se marca como “bug”. La plataforma al ser un prototipo es mejor dejar estas llamadas a consolas como guías.

El uso Service Workers puede tener consecuencias en la funcionalidad de la aplicación, ya que este se ejecuta en segundo plano y permite realizar tareas como el almacenamiento en caché, las notificaciones push y la gestión de eventos de red.

El uso en el “background” para usar un fondo con animación de tipo “gradiente” se va a conservar ya que sin este elemento esto sería imposible.

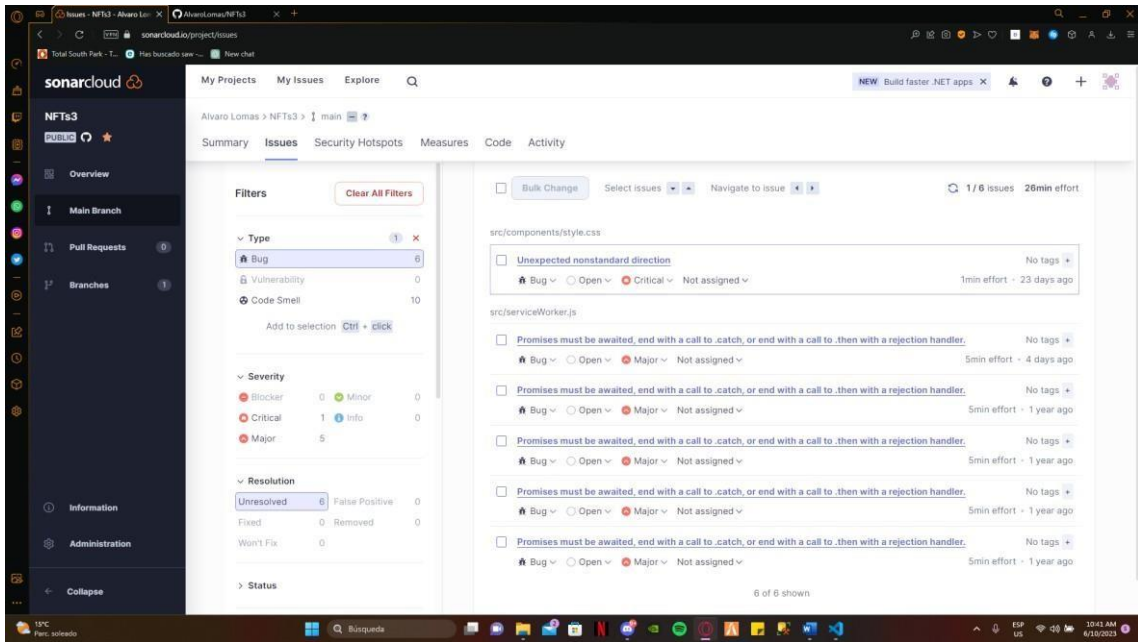


Figura 23. Apartado de bugs encontrados para Fiabilidad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

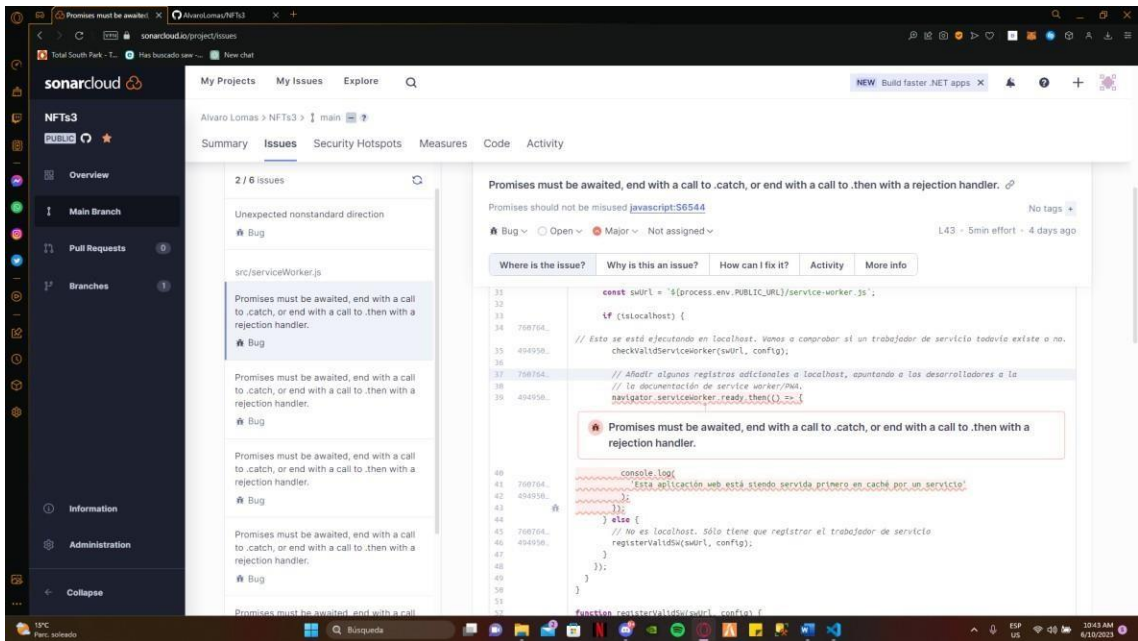


Figura 24. Ejemplo de bug encontrado para Fiabilidad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Seguridad:

El "Security Rating" es de calificación A, esto indica que el proyecto ha recibido una calificación alta en términos de seguridad. Esta calificación indica que se han implementado buenas prácticas de seguridad en el código y la configuración del proyecto.

Los cambios para tener menos Code Smells fue la eliminación de comentarios y cambio en “missing keys”.

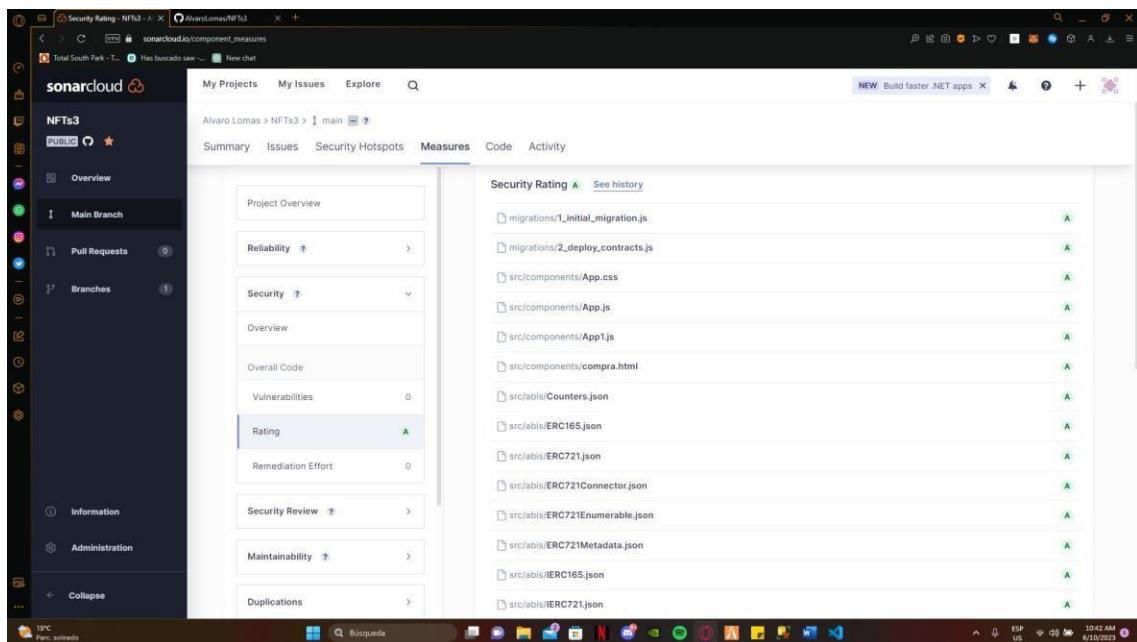


Figura 25. Apartado de Seguridad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Mantenibilidad:

Esta métrica nos indica que existen 10 Code Smells, siendo esta menor al 5% total. Se solucionaron 2 de las 12 encontradas, las demás fueron obviadas debido al funcionamiento del sistema.

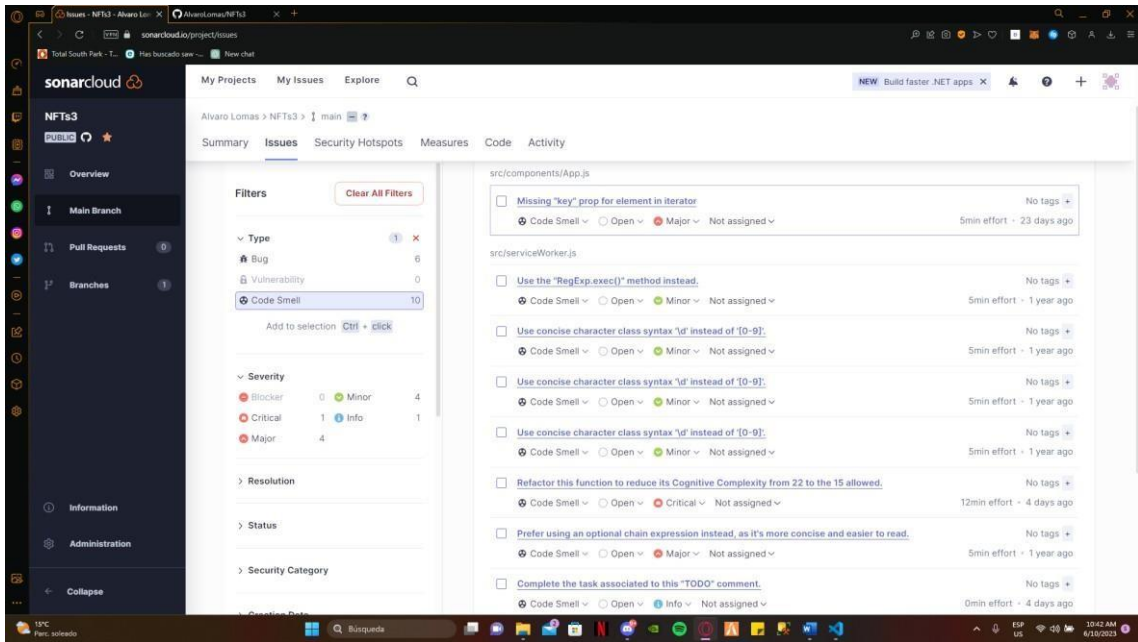


Figura 26. Apartado de code smells encontradas para Mantenibilidad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

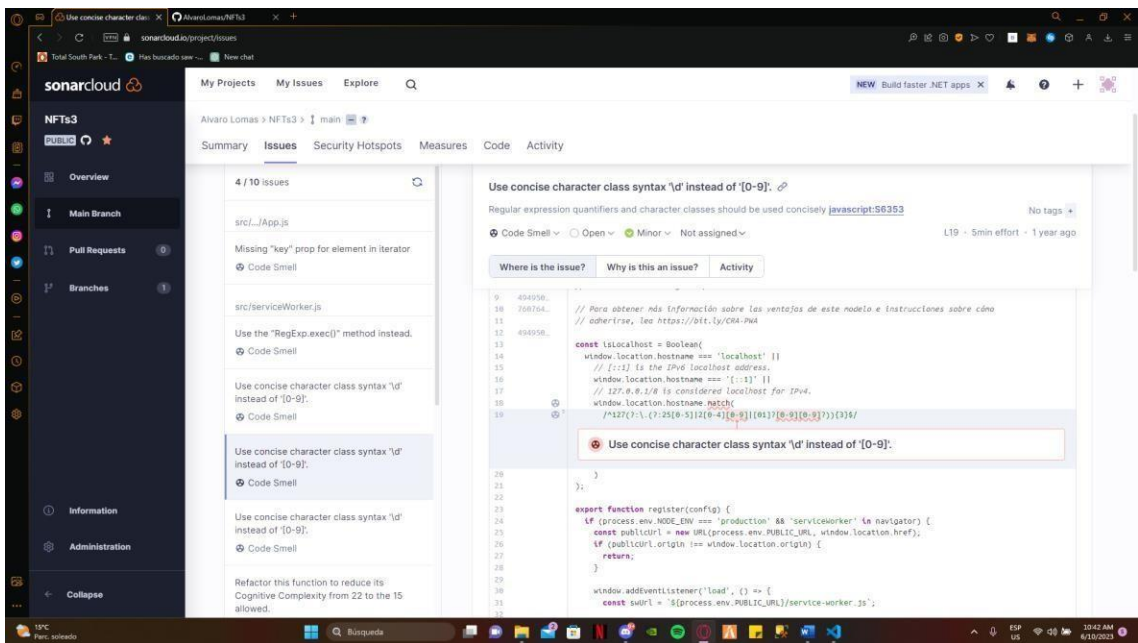


Figura 27. Ejemplo de code smells encontrado para Mantenibilidad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Revisión de Seguridad:

Se han encontrado dos “Puntos de acceso de seguridad”, estos no pueden ser modificados ni cambiados, ya que especifican scripts para el uso de “.jquery” y “MetaMask” respectivamente.

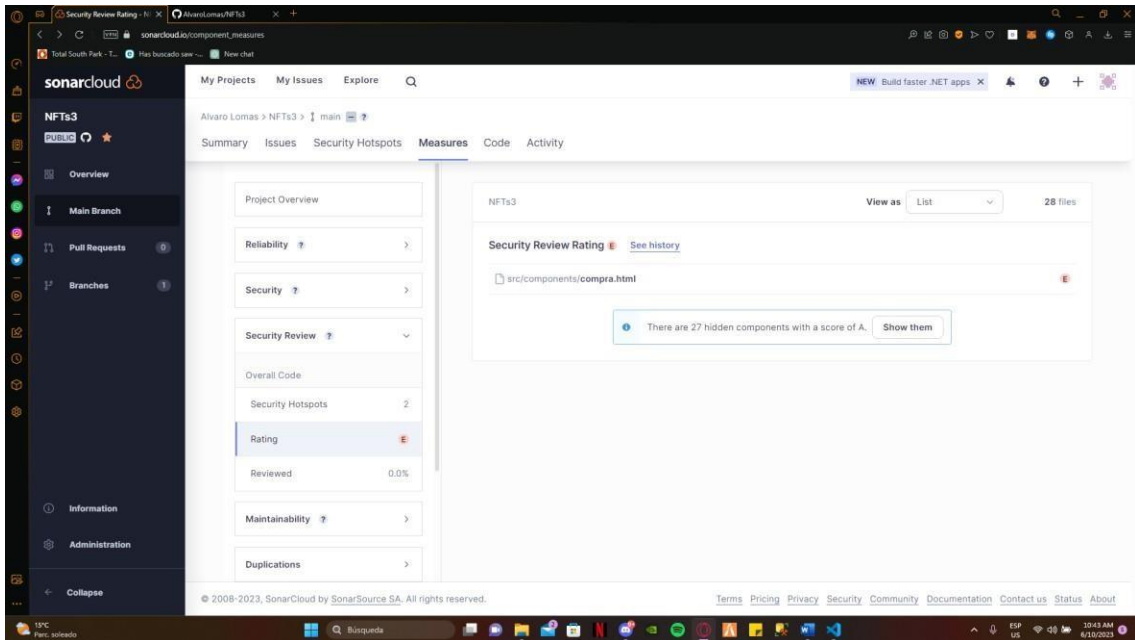


Figura 28. Apartado de Revisión de Seguridad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

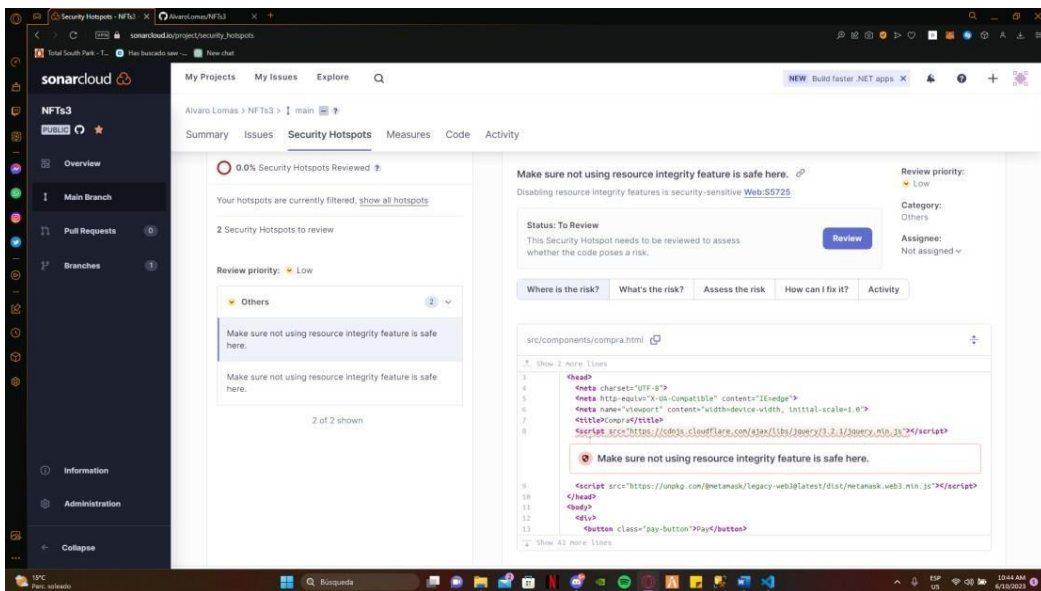


Figura 29. Ejemplo de problema encontrado para el apartado de Revisión de Seguridad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

5.1.2 COMPARACIÓN DE RESULTADOS

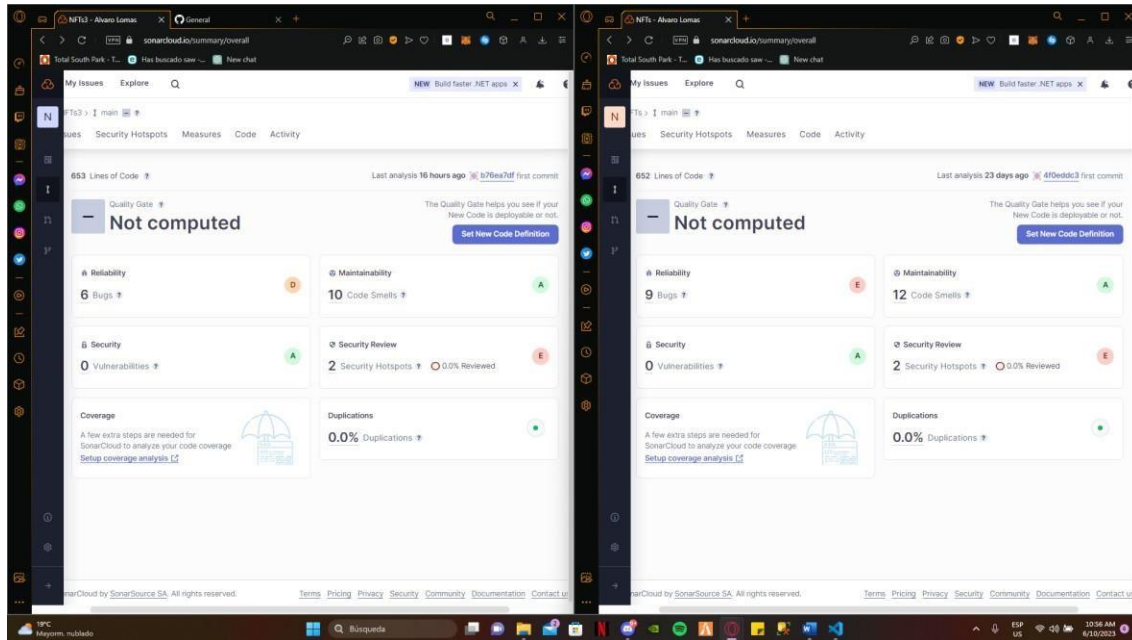


Figura 30. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código antiguo (derecha).

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Fiabilidad:

Como se observa en la figura 31, se evidencia en el lado izquierdo la corrección de 3 bugs (Code Smells) que nos sirven para una limpieza de código y mejorar la calidad de este. En la parte derecha de la figura se observa el código original que cuenta con 9 bugs entre los cuales tenemos problemas en “service worker”, “style.css” y “compra.html”.

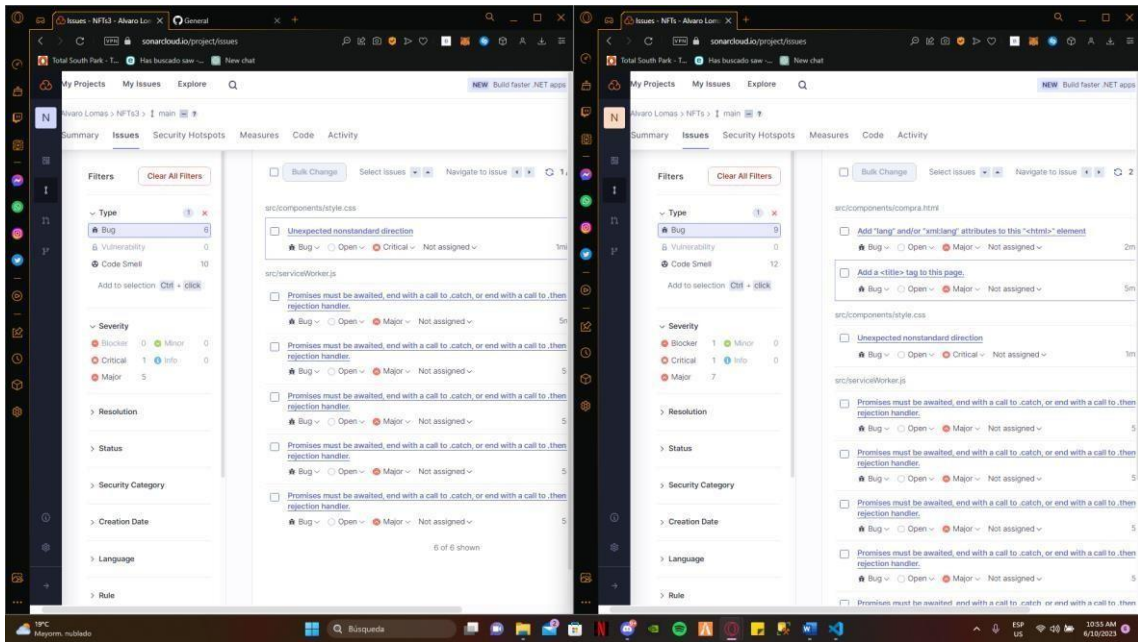


Figura 31. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Fiabilidad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Seguridad:

Como se puede observar en la figura 32, la seguridad manejada en cuanto a al sistema realizado es excelente, teniendo una calificación muy buena y evitando algún problema.

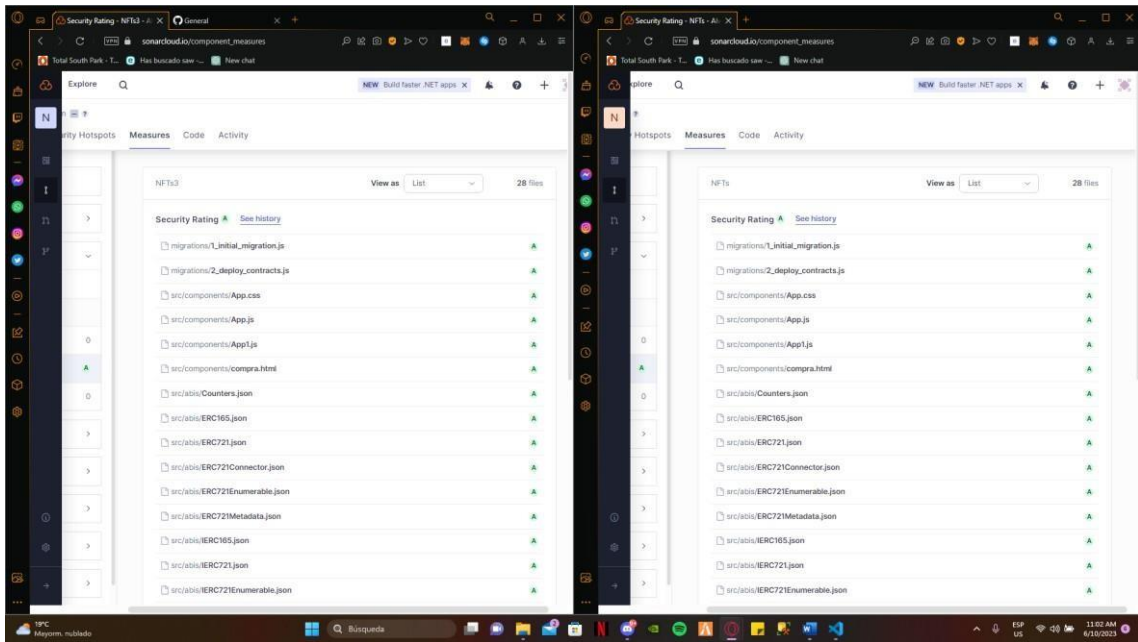


Figura 32. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Seguridad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Mantenibilidad:

Como se puede observar en la figura 33, la mantenibilidad o facilidad que tiene el sistema para modificar y adaptarse o mejorarse es excelente, teniendo una buena capacidad de cambios.

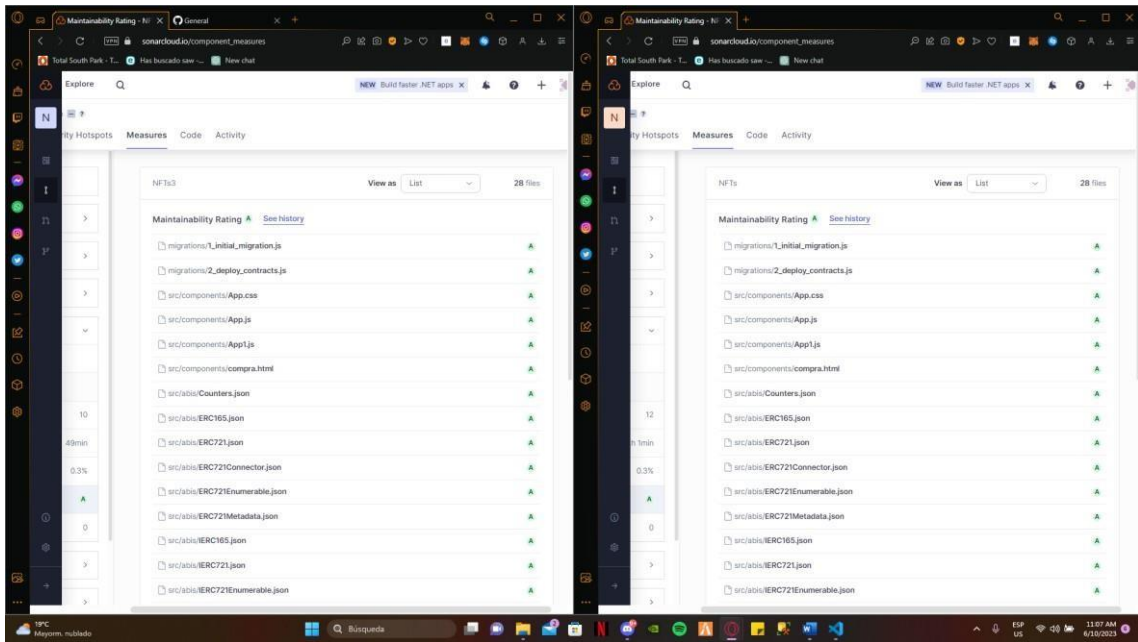


Figura 33. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Mantenibilidad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Revisión de Seguridad:

Esta métrica no se ha podido mejorar como se evidencia en la figura 34, ya que se utilizan scripts necesarios para el correcto funcionamiento de la aplicación web, sin estas varias operaciones no se pueden concretar correctamente.

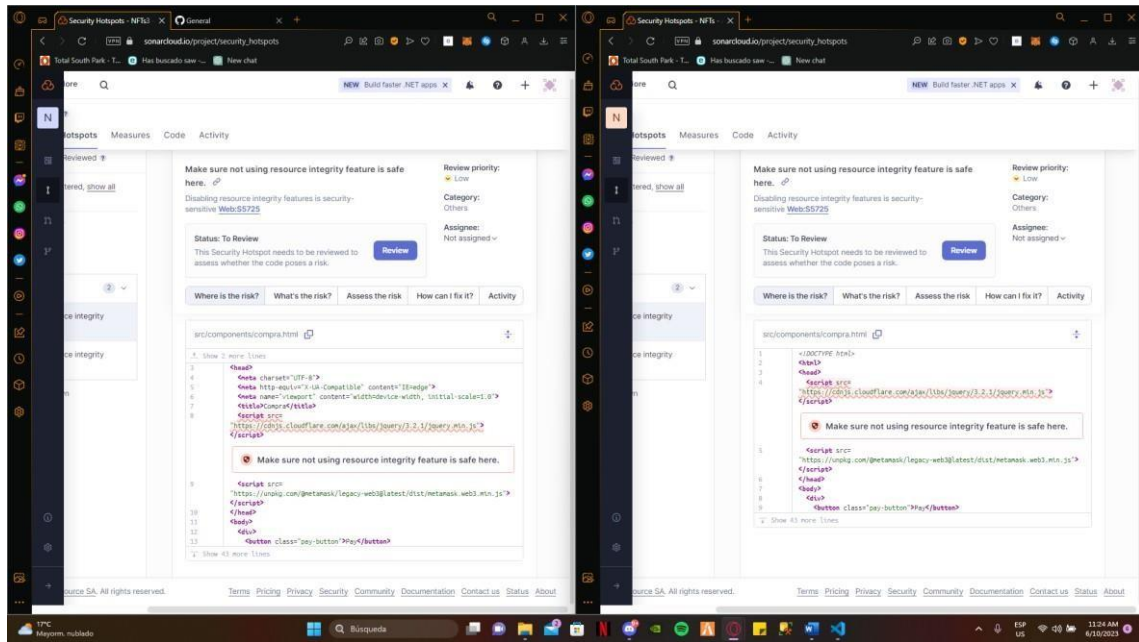


Figura 34. Resumen de las pruebas en SonarCloud con código corregido (izquierda) y código original (derecha) en el apartado de Revisión de Seguridad.

Elaborado por: Steven Sarmiento y Alvaro Lomas.

5.2 PRUEBAS DE CAJA NEGRA.

Comprobar el correcto funcionamiento del prototipo. Para ello se enfoca en las entradas y salidas del sistema, además del comportamiento esperado del mismo.

En la Tabla 18 muestra los resultados para la tarea “CREAR COLECCIÓN NFT”, en donde se destaca el funcionamiento óptimo del programa de unión de layers.

N°	Tarea	Acción	Resultado
1	CREAR COLECCIÓN NFT	Diseño de layers	Layers correctos y descargados
2		Ingreso de layers al programa para su unión.	Error: Cantidad de layers insuficientes o cantidad de uniones excedidas
3		Ingreso de layers al programa para su unión.	Creación de NFT con sus respectivos .json de información.

Tabla 18 Pruebas de caja negra – Crear colección NFT

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la Tabla 19 muestra los resultados para la tarea “CONEXIÓN CON METAMASK”, en el cual previamente se comprobaron las versiones de Ganache (v2.5.4) que sea compatible con MetaMask.

N°	Tarea	Acción	Resultado
1	CONEXIÓN CON METAMASK	Seleccionar un ambiente de prueba en Ganache.	Ambiente vacío, ETH insuficiente.
2		Seleccionar un ambiente de prueba en Ganache.	Llave privada correcta, ETH suficiente para realizar las transacciones.
3		Insertar la llave privada de Ganache en MetaMask.	Error, llave incorrecta.
4		Insertar la llave privada de Ganache en MetaMask.	Llave correcta, ambiente de pruebas listo para usar.

Tabla 19 Pruebas de caja negra – Conexión con MetaMask

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la Tabla 20 muestra los resultados para la tarea “AGREGAR NFT”.

N°	Tarea	Acción	Resultado
1	AGREGAR NFT	Seleccionar NFTs para subir a la base de datos digital.	Listado vacío, error al subir imágenes
2		Seleccionar NFTs para subir a la base de datos digital.	Colección de NFT en la base de datos digital
3		Subir NFT con su enlace desde la base de datos digital.	Error al subir NFT, campo vacío.
4		Subir NFT con su enlace desde la base de datos digital.	Ventana emergente de MetaMask
5		Comprobar Datos correctos en MetaMask y el valor de ETH a debitar	Error, los datos son incorrectos o el valor a debitar está vacío.
6		Comprobar Datos correctos en MetaMask y el valor de ETH a debitar.	Datos correctos, NFT insertado en la galería del prototipo.

Tabla 20 Pruebas de caja negra – Agregar NFT

Elaborado por: Steven Sarmiento y Alvaro Lomas.

En la Tabla 21 muestra los resultados para la tarea “COMPRAR NFT”.

N°	Tarea	Acción	Resultado
1	COMPRAR NFT	Seleccionar NFT a comprar	Ventana nueva para realizar la transacción.
2		Dar clic en el botón comprar NFT.	Ventana emergente de MetaMask.
3		Comprobar Datos correctos en MetaMask y el valor de ETH a debitar.	Error, los datos son incorrectos o el valor a debitar está vacío.

4		Comprobar Datos correctos en MetaMask y el valor de ETH a debitar.	Mensaje de pago correcto.
----------	--	--	---------------------------

Tabla 21 Pruebas de caja negra – Comprar NFT

Elaborado por: Steven Sarmiento y Alvaro Lomas.

5.3 PRUEBAS DE ACEPTACIÓN

Prueba de Aceptación Conexión con MetaMask	
Código	KUPS-001
Requerimiento evaluado	Conectar a MetaMask
Descripción	El sistema se conecta con la billetera ETH, MetaMask.
Resultado esperado	El sistema logra conectarse a MetaMask con la llave privada brindada por Ganache.
Resultado obtenido	Resultado esperado
Evaluación	Revisado por: Julio Proaño

Tabla 22 Pruebas de aceptación– MetaMask

Elaborado por: Steven Sarmiento y Alvaro Lomas.

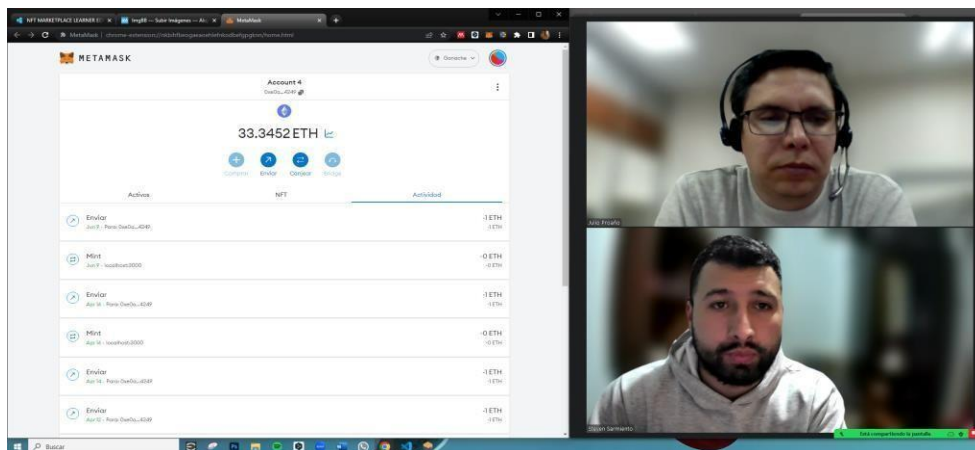


Figura 35. Evidencia para Prueba de aceptación – Conexión .

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Prueba de Aceptación Agregar NFT	
Código	KUPS-002
Requerimiento evaluado	Agregar NFT
Descripción	El sistema permite agregar NFTs con la dirección web de la base de datos digital y su respectivo debido transaccional de ETH.
Resultado esperado	El sistema sube los nuevos NFT validando los mismos con los contratos inteligentes creados.
Resultado obtenido	Resultado esperado
Evaluación	Revisado por: Julio Proaño

Tabla 23 Pruebas de aceptación– Agregar

Elaborado por: Steven Sarmiento y Alvaro Lomas.

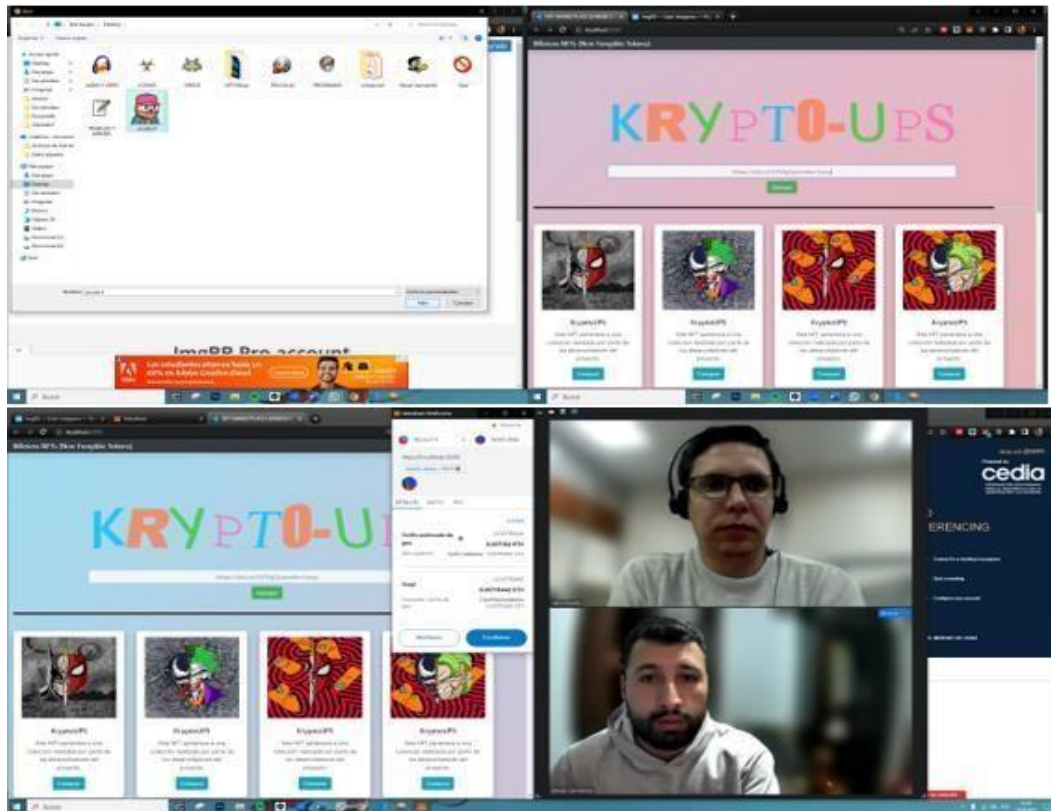


Figura 36. Evidencia para Prueba de aceptación – Agregar .

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Prueba de Aceptación Galería de NFT	
Código	KUPS-003
Requerimiento evaluado	Visualizar Galería de NFT
Descripción	El sistema permite visualizar la galería de NFTs.
Resultado esperado	El sistema al actualizarse permite observar los NFTs agregados.
Resultado obtenido	Resultado esperado
Evaluación	Revisado por: Julio Proaño

Tabla 24 Pruebas de aceptación– Galería

Elaborado por: Steven Sarmiento y Alvaro Lomas.

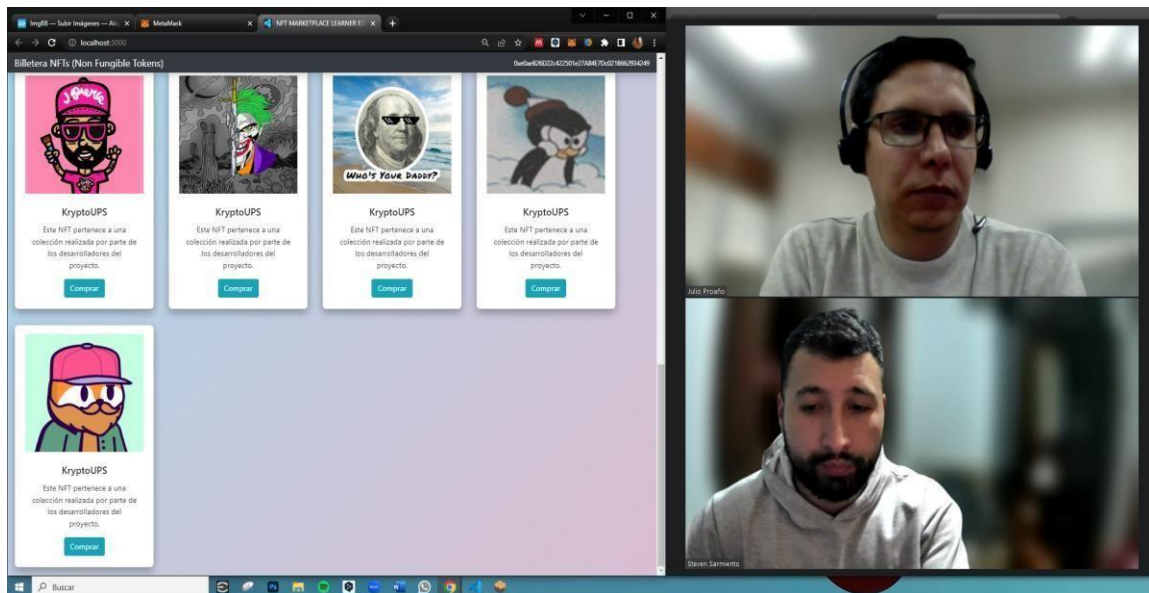


Figura 37. Evidencia para Prueba de aceptación – Galería .

Elaborado por: Steven Sarmiento y Alvaro Lomas.

Prueba de Aceptación Comprar NFT	
Código	KUPS-004
Requerimiento evaluado	Comprar NFT
Descripción	El sistema permite realizar la compra de los NFT mediante el débito respectivo de ETH.
Resultado esperado	El sistema al actualizarse permite comprar los NFTs alojados en la galería del sistema.
Resultado obtenido	Resultado esperado
Evaluación	Revisado por: Julio Proaño

Tabla 25 Pruebas de aceptación – Comprar

Elaborado por: Steven Sarmiento y Alvaro Lomas.



Figura 38. Evidencia para Prueba de aceptación – Comprar .

Elaborado por: Steven Sarmiento y Alvaro Lomas.

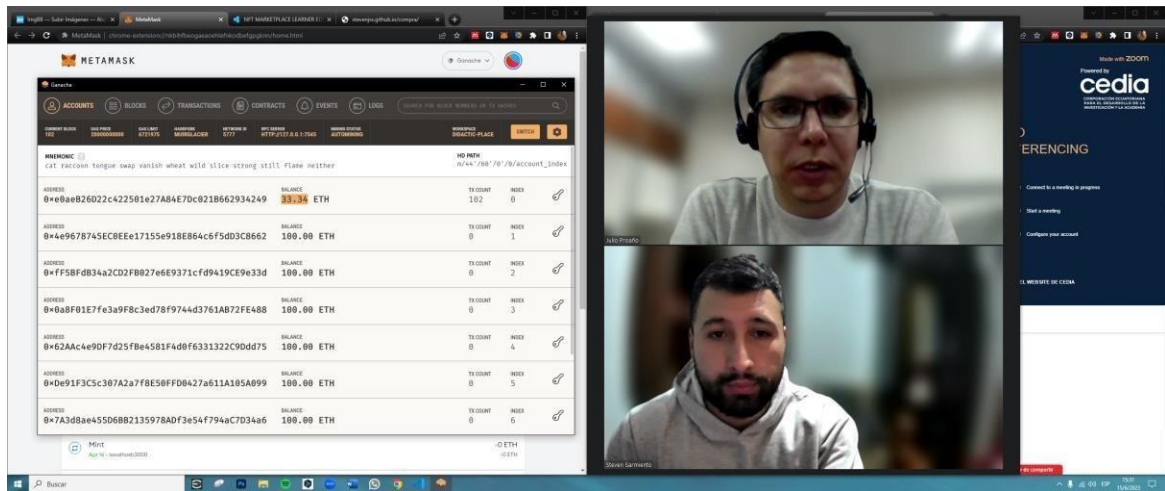


Figura 39. Evidencia para Prueba de aceptación – Débito de ETH en Ganache .

Elaborado por: Steven Sarmiento y Alvaro Lomas.

- Se logró diseñar e implementar exitosamente en prototipo de una billetera virtual fría para NFT en un servidor local. Se proporcionó al usuario una web fluida y sin interrupciones, permitiendo gestionar sus tokens no fungibles de manera eficiente y conveniente. Este logro significa un avance significativo en cuanto a transacciones digitales con criptomonedas, abriendo así las puertas a nuevas posibilidades para usar los NFTs.
- Se manejó y gestionó mediante las pruebas realizadas algunos aspectos a tomar en cuenta cómo realizar una limpieza de código y resolver algunos bugs en el programa. Sin embargo, una vez solucionados estos caben recalcar que desde la primera prueba se cumplió el objetivo de operar que las transacciones sean seguras para cualquier usuario mediante el uso de diferentes estándares, contratos inteligentes y migraciones, los mismos que brindan minimización de riesgos de seguridad, reglas y condiciones para transacciones, integridad de transacciones y facilitar su integración, entre otros.
- Se estableció un punto de partida importante desde el prototipo creado, ya que así se pueden sentar las bases para desarrollos que puedan existir en el futuro además de las mejoras respectivas, optimizando y perfeccionando más la experiencia del usuario y adaptando esta nueva tecnología.
- Se constituyó a Ganache de vital importancia en el proyecto, ya que sin este software la implementación de este prototipo sería casi imposible, esto sucede porque ganache nos proporciona diferentes redes con criptomonedas Ethereum para poder realizar las transacciones necesarias y garantizar su correcto funcionamiento.

- La implementación del software con React.js ayudó construyendo una interfaz de usuario útil e interactiva además de eficiente, además la estructura y semántica de HTML proporcionó elementos vitales para asegurar que el contenido utilizado esté correctamente constituido.

VII

RECOMENDACIONES

- Se recomienda leer y conocer bien sobre el uso y manejo de los NFTs, la red Ethereum y blockchain, ya que estos son de carácter fundamental para formar las bases de las cuales se debe partir para realizar esta implementación.
- Dado que las transacciones de NFTs involucran activos valiosos, se debe priorizar la seguridad en implementación de la billetera, es por eso quien también se debe conocer sobre las migraciones, contratos inteligentes y Solidity. Para este último se puede utilizar Remix, el cual es un IDE que realiza una ejecución en la cadena de bloques de Ethereum, así practicando, estableciendo y automatizando los diferentes acuerdos y transacciones digitales.
- Se deben realizar siempre pruebas de funcionamiento del aplicativo, de tal manera se garantiza una robustez y eficacia de la billetera virtual. Para ello es bueno hacer uso de herramientas digitales como SonarCloud o metodologías para asegurarse que la creación sea sólida.

VIII REFERENCIAS BIBLIOGRÁFICAS

- About / MetaMask. (n.d.). Retrieved February 26, 2023, from <https://metamask.io/about/>
- About / Node.js. (n.d.). Retrieved February 26, 2023, from <https://nodejs.org/en/about/>
- Alharby, M., & van Moorsel, A. (2017). *Blockchain-based Smart Contracts: A Systematic Mapping Study*. 125–140. <https://doi.org/10.5121/csit.2017.71011>
- Álvarez-Díaz, L. J., & Álvarez-Díaz, L. J. (2019). Criptomonedas: Evolución, crecimiento y perspectivas del Bitcoin. *Población y Desarrollo*, 25(49), 130–142. <https://doi.org/10.18004/PDFCE/2076-054X/2019.025.49.130-142>
- Arias Sánchez, A., López, J., Xavier, V., & Guillén, V. (n.d.). Estimación del Coste del Gas en transacciones de Ethereum mediante Deep Learning. <https://openaccess.uoc.edu/bitstream/10609/147467/7/antariasTFM0123presentacion.pdf>
- Celle, R. (2022). *NFTS AND A NEW VISION OF BUSINESSES ANCHORED IN BLOCKCHAIN TECHNOLOGY*. Retrieved June 15, 2023, from https://www.palermo.edu/negocios/cbrs/pdf/pbr25/00_PBR_25_04.pdf
- DARIUS GOVINDASAMY, A., & UMBER, J. (2022). FINDING NFTS (NON-FUNGIABLE TOKENS) USING A GIVEN ETHEREUM WALLET ADDRESS AN OPEN SEA STUDY | *Asian Journal of Advances in Research*. (n.d.). Retrieved June 15, 2023, from <https://www.mbimph.com/index.php/AJOAIR/article/view/2937>
- Di Laudo, A. (2023). *Resumen de Criptomonedas: propuestas legislativas para Argentina*. *Revista Boliviana de Derecho*, ISSN-e 2070-8157, No. 35, 2023, Págs. 438-463, 35, 438–463. Retrieved June 15, 2023, from <https://dialnet.unirioja.es/servlet/articulo?codigo=8778758&info=resumen&idioma=ENG>
- Dori, A. (n.d.). Blockchain. *La revolución industrial de internet - Alexander Preukschat*. Retrieved June 15, 2023, from https://www.academia.edu/36701339/Blockchain_La_revolución_industrial_de_internet_Alexander_Preukschat
- Fang, F., Ventre, C., Basios, M. et al. Cryptocurrency trading: a comprehensive survey. *Financ Innov* 8, 13 (2022). <https://doi.org/10.1186/s40854-021-00321-6>
- Finzer, D. (2020). *The Non-Fungible Token Bible: Everything you need to know about NFTs | OpenSea*. (n.d.). Retrieved June 15, 2023, from https://opensea.io/blog/guides/non-fungible-tokens/#Non-Ethereum_standards

- Gabela, R. (2019). *Colegio de Jurisprudencia Criptomonedas como medios comisorios de delitos de estafa y lavado de activos: Mecanismos para impedir el uso delictivo de las criptomonedas*. <http://repositorio.usfq.edu.ec/handle/23000/8401>
- Ganache | Overview - Truffle Suite. (n.d.). Retrieved February 26, 2023, from <https://trufflesuite.com/docs/ganache/>
- Informačních Technologí, F. (n.d.). *FACULTY OF INFORMATION TECHNOLOGY VIRTUAL WALLET COMPATIBLE WITH CRYPTOCURRENCY VIRTUÁLNÍ PENĚŽENKA KOMPATIBILNÍ S KRYPTOMĚNOU*. Retrieved February 26, 2023, from <http://www.fit.vutbr.cz/info/szz/>
- Inicio | ethereum.org. (n.d.). Retrieved February 26, 2023, from <https://ethereum.org/es/>
- Introduction | MetaMask developer documentation. (n.d.). Retrieved June 15, 2023, from <https://docs.metamask.io/wallet/>
- JSON. (n.d.). Retrieved February 26, 2023, from <https://www.json.org/json-en.html>
- Marchesi, L., Marchesi, M., Destefanis, G., Barabino, G., & Tigano, D. (2020). Design Patterns for Gas Optimization in Ethereum. IWBOSE 2020 - Proceedings of the 2020 IEEE 3rd International Workshop on Blockchain Oriented Software Engineering, 9–15. <https://doi.org/10.1109/IWBOSE50093.2020.9050163>
- Morocho Sagbay, N. X., & Mosquera Loayza, R. D. (2020). La tecnología blockchain y sus posibilidades de uso en la provincia de El Oro. <http://repositorio.utmachala.edu.ec/handle/48000/16236>
- Sánchez, M. J. (2019). *Billetera Virtual: ventajas y desventajas de su implementación en Argentina*. <http://repositorio.udesa.edu.ar/jspui/handle/10908/16752>
- Seigneur, J.-M., & Moreno, S. (2023). NFT Trust Survey. Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, 241–244. <https://doi.org/10.1145/3555776.3577824>
- Solidity Programming Language | The Solidity language portal is a comprehensive information page for the Solidity programming language. It features documentation, binaries, blog, resources & more. (n.d.). Retrieved February 26, 2023, from <https://soliditylang.org/>
- Suratkar, S., Shirole, M., & Bhirud, S. (2020). Cryptocurrency Wallet: A Review. *4th International Conference on Computer, Communication and Signal Processing, ICCSP 2020*. <https://doi.org/10.1109/ICCCSP49186.2020.9315193>
- Tabatabaei, M. H., Vitenberg, R., & Veeraragavan, N. R. (2022). *Understanding blockchain: definitions, architecture, design, and system comparison*. <https://doi.org/10.48550/arxiv.2207.02264>

Tókenes no fungibles (NFT) | ethereum.org. (n.d.). Retrieved February 24, 2023, from <https://ethereum.org/es/nft/#main-content>

Truffle | Overview - Truffle Suite. (n.d.). Retrieved February 26, 2023, from <https://trufflesuite.com/docs/truffle/>

Valencia Chávez, J. A., Yagual Mindiola, W. X., & Campoverde Aguirre, R. D. (2022). *Estudio del ecosistema y funcionamiento de los NFT para su posible incorporación en un portafolio de inversión en el Ecuador.* <http://www.dspace.espol.edu.ec/handle/123456789/56004>

Villameriel, M. I. (2019). GRADO EN COMERCIO TRABAJO FIN DE GRADO “BLOCKCHAIN Y CRIPTOMONEDAS” Trabajo presentado por: INÉS VILLAMERIEL MARTÍNEZ. www.uvadoc.uva.es Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges.* <https://doi.org/10.48550/arxiv.2105.07447>

What is JavaScript? A Definition of the JS Programming Language. (n.d.). Retrieved February 26, 2023, from <https://www.freecodecamp.org/news/what-is-javascript-definition-of-js/>

White, B., Mahanti, A., & Passi, K. (2022). Characterizing the OpenSea NFT Marketplace. *WWW 2022 - Companion Proceedings of the Web Conference 2022*, 488–496. <https://doi.org/10.1145/3487553.3524629>