UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD: EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS

DE LA INFORMACIÓN

TEMA:

"DISEÑO DE UNA GUÍA PARA LA ELABORACIÓN DE "SMART CONTRACTS" EN LA RED DE CARDANO PARA LA EMPRESA NAVIERA PANOIL."

AUTOR:

ORRALA MOREIRA JULIO ANTONIO

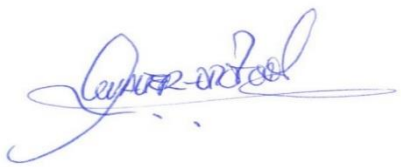
LA LIBERTAD – ECUADOR

PAO 2022-1

APROBACION DEL TUTOR

En mi calidad de tutor del trabajo componente practico del examen de carácter complexivo: “Diseño de una guía para la elaboración de “Diseño de una guía para la elaboración de “Smart Contracts” en la red de Cardano para la empresa naviera PANOIL”, elaborado por el Sr. Orrala Moreira Julio Antonio, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, lo apruebo en todas sus partes.

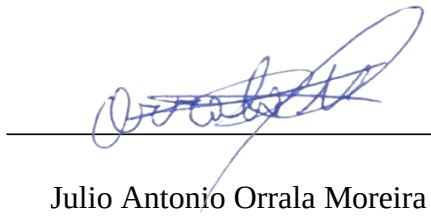
La Libertad, agosto del 2022



Ing. Walter Orozco

DECLARACIÓN

El contenido del presente componente practico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



Julio Antonio Orrala Moreira

AGRADECIMIENTO

Primero agradecer a mis padres, por darme su apoyo incondicional con mis estudios y darme la fuerza para seguir en la lucha de alcanzar mi meta de ser un profesional.

A mis Docentes, por compartir su sabiduría y experiencia por medio de sus cátedras, los valores enseñados siempre formaran parte de los futuros profesionales que están formando, un agradecimiento especial a aquellos tutores del presente trabajo realzado, por ser una guía y tener paciencia.

A mis compañeros de clases, que dentro de los salones siempre existió el respeto y palabras de aliento necesarias para juntos cumplir con esta meta, especialmente aquellos compañeros con los que se ha logrado tener un vínculo muy cercano apoyándonos mutuamente y no rendirnos en el camino.

A la Universidad Estatal Península de Santa Elena, por abrir sus puertas y formarme profesionalmente.

Julio Antonio Orrala Moreira

DEDICATORIA

A mi abuelita por siempre cuidarme y procurar mi bienestar, brindando me su sabiduría y consejo.

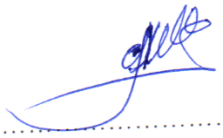
A mi madre por ser un pilar fundamental en mi vida, guiándome por el camino correcto y siendo un ejemplo para seguir, demostrando su amor y apoyo incondicional.

A mi padre, que siempre me apoya brindándome su sabiduría y apoyo incondicional demostrando su interés y amor de manera única, por siempre brindarme la libertad de escoger el camino que deseo seguir.

A mi pareja y amigos que me apoyaron siempre desde el inicio de la carrera hasta ahora que está llegando a su final, dándome la motivación necesaria para lograr mis metas.

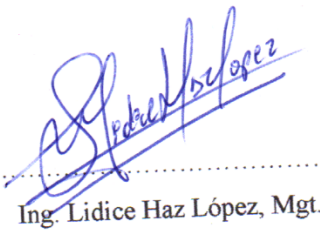
Julio Antonio Orrala Moreira

TRIBUNAL DE GRADO



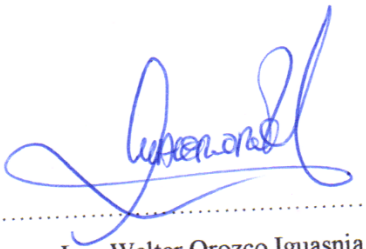
Ing. Jaime Orozco Iguasnia, Mgt

DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN



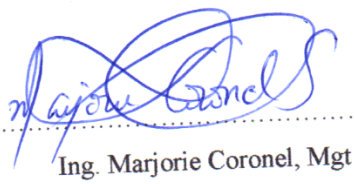
Ing. Lidice Haz López, Mgt.

DOCENTE ESPECIALISTA



Ing. Walter Orozco Iguasnia, Mgt

DONCENTE TUTOR



Ing. Marjorie Coronel, Mgt

DOCENTE GUÍA UIC

RESUMEN

El presente proyecto se usará la tecnología Blockchain aplicada a “Smart Contracts”, este tipo de contratos sirve como mediador entre las partes involucradas, verificando que se cumpla lo acordado sin la necesidad de un tercero. Las empresas navieras manejan transacciones mucho capital y el tiempo en que reciben el pago de sus servicios depende del cliente al cual se atendió, sumando la tarifa de transacciones entre entidades bancarias internacionales lo cual genera un gasto adicional al cliente. Por ello se apreciará el diseño de una guía para la elaboración de “Smart Contracts”, en base a la red de Cardano, para su elaboración se ha establecido el uso de cuatro fases principales tomando como base una metodología para el diseño de contratos inteligentes, la cual considera la identificación las organizaciones y sus procesos, las entidades y atributos necesarios, tomando en cuenta las operaciones que irán almacenadas en la cadena de bloques, simulando su ejecución en Marlowe Playground usando la interfaz de Blockly y el lenguaje de programación funcional Haskell. Como resultado la guía permitirá saber y fortalecer los conocimientos de Blockchain y criptomonedas, plasmando una de las formas de realizar contratos inteligentes de una manera fácil.

Palabras clave: Smart Contracts; Blockchain; Cardano; Haskell; Marlowe.

TABLA DE CONTENIDOS

ÍNDICES DE TABLAS

ÍNDICES DE FIGURAS

LISTA DE ANEXOS

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1. ANTECEDENTES

Actualmente la elaboración de un contrato requiere de dos entidades involucradas y un ente validador, donde se declara de manera específica y objetiva como será llevado. Todas las relaciones contractuales se llevan a cabo teniendo confianza del cumplimiento de este, es prioritario tratar de manera adecuada los términos de un contrato, eliminando los factores asimétricos de la información que se puedan presentar, el incumplimiento de una de las partes del contrato trae consigo la pérdida de confianza, de clientela o de credibilidad y el aumento de condiciones para la elaboración de futuros contratos [1].

La empresa Naviera con un servicio moderno de lanchas enfocado en el aprovisionamiento y traslado de víveres, transporte de tripulantes, desalojo de desechos y encomiendas para embarcaciones nacionales e internacionales que arriban al puerto de La Libertad y Monteverde [2].

Mediante una entrevista oral realizada a un empleado de la agencia naviera, se ha recopilado información sobre los procesos a realizar que brinda. Primero el cliente solicita una cotización de los servicios por medio del portal web de la empresa o por medio del correo organizacional. El cliente decide si adquirir los servicios, luego se procede a realizar lo acordado anteriormente, donde se brinda el servicio y luego que este termina se pasa una factura de lo que se realizó, después se procede al pago los servicios adquiridos en un proceso que demora aproximadamente más de quince días (Anexo 1).

Al tratarse de gran valor económico la tarifa de transacción es de un alto costo, tomando en consideración el cambio de divisas, el costo final para el cliente puede ser muy elevado. Cabe recalcar que son los valores autorizados por la Junta Bancaria [3]. Todo el proceso se da a través de la confianza, el cliente no paga por los servicios hasta que este realizado por completo y la empresa confía en que recibirá un pago por que se trata de empresas internacionales.

En Barcelona España una revista de investigación de tecnologías de la información, uno de sus artículos referentes a contratos inteligentes, menciona la diferencia a los contratos

electrónicos, prestando atención a los elementos de voluntad y el consentimiento [4]. Factores que son indispensables en contratos y la mejora al usar “Smart Contracts”.

En la Universidad Externado en Colombia, en una revista científica enfocada en Blockchain y contratos inteligentes, menciona la inmutabilidad de estos, no es posible modificarlos una vez estén subido a la cadena de bloques [5]. No abarca información sobre cómo ponerlos a prueba o simular la ejecución del Smart Contract.

En una Publicación arbitrada del Colegio de Jurisprudencia de la Universidad San Francisco de Quito. Habla sobre Los “Smart Contracts” como alternativa para la modernización de recaudación tributaria en Ecuador, donde menciona que los contratos son auto ejecutables, su eficiencia y seguridad al tratarse de tecnología Blockchain, centrándose en aspectos legales [6].

Los avances tecnológicos se han vuelto indispensables para los negocios, mejorando ciertos procesos y reduciendo tiempos para obtener los resultados. La tecnología Blockchain trajo consigo los contratos inteligentes, estos ayudan al cumplimiento de los términos declarados en los contratos sin intermediarios, otorgando otro método de pagos a los clientes extranjeros.

1.2. DESCRIPCIÓN DEL PROYECTO

El siguiente proyecto propone el diseño de una guía para elaborar contratos inteligentes para las personas con conocimientos básicos en Blockchain y criptomonedas, o en un caso la sociedad desee obtener conocimientos necesarios y se sienta atraída en saber cómo aplicar estos contratos.

El presente documento se tomará en cuenta factores muy importantes las cuales son basarse en documentación en línea para la elaboración de este proyecto, definir las herramientas de software a utilizar para la simulación o implementación de contratos inteligentes tomado en cuenta la lectura de los artículos relacionados con el tema planteado. Las fases que conforman este proyecto son:

Fase de Identificación de las organizaciones involucradas y sus procesos de negocio

Para empezar el primer paso es determinar cuáles son las organizaciones involucradas en el proyecto, para ello se puede consultar el historial de los clientes que han accedido a los servicios, en caso de ser otras empresas u organizaciones, tener en cuenta su procedencia,

debido a que ciertos países las políticas referentes a estos tipos de contratos o vinculación con las criptomonedas no son permitidas. Una vez realizado lo anterior es necesario definir los procesos de negocio. Para identificarlos se puede consultar si ya existe documentación de estos, los cuales pueden ser automatizados en las organizaciones involucradas [7].

Se pueden almacenar todos los datos relacionados en la Blockchain, pero no siempre es recomendable, debido a la capacidad de almacenamiento de un bloque es relativamente baja. Es preferible guardar solo la información requerida de las características que esta ofrece.

Para ayudar a decidir la información que debe almacenarse se debe responder las siguientes preguntas. ¿el atributo es de interés para más de una organización involucrada en el sistema?, de ser así, ¿el atributo requiere de la propiedad de no repudio?, ¿es de interés para las organizaciones involucradas obtener información acerca de las transacciones que han modificado el atributo? Si se responde que sí a las preguntas anteriores es muy probable que el dato que está siendo evaluado deba ser almacenado en la cadena de bloques [7].

Fase de Identificación las entidades y los atributos requeridos para soportar los procesos de negocio.

Una vez que se identificaron los diferentes atributos que serán almacenados en la cadena de bloques, es necesario definir las diferentes operaciones o acciones que se requieren realizar sobre los atributos para cumplir con el objetivo del proceso de negocio. Para realizar dicha tarea es necesario plantearse la siguiente pregunta: ¿esta actividad modifica los atributos almacenados en la cadena? Si se responde positivamente a dicha pregunta entonces la actividad deberá ser implementada mediante un contrato inteligente [7].

Fase de Identificación de datos de entrada, procesamiento y salida.

La empresa maneja cinco pasos para brindar servicios, donde cada uno de estos es fundamental para el cumplimiento de un contrato establecido (Anexo 3). se divide de la siguiente manera (Anexo 4.):

Entradas. _ Solicitud de servicios por medio del sitio web de la empresa: El cliente se comunica con la empresa a través de su portal web, donde especifica el servicio que desea adquirir, el contacto es a través de correo electrónico.

Método de pago: El método de pago es por medio de transferencia bancaria a una cuenta en Estado Unidos para las empresas internacionales y para las empresas locales se usan otros bancos locales como el banco de Guayaquil. Siempre se realiza el pago antes de la adquisición de servicios debido a los recursos que deben moverse para el cumplimiento de estos.

Procesamiento. _ Validación de pago: Se espera hasta que el pago este realizado y confirmado con su respectiva entidad financiera.

facturación: Se realiza la factura de los servicios que se van a brindar, los costos netos de la empresa, no incluye los valores adicionales de comisiones por parte de las entidades bancarias.

Salidas. _ Informe: Se detalla las actividades realizadas por parte de la empresa, en donde se redacta el cumplimiento de los servicios y es entregado al capitán o responsable de cada barco.

Servicio: Se realiza la actividad detallada en los servicios que brinda la empresa, cumpliendo con plazos y fechas establecidos.

Fase de desarrollo o simulación.

Se procede a codificar lo detallado anteriormente, para ello se usa Marlowe, con esta herramienta se puede simular una interacción directa con la Blockchain, y así poder especificar los “Smart Contracts”, tiene un ambiente de pruebas en el cual se puede verificar que todo funcione correctamente, en caso de que exista un error o problema se procede a comunicarlo y a ver una posible solución y continuar con el desarrollo. El tiempo de desarrollo dependerá del tipo de contrato, la complejidad de este y los factores para tener en cuenta, por ello se requiere que sea muy específico y medible.

Para la simulación de estos contratos es necesario utilizar herramientas que estén en la red de Cardano, las cuales son las siguientes.

Marlowe: es el lenguaje específico del dominio (DSL) que permite a los usuarios crear aplicaciones Blockchain adaptadas a los contratos financieros. Con Marlowe DSL, se garantiza una enorme eficiencia debido a la seguridad mejorada, más certeza y garantías [8] (Anexo 5).

De acuerdo con la Resolución RCF-FST-SO-09 No. 03-2021 del Consejo de la Facultad de Sistemas y Telecomunicaciones emitido en la Universidad Estatal Península de Santa Elena, el proyecto presente contribuye con la línea de investigación "Tecnología y Sistemas de la Información (TSI)" en TSI adaptables e inteligentes [9].

1.3. OBJETIVOS DEL PROYECTO

1.3.1. OBJETIVO GENERAL

- Diseñar una guía para la elaboración de "Smart Contracts" en la red de Cardano usando herramientas como Marlowe para la simulación de la ejecución de los contratos.

1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar los procesos actuales de la empresa naviera para la elaboración de contratos.
- Definir las fases para la elaboración de "Smart Contracts"
- Simular la ejecución de un contrato inteligente con la herramienta Marlowe

1.4. JUSTIFICACIÓN

Cada vez más startup se interesan por la tecnología descentralizada que brinda la Blockchain para el desarrollo de nuevos modelos de negocio descentralizados, esta presenta diferentes casos éxitos en otros sectores de negocio en el sector financiero, hoy en día las transacciones interbancarias pueden tardar varios días para ser aprobadas en algunos casos y siempre debe realizarse en horario de oficina, con la tecnología Blockchain esto son procesados a cualquier hora y el tiempo en ser completadas es cuestión de minutos. Los "Smart Contracts" son sistemas que facilitan la ejecución de

contratos mediante cadena de bloques, el intermediario como entidad que vigila que se cumpla un contrato puede ser eliminado de la ecuación [10].

Existen empresas que trabajan con este tipo de tecnología, Cardano es una de estas, cerca de 900 empresas que conforman Fortune 500 trabajan bajo esta red [11]. Una de estas es Walmart, esta empresa busca agregar como método de pago transacciones por criptomoneda, se debe a su alto nivel de escalabilidad en transacciones que se adaptan a los requerimientos de esta empresa y la seguridad de los pagos. Ha optado por esta Divisa digital por que pertenece a la tercera generación de estas, quiere decir, viene solucionando errores de sus predecesores [12].

Utilizar "Smart Contracts" para el pago de servicios nos ayuda a tener mejor confianza en el cumplimiento de este, reduciendo costos por parte del contratante por transferencias interbancarias en horas laborales, logrando ampliar el horario de recepción de servicios. Asegurando que el pago este realizado por parte del contratante y que no existirá ningún tipo de incumplimiento hasta que el servicio este completado, entonces se liberará el pago logrando que el contratante tenga la certeza que en caso de incumplimiento tenga un reembolso seguro.

Elaborar "Smart Contracts" con Marlowe ayuda al entendimiento general del contrato debido a su interfaz gráfica, quiere decir que personas no relacionadas con lenguaje de codificación o algoritmos entiendan a la perfección cómo funciona y como está estructurado, también están basados en contratos existentes, en caso de no entender la interfaz gráfica se puede leer el contrato en forma de texto y lograr entender los términos establecidos en este.

Al agregar otro método de pago los clientes tienen la opción de escoger cual es la que más se adecua a sus necesidades, en caso de criptomonedas es más seguro, las transacciones son públicas y anónimas, mantiene confidencialidad con los clientes y no requieres altos costos por transferir los fondos de una billetera a otra.

El presente proyecto está direccionado al plan de Creación de Oportunidades 2021-2025, haciendo énfasis en la Directriz 1, el cual detalla lo siguiente:

Directriz 1: Soporte territorial para la garantía de derechos [13].

Lineamientos territorial A. Acceso equitativo a servicios y reducción de brechas territoriales.

A4. Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios.

Objetivos del eje económico [13]

Objetivo 2. Impulsar un sistema económico con reglas claras que fomente el comercio exterior, turismo, atracción de inversiones y modernización del sistema financiero nacional.

Política 2.2. Promover un adecuado entorno de negocios que permita la atracción de inversiones y las asociaciones públicas-privadas.

Objetivos del eje social [13]

Objetivo 5. Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social.

Política 5.5 Mejorar la conectividad digital y acceso a nuevas tecnologías de la población.

1.5. ALCANCE

La elaboración de esta guía para elaborar contratos inteligentes en la red de Cardano permitirá obtener un nivel de conocimiento sobre la implementación o simulación de estos, hacia las personas que estén dispuestas a indagar sobre este tipo de tecnología.

El proyecto está basado para el pago de servicios en la empresa naviera "PANOIL" donde los pagos dependen de bancos centrales, los cuales tienen sus respectivas comisiones por transacciones y se ejecutan en un horario establecido. Para ello se trabaja con el área de Operaciones, la cual se encarga de comunicarse con el cliente y coordinar el pago de los servicios. Esta área posee la información necesaria para la elaboración de un contrato.

La implementación de Smart Contracts permitirá la eficiencia y verificación de pagos de manera más rápida y segura, con un registro inmutable, para tener un mejor seguimiento de estos movimientos transnacionales de la empresa, de manera anónima y publica.

Es importante resaltar que la implementación de Smart Contracts requiere de ciertos conocimientos básicos de criptomonedas, en especial Cardano, que es en la red que

se trabajara para los contratos inteligentes. A continuación, se especifica que se espera lograr en cada fase.

Fase de Identificación de las organizaciones involucradas y sus procesos de negocio

- Método basado en el historial de clientes
- Análisis de datos fundamentales para subir al Blockchain

Fase de Identificación las entidades y los atributos requeridos para soportar los procesos de negocio.

- Analizar las acciones a realizar
- Detallar el proceso de los servicios brindados
- No incluye posibles modificaciones futuras

Fase de Identificación de datos de entrada, procesamiento y salida.

- Analizar las variables fundamentales para la codificación de los contratos

Fase de desarrollo o simulación.

- Usar herramientas de la red de Cardano como ambiente de simulación.
- Interpretar las acciones del contrato durante su ejecución
- No se implementará un contrato en la red de Cardano.
- No se ejecutará un contrato real entre la empresa y el cliente.

CAPÍTULO II

2.1. MARCO CONCEPTUAL

2.1.1. ADA: Ada es la ficha nativa de Cardano; lleva el nombre de Ada Lovelace, una matemática del siglo XIX que es reconocida como la primera programadora de computadoras y es hija del poeta Lord Byron; Ada es una moneda digital. Cualquier usuario, ubicado en cualquier parte del mundo, puede usar ADA como un intercambio seguro de valor, sin necesidad de que un tercero medie en el intercambio. Cada transacción se registra de forma permanente, segura y transparente en la cadena de bloques de Cardano [14] (Anexo 7).

2.1.2. Blockchain: Blockchain es un libro mayor compartido e inmutable que facilita el proceso de registro de transacciones y de seguimiento de activos en una red de negocios. Un activo puede ser tangible (una casa, un auto, dinero en efectivo, terrenos) o intangible (propiedad intelectual, patentes, derechos de autor, marcas); prácticamente cualquier cosa de valor puede ser rastreada y comercializada en una red de Blockchain, reduciendo el riesgo y los costos para todos los involucrados [15].

2.1.3. Blockly: es un tipo de kit de desarrollo de lenguaje de bloques visuales que permite la construcción rápida de nuevos lenguajes de programación visuales basados en bloques para abordar un enfoque pedagógico o de contenido específico [16].

2.1.4. Cardano: Cardano es la primera plataforma de cadena de bloques que se construye a través de investigaciones revisadas por pares, para ser lo suficientemente segura como para proteger los datos de miles de millones, lo suficientemente escalable para adaptarse a los sistemas globales y lo suficientemente sólida como para respaldar el cambio fundamental [17] (Anexo 6).

2.1.5. Contrato: m. Pacto o convenio, oral o escrito, entre partes que se obligan sobre materia o cosa determinada, y a cuyo cumplimiento pueden ser compelidas [18]. Es decir, es un acuerdo voluntario entre dos partes, llamadas deudor y acreedor, que pueden ser físicas o jurídicas; además, cada parte puede estar constituida por más de una persona, así, puede haber más de un deudor y/o más de un acreedor vinculados por el contrato [19].

2.1.6. Criptomoneda: Moneda virtual gestionada por una red de computadoras descentralizadas que cuenta con un sistema de encriptación para asegurar las

transacciones entre usuarios [20]. Estas técnicas de cifrado sirven para regular la generación de unidades monetarias y verificar la transferencia de fondos. No necesitan de un banco central u otra institución que las controle [21].

2.1.7. Divisa: Moneda extranjera referida a la unidad del país de que se trata [22]. También es preciso diferenciar entre divisa y moneda. Mientras que la segunda hace referencia al conjunto de metales y papel, que es lo que se considera dinero en metálico, la divisa hace referencia al término nominativo de la moneda de otro país. Al final de este artículo, ampliaremos la explicación sobre la diferencia entre moneda y divisa [23].

2.1.8. DSL: Domain Specific Languages, está especializado en modelar o resolver un conjunto específico de problemas [24]. Esto contrasta con un lenguaje de propósito general (GPL), que es ampliamente aplicable en todos los dominios. Hay una amplia variedad de DSL, que van desde lenguajes ampliamente utilizados para dominios comunes, como HTML para páginas web [25].

2.1.9. Haskell: Haskell es un lenguaje funcional puro, de propósito general, que incluye muchas de las últimas innovaciones en el desarrollo de los lenguajes de programación funcional, como son las funciones de orden superior, evaluación perezosa, tipos polimórficos estáticos, tipos definidos por el usuario, encaje por patrones, y definiciones de listas por comprehensión [26].

2.1.10. Marlowe: es un nuevo lenguaje para modelar instrumentos financieros como contratos inteligentes en una cadena de bloques; ha sido diseñado para personas que son ingenieros comerciales o expertos en la materia en lugar de desarrolladores experimentados; también es un lenguaje específico de dominio simple (DSL) que comprende una pequeña cantidad de componentes básicos poderosos que se pueden ensamblar en contratos financieros expresivos; está integrado en el lenguaje Haskell, que tiene su propio ecosistema establecido y marco de pruebas [27]. (Anexo 8).

2.1.11. Slot: Unidad de tiempo de la red Cardano que dura un segundo, dentro de cada Slot puede existir la posibilidad de crear un bloque [28].

2.1.12. Smart Contracts: es un tipo especial de instrucciones que es almacenada en la Blockchain. Y que además tiene la capacidad de autoejecutar acciones de acuerdo con

una serie de parámetros ya programados. Todo esto de forma inmutable, transparente y completamente segura [29].

2.1.13. Wallet: también conocida como billetera digital, es un monedero virtual de criptomonedas que te permite consultar tu saldo, operar entre distintas redes Blockchain y firmar tus propias transacciones [30]. También el término wallet hace referencia a una cartera, billetera o monedero virtual en el que podemos gestionar nuestros activos criptográficos. Es un software o hardware diseñado exclusivamente para almacenar y gestionar las claves públicas y claves privadas de nuestras criptomonedas [31].

2.2. MARCO TEÓRICO

2.2.1. Branch based blockchain technology in intelligent vehicle

Para tener mejor conocimiento sobre la cadena de bloques es fundamental conocer que los bloques son la unidad fundamental de esta cadena y está conformado de un conjunto de transacciones que como explica Singh y Kim "fueron realizadas en un periodo determinado de tiempo" [32]. Pero estos bloques por sí solos no representan mucho, sino que requieren de un nexo que los una en lo que se denomina la cadena y "los bloques se conforman de tal manera que cada bloque nuevo está criptográficamente conectado al bloque anterior" [33].

2.2.2. El Smart legal Contract como nueva forma de contratación en el código de comercio ecuatoriano

Los Smart legal Contracts son una figura jurídica con alto potencial de crecimiento que marca grandes expectativas en su aplicación, pues son un medio seguro y eficaz de contratación capaz de ejecutarse automáticamente gracias a la tecnología Blockchain cuando se verifica el cumplimiento de una condición, esta cualidad no puede ser ignorada pues ningún otro mecanismo conocido en Derecho ha logrado aportar seguridad jurídica a las partes de la manera que lo hace un contrato legal inteligente [34].

Se ha corroborado que la ejecución de los contractos inteligentes responde a criterios objetivos, es decir únicamente se puede desencadenar una consecuencia si el hecho comprobable implica una valoración material, esta afirmación se da gracias a la lógica Booleana por la cual funcionan los contratos inteligentes; por el contrario, no se pueden verificar circunstancias que estén sujetas a interpretación, por lo que su aplicación se

muestra limitada técnicamente, a pesar de ello, existen varias áreas en las que un contrato inteligente puede ser perfectamente aplicado y de esta manera aprovechar todo su potencial; como, por ejemplo, es posible utilizar al legaltech para implementar Smart legal Contracts dentro de la oferta de servicios jurídicos como una herramienta totalmente innovadora dejando de lado a los contratos celebrados de forma tradicional [34].

2.2.3. Los contratos inteligentes en España.

Impresionante capacidad del Smart Contract de ejecutarse automáticamente cuando se verifica el cumplimiento de la condición; esto aporta una seguridad jurídica que no está al alcance de ningún otro mecanismo conocido en Derecho y alivia a las partes contratantes, en el sentido de que saben que el incumplimiento de alguna de ellas no es una opción, conocedoras de que el acuerdo se ejecutará, para lo bueno y para lo malo, hasta sus últimas consecuencias, eliminando de esta manera un vicio del ser humano que nació a la misma vez que el primer acuerdo de voluntades: la inobservancia de este [35].

2.2.4. Estado legal de los contratos inteligentes: características, papel, significado

Usando la tecnología Blockchain, los contratos inteligentes se ejecutan automáticamente, lo que brinda oportunidades adicionales para reducir los gastos de los participantes en las relaciones que surgen de la conclusión de una transacción y el cumplimiento de sus condiciones; las interacciones multilaterales implementadas a través de contratos inteligentes pueden reducir los costos de las operaciones y controlarlas, aumentar la velocidad de las operaciones y reducir los riesgos asociados con las acciones deshonestas de las partes, y minimizar o excluir completamente a los intermediarios de la transacción; la legislación debe prever la posibilidad de utilizar contratos inteligentes con contratos existentes [36].

Por lo tanto, mediante el uso de contratos inteligentes, es posible realizar pagos regulares de alquiler, gestionar la entrega de bienes y pagar préstamos. Un contrato inteligente es un código de programa basado en la tecnología Blockchain, que por sus características jurídicas es un mensaje con significado jurídico registrado en un lenguaje (lenguaje artificial) y sellado con una firma digital electrónica de cada una de las partes (o certificado con una clave especial) [36].

Las principales ventajas de un contrato inteligente incluyen su observabilidad: la capacidad de monitorear la ejecución del contrato en todas las etapas y asegurarse de que la contraparte completó su parte de la transacción; verificabilidad y la existencia de un mecanismo para hacer cumplir las disposiciones del contrato inteligente; la investigación adicional sobre el tema debería considerar la posibilidad de utilizar contratos inteligentes en el derecho contractual, el estado de los contratos inteligentes como prueba absoluta en los tribunales y la regulación legislativa del estado legal de los contratos inteligentes a nivel internacional [36].

2.2.5. Posibles usos de los contratos inteligentes en una Blockchain para el comercio de bienes y servicios

El Blockchain es una plataforma la cual tiene un amplio número de usos en materia de comercio electrónico lo cual puede hacer pensar vendría siendo la nueva clase de inteligencia artificial del internet de las cosas que debemos estar aceptando para que cada vez surjan mejores formas y más facilidad de aplicación de la Blockchain a más procesos diarios de nuestra vida [37].

El uso de plataformas que realizan los contratos de una manera más sencilla es la idea que deberían estar realizándose o proyectándose las personas que ejercen o estudian el derecho y especializarse en programación para así efectuar contratos legales electrónicos para que sea vaya creando una nueva rama estudio y así mejorar cada día la aceptación a nivel mundial de los contratos inteligentes para mejorar lo que conocemos el internet de las cosas [37].

La auto ejecutabilidad es uno de los elementos esenciales al momento de la utilización o del consentimiento de estos contratos, ya que al poderse usar como herramienta de cumplimientos de requisitos sin necesidad que alguien interceda para hacer cumplir a las partes, solo con el simple hecho de que ambas partes pertenezcan o se encuentren dentro de la Blockchain, este se ejecuta solo, si la parte vendedora no cumple con los pactado automáticamente el dinero negociado dentro de la cadena de bloques [37].

2.3. METODOLOGÍA

2.3.1. Metodología de investigación

Los estudios exploratorios buscan hechos sin el objetivo de predecir las relaciones existentes entre las variables. Se utilizan en situaciones en las cuales se tiene poca información o no ha sido investigada [38]. Se usará una metodología exploratoria por medio de una recopilación documental y bibliográfica, indagando y recolectando información de diferentes fuentes de acuerdo con el proyecto planteado. Debido a que la en los resultados de búsqueda aparece varios estudios jurídicos referente a los "Smart Contracts", y la implementación de estos a nivel nacional son escasos.

La investigación diagnóstica es un método de estudio mediante el cual se logra conocer lo que ocurre en una situación específica [39]. Se usará la entrevista realizada a un agente naviero que forma parte de la empresa y la información obtenida en la web.

2.3.3. Variables

Evidenciar la reducción de tiempo de realización de los pagos a realizar por parte del cliente hacia la empresa.

Reducción del costo de transacciones para el cliente para el pago de servicios hacia la empresa

2.3.4 Técnicas de recolección de información

Para la recolección de información se han usado dos tipos de técnicas que son de entrevista y recopilación documental y bibliográfica.

La entrevista oral fue dirigida a la persona que forma parte del proceso del cumplimiento de los servicios de la empresa, por medio de un cuestionario, establecido de preguntas referentes a los procesos necesarios para el cumplimiento del contrato. (Anexo 1).

En recopilación documental y bibliográfica, se busca información de diferentes fuentes bibliográficas de acuerdo con el tema establecido, para poder tener una mejor idea con respecto a la elaboración de la guía, y de proyectos similares.

2.3.5. Metodología de desarrollo de guía

Con el fin de realizar una investigación de calidad en este proyecto, se plantea utilizar una propuesta metodológica para el diseño de contratos inteligentes, esta propuesta es adecuada para establecer las fases a seguir para elaborar “Smart Contracts” [7].

Las características principales son:

- Identificación de las partes involucradas [7].
- Identificar los procesos de negocio [7].
- Reconocer la información necesaria para los contratos [7].

Se enfoca en 3 fases:

- Recolección de información.
- Análisis de información.
- Desarrollo de contrato.

CAPITULO III

3. PROPUESTA

3.1. DESCRIPCIÓN

Esta guía detalla las fases a seguir para realizar un Smart Contract, tomando en cuenta la información obtenida de la empresa con la que se trabaja. El contrato pasara por distintas fases hasta tener lo necesario para poder simular una ejecución en la cadena de bloques de la red de Cardano. Se usará la criptomoneda ADA, esta es propia de Cardano, se la considero por que no existe comisiones de transacciones entre esta moneda, siempre y cuando sea parte de la red.

Para poder elaborar un Smart Contract se realizan las siguientes cuatro fases.

3.2. Fase de identificación de las organizaciones involucradas y sus procesos de negocio [7].

Para identificar las organizaciones involucradas, se toma en cuenta quienes son parte del proceso de negocio, es decir las empresas o personas que llegan a un acuerdo.

En este caso son: La **empresa** que brinda los servicios navieros, el **cliente** y un **banco internacional**. Para identificar los procesos de negocio se debe entrevistar a una persona que tenga conocimiento o sea parte de estos procesos, con esa información se puede saber qué tipo de negocio es y cómo es llevado a cabo.

En el caso actual se entrevistó a una persona que forma parte de la empresa y se investigó en internet los servicios que ofrece la empresa, los cuales son los siguientes:

- Aprovisionamiento y traslado de víveres
- Transporte de tripulantes
- Desalojo de desechos y encomiendas
- Toma de combustible

Para tener un mejor ejemplo se hará uso del proceso de negocio de Toma de combustibles.

	FACTOR	TARIFF	BASIS IN CALCULATION	PARTIAL	US. DOLLAR
PETROLEUM TERMINAL DUES					**6805,69**
Bunkering only call / Minimun tariff USD 1,496.47	GRT	0,06	+ 12% VAT / Minimun Tariff USD 1498,47	2329,99	
PILOTAGE (PRIVATE)					
Pilotage	GRT	0,06	GRT per maneuver + 12% VAT / 1 man.	2450,50	
SAFETY INSPECTIONS AND POLLUTION PREVENTION					
Pollution prevention	GRT	0,01	GRT per day or fraction / 1 period	394,55	
MARITIME PROTECTION					
ISPS Code aplication	DAY/FRACTION	116,01	per day or fraction + 12% VAT / 1 period	129,93	
LAUNCHES					
Launch for reception/dispatch	2	226,22	per hour or fraction /2 hours	452,44	
Launch for support to Pilot	2	162,43	per hour or fraction /2 hours	324,86	
Launch for Safety inspector	2	162,43	per hour or fraction +12% VAT/2 hours	363,84	
ANCHORAGE					
Anchorage in non commecial operations (BUNKER SURVEY)	LOA	1798,0	per day or fraction /1 day (bunker survey)	359,58	
PORT DUES					**763,50**
Light and buoy dues	GRT	0,01	Taridd for Bunkering Only	358,68	
Migration (Reception & Dispatch)/Traffic Permit	IN/OUT	15,00	USD 15,00 per maneuover (arrival/departure)	30,00	
Goverment Tax (Consular Dues)		310,00	per call	310,00	
BOC authorization of SPTMF (Maritime Authority)		64,82	Lumpsum	64,82	
AGENCY SERVICE					**3524,58**
Shore mobilization for Port Authorities & Agents/delivery of documents/payment of invoices/local communications forms/ use of VHF frecuency (FICED)		250,00	Lumpsum	250,00	
Service Boat for Agent signs outward clearance previous Sailing authorization		162,43	per hour / 2 hours	324,86	
AGENCY FEE For the first 3 days. Additional fee as from 4yh day USD 100.00/day		1000,00	for the first 3 days	1000,00	
Bunker surveyor service (only to vessel) Interins Co. + ISPS permit		750,00	Only to vessel + USD 50,00 ISPS PERMIT	800,00	
Launch service for bunker surveyor		162,43	per hour or fraction / 2 hours	324,86	
Fumitation of vessel as per port Regulations		500,00	Lumpsum	500,00	
Launch for Fumigation		162,43	per hour or graction / 2 hours	324,86	
Unforeseen (DHL for sending bunker simple, or any Other - WITH VOUCHERS ONLY)					
				TOTAL	11093,77

Tabla 1. Costos Portuarios [40].

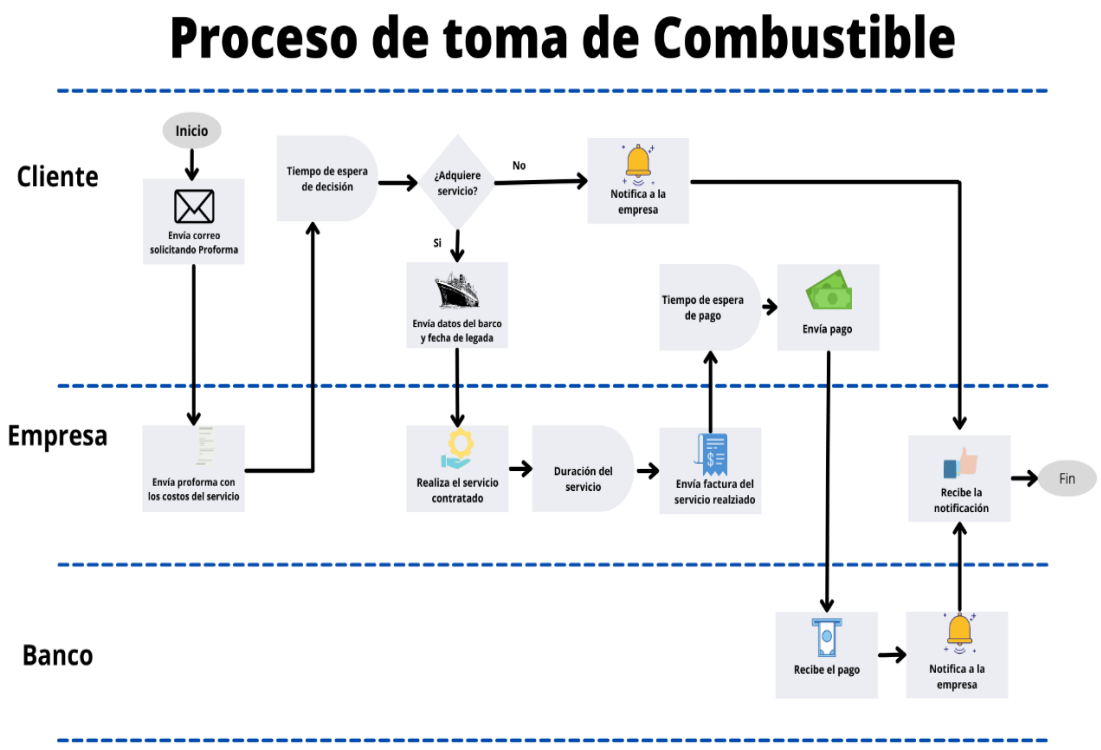


Figura 1. Proceso de toma de combustible

Historial de clientes

Para tener una idea general sobre a qué tipo de cliente se dirige el Smart contract se toma en cuenta el historial de los clientes con los cuales ha trabajado la empresa.

Empresas extranjeras

- Inchape Shipping Services
- Tafigua

Por lo general son empresas con servicios de transporte o cargas de combustible por medios marinos.

3.3. Fase de Identificación las entidades y los atributos requeridos para soportar los procesos de negocio [7].

Una vez se identifican las organizaciones, se puede averiguar cuáles serían las entidades que participan y los procesos que realizan cada una. Para identificar las entidades se toma de referencia la figura de Proceso de toma de combustible.

Las entidades identificadas son:

El Cliente en el caso de las empresas que manejan los barcos la persona encargada se llama “Armador”.

La empresa, en este caso es la persona que se encarga de verificar que existe el pago a esta persona de la denomina como “Contador”.

El banco, en este caso el banco no se tomará en cuenta, debido a que es un método de pago tradicional muy aparte de los Smart Contract basados en criptomonedas. Por ello la entidad llamada “Blockchain” ocupa su lugar.

En cada una de estas identidades se identificó sus atributos correspondientes.

Entidades

Cliente: Nombre, dirección, teléfono, email, nombre del barco, bandera, Total de Toneladas, largo del barco, Wallet.

Empresa: Nombre, dirección, teléfono, email, Costo del Servicio, wallet

Blockchain: id transacciones, slots, validador.

Los atributos son los datos que conforman cada una de las entidades encontradas, estos deben ser analizados para que sean parte de la cadena de bloques, y esta información quede reflejada, para ello nos hacemos las siguientes preguntas.

¿El atributo es de interés para más de una organización involucrada en el sistema? [7].

Wallet si es de interés para ambas partes, esta es la dirección a la cual se va a enviar el pago y es indispensable para la cadena de bloques, para tener el registro de donde se envía y cual recibe.

Precio del servicio si es de interés, en este se ve reflejado el monto a pagar por parte del cliente, y el monto que debe recibir la empresa, también es la cantidad de ADA que el contrato bloquea al cliente y si se cumple lo acordado es transferido a la empresa.

¿Es de interés para las organizaciones involucradas obtener información acerca de las transacciones que han modificado el atributo? [7].

Si, debido a que el costo de los servicios no debe cambiar durante el proceso, en caso de que esto ocurra podría implicar un proceso malicioso.

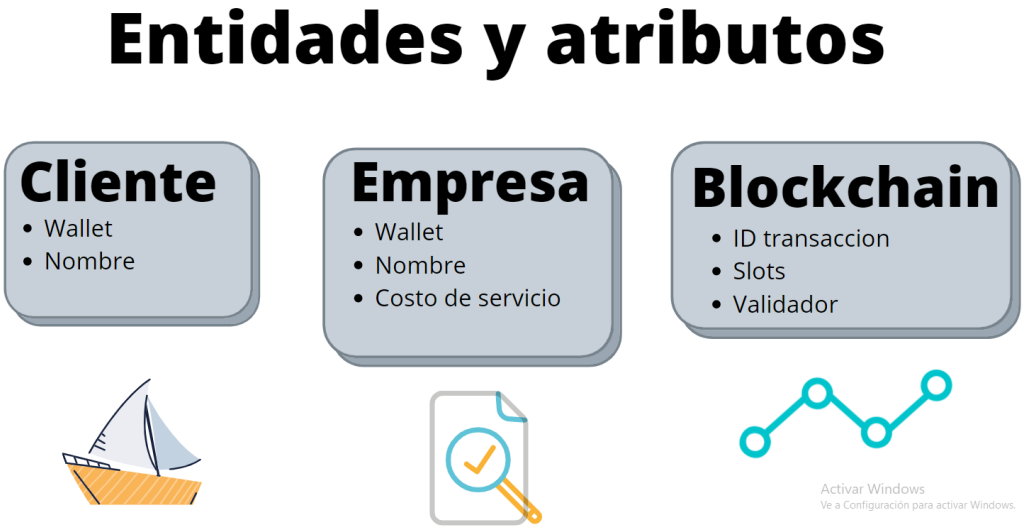


Figura 2. Entidades y atributos esenciales para la Blockchain

Todos los atributos para los cuales se obtenga una respuesta negativa podrán ser gestionados por una base de datos tradicional.

3.4. Fase de Identificación de datos de entrada, procesamiento y salida [7].

Para identificar cada uno de estos elementos se analiza el proceso actual que existe y como seria ponerlo dentro de un contrato inteligente, tomando en cuenta que este debe tener Slots para controlar el tiempo que dura el contrato. Estos son ingresados antes de iniciar el contrato. También se debe tomar en cuenta la dirección de las Wallets por que entre estas cuentas se realizara las transacciones y se validara al final del contrato, a continuación, se muestra las entradas procesamientos y salidas.

Las entradas

- **Direcciones de las wallets**: Esta serán las direcciones en las que se deposite la cantidad de criptomoneda correspondientes al finalizar el contrato.
- **Costo de servicio**: La cantidad de criptomonedas que serán depositadas al final del contrato
- **Slot final:** tiempo límite de ejecución del contrato.
- **Slots de límite de respuesta de queja**: El tiempo que se espera para que se responda a la queja, si no se responde en ese tiempo se cancela el contrato

- **Slot límite de solución d problema**: tiempo que debe transcurrir para solucionar el problema.
- **Slot límite de confirmación de solución**: tiempo límite de confirmar la solución del problema.
- **Validador**: dato que ingresa el cliente o la empresa para notificar que todo está correcto o hay un problema.

Los procesos

- **Deposito inicial:** El cliente deposita el costo de servicio a la empresa.
- **Reembolso:** en caso de que exista un problema el dinero volverá al cliente
- **Depósito de problema solucionado:** el cliente le paga a la empresa cuando esta soluciona el problema.
- **Fin del contrato:** al finalizar el contrato las criptomonedas son depositadas según lo indique el contrato.

Las salidas

- **Informe de las transacciones realizadas:** se detalla los movimientos realizados dentro del contrato.

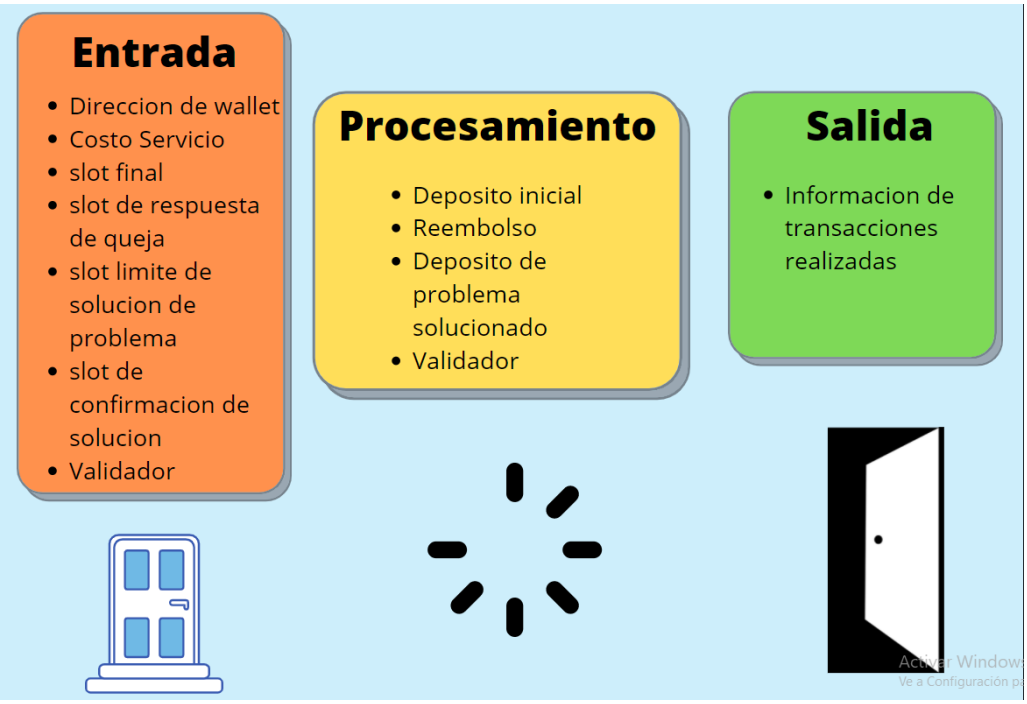


Figura 3. Datos de Entrada, Procesamiento y Salida.

3.5. Fase de desarrollo o simulación.

En esta fase se utilizará MarlowePlaygorund (https://play.marlowe-finance.io/#/), es una herramienta propia de la Red de Cardano para la simulación de los Smart Contract, esta plataforma posee ejemplos de contratos inteligentes.

Con los datos analizados y obtenidos de las tres fases anteriores se procede a realizar un diagrama de flujo que refleje el funcionamiento del Smart Contract, basándonos en otros contratos ya existentes otorgados por la herramienta de simulación. Para ello se coloca las Entidades ya identificadas.

El **Armador** es la persona encargada de pagar los servicios contratados por la empresa, es el cliente.

El **Contador** es la persona encargada de validar los pagos recibidos, es parte de la empresa.

El **Smart Contract** es el lugar donde ocurren todos los movimientos transaccionales, al final del contrato se encarga de depositar el monto acordado a la cuenta del último movimiento realizado.

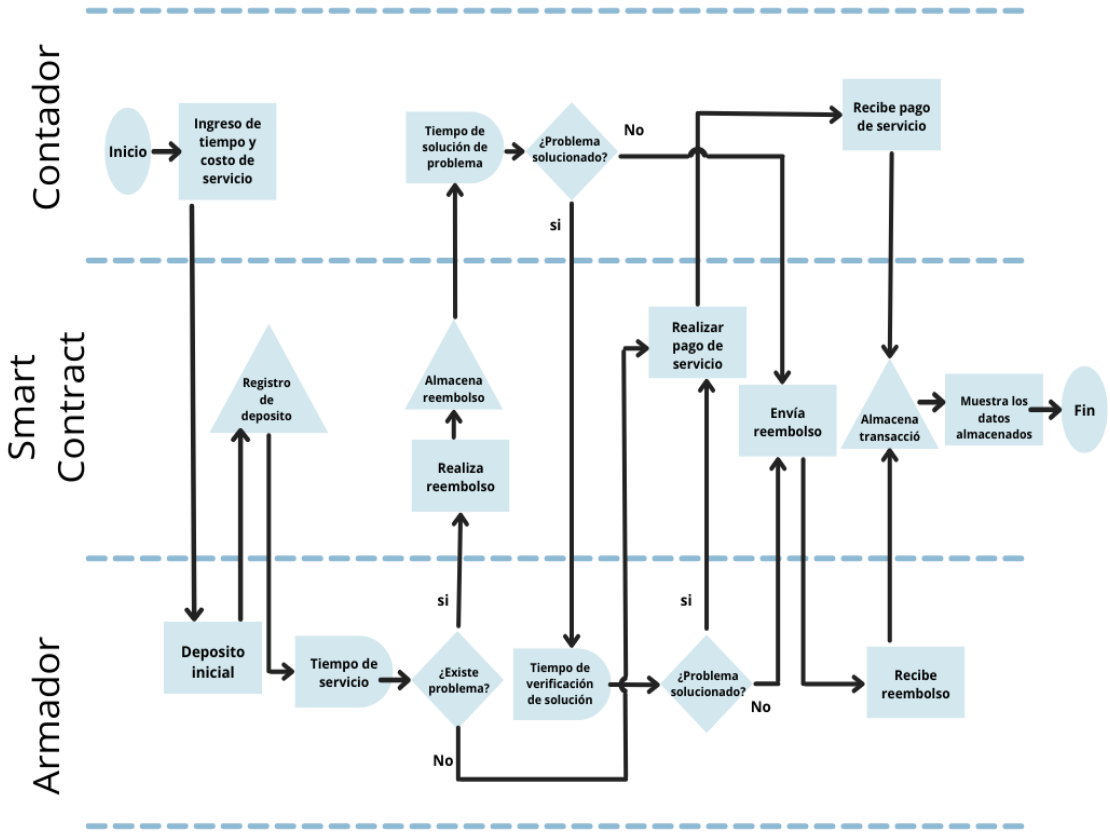


Figura 4. Diagrama de Procesos del contrato inteligente y sus acciones

Antes de iniciar el contrato se debe ingresar el tiempo límite que debe durar, el tiempo está basado en slots que es equivalente a un segundo, este tiempo se da si no existe ningún inconveniente, luego está el tiempo límite de respuesta de queja, donde se espera que el Contador responda a la queja del Armador, también está el tiempo límite de solución de problema, en el cual se debe solucionar el problema para proceder a notificar al Armador sobre esto. También está el tiempo de respuesta de confirmación, en el cual el Armador debe contestar si el problema está solucionado.

El contrato inicia con un primer depósito por parte del Amador o Cliente hacia el Contador o Empresa, luego el Armador verifica si existe algún problema, si no existe el contrato concluye depositando el valor acordado en la cuenta del Contador. Si el Armador visualiza un problema el Contador le reembolsa su dinero, en este caso el Contador debe buscar soluciones al problema, si no hay solución al problema el contrato concluye con el reembolso antes realizado. Si existe una solución el Armador debe verificar que el problema este solucionado, en caso de que no esté solucionado el problema el contrato concluye. Si el problema está solucionado procede a depositar el pago de los servicios y el contrato finaliza y muestra las transacciones realizadas durante todo el proceso.

Con la ayuda del diagrama de procesos y con las entidades y sus atributos identificados, podemos simular el proceso completo de un Smart Contract. Usando Marlowe que tiene Blockly para un mejor entendimiento, esto solo es posible en el simulador, para poder subir esto a una cadena de bloques se requiere otro lenguaje de programación, el cual es Haskell.

Se usan variables llamadas “Role”, en el cual se ingresa el nombre de los involucrados en el contrato, en este caso sería Armador y Contador, el bloque rojo llamado “Constant Param” sirve para declarar la variable de costo de servicio, se lo coloca así porque el precio vario con el servicio brindado. Y se usa un bloque naranja llamado “ada”, representando la criptomoneda por defecto e la red

El bloque general se llama “Contract” dentro de este se ejecuta todas las especificaciones del contrato. El bloque el cual inicia el contrato se llama “When”, dentro de este se especifica las acciones a realizar y tiene un parámetro llamado “after slot” que marca el tiempo de duración de estas acciones. Se usa un bloque amarillo llamado “Deposit” en el cual especifica la cuenta que recibirá el pago, el monto con el que se trabajará, el tipo de moneda y de que cuenta vendrá el pago.

Luego se usa otro bloque amarillo el cual tiene por nombre “Choice”, donde se le pone nombre a la opción, se pone quien puede escoger la opción, en este caso el Rol y un bloque verde llamado “between”, para que aparezca la opción a la hora de simulación.

Se usa un Bloque Morado llamado “Pay”, en el cual se realiza un pago donde se especifica la cuenta que recibirá el pago, el monto, la moneda y la cuenta que realiza el pago. Este se diferencia al Bloque amarillo “Deposit” por qué se usa para un reembolso de pagos dentro del contrato.

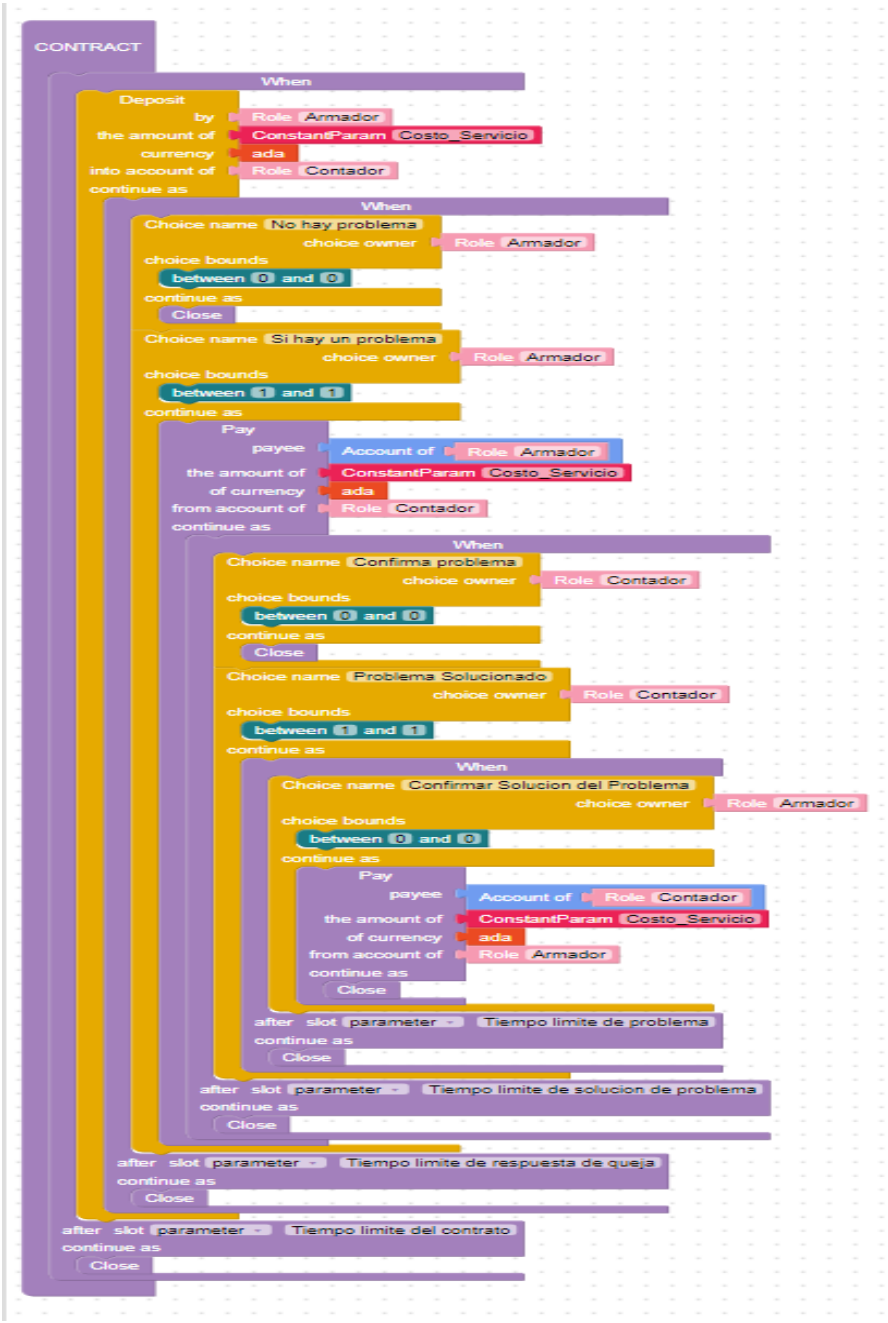


Figura 5. Smart Contract en Marlowe con Blockly

Para poder codificar lo plasmado en la figura 5 en la cadena de bloques se requiere tener el contrato escrito en Haskell, el cual es un lenguaje de programación funcional compatible con la cadena de bloques. Por ello también se realizó el contrato en este lenguaje de programación.

```
{-# LANGUAGE OverloadedStrings #-}
module Escrow where

import Language.Marlowe.Extended

main :: IO ()
main = print . pretty $ contract

-- Declaracion de variables

explicitRefunds :: Bool
explicitRefunds = False

--Declaracion de roles, las entidades que forman parte del proceso de negocio
empresa, cliente :: Party
empresa = Role "Contador"
cliente = Role "Armador"

--Costo del servicio, este se valdiara en ADA
price :: Value
price = ConstantParam "Costo de servicio"

--Declaracion de los tiempos de respuesta y tiempo de total del contrato
depositTimeout, disputeTimeout, answerTimeout, arbitrageTimeout :: Timeout
depositTimeout = SlotParam "Tiempo limite de contrato"
disputeTimeout = SlotParam "Tiempo limite de problema"
answerTimeout = SlotParam "tiempo limite de solucion de problema"
arbitrageTimeout = SlotParam "tiempo limite de respuesta de queja"

--declaracion de las opciones a elegir
choice :: ChoiceName -> Party -> Integer -> Contract -> Case
choice choiceName chooser choiceValue = Case (Choice (ChoiceId choiceName chooser)
                                                     [Bound choiceValue choiceValue])

--Depostio inicial
deposit :: Timeout -> Contract -> Contract -> Contract
deposit timeout timeoutContinuation continuation =
    When [Case (Deposit empresa cliente ada price) continuation]
         timeout
         timeoutContinuation

--Nombre de la opcion a escoger
choices :: Timeout -> Party -> Contract -> [(Integer, ChoiceName, Contract)] -> Contract
choices timeout chooser timeoutContinuation list =
    When [choice choiceName chooser choiceValue continuation
          | (choiceValue, choiceName, continuation) <- list]
         timeout
         timeoutContinuation

--Pago a empresa o reembolso
empresaAcliente, pagarEmpresa :: Contract -> Contract
empresaAcliente = Pay empresa (Account cliente) ada price
pagarEmpresa = Pay cliente (Party empresa) ada price

--Pago a las Wallets correpondientes al final del contrato
refundBuyer :: Contract
refundBuyer
 | explicitRefunds = Pay cliente (Party cliente) ada price Close
 | otherwise = Close

refundSeller :: Contract
refundSeller
 | explicitRefunds = Pay empresa (Party empresa) ada price Close
 | otherwise = Close

--Contrato
contract :: Contract
contract = deposit depositTimeout Close $
           choices disputeTimeout cliente refundSeller
             [ (0, "No hay problema"
               , refundSeller
               )
             , (1, "si hay un problema"
               , empresaAcliente $
                 choices answerTimeout empresa refundBuyer
                   [ (1, "Confirm problem"
                     , refundBuyer
                     )
                   , (0, "Problema solucionado"
                     , choices arbitrageTimeout cliente refundBuyer
                         [ (0, "Confrimar solucion"
                           , pagarEmpresa
                             Close
                           )
                         , (1, "Problema  no solucionado"
                           , refundBuyer
                           )
                         ]
                     )
                   ]
               )
             ]
```

Figura 6. Smart Contract en Haskell

La simulación en ambos casos seria la misma, debido a que son dos maneras distintas de ver el algoritmo, pero el objetivo es el mismo.

Primero se ingresa el Slot inicial, en este caso sería el cero, pero si se logra colocarlo en la cadena de bloques debe corresponder al que está actualmente.

Luego se ingresa los tiempos a considerar dentro del contrato, estos tiempos deben estar entro del tiempo límite del contrato. Por último, se ingresa el costo del servicio y se empieza a simular.

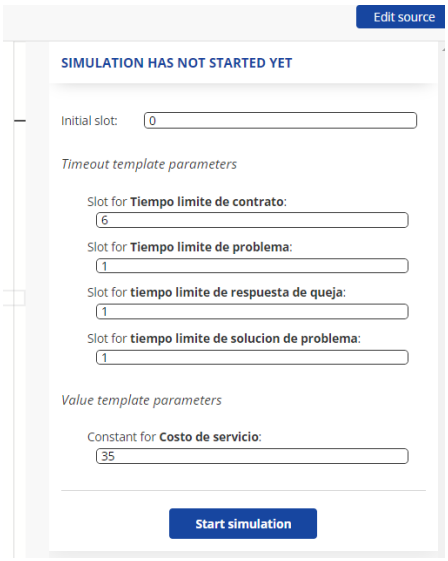


Figura 7. Ingreso de los datos de entrada

Luego se inicia la simulación, en la cual nos indica la primera acción del Armado, el cual realiza el primer deposito dentro del contrato.

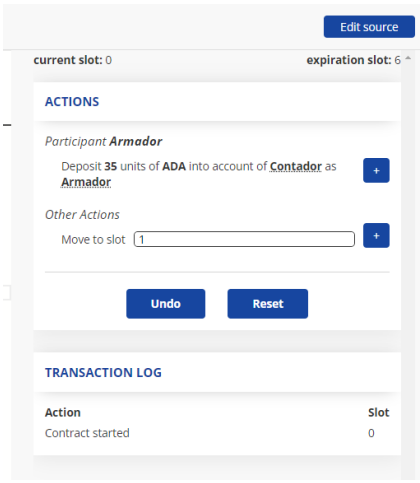


Figura 8. Primera acción dentro del contrato

Una vez se realice el depósito el Armador ve si la situación está en orden, en caso de escoger que no existe un problema el contrato terminara inmediatamente.

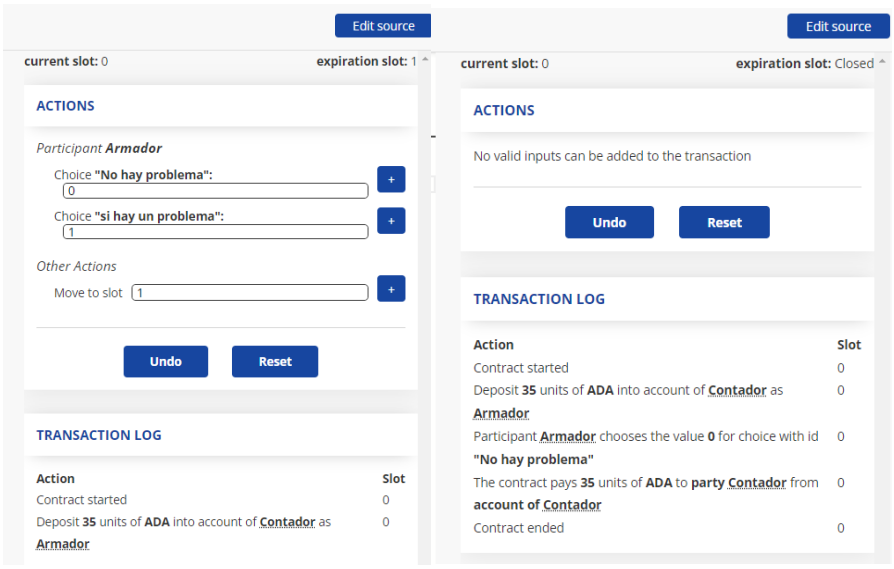


Figura 9. No existe ningún problema

En el caso que si exista un problema el contrato reembolsa el monto a la cuenta del Armador y se espera la respuesta del Contador, si no se soluciona el problema o no existe solución en contrato termina.

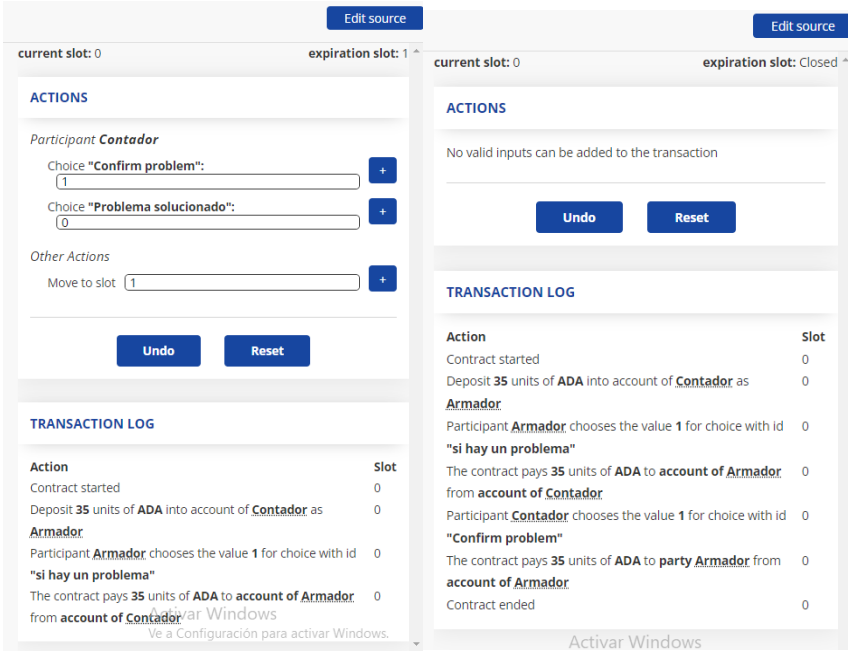


Figura 10. Confirma problema y termina el contrato.

En el caso que el problema se soluciones este procederá a consultar al Armador si se solucionó el problema, el cual puede confirmar esta solución o cancelar el contrato seleccionando ir al slot final. En este caso el Afirmo que si existió solución del problema y Procede a depositar el monto a la cuenta del Contador automáticamente y el contrato finaliza dándonos a conocer los movimientos hechos durante todo el proceso

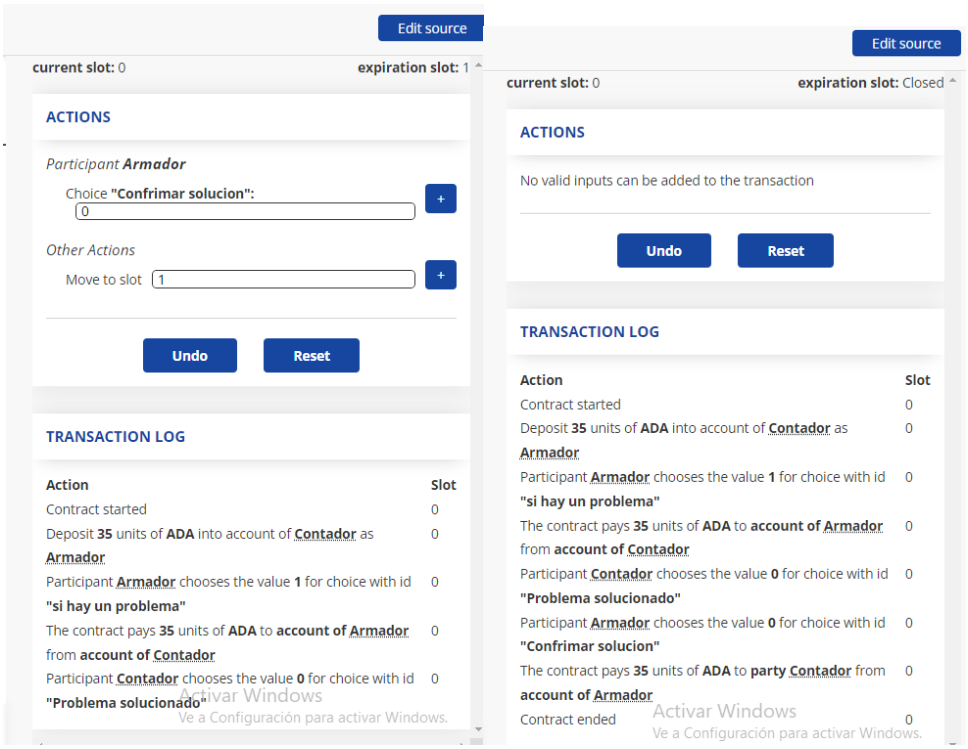


Figura 11. Finalización del contrato.

3.6. Lista de requerimientos

R1. Analizar el proceso actual del negocio con el que se trabaja.

R2. La investigación deberá ser simulada por una herramienta web perteneciente a Cardano.

R3. Diagramar procesos para el entendimiento del Smart Contract.

R4. La guía debe permitir detectar los elementos necesarios para armar un Contrato inteligente.

R5. La guía se generará de tal forma que permita al usuario realizar las fases planteadas comprendiendo cada proceso.

R6. Se usarán el lenguaje de programación Haskell y Blockly para digitalizar el contrato.

R7. Conocimiento sobre Blockchain y Criptomonedas.

R8. Identificar los procesos del negocio por medio de un miembro de la empresa que conozca el proceso completo de los servicios.

R9. La cadena de Bloques ayudara a mantener la información de manera confidencial, integra y segura.

R10. Los métodos de recolección de información se deben dar a través de encuestas orales o escritas.

R11. El contrato realizado por la guía debe ser entendible para todo tipo de usuario interesado en el proyecto.

R12. No se requerirá de un ente validador en las transacciones de capital entre billeteras virtuales.

R13. La guía está dirigida para personas interesadas en la Tecnología Blockchain y criptomonedas

R14. Los tiempos de espera dentro del contrato deben ser ingresados antes de la ejecución

R15. El informe de las transacciones realizadas durante el contrato se da en la herramienta de simulación al finalizar el contrato.

CONCLUSIONES

- Para el desarrollo de la guía se aplicó conocimiento de Blockchain y criptomonedas, dando a conocer una de las formas de realizar contratos inteligentes.
- Las fases aplicadas en el proyecto tienen su base en una propuesta metodológica para el desarrollo de Smart Contracts; la información referente al desarrollo se centró en otro tipo de moneda y no la plasmada en el proyecto, por ello se realiza el caso de estudio dentro de la red de Cardano debido a los beneficios que trae usar esta cadena de bloques.
- La recolección de información es crucial para detectar los datos e información que deberá ir plasmada en el contrato y ser subidos a la Blockchain, por ello es

necesario conocer cómo funciona la empresa y sus procesos de negocio, tomando uno de estos procesos como base para la implementación del contrato inteligente.

- Los resultados de las variables son demostrables debido a que el tiempo se ve definido en el contrato reduciendo o fijando un lapso hasta la culminación de este, la reducción de costos es plasmada al usar la cadena de bloques de Cardano porque esta no tiene comisiones si se usa una wallet de esta misma red.

RECOMENDAICONES

- Tener en cuenta que la herramienta de simulación solo sirve para observar el funcionamiento de un contrato real, y que se puede modificar de acuerdo con los procesos que tenga cada organización.
- Conocer diferentes criptomonedas permitirá conocer nuevas alternativas para la creación de Smart Contracts, la metodología desarrollada en la guía es completamente aplicable.
- Para evitar que exista una comisión por transacción es necesario utilizar una wallet perteneciente a la red de Cardano y realizar las transacciones entre estas billeteras virtuales.
- La guía contempla los pasos a seguir para crear un contrato inteligente independientemente de la red que se utilice, se identifican todos los fatores fundamentales y su implementación cambia de acuerdo con la criptodivisa que se use o la red en la que se ejecute el contrato.

BIBLIOGRAFÍA

[1] R. Sarmiento Lotero, «TEORÍA DE LOS CONTRATOS: UN ENFOQUE ECONÓMICO,» *Cuadernos Latinoamericanos de Administración,* vol. 1, pp. 11-24.

[2] Panoil, «Panoil,» 2019. [En línea]. Available: https://panoil.com.ec/ .

[3] Superintendencia de bancos y seguros, «Superbancos,» 22 enero 2013. [En línea]. Available: https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2017/06/L1_XIV_cap_I.pdf.

[4] J. P. Valencia Ramírez, «RITI,» *Contratos Inteligentes,* vol. 7, nº 14, 2019.

[5] J. A. Padilla Sánchez, «Blockchain y contratos inteligentes: aproximacion a sus problemáticas y retos jurídicos,» *Revista de Derecho Privado,* nº 39, pp. 175 - 201, 2020.

[6] E. Nova Z, C. Escobar M, M. J. Cajas A y L. Fuentes O, «Los Smart Contracts como alternativa para la modernización de recaudación tributaria en Ecuador,» *Iuris Dictio,* vol. 26, nº 26, 2020.

[7] C. Omar Solis, E. Pérez Cortés y H. Cervantes Maceda, «Hacia una metodologia para el diseño de contratos inteligentes,» *ReCIBE, Revista electrónica de computación, Informática, Biomédica y Electrónica,* vol. 8, nº 1, 2019.

[8] K. Tommy, «Marlowe,» Developers Cardano, 4 5 2022. [En línea]. Available: https://developers.cardano.org/docs/smart-contracts/marlowe.

[9] Consejo FACSISTEL, *Resolución RCF-FST-SO-09 No. 03,* La Libertad, Santa Elena, 2021.

[10] Datta Business Innovarion, «Blockchain revoluciona,» *Computerworld 312,* pp. 42-43, 2018.

[11] Criptoinforme, «Fundación Cardano: «Cerca de 900 empresas interesadas en trabajar con Cardano están en proceso,» Criptoinforme, 20 mayo 2021. [En línea]. Available: https://criptoinforme.com/altcoins/fundacion-cardano-cerca-de-900-empresas-interesadas-en-trabajar-con-cardano-estan-en-proceso/.

[12] Cripto Millonarios, «Walmart Se Asocia Con CARDANO?,» 2021 septiembre 26. [En línea]. Available: https://www.youtube.com/watch?v=aw970CfwUqM.

[13] Secretaría Nacional de Planificación, «Plan de Creación de Oportunidades 2021-2025,» 2021. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf.

[14] Corporacion Cardano, «What is ADA?,» Cardano, 2022. [En línea]. Available: https://cardano.org/what-is-ada/.

[15] IBM, «What is blockchain technology?,» IBM, [En línea]. Available: https://www.ibm.com/topics/what-is-blockchain.

[16] J. Tower y J. Gray, «Blockly Language Creation and Applications: Visual Programming for Media Computation and Bluetooth Robotics Control,» 24 02 2015. [En línea]. Available: https://dl.acm.org/doi/abs/10.1145/2676723.2691871.

[17] Corporacion Cardano, «Cardano.org,» Cardano, 2022. [En línea]. Available: https://cardano.org/.

[18] Real Academia Española, «Contrato,» Real Academia Española, 2021. [En línea]. Available: https://dle.rae.es/contrato?m=form.

[19] S. Gil, «Contrato,» Economipedia, 6 febrero 2016. [En línea]. Available: https://economipedia.com/definiciones/contrato.html.

[20] Real Academia Española, «Criptomoneda,» Real Academia Española, [En línea]. Available: https://dle.rae.es/criptomoneda?m=form.

[21] I. B. Ferre, «Criptomoneda,» Economipedia, 25 septiembre 2017. [En línea]. Available: https://economipedia.com/definiciones/criptomoneda.html.

[22] Real Academia Española., «Divisa.,» En Diccionario de la lengua española., [En línea]. Available: https://dle.rae.es/divisa.

[23] S. J. Pedrosa, «Divisa,» Economipedia, 12 enero 2016. [En línea]. Available: https://economipedia.com/definiciones/divisa.html.

[24] E. Amodeo, «¿Qué son los DSL (Domain Specific Languages)?,» eamodeorubio.wordpress, 13 09 2010. [En línea]. Available: https://eamodeorubio.wordpress.com/2010/09/13/%C2%BFque-son-los-dsl-domain-specific-languages/.

[25] CodeDocs, «Domain-specific language,» CodeDocs.org, 2022. [En línea]. Available: https://codedocs.org/what-is/domain-specific-language.

[26] Y. Perez Ortiz, «Sistema integrado de medios para la programacion funcional con el lenguaje HASKELL,» 10 2014. [En línea]. Available: http://roa.ult.edu.cu/handle/123456789/3130.

[27] Developers Cardano, «Marlowe | cardano developer portal,» developer.cardano.org, 2022. [En línea]. Available: https://developers.cardano.org/docs/smart-contracts/marlowe.

[28] L. Cuban, «Cómo comenzar con el Staking en Cardano, guía para novatos,» Cardano, 2021. [En línea]. Available: https://forum.cardano.org/t/como-comenzar-con-el-staking-en-cardano-guia-para-novatos/44640.

[29] Bit2me Academy, «Smart Contracts: ¿Qué son , cómo funcionan y qué aportan?,» Bit2me, 2022. [En línea]. Available: https://academy.bit2me.com/que-son-los-smart-contracts/.

[30] J. Jabalera, «Qué es una ‘wallet’ o monedero de criptomonedas y cómo se usa,» Forbes, 16 noviembre 2021. [En línea]. Available: https://forbes.es/criptomonedas/125754/que-es-una-wallet-o-monedero-de-criptomonedas-y-como-se-usa/.

[31] Bit2me Academy, «Qué es una wallet de criptomonedas o monedeo de criptomonedas,» Bit2me, 2022. [En línea]. Available: https://academy.bit2me.com/wallet-monederos-criptomonedas/#Que_es_una_wallet_de_criptomonedas.

[32] M. Singh y S. Kim, «Branch based blockchain technology in intelligent vehicle,» *Computer Networks,* vol. 145, pp. 2019-131, 2018.

[33] I. Makhdoom, M. Abolhasan, H. Abbas y W. Ni, «Blockchain's adoption in IoT: The challenges, and a way forward,» *Journal of Network and Computer Applications,* vol. 125, pp. 251-279, 2019.

[34] D. G. Villafuerte Guerrero, «El Smart Contract como nueva forma de contratacion en el codigo de comercio Ecuatoriano.,» 2020. [En línea]. Available: http://repositorio.puce.edu.ec/bitstream/handle/22000/18563/TESIS%20Gabriela%20Villafuerte%20Guerrero.pdf?sequence=1&isAllowed=y.

[35] P. Medina Fernández, «Los contratos inteligentes en España,» 2019. [En línea]. Available: https://riull.ull.es/xmlui/handle/915/14876.

[36] E. Anatolyevna Kirillova, V. Vladimirovna Bogdan, I. Lagutin y E. Dmitrievich Gorevoy, «Estado legal de los contratos inteligentes: características, papel, significado,» *Jurídicas CUC,* vol. 15, nº 1, pp. 285-300, 2019.

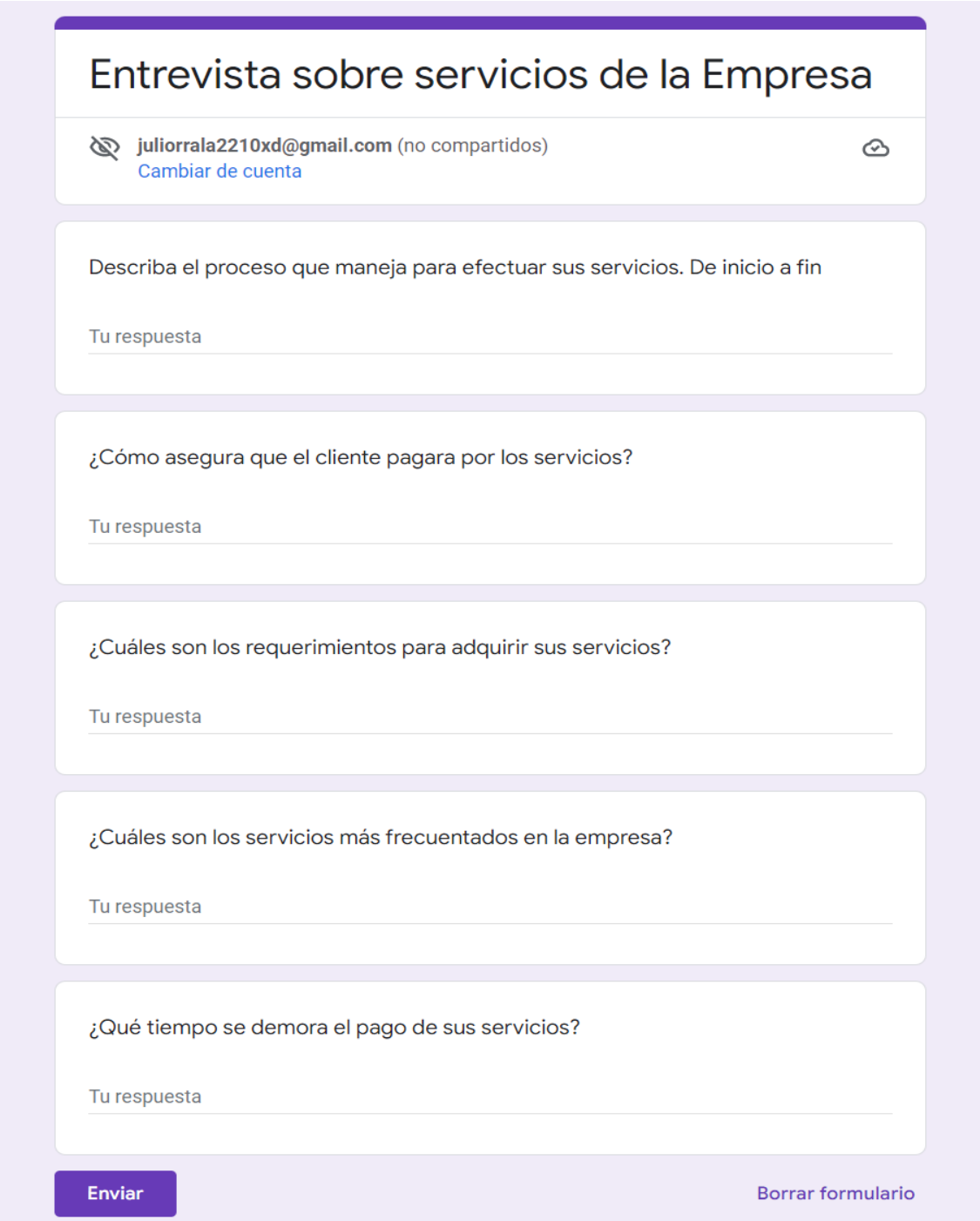
[37] A. Carvajal Guerreo y Y. H. Suarez Lobo, «Posibles usos de los contratos inteligentes en una blockhain para el comercio de bienes y servicios.,» *Visión Internacional (Cúcuta),* vol. 4, nº 1, pp. 27-40, 2021.

[38] H. L. Avila Baray, Introducicon a la Metodologia dde la investigacion., CD. Cuauhtemoc, Chihuahua, Mexico.: Edicion Electronica, 2006.

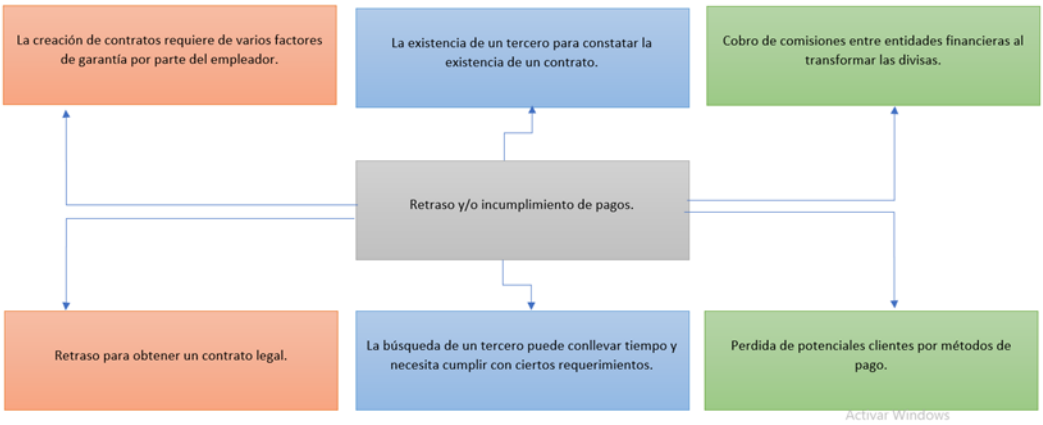
[39] G. Gonzáles, «Investigación diagnóstica: características, técnicas, tipos, ejemplos,» Lifeder, 2 marzo 2020. [En línea]. Available: https://www.lifeder.com/investigacion-diagnostica/.

[40] TECNISEA, *B.O.C. PROFORMA DA,* La Libertad, 2021.

ANEXOS:

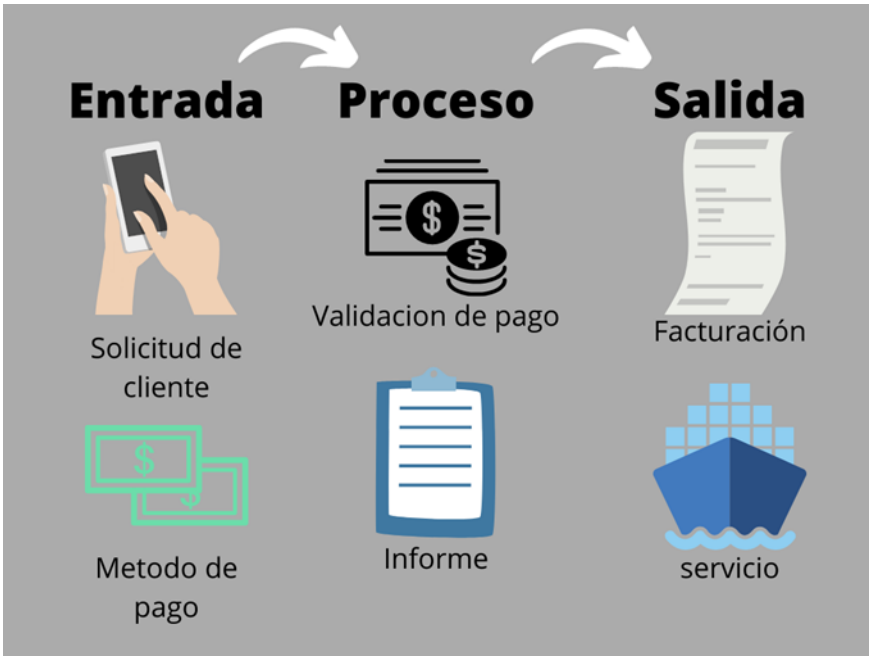


Anexo 1. Formato de entrevista

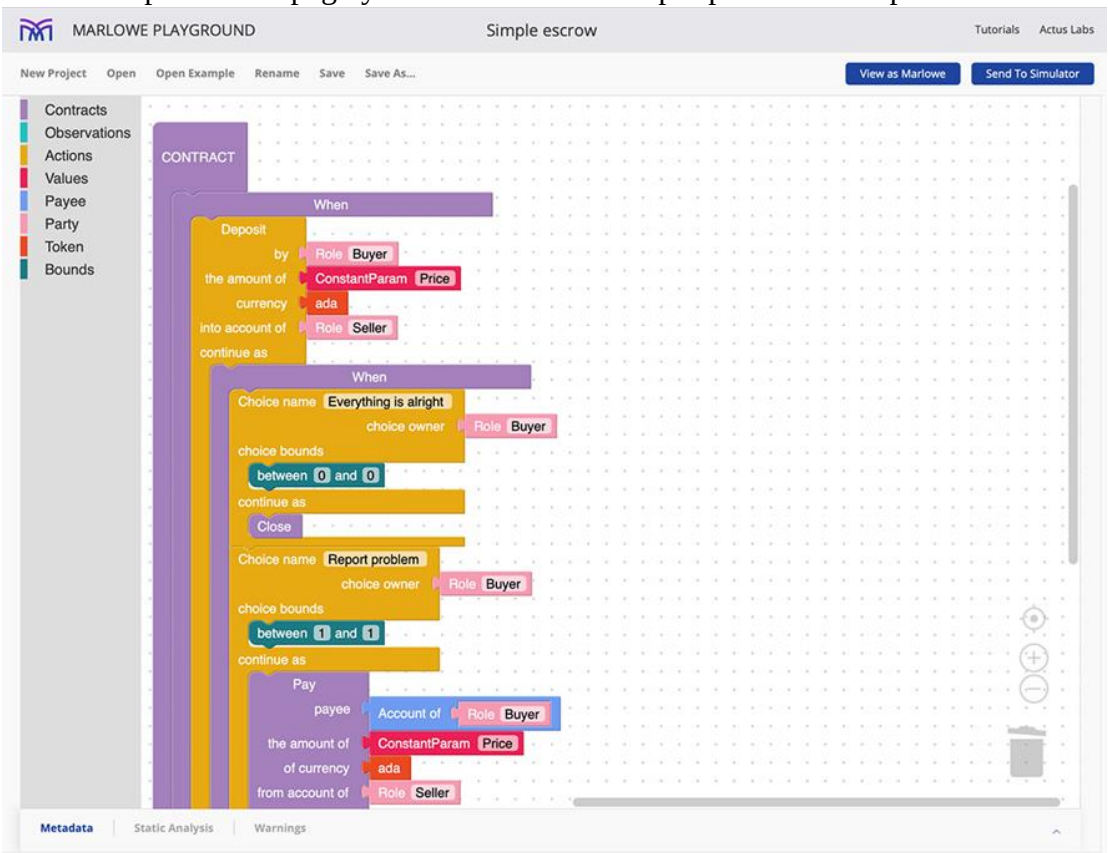


Anexo 2. Árbol de problemas, especifica el problema principal de los pagos de servicios.

Anexo 3. Proceso actual de la empresa, se detalla los cinco pasos que realiza la empresa para la adquisición de sus servicios.



Anexo 4. Datos de entrada, proceso y salida. Detalla la información que entra, el proceso de pago y la salida de servicios por parte de la empresa.



Anexo 5. Marlowe Playground, Para tener un mejor entendimiento del funcionamiento del contrato inteligente.

Anexo 6. Figura representativa de la Corporación Cardano

Anexo 7. Representación de la criptodivisa ADA moneda oficial de la corporación Cardano

```
{-# LANGUAGE OverloadedStrings #-}
module Escrow where

import Language.Marlowe.Extended

main :: IO ()
main = print . pretty $ contract

-- Declaracion de variables

explicitRefunds :: Bool
explicitRefunds = False

--Declaracion de roles, las entidades que forman parte del proceso de negocio
empresa, cliente :: Party
empresa = Role "Contador"
cliente = Role "Armador"

--Costo del servicio, este se valdiara en ADA
price :: Value
price = ConstantParam "Costo de servicio"

--Declaracion de los tiempos de respuesta y tiempo de total del contrato
depositTimeout, disputeTimeout, answerTimeout, arbitrageTimeout :: Timeout
depositTimeout = SlotParam "Tiempo limite de contrato"
disputeTimeout = SlotParam "Tiempo limite de problema"
answerTimeout = SlotParam "tiempo limite de solucion de problema"
arbitrageTimeout = SlotParam "tiempo limite de respuesta de queja"

--declaracion de las opciones a elegir
choice :: ChoiceName -> Party -> Integer -> Contract -> Case
choice choiceName chooser choiceValue = Case (Choice (ChoiceId choiceName chooser)
                                        [Bound choiceValue choiceValue])

--Depostio inicial
deposit :: Timeout -> Contract -> Contract -> Contract
deposit timeout timeoutContinuation continuation =
   When [Case (Deposit empresa cliente ada price) continuation]
       timeout
       timeoutContinuation

--Nombre de la opcion a escoger
choices :: Timeout -> Party -> Contract -> [(Integer, ChoiceName, Contract)] -> Contract
choices timeout chooser timeoutContinuation list =
   When [choice choiceName chooser choiceValue continuation
        | (choiceValue, choiceName, continuation) <- list]
       timeout
       timeoutContinuation

--Pago a empresa o reembolso
empresaAcliente, pagarEmpresa :: Contract -> Contract
empresaAcliente = Pay empresa (Account cliente) ada price
pagarEmpresa = Pay cliente (Party empresa) ada price

--Pago a las Wallets correpondientes al final del contrato
refundBuyer :: Contract
refundBuyer
 | explicitRefunds = Pay cliente (Party cliente) ada price Close
 | otherwise = Close

refundSeller :: Contract
refundSeller
 | explicitRefunds = Pay empresa (Party empresa) ada price Close
 | otherwise = Close

--Contrato
contract :: Contract
contract = deposit depositTimeout Close $
         choices disputeTimeout cliente refundSeller
           [ (0, "No hay problema"
             , refundSeller
             )
           , (1, "si hay un problema"
             , empresaAcliente $
               choices answerTimeout empresa refundBuyer
                 [ (1, "Confirm problem"
                   , refundBuyer
                   )
                 , (0, "Problema solucionado"
                   , choices arbitrageTimeout cliente refundBuyer
                       [ (0, "Confrimar solucion"
                         , pagarEmpresa
                           Close
                         )
                       , (1, "Problema  no solucionado"
                         , refundBuyer
                         )
                       ]
                   )
                 ]
```

Anexo 8. Codigo en Haskell del Smart Contract.

Anexo 9. Logo de Marlowe, herramienta para simular contratos inteligentes.

La Libertad, 6 de octubre del 2022

CERTIFICADO ANTIPLAGIO

En mi calidad de tutor del trabajo de titulación denominado "**DISEÑO DE UNA GUÍA PARA LA ELABORACIÓN DE SMART CONTRACTS EN LA RED DE CARDANO PARA LA EMPRESA NAVIERA PANOIL**", elaborado por el estudiante **ORRALA MOREIRA JULIO ANTONIO**, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniero en Tecnologías de la Información, me permito declarar que una vez analizado en el sistema antiplagio URKUND, luego de haber cumplido los requerimientos exigidos de valoración, el presente proyecto ejecutado, se encuentra con 1% de la valoración permitida, por consiguiente se procede a emitir el presente informe


Ouriginal

DETALLES DEL ENVÍO

REMITENTE
OROZCO IGUASNIA WALTER ARMANDO

ARCHIVO
COMPONENTE TEORICO -JULIO ORRALA.docx

FECHA DE ENVÍO (ECT)
2022-10-06T17:50:00

NÚMERO DE ENVÍO
145739822

PALABRAS
9850

MENSAJE
Revisión de similitud trabajo de Julio Orrala

COMPONENTE TEORICO -JULIO ORRALA.docx
OROZCO IGUASNIA W ALTER ARMANDO — today at 10:50 AM
UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

Componente Práctico Julio Orrala
Revisión de similitud trabajo de Julio Orrala

1%	9850	100%
Similarity	Words	Largest Match (%)
4.7MB	**docx**	**D145739822**
Size	File Type	Submission ID

Atentamente,

Ing. Walter Orozco Iguasnia
DOCENTE
Copia: archivo.

Anexo 10. Certificado de Antiplagio