Práctica 2: El uso de Blockchain y Smart Contracts para modelo de negocio

Datos Masivos y Encadenados

Alberto Royo Valle (100481813)
Alejandro Sanz Fernández (100490797)
Arash Kazemi Díaz (100384030)
Julian Quintero Bejarano(100460445)
Pablo González Tamames (100483806)
Pablo Peñuela Rodríguez (100488691)

Computer Science and Engineering Deparment

Índice

1. Resumen ejecutivo

Este proyecto se ha basado en nuestra primera práctica, la cual consistió en desarrollar una aplicación en la que conectamos diferentes fuentes de datos para ofrecer un servicio de planes turísticos como planes vacacionales a personas interesadas en visitar las capitales europeas. Para ello, se diseña en la parte práctica de esta asignatura una aplicación que propone como destinos las capitales europeas, un número de planes a realizar en las mismas y una ruta al aeropuerto más cercano con una lista de los vuelos más baratos. Ahora se pretende llevar el proyecto un paso más allá y, empleando blockchain y smart contracts desarrollar ideas de negocio en torno a los servicios que se pueden ofrecer con la aplicación.

Mediante el uso de la tecnología blockchain y smart contracts se pretende aprovechar la seguridad y la confianza que se desprende de ambos para, así, conseguir también la confianza del cliente a la hora de utilizar los métodos de pago que nuestra aplicación pondrá a disposición de los clientes que la usen, esta servirá tanto para contratar los paquetes vacacionales; para que las empresas (sobre todo relacionadas al sector del turismo) puedan anunciar sus servicios y productos; para obtener los créditos de la aplicación definidos mas adelante y al mismo tiempo hacer uso de estos. Teniendo en cuenta las características de los tipos de blockchain, se considera que la opción mas viable para implementar el modelo de negocio es una **blockchain privada** con un mecanismo de consenso de **prueba de participación (Pos)**. Esto permitirá tener una autoridad centralizada, por lo que se podrían implementar cambios y resolver problemas rápidamente, tendrá buena escalabilidad, ofrecer mayor niveles de privacidad a nuestros clientes y validar transacciones automáticamente.

Se implementarán los smart contract para cada uno de los servicios que se ponen a disposición del cliente. En este proyecto hay un total de cuatro, cada uno dedicado a un apartado:

- **Smart contract 1**: Contrato sobre los paquetes vacacionales ofrecidos.
- **Smart contract 2**: Contrato para las empresas que quieran anunciarse en nuestra aplicación.
- **Smart contract 3**: Contrato sobre la obtención de créditos.
- **Smart contract 4**: Contrato sobre el gasto de los créditos.

Con estos smart contract se pretende dar seguridad y confianza a todos los usuarios de los diferentes servicios. Todos ellos serán descritos en los siguientes apartados.

2. Descripción de la idea

En primer lugar se desarrollará un sistema para pedir y almacenar los datos del usuario. Esta suscripción inicial será gratuita y solo se utilizarán dichos datos para su correcto tratamiento, en esta suscripción se le pedirán los datos necesarios para poder, en su nombre, contratar todos los elementos necesarios que se requieran para la reserva del paquete vacacional como nombre y apellidos, dni, dirección, etc, para poder reservar, por ejemplo, vuelos y hoteles.

Una vez realizada la suscripción, al cliente se le dotará dentro de la misma, de una clave privada que recibirá de tal manera que nadie tenga posibilidad de averiguarla, incluidos nosotros como dueños de la aplicación, siempre con total posibilidad de cambiarla a gusto del cliente. A partir de esa clave privada se generará una clave pública asociada y una dirección derivada de esa clave pública, todo ello con funciones hash, para con ella poder comentar e interactuar con los demás usuarios en los chats habilitados para ello o mandarse mensajes privados, también codificados con hash, a través de la aplicación. En este punto se utilizarán las funciones hash para cifrar los mensajes y que nadie salvo los propios usuarios involucrados en la comunicación sean capaces de leerlo. Esto será posible si el emisor del mensaje conoce la dirección del usuario receptor y el mensaje del emisor solo podrá ser descifrado con la clave privada del usuario dueño de la dirección a la que se envía el mensaje.

La aplicación tendrá un chat común en la aplicación en la que comentar y charlar, posibilidad de comentar en los espacios diseñados para ello los paquetes de viajes ofrecidos por la aplicación y los ya mencionados mensajes privados. Todos estos mensajes estarán codificados siendo solo descifrables para, en el caso del chat común o los comentarios de los paquetes, todos los usuarios suscritos a la aplicación dejando fuera a toda persona ajena a la misma, y en el caso de los mensajes privados solo a los participantes en la conversación, ya sean dos personas o varias personas.

Una vez obtenidas las claves necesarias también se pondrá a disposición del cliente una cartera o wallet con la que podrá realizar las compras de los paquetes vacacionales, contratar los descuentos o los paquetes premium reservados solo a los mejores clientes. Esta cartera dispondrá de dos direcciones, una para pagar con el dinero de la misma y una segunda dirección, llamada dirección de cambio, con la que se pretende evitar el doble pago. Para ello, el funcionamiento del método de pago será como sigue: si queremos pagar cualquier servicio mediante nuestra cartera o wallet, siempre enviaremos todo el dinero y se devolverá en la dirección de cambio. Nuestra cartera o Wallet está preparada para manejar las dos direcciones.

Se implementará en la aplicación un sistema de moneda virtual, créditos, canjeables por viajes, descuentos, asesoramiento, puntos y hasta invitaciones a eventos. Estos créditos tendrán varias maneras de obtenerse: mediante el uso de nuestra aplicación; contratando paquetes vacacionales, comentando opiniones sobre los mismos, utilizando el chat de nuestra app y mediante el pago por transferencia bancaria a nuestra cuenta de empresa.

2.1. Niveles de usuarios

En la aplicación se tendrá diferentes niveles de usuarios en función de cuanto use la aplicación. Las políticas de definición de segmentos vienen dadas por:

1. **Nivel novato**: es el nivel mas bajo de usuario,es el usuario que aún no ha realizado ninguna compra o muy pocas de ellas.

   - Programas de puntos o recompensas que permitan a los clientes canjear sus puntos por descuentos en sus planes vacacionales o por otros beneficios.

2. **Nivel intermedio**: es el nivel en el que el usuario ha contratado algunos viajes con la app y ha participado activamente en la aplicación.

   - Asesoramiento personalizado para ayudar a los clientes a elegir los planes vacacionales que mejor se ajusten a sus necesidades y preferencias.
   - Programas de puntos o recompensas que permitan a los mejores clientes canjear sus puntos por descuentos en sus planes vacacionales o por otros beneficios.

3. **Nivel superior**: es el nivel en el que ha contratado bastantes paquetes vacacionales con la aplicación y es un miembro activo dentro de la aplicación.

   Los beneficios que podríamos ofrecer a este tipo de clientes podrían ser:

   - Descuentos exclusivos en sus planes vacacionales, prioridad en la reserva de planes vacacionales y en el atención al cliente ,acceso a planes vacacionales exclusivos que solo estén disponibles para los mejores clientes.
   - Asesoramiento personalizado para ayudar a los clientes a elegir los planes vacacionales que mejor se ajusten a sus necesidades y preferencias.
   - Programas de puntos o recompensas que permitan a los clientes canjear sus puntos por descuentos en sus planes vacacionales o por otros beneficios.

4. **Nivel premium**: este nivel solo se alcanza haciendo uso de la moneda virtual o realizando el pago del mismo. Con este nivel de usuario se le permite tener acceso a descuentos y paquetes vacacionales especiales para estos usuarios.

   Los beneficios que podríamos ofrecer a estos usuarios serían:

   - Descuentos exclusivos en sus planes vacacionales, prioridad en la reserva de planes vacacionales y en el atención al cliente, acceso a planes vacacionales exclusivos que solo estén disponibles para los mejores clientes.
   - Asesoramiento personalizado para ayudar a los mejores clientes a elegir los planes vacacionales que mejor se ajusten a sus necesidades y preferencias.
   - Programas de puntos o recompensas que permitan a los mejores clientes canjear sus puntos por descuentos en sus planes vacacionales o por otros beneficios.
   - Invitaciones a eventos exclusivos, como fiestas o viajes de incentivos, solo para los mejores clientes.

3. Tipo de blockchain

Existen diferentes tipos de blockchains, que se diferencian en función de su accesibilidad, su grado de descentralización y su uso de consenso entre los usuarios. Las principales categorías de blockchains son:

3.1. Según accesibilidad y descentralización

En este caso veremos las principales ventajas y desventajas de las blockchains publicas y privadas.

1. Blockchains públicas: son redes abiertas a cualquier usuario que desee unirse y participar en la validación de transacciones. La blockchain de Bitcoin es un ejemplo de una blockchain pública. Las principales ventajas de las blockchains públicas son:

   - Transparencia: las transacciones y los datos almacenados en una blockchain pública son visibles para todos los usuarios.
   - Descentralización: las blockchains públicas no están controladas por una autoridad central, lo que las hace resistentes a la censura y la manipulación.
   - Seguridad: las blockchains públicas utilizan criptografía y consenso entre los usuarios para mantener la seguridad de la red y validar las transacciones.
   - Inmutabilidad: una vez que se registran datos en una blockchain pública, no pueden ser modificados o eliminados.

   Las principales desventajas de las blockchains públicas son:

   - Escalabilidad: debido a la alta demanda, las blockchains públicas a menudo tienen problemas de escalabilidad y pueden tener tasas de transacción lentas o costosas.
   - Privacidad: como las transacciones y los datos en una blockchain pública son visibles para todos los usuarios, pueden ser potencialmente expuestos a terceros.

2. **Blockchains privadas**: son redes que solo pueden ser utilizadas por un grupo seleccionado de usuarios autorizados. Estas blockchains suelen estar controladas por una autoridad central. Las blockchains privadas son similares a las blockchains públicas en cuanto a su funcionamiento y características, pero tienen algunas diferencias clave. Las principales ventajas de las blockchains privadas son:

   - Control: las blockchains privadas son controladas por una autoridad central, lo que les permite implementar cambios rápidamente y resolver problemas de forma más eficiente.

- Escalabilidad: como solo un grupo seleccionado de usuarios tiene acceso a una blockchain privada, estas redes suelen ser más escalables que las blockchains públicas.
- Privacidad: las blockchains privadas ofrecen un mayor grado de privacidad, ya que solo los usuarios autorizados pueden ver las transacciones y los datos almacenados en la red.

Las principales desventajas de las blockchains privadas son:

- Centralización: al estar controladas por una autoridad central, las blockchains privadas pierden la descentralización y la resistencia a la censura que caracterizan a las blockchains públicas.
- Falta de transparencia: como solo un grupo seleccionado de usuarios tiene acceso a una blockchain privada, puede ser difícil verificar la integridad de la red y las transacciones que se realizan en ella.

3. Blockchains de consorcio: son una combinación entre las blockchains públicas y privadas, en las que un grupo de participantes autorizados tiene permiso para validar transacciones y mantener la red.

3.2. Según mecanismo de consenso

Además de estas categorías generales, también existen diferentes tipos de blockchains en función del mecanismo de consenso utilizado por la red para validar las transacciones. Algunos de los tipos de blockchains más comunes en función de su mecanismo de consenso son:

- Blockchains de prueba de trabajo (PoW): utilizan un mecanismo de consenso en el que los usuarios deben resolver un problema matemático para validar transacciones y agregarlas a la cadena de bloques. La blockchain de Bitcoin utiliza un mecanismo de consenso de prueba de trabajo.
- **Blockchains de prueba de participación (PoS)**: utilizan un mecanismo de consenso en el que los usuarios deben poseer cierta cantidad de tokens de la red para validar transacciones y agregarlas a la cadena de bloques.
- Blockchains de autorización: utilizan un mecanismo de consenso en el que solo un grupo seleccionado de nodos autorizados pueden validar transacciones y agregarlas a la cadena de bloques.

Teniendo en cuenta las características de los tipos de blockchain, se considera que la opción mas viable para implementar nuestro modelo de negocio es una **blockchain privada** con un mecanismo de consenso de **prueba de participación (Pos)**. Esto permitirá tener una autoridad centralizada, por lo que se podrían implementar cambios y resolver problemas rápidamente, tendrá buena escalabilidad, ofrecer mayor niveles de privacidad a nuestros clientes y validar transacciones automáticamente.

Llegados a este punto, para implementar los contratos inteligentes en nuestra plataforma usaremos el lenguaje de programación de Ethereum, Solidity. Al mismo tiempo obtendremos Remix como la plataforma de desarrollo de Ethereum en donde escribiremos y compilaremos nuestros contratos inteligentes.

Usaremos MetaMask como billetera digital compatible con Ethereum, esta herramienta ayudará a implementar nuestro contrato inteligente en la cadena de bloques de Ethereum. Utilizaremos la billetera digital para enviar una transacción que implemente el contrato inteligente respectivo a cada cliente en la cadena de bloques. Finalmente utilizaremos Infura como plataforma en la nube para administrar y interactuar con su contrato inteligente implementado. Para tener todos los procesos controlados se debe realizar pruebas adicionales para asegurarse de que los contratos inteligentes funcionan como se espera.

4. Smart contracts

Para nuestra aplicación que ofrece planes vacacionales a diferentes destinos. Un smart contract podría ayudar a automatizar el proceso de compra y pago de los planes vacacionales. Por ejemplo, cuando un usuario compra un plan vacacional a través de nuestra aplicación, el smart contract podría verificar automáticamente que el pago se ha realizado de manera correcta y completa. Una vez que se confirma el pago, el smart contract podría enviar una confirmación al usuario y liberar el plan vacacional para que el usuario lo pueda utilizar.

Además, el smart contract podría ayudar a gestionar el seguimiento del plan vacacional del usuario. Por ejemplo, si el usuario decide cambiar o cancelar su plan vacacional, el smart contract podría hacerse cargo de las devoluciones y reembolsos correspondientes de manera automática. Por lo tanto un smart contract podría ayudar a automatizar y simplificar muchos aspectos del proceso de compra y gestión de planes vacacionales en tu aplicación. Esto podría hacer que el proceso sea más eficiente y seguro para ti y tus usuarios.
En esta sección se tratará de explicar detalladamente los distintos smart contract para cada requerimiento.

4.1. Smart contract 1

El primer smart contract es el encargado de tramitar con seguridad y exactitud el proceso a seguir en caso de que un usuario decida contratar con la aplicación un paquete vacacional. Para ello serán necesarios los siguientes indicadores o identificadores:

- Identificadores del usuario: sus datos personales para poder hacer las distintas reservas en los servicios requeridos.
- Identificador del paquete vacacional contratado
- Fecha de ida
- Fecha de vuelta
- identificador del hotel
- identificador del vuelo
- identificadores de los planes propuestos por la aplicación
- Número de cuenta de ingreso

Con este smart contract lo que se pretende es controlar de manera eficiente y segura el contrato del paquete vacacional en su totalidad, para ello, el smart contract actuará de la siguiente manera:

- En primer lugar se realiza el pago por parte del usuario a la cuenta que se le proporciona, una cuenta del tipo ESXX xxxx xxxx xxxx xxxxxxxx desde el número de cuenta que tenga asociado al usuario suscrito nuestra aplicación.
- En segundo lugar lo que el smart contract debe de hacer es comprobar que dicho pago se ha realizado, para ello, el smart contract utilizará un oráculo para inspeccionar si el pago esta efectivamente hecho o no y así poder proceder con los siguientes pasos.
- Si el pago no se ha realizado el proceso acaba aquí con una notificación al usuario. En caso de que el proceso siga se procederá a la comprobación de las fechas de salida y de regreso para la reserva de los vuelos y hoteles. En caso de no haber reserva posible para esas fechas el smart contract propondrá otros vuelos y hoteles y se le notificará al usuario. En caso de decir que si se procede a reservar tanto el vuelo como el avión, en caso contrario se ordenará la devolución del dinero al usuario.

- Una vez reservados todos los elementos necesarios para la realizar el viaje se abren de nuevo distintas opciones.
  En caso de haber podido reservar el paquete de viaje original se comprobará si el usuario dispone de algún descuento por compra de créditos o por ser usuario premium y se le aplicará al precio final. En caso de no haber conseguido el paquete vacacional original y haber optado por unos vuelos y hoteles distintos, primeramente se devolverá la diferencia con respecto al plan inicial y posteriormente se comprobará si tiene descuentos o es miembro premium y se le aplicará el descuento sobre el precio final.
- Una vez realizado el pago el usuario tendrá hasta 2 semanas antes para cancelar el paquete vacacional. En caso de sobrepasar ese tiempo o contratar el paquete vacacional dentro de esas 2 semanas, el usuario perderá su dinero salvo causas excepcionales.

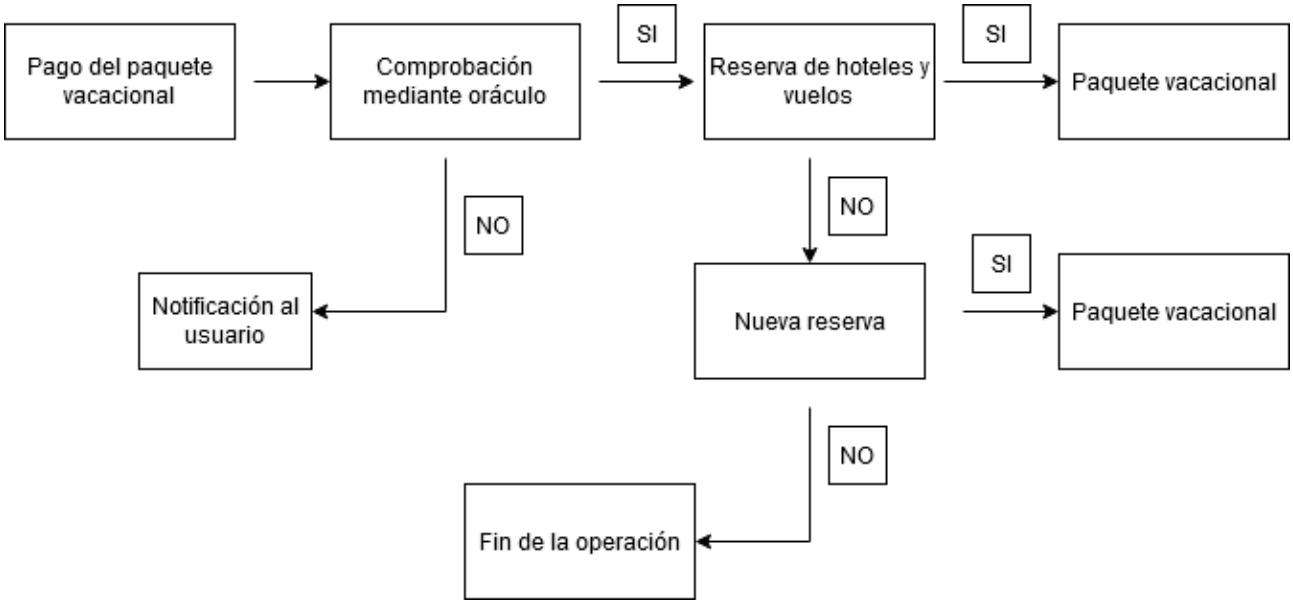

Figura 1: Diagrama de Flujo gestión de planes vacacionales

Los métodos que utilizaremos para este smart contract son los siguientes:

- Oráculo(): se encarga de verificar si el pago ha sido realizado con éxito o si no lo ha sido.
- reserva.hotel(): se encarga de reservar el hotel.
- reserva.vuelo(): se encarga de reservar el vuelo.
- notificacion.usuario(): para notificar si se ha reservado el paquete original con éxito o si por el contrario propone otros vuelos y hoteles diferentes a los originales.
- devolucion.dinero(): se encarga de devolver el dinero en caso negativo a la nueva propuesta hecha en caso de que no se haya podido reservar el producto original o, en caso de que se haya contratado, devolver la diferencia con el producto original. También se ocupa de devolver el dinero en caso de cancelación según las condiciones.

4.2. Smart contract 2

Este smart contract se encarga de que las empresas ajenas y que quieran anunciarse con la app puedan hacerlo mediante la seguridad que este smart contract propicia, para el siguiente smart contract necesitaremos:

- Identificador de la empresa que contrata nuestra aplicación: del mismo modo que al usuario se le piden los datos personales a las empresas que deseen contratar con la app se les pedirá el cif, dirección fiscal y el nombre para poder realizar correctamente la facturación del contrato por publicidad.
- Identificador propio: también se deberá proporcionar nuestros datos fiscales a la empresa contratante de nuestros servicios.
- Identificador de nuestro numero de cuenta: el archiconocido ESXX XXXX XXXX XXXXXXXX
- Identificador del número de cuenta de su empresa: con el propósito de poder realizar la transacción correctamente.

Este smart contract se encarga de la correcta transacción para el contrato de publicidad en nuestra aplicación, para ello el smart contract realizará los siguientes pasos:

- En primer lugar se realiza el pago por parte de la empresa interesada en contratar nuestros servicios de publicidad a la cuenta que se le proporcione, a continuación, el smart contract realiza las labores de verificación mediante un oráculo y comprueba que el ingreso ha sido realizado.
- una vez realizada la comprobación del ingreso bancario la empresa interesada enseña lo que quiere publicar exactamente en nuestra aplicación, esa publicación pasa a manos de una persona que verificará si el contenido a publicar es apto para nuestra aplicación o si por el contrario no lo es.
- en caso de no ser aceptada se devuelve el dinero a la empresa contratante y, si sigue interesada, se deberá volver a empezar todo el proceso. En caso de una verificación positiva el anuncio será publicado en nuestra aplicación durante un periodo de tiempo proporcional al dinero que se haya pagado.

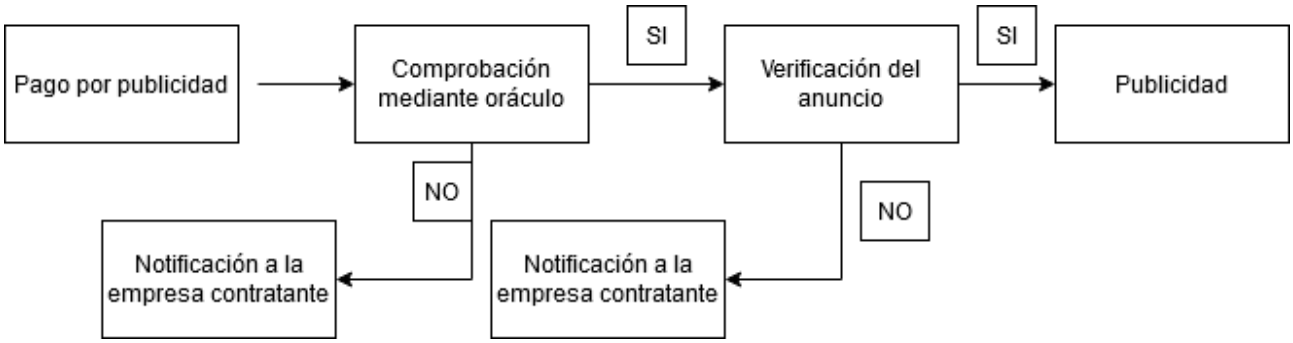

Figura 2: Diagrama de Flujo gestión de publicidad

Para este smart contract los métodos que se utilizarán son los siguientes:

- Oraculo(): este método, como en el caso anterior, se utiliza para comprobar que efecivmamente el pago ha sido realizado.
- devolucion.dinero(): si la empresa no pasa el proceso de verificación por parte de la persona al cargo se le devolverá la totalidad de su dinero.

4.3. Smart contract 3

Este smart contract se encarga de la compra de créditos, nuestra moneda virtual, o de la compra del usuario premium. Para ello serán necesarios los siguientes identificadores:

- Identificador del usuario: nombre y apellidos, dni, dirección, etc, con el fin de poder realizar la compra correctamente.
- Identificador de los créditos: en caso de que se quiera comprar créditos.
- Identificador de usuario premium: en cas de que se quiera adquirir el usuario premium.
- Nuestros propios identificadores.

Este smart contract se encarga de la correcta adquisición de los productos ofrecidos: los créditos y el usuario premium. De nuevo, para dotar de mayor seguridad al proceso y así ganarse la confianza del usuario. El smart contract procederá de la siguiente manera:

- En primer lugar, el cliente realiza el ingreso a la cuenta que se le proporcione haciendo uso de los identificadores de los cuales es propietario.
- En segundo lugar, mediante un oráculo, el smart contract comprueba que se ha realizado dicho pago.
- En tercer lugar, una vez se ha verificado el pago, se procede a proporcionar al usuario el número de créditos proporcional al precio pagado o, en caso de haber contratado el usuario premium, se procederá a otorgarle ese distintivo durante el tiempo proporcional al precio pagado por ello.

Este smart contract se encarga de la correcta transacción para la obtención de créditos o del usuario premium de nuestra aplicación, para ello el smart contract procederá de la siguiente manera:

- En primer lugar el cliente ingresará el dinero en la cuenta que se le proporcione, la misma cuenta que para el resto de smart contracts.
- En segundo lugar, una vez verificado el pago del cliente se procederá a la entrega del producto o productos. Una vez el cliente haya pagado, se procederá a realizar el ingreso de los créditos en la cartera proporcionada al cliente y que el mismo podrá emplear a su antojo. En caso de haber adquirido el usuario premium el smart contract procederá a otorgar durante un periodo proporcional al precio pagado al cliente.

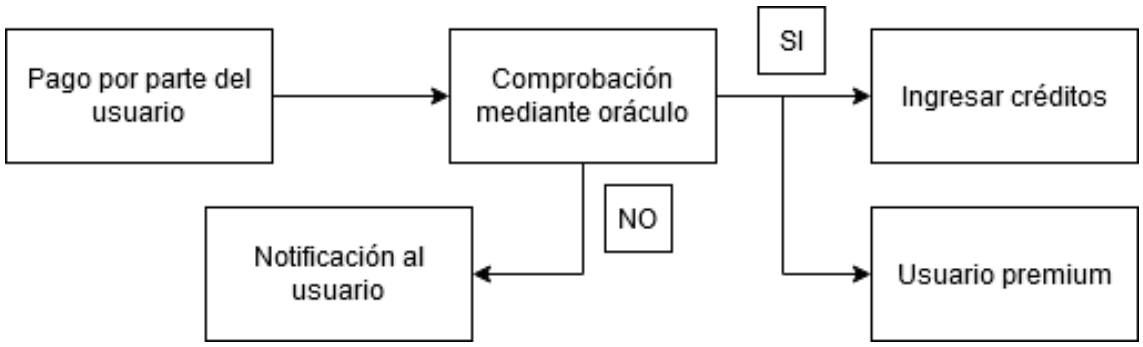

Figura 3: Diagrama de Flujo gestión de Créditos

Para este smart contract se necesitarán los siguientes métodos:

- Oraculo(): para que el smart contract verifique si el pago ha sido realizado.
- ingresar.creditos: para el caso en el que el usuario este adquiriendo créditos. Este método se encarga de ingresar en la cartera o wallet de nuestro cliente el número de créditos proporcional al precio pagado por ellos.
- premium.user(): para el caso en el que el usuario esta adquiriendo el paquete premium. Este metodo se encarga de otorgar el paquete premium el tiempo proporcional al precio pagado por el mismo.

4.4. Smart contract 4

Este smart contract es el encargado de realizar las transacciones con los créditos, la moneda virtual proporcionada por la aplicación para su uso en la misma y poder optar a descuentos, paquetes premium, etc. Para el correcto funcionamiento de este smart contract necesitaremos los siguientes identificadores:

- Identificador de usuario: datos personales, clave pública y clave privada.
- Identificador de la cartera o wallet: la dirección de la cartera que el usuario maneja con sus claves.
- Dirección de cambio: es la dirección a la cual se envía la diferencia entre los créditos que cueste el producto a comprar y los créditos que haya en la cartera o wallet. Esto es porque siempre que se realice una compra con créditos se paga con la totalidad del dinero que haya en la cartera para así evitar dobles pagos.
- Identificador del producto que se quiere adquirir por parte del usuario.
- Generador de firma digital a partir de la clave privada para dotar a la operación de mayor seguridad, como una criptocalculadora.

Este smart contract es el que se encarga de gestionar las compras mediante los créditos de nuestra aplicación. Funciona de manera parecida a la que trabaja un banco con sus transacciones. El smart contract sigue los siguientes pasos:

- En primer lugar el usuario identifica el paquete que se quiere comprar, ya sea un descuento, un usuario premium o un paquete vacacional.
- En segundo lugar, una vez identificado el paquete a comprar, llega el momento de la compra en el que el usuario canjea los créditos por el producto de tal manera que al hacerlo, envía todos los créditos a la espera de que se le devuelvan los créditos sobrantes.
- Para realizar la compra el usuario deberá firmar la operación. Esto se realizará con el generador de firmas de la aplicación que será como una criptocalculadora en la cual, introduciendo la clave privada se genera un código mediante una función hash. Ese código se introduce como la firma electrónica de la operación. Esta firma será diferente para cada operación y así proteger aún más la clave privada.
- Una vez firmada la operación se produce el envío de los créditos desde la cartera del usuario hacia la del producto y, la diferencia, se devuelve a la dirección de cambio de la cartera del usuario para así evitar el doble pago.

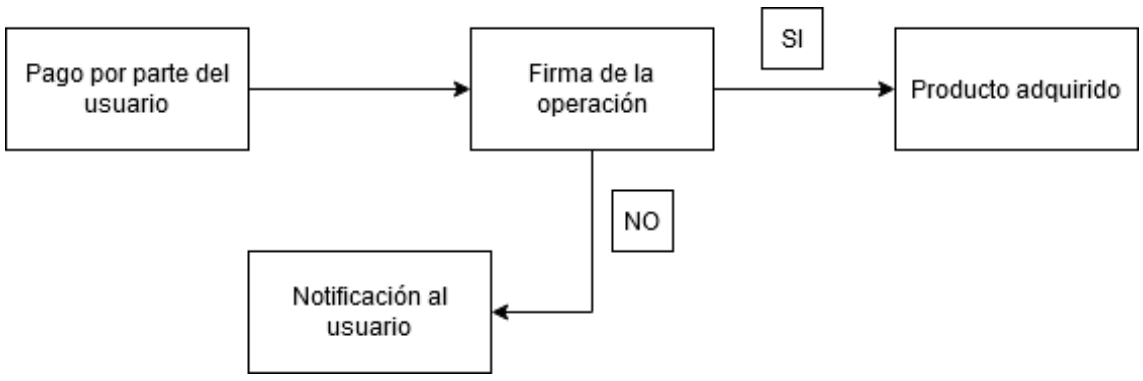

Figura 4: Diagrama de Flujo gestión de uso de tokens

Para este smart contract necesitaremos los siguientes métodos:

- ingreso.creditos(): el cual se encarga de traspasar los créditos desde la cartera del usuario.
- devolucion.creditos(): el cual se encarga de devolver los créditos sobrantes de vuelta a la cartera del usuario mediante la dirección de cambio.

5. Elementos a tener en cuenta en la implementación futura

A la hora de implementar todo las ideas expuestas en esta primera aproximación habría que tener en cuenta varias cosas. En un primer lugar, muy posiblemente se necesiten los dos tipos de blockchain, la privada para todo lo que tenga que ver con transacciones y con métodos de pago y así conseguir dotar de mayor privacidad todo lo que tenga que ver con estas transacciones, y la otra blockchain, una blockchain pública para cosas que no requieran tanta privacidad como el chat de la aplicación.

A la hora de administrar los datos que tuviésemos de los usuarios que se suscriban a nuestra aplicación habría que tener mucho cuidado a la hora de tener en cuenta todo lo respectivo a la privacidad de los mismos, habría que tener cuidado a la hora de cumplir todos los requisitos que la ley de protección de datos establece para poder manejar los mismos y dotarles de la privacidad que se requiera.

Los métodos utilizados están del todo someramente definidos, a la hora de programar lo mas seguro es que se encuentre con numerosos problemas y con posibles acciones que no podemos completar. Habría que valorar también el coste económico de las mismas, ya que una blockchain no siempre es gratuita y si requerimos los servicios de otra empresa que proporcione la blockchain habría que ver la posibilidad de poder pagarlo.

Sería interesante poder dar a elegir a nuestros usuarios una lista de destinos mas amplia, no solo las capitales europeas sino, por ejemplo, aumentarlo a todas las capitales del mundo o todas las ciudades de interés cultural o cualquier otro interés para nuestros usuarios y sugerirles ciudades en función de sus gustos o viajes anteriores. Esto llevaría a tener que realizar un estudio detallado de todas esas ciudades, el clima, el tiempo, sus costumbres, lugares de interés, seguridad de la ciudad, etc.

Habría que tener en cuenta que otras plataformas utilizar a la hora de crear la blockchain. Plataformas como IBM, Amazon, etc, ver las ventajas que ofrece cada una con respecto a la implementación, privacidad y seguridad y el precio por el que ofertan sus servicios.

Decidir con que empresas vamos a querer trabajar, empezar relaciones con ellas y mostrarles nuestros servicios. Proponerles un modelo de negocio en la que ambos salgamos beneficiados. Tendríamos que sentar las bases de los acuerdos para los descuentos con respecto a los paquetes vacacionales para así dar un valor claro y único con respecto a cada descuento a la hora de ofrecerlo al usuario.

La implementación de la moneda virtual y sus posibles requerimientos legales.

La implementación del chat, de los espacios para comentar sobre los paquetes vacacionales y los mensajes privados. Habría que buscar un generador hash para conseguir lo mencionado anteriormente. Un chat común en el que la gente pueda participar en la medida que ellos deseen pero que los mensajes solo sean leídos por los participantes de ese chat común y no por gente ajena a la aplicación. Un chat privado en el que las personas puedan mandarse mensajes privados sin que los lean el resto de usuarios. Y un espacio para comentar los paquetes vacacionales que, del mismo modo que el chat común, pueda ser leído por la gente de la aplicación, y así poder recibir feedback del lugar de destino como de los servicios recibidos, pero sin que sean leídos por gente de fuera de la aplicación

6. Conclusiones

En el presente trabajo hemos presentado una solución basada en los conceptos de Blockchain y Smart Contracts. Se ha visto cómo a través de este tipo de tecnología se pueden gestionar procesos transaccionales con nuestros clientes, ya sean clientes clientes de consumo masivo o empresas. Permitirá automatizar muchos aspectos del proceso de compra de planes vacacionales, solicitudes de crédito en función de la venta de planes, renta de espacios publicitarios y gestión de planes vacacionales lo que puede hacer que el proceso sea más rápido y eficiente. Ayudará a proteger las transacciones y activos de posibles ataques cibernéticos, por lo que se tendrá altos niveles de seguridad en todas las transacciones. La aplicación contará con mayor transparencia con las personas y las empresas al verificar y comprobar las transacciones de manera segura y transparente. Esto ayuda a aumentar la confianza y la credibilidad de nuestro negocio. Al utilizar el blockchain, se logra automatizar y simplificar muchos aspectos del proceso de registro y verificación de transacciones. Esto ayuda a reducir los costos y aumentar la eficiencia del negocio.

En este caso, se han diseñado cuatro Smart Contracts, uno para la compra de paquetes vacacionales, otro para el alquiler de espacios publicitarios de empresas del sector turístico, otro para la obtención de crédito y otra para el gasto. Al usar una blockchain privada con un mecanismo de consenso de prueba de participación permite garantizar la centralidad, reaccionar rápidamente a cambios necesarios, escalabilidad en el consumo masivo y ofrecer altos niveles de privacidad a nuestros clientes y validar transacciones automáticamente.

Los smart contracts permiten automatizar muchos aspectos del proceso de compra y gestión de planes vacacionales, lo que puede hacer que el proceso sea más rápido y eficiente. Al automatizar el proceso de compra y gestión de planes vacacionales, podrá reducir los costos de intermediación y evitar errores costosos. Al automatizar el proceso de compra y gestión de planes vacacionales, podrías proporcionar una experiencia más rápida y sencilla para los usuarios. Esto podría aumentar su satisfacción y fidelización.

Durante el trabajo no solo se han dado algunos detalles técnicos sobre los Smart Contracts como los métodos o atributos que utilizarán, sino que también se ha hablado de los distintos elementos que se deberán tener en cuenta a largo plazo en el sistema, entre los que se destaca la privacidad, que podría ser implementada haciendo uso de criptografía de clave pública. El objetivo de esto es el de asegurar en todo momento la privacidad de los usuarios, protegiendo todos los datos personales almacenados en el sistema.

En el presente proyecto se ha intentado dar cobertura a las necesidades vacacionales de la gente que se suscriba a nuestra aplicación. Para ello se ha empezó el proyecto solo con las capitales europeas pero con vistas a poder ampliarse a todos los destinos que sean considerados de interés. Se podría empezar por los continentes adyacentes debido a su mayor parecido con nuestra cultura y luego ir añadiendo el resto de culturas en función de como vaya creciendo nuestro negocio e ir, no solo ofreciendo mas destinos sino más salidas, es decir, extender la cobertura a otros países y preparar paquetes vacacionales para cada ciudad a la que se extienda y así dar cobertura o tener alcance a un mayor número de personas. Como vemos el proyecto tiene una gran escalabilidad.

Hemos discutido en los usos del blockchain y concluimos que puede ser utilizado para desarrollar sistemas financieros más inclusivos, especialmente en regiones donde el acceso a servicios financieros tradicionales es limitado. Por ejemplo, las criptomonedas basadas en el blockchain pueden proporcionar una forma de realizar transacciones financieras sin depender de un banco o de una red de pagos centralizada.

Tambien hemos concluido que el blockchain puede ser utilizado para mejorar la sostenibilidad y el impacto ambiental de los procesos de producción y consumo. Por ejemplo, se pueden utilizar soluciones basadas en el blockchain para llevar un registro de la procedencia y el impacto ambiental de los productos y para promover prácticas más sostenibles. También, puede ser utilizado para dar a los individuos un mayor control y propiedad sobre sus datos y activos digitales. Esto puede ayudar a promover la autonomía y el empoderamiento de los individuos en un mundo cada vez más digital.

El blockchain puede tener un impacto social significativo al promover la transparencia, la inclusión financiera, el desarrollo sostenible y el empoderamiento de individuos. Sin embargo, es importante tener en cuenta que el impacto social del blockchain dependerá en gran medida de cómo se utilice y de las políticas y regulaciones que lo rodean.

Finalmente, en nombre de todos los miembros del equipo, se concluye que la realización del presente trabajo ha resultado ser una experiencia muy enriquecedora, puesto que se ha podido obtener información sobre una de las últimas tecnologías del mercado como es la tecnología blockchain, entendiendo las diferencias entre cadenas privadas y públicas, así como el funcionamiento de los Smart Contracts, que constituyen una novedosa herramienta para la gestión automática y segura de contratos en diferentes dominios.