UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

MÁSTER EN ETHEREUM, TECNOLOGÍA BLOCKCHAIN Y CRIPTOECONOMÍA

Trabajo Fin de Máster

DISEÑO E IMPLEMENTACIÓN DE UNA DAPP PARA OFRECER SERVICIOS DE RENTING/LEASING PARA EL SECTOR AUTOMOVILÍSTICO

Pedro Cerón
Omar Lozano
Rafael Pérez
2019

UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

DISEÑO E IMPLEMENTACIÓN DE UNA DAPP
PARA OFRECER SERVICIOS DE RENTING/LEASING
PARA EL SECTOR AUTOMOVILÍSTICO

Trabajo Fin de Máster

Autor: Pedro Cerón / Omar Lozano / Rafael Pérez

Director: Alberto Ballesteros Rodríguez

Tribunal:

Presidente: ……..

Vocal 1º: ……..

Vocal 2º: ……..

Calificación: ……..

Fecha: …… de abril de 2019

Palabras de agradecimiento en forma de dedicatoria.

Resumen

Resumen del PFM

Palabras clave

Palabras, clave, separadas, por, comas

Índice

I. Introducción

Aunque quizá no seamos consciente, nos encontramos siendo actores principales de un cambio en el paradigma sobre cómo hacer las cosas, fruto especialmente de dos acontecimientos que cambiaron el mundo:

- Por un lado, la fuerte crisis económica de los años 2.000
- Por otro lado, la revolución tecnológica en la que estamos inmersos.

Como resultado del primer punto, la gente reclama más y más un mundo descentralizado y que nuestro dinero, acciones y riesgo no dependa de personas y entidades que puedan llevarnos a repetir situaciones anteriores como resultado de la mala praxis de estas. Es por ello por lo que se está creando un movimiento de descentralización siendo el sector financiero el mayor afectado por ello.

Por ello, hemos sido testigos de un descenso en demanda de crédito o deuda por parte de los particulares para satisfacer sus necesidades. No obstante, este sigue siendo un mercado con un movimiento muy alto y las entidades financieras están trabajando en la explotación de fórmulas y nuevos productos para, no solo mantener los niveles, si no aumentarlos[1].

Y esto, combinado con este momento tan disruptivo a nivel tecnológico, está naciendo y consolidándose un nuevo modelo de negocio apoyado en las nuevas tecnologías (Blockchain, Cloud, IA, IoT…) y la aparición de nuevos actores que se salen de los patrones clásicos establecidos, ya sean en el negocio bancaria (empresas Fintech), en el sector asegurado (Insurtech), regulatorio (Regurtech), etc.

En este proyecto de fin de máster se presenta una aplicación para la gestión de operaciones de rentings/leasing de automóviles sobre blockchain, sentando además las bases para ampliar sus funcionalidades y operativa.

No obstante, dado las limitaciones presupuestarias y de tiempo, hemos de ceñir el alcance del proyecto a las funciones que hemos considerado básicas, pero a futuro podría consolidar más servicios y opciones.

[1] https://elpais.com/economia/2018/02/01/actualidad/1517515718_449357.html, enero 2019.

II. Parte Teórica

1.1. Blockchain

Blockchain es una las tecnologías que están en el selecto grupo de tecnologías disruptivas sobre las que se tiene puesta las esperanzas para formar parte de la revolución tecnológica en la que nos encontramos.

Concretamente, se definiría como "***una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionadas entre sí matemáticamente***" (Álex Preukschat. Blokchain: La revolución industrial de Internet. Cap1)[2]. Es decir:

- **Distribuida**: como otros servicios p2p existentes e históricos, la base de datos se encuentra compartida entre todos los nodos que conforman la red. De esta manera, se consigue una de sus grandes ventajas como es la tolerancia a los fallos, permitiendo que no sólo haya un punto de control reduciendo el riesgo de ataque y caída de todo el sistema.
- **Protegida Criptográficamente:** toda la información que se almacena está cifrada utilizando técnicas y algoritmos criptográficos, de tal modo que permite asegurar la incorruptibilidad, transparencia, trazabilidad y el fraude en cuanto a la información almacenada.
- **Relacionados entre sí matemáticamente**: el minado de los bloques y por tanto "cierre" de la información almacenada, deriva del uso de algoritmos matemáticos como la "Prueba de Trabajo" (proof of work en inglés).

Blockchain es una de las tecnologías, posiblemente la que mayor impacto y repercusión potencial, innovadoras que han venido para cambiar el mundo y revolucionar todos los sectores económicos y, especialmente, el mundo financiero. ¿Por qué? Pues debido fundamentalmente a una serie de puntos, entre otros:

1. Desintermediación
2. Confiabilidad
3. Seguridad

Desintermediación

Quizá el punto más clave de todos. Como hemos avanzado antes, los acontecimientos sucedidos a nivel mundial durante los últimos años principalmente consecuencia de la brutal crisis económica, los usuarios hemos perdido confianza en los sistemas tradicionales y demandemos una mayor propiedad de nuestra información y, por consiguiente, nuestro dinero.

Además, este sistema tan obsoleto, presenta una serie de retos por resolver:[3]

1. Costes excesivos de las operaciones y transacciones.
2. Tarifas poco ajustadas con las expectativas de clientes y usuarios.
3. Frecuentes retrasos, que restan eficacia a los trámites y encarecen las gestiones.

[2] Álex Preukschat. Blokchain: La revolución industrial de Internet (https://libroblockchain.com/revolucion/)
[3] https://retos-directivos.eae.es/blockchain-y-la-ficcion-de-la-desintermediacion-financiera/

4. Falta de seguridad en un sistema que queda vulnerable al fraude y los ataques.

Para ello, blockchain se presenta como la solución perfecta. Eliminando a los intermediarios actuales, nos permite que seamos nosotros quienes (como pasa en el caso de las redes sociales) tejamos nuestras propias redes o formemos parte de ellas, y seamos nosotros quienes decidamos qué hacer y cómo hacer las cosas.

Este último punto es quizás a día de hoy uno de las mayores barreras que juegan en contra de la evolución, tal y como se comenta en el siguiente artículo: [4] "*El problema al que se enfrenta BitCoin, y otras monedas similares, es el usual en este tipo de cambios de paradigma: la falta de confianza. La gente se siente razonablemente segura con el sistema actual, y los ahorros son algo demasiado serio para hacer apuestas. Una red financiera descentralizada de la que nadie (o todos) se hace responsable transmite la sensación de que o bien no hay ningún tipo de control o , aún peor, de que alguien la controla entre bambalinas sin nuestro conocimiento."* Y es aquí donde enlazamos con el siguiente punto clave:

Confiabilidad

Una de las características claves de Blockchain es que permite la interacción y la generación de transacciones entre pares, sin necesidad de intermediarios y sin necesidad de establecer lazos confiables entre ellos. Es decir, yo puedo hacer cualquier tipo de transacción de cualquier tipo (económica, datos,etc..) sin conocer a la otra persona pero con la seguridad de que "*los datos de las transacciones son imposibles de falsificar una vez registrados"*[5]. Y esto es porque Blockchain aporta además la seguridad necesaria para que no se puedan producir fraudes económicos, aportando la transparencia que se viene demandando en el sector financiero especialmente tras los acontecimientos acaecidos con motivo de la crisis financiera sufrida.

Seguridad

Aunque quizá este punto sea uno de los más pendientes de desarrollar, y por supuesto Blockchain no se libra de los numerosos ataques de robos de criptomonedas, Blockchain ofrece especialmente seguridad desde el punto de vista de fraude económico. Es decir, Blockchain evita lo que comúnmente se puede llamar "Contabilidad B". Es decir, hablamos de seguridad económica. Todas las transacciones quedan registradas de manera inmutables gracias a la aplicación de técnicas criptográfica. Y no sólo para evitar fraude en cuanto a manipulación o malversación de transacciones, sino para prevención de modificación de datos, preservar la privacidad de la identidad digital, …

Por todo esto, además por supuesto de otros puntos claves, el sector financiero al igual que otros sectores tiene que adaptarse a las nuevas posibilidad que ofrece Blockchain. Pero no sólo Blockchain. El sector financiero está experimentando en los últimos años una gran revolución con la aparición de estas nuevas tecnologías y la aparición de nuevas start-ups que está revolucionando un sector que se pensaba que era tan estabilizado en unos principios como hasta ahora. Un ejemplo de algunas de start-ups han son Transferwise, Simple, Atom Bank…

[4] https://elpais.com/tecnologia/2018/02/26/actualidad/1519642606_449102.html
[5] http://www.expansion.com/economia-digital/innovacion/2018/07/11/5b43a10b22601dff438b463c.html

1.2. Ethereum

Desarrollada por Vitalik Buterin como una evolución y mejora de Bitcoin, Ethereum es ***un protocolo, tecnología o plataforma descentralizada y de código abierto que ejecuta programas llamados smart contracts, y que utiliza blockchain para sincronizar y almacenar los cambios de estado del sistema, junto con una criptomoneda llamada ether para medir y restringir los costos de los recursos de ejecución***. (Mastering Ethereum.Andreas Antonopoulos, Gavin Wood Ph.D)[6]

Como se ve en la definición, en esencia no deberá distar mucho respecto al protocolo bitcoin más allá de la posibilidad de programación y uso de smart contracts además de utilizar una criptomoneda propia, pero en detalle se diferencian entre otros en [7] [8]:

- Lo primero es el propio diseño u objetivo de los propios protocolos. Mientras que Bitcoin fue diseñado para convertirse e*n un sistema de contabilidad seguro e inmutable fuera del control del sector financiero, Ethereum está diseñado como una "computadora descentralizada del mundo" donde la funcionalidad Turing-completa permite a los usuarios crear y ejecutar aplicaciones en la red a través de la Máquina Virtual de Ethereum. (EVM).* Es decir, Ethereum está diseñado explícitamente para facilitar los contratos inteligentes completos de Turing y las aplicaciones descentralizadas en su red.
- Bitcoin crea 12.5 bitcoins nuevos cada 10 minutos, habiéndose establecido un límite fijo de 21 millones. Ethereum crea 3 ethers cada 15 segundos, pero sin tope fijo.
- Los bloques son creados, de media, cada 15 segundos mientras que en Bitcoin estos llevan un promedio de 10 minutos. Además, los bloques de Bitcoin tienen un tamaño máximo de 1 MB, pudiendo procesar 4 transacciones por segundo por las 15 de Ethereum.
- El algoritmo de hash de Ethereum es Ethash, mientras que Bitcoin usa el SHA-256.
- En cuanto al proceso de minería, Ethereum aún usa minería similar a Bitcoin en un esquema de PoW, está en proceso de decidir si cambiar por el uso de “Proof of Stake” (PoS).

[6] Mastering Ethereum: Building Smart Contracts and DApps. Andreas Antonopoulos, Gavin Wood Ph.D. https://github.com/ethereumbook/ethereumbook/blob/develop/01what-is.asciidoc

[7] https://medium.com/blockmatics-blog/top-10-differences-between-bitcoin-and-ethereum-d2d3dd62101

[8] https://blockonomi.com/ethereum-vs-bitcoin/

En el siguiente cuadro comparativo se puede ver en detalle las diferencias entre uno y otro protocolo [9]

	BITCOIN	ETHEREUM
NACIMIENTO DE LA PLATAFORMA	18 de agosto de 2008 (registro del dominio 'Bitcoin.org'). 31 de octubre de 2008 fecha de su White Paper.	Diciembre de 2013
FECHA 1ER BLOQUE MINADO	3 de enero de 2009	30 de Julio de 2014
CREADOR DE LA PLATAFORMA	Satoshi Nakamoto, del cual no se sabe quién es o quiénes son (en caso de pseudónimo de una organización)	Vitalik Buterin; Otros co-fundadores incluidos Gavin Wood y Joseph Lubin
FUNCIÓN PRINCIPAL DE LA PLATAFORMA	Sistema de pago descentralizado, rápido y seguro, al igual que su propia moneda.	Plataforma de ejecución de contratos inteligentes y aplicaciones descentralizadas (dApps)
TECNOLOGÍA USADA	Blockchain (Cadena de bloques)	
REDES USADAS	Mainnet (Red principal) y Testnet (Red de prueba)	
ALGORITMO DE SEGURIDAD	SHA2, concretamente SHA256	Ethash, una mezcla de protocolos SHA3
HARDWARE CORRECTO PARA LA MINERÍA	ASIC	GPU y CPU
LENGUAJE DE PROGRAMACIÓN	C++	Turing Complete
SE PUEDEN CONSIDERAR	Criptomonedas descentralizadas	
TIPO DE CRIPTOMONEDA	Moneda virtual	Token o ficha digital
USO CRIPTOMONEDA	Pagos. Competir con las divisas fiat y el oro. También como inversión	Operar dentro de la red Ethereum: crear aplicaciones descentralizadas y ejecutar contratos inteligentes. También como inversión
CRIPTOMONEDA	Bitcoin (BTC)	Ether (ETH)
DECIMALES	8	18
CANTIDAD MÁXIMA A EMITIR DE CRIPTOMONEDA	21 millones de bitcoin en total, por lo tanto, deflacionaria	18 millones por año, por lo tanto, inflacionaria
CREACIÓN DE CRIPTOMONEDAS A TRAVÉS DE	Minería	
SISTEMA DE MINERÍA	Proof of Work (PoW) o Prueba de Trabajo	
CANTIDAD DE RECOMPENSA DE LA MINERÍA	Actualmente 12,5 bitcoin por bloque. Cada 210.000 bloque decrece a la mitad	3 Ether por bloque desde la introducción de la etapa Metrópolis. Anteriormente fue de 5 Ether por bloque
MÉTODO DE RECOMPENSA DE LOS MINEROS	Por validación de bloques	Por validación de bloques, de transacciones y por ejecución de contratos inteligentes
PROCESAMIENTO DE LOS BLOQUES	Cada 10 minutos (600 segundos)	Cada 16 segundos
TAMAÑO DE LOS BLOQUES	1 Mb como máximo	Sin definir, pero muy por debajo de 1 Mb
RECÁLCULO DE LA DIFICULTAD DE MINADO	Cada 2016 bloques minados	Cada bloque minado
COSTE TRANSACCION	Todas por igual	Depende del Gas

[9] https://miethereum.com/ether/bitcoin-vs-ethereum/

1.3. Smart Contract

Los smart contract, como hemos comentado anteriormente, son el principal punto de atracción de Ethereum, y la posibilidad que abrió a su programación.

Un smart contract no es otra cosa que la redacción de un contrato “normal” físico bajo lenguaje y código de programación, de tal manera que trabaje de manera independiente y por tanto se ejecute cuando se cumplan las condiciones establecidas y pactadas en el código.

Es decir, a través del uso de smart contract se eliminan intermediarios, quedando como agentes del contrato los propios intervinientes e interesados.

Las principales características de los smart contracts serían:

- Precisión
- Rendición de cuentas (las partes implicadas saben en todo momento en que estado se encuentra el contrato)
- Velocidad
- Seguridad
- Consistencia

No obstante, también presenta una serie de limitaciones, entre las que destacan:

- **Errores de código**. Es decir, al ser programados los smart contracts, se incluyan errores accidentales que puedan alterar el funcionamiento y el resultado del contrato.
- **Lógica incorrecta**. Deliberadamente o sin querer, pero muy análogo al anterior no existe una comprobación de que el programador pueda manipular intencionadamente el contrato. Por ejemplo, que en caso que se cumpla una condición para hacer una transferencia, esta se dirija al wallet del programador en vez de a la del beneficiario.
- **Regulación e impuestos.** Esto es prácticamente para todas las plataformas blockachain, y casi todas las tecnologías innovadoras. En el caso anterior, ¿Cómo se puede reclamar el fraude? ¿Quién lo regula y sanciona? Y en el caso de las transferencias, ¿qué impuestos habría que pagar por una transacción económica, como por ejemplo el traspaso de un activo?

1.4. Renting/Leasing

Un producto de renting o leasing son productos de financiación especializada que nacieron como apoyo a las empresas para financiar las adquisiciones y uso de bienes, especialmente en cuanto a maquinaria, vehículos, inmobiliarios, etc…

Básicamente, son contratos de arrendamiento de bienes a largo plazo entre dos partes y en las que se pacta, entre otros, el pago de cuota periódica (mensual por lo general), el pago o no de una cuota inicial y el pago de una cuota final al final del contrato.

¿Qué diferencias hay? Por un lado, la principal es que uno se trata de un arrendamiento operativo (renting) mientras que el otro es un arrendamiento financiero (leasing). Esto en la práctica [10], consiste en que para las operaciones de renting, la formalización contractual se basa en un consentimiento entre ambas partes siendo la empresa de renting la propietaria del producto arrendado.

Por su parte, un leasing al tratarse de un arrendamiento financiero regulado por ley, se formaliza a través de una entidad de crédito. transfiriendo los riesgos y beneficios derivados de la propiedad. Además, es obligatorio la inclusión de un derecho de compra, siendo opcional en los contratos de renting.

Otra diferencia clave, es que mientras que los contratos y servicios de leasing están disponibles únicamente para empresas, las operaciones de renting también se encuentran disponibles y son operativas para particulares.

[10] https://www.leaseplango.es/blog/renting/renting-leasing-diferencias/

1.5. Blockchain y Renting/Leasing

Blockchain es una tecnología con un previsible gran crecimiento dentro de los sectores logístico, financiero y de seguros [11] [12]. Las ventajas fundamentales que puede ofrecer a un servicio de renting/leasing de coches (en donde se pueden integrar los 3 sectores) se pueden resumir en las siguientes[13]:

- **Trazabilidad de todo el proceso:** Tanto las terceras partes (compañías de financiación, aseguradora, recambios etc) como el cliente final pueden comprobar en tiempo real los cambios de estado del bien.
- **Confianza:** Como consecuencia del punto anterior y debido a la inmutabilidad de la cadena de bloques, las partes interesadas pueden tener la certeza de que el proceso se ejecuta de forma correcta y legal. Uno de los beneficios fundamentales que puede aportar este aspecto es la fidelización del cliente final (si además el servicio prestado es bueno).
- **Precios justos:** El cliente final sabe el precio exacto de los bienes por los que está consumiendo un servicio (por ejemplo: al poder tener acceso a la información de la cadena de bloques, puede saber a qué precio el taller adquirió los repuestos y qué beneficio obtiene éste por su servicio).
- **Interconectividad:** Mediante la utilización de dispositivos IoT que envíen datos de geolocalización y del movimiento de los vehículos a la Blockchain, se puede crear un sistema de seguro que repercute únicamente en el cliente final en función de la utilización del vehículo y del tipo de vía por la que transita.

Por otra parte, en el mercado existen aplicaciones basadas en tecnología Blockchain que intentan dar solución a la problemática de la creación de una Dapp que dé soporte a los servicios de leasing en el entorno automovilístico. Cabe destacar entre ellas, la desarrollada por IBM en julio del 2016 [14]. Dicha aplicación hace uso de una plataforma Blockchain integrada en un entorno cloud. A diferencia de otras plataformas, en **IBM Blockchain Platform** [15]:

1. Estamos ante una red permisionada.
2. No requiere el uso de criptodivisas.
3. Las transacciones son confidenciales y visibles a partes seleccionadas.

[11] How Blockchain may impact logistics, supply chain and transportation: A conversation with the blockchain in the transport area. https://www.forbes.com/sites/insights-penske/2018/09/04/how-blockchain-may-impact-logistics-supply-chain-and-transportation-a-conversation-with-the-blockchain-in-transport-alliance/#2a8e2f95f2b3, enero del 2019.

[12] Blockchain in insurance: Application and pursuing a path to adoption: https://www.ey.com/Publication/vwLUAssets/EY-blockhain-in-insurance/$FILE/EY-blockhain-in-insurance.pdf, enero del 2019.

[13] https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-the-supply-chain-three/$FILE/ey-blockchain-and-the-supply-chain-three.pdf, enero del 2019

[14] IBM Blockchain car lease demo: https://developer.ibm.com/tv/ibm-blockchain-car-lease-demo/, enero del 2019.

[15] IBM Blockchain Platform: https://www.ibm.com/es-es/marketplace/cloud-based-blockchain-platform/details, enero 2019.

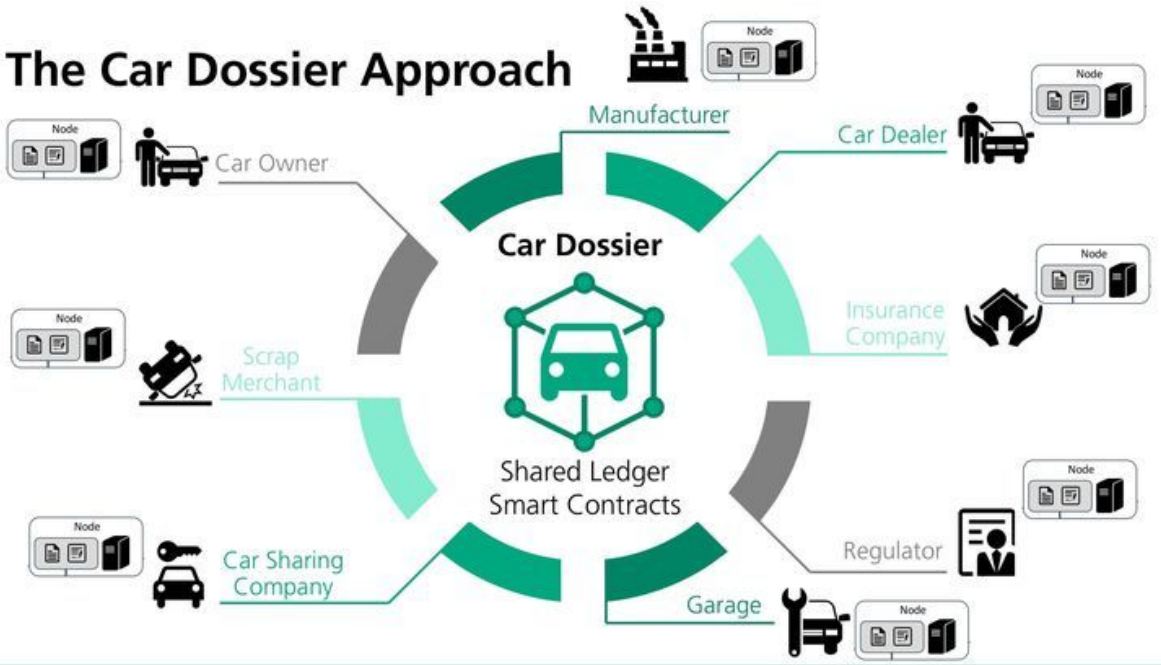


Imagen: Modelo Relación Actores Ciclo Vida Renting Coche.
Fuente: https://d5cplpsrt2s33.cloudfront.net/m/7a688abb11b5a7de/ASPECT_768-blog_comms_car_dossier_web.jpg

III. Objetivos y requisitos funcionales

De cara al desarrollo de esta plataforma, y en base a los plazos de ejecución, planteamos un desarrollo faseado, siendo el objetivo principal de esta primera fase correspondiente al TFM la elaboración de una Dapp que permita gestionar a través de smart contracts los contratos que se firman entre cliente, entidad financiera y entidad aseguradora. Esto incluiría no sólo la programación de estos, si no el desarrollo del front de acceso y gestión.

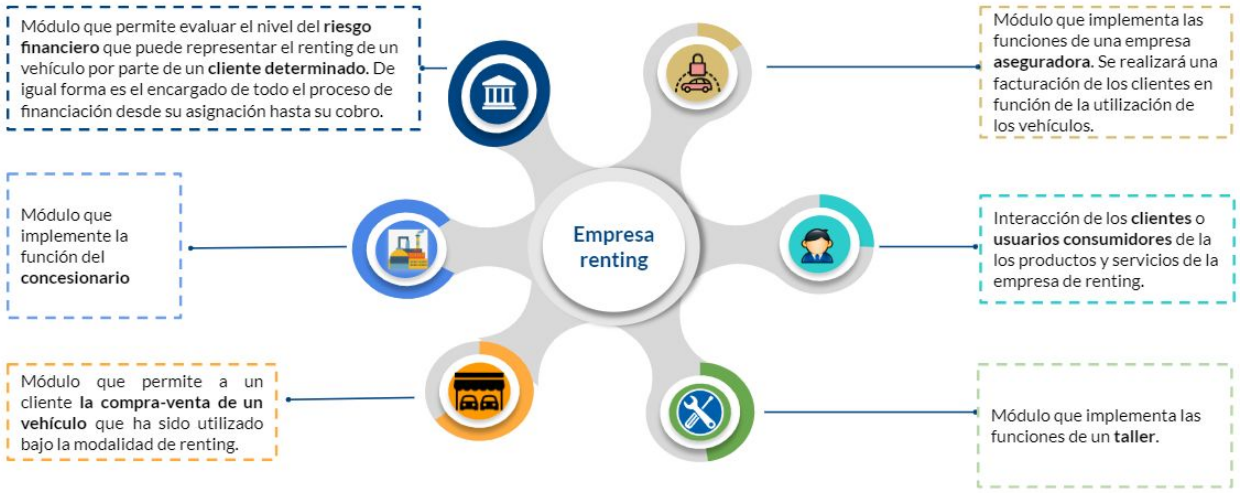
Es decir, en esta primera fase planteamos los siguientes objetivos de desarrollo:

- **Creación de una Dapp** que permita interconectar a todos los distintos usuarios y agentes que participan en la gestión del ciclo de vida de una operación de renting de automóviles. En esta primera fase, el objetivo es la construcción de los elementos considerados básicos (y ampliable en futuras fases con el desarrollos de nuevos módulos, de cara a futuro de poder integrar todo el proceso en una misma plataforma) y que incluye especialmente la posibilidad de firma y automatización de la ejecución de la ejecución de los contratos entre usuarios. La Dapp cumplirá con los siguientes requisitos:
    - **Funcionará en servidor local.**
    - **Acceso a la aplicación a través de la URL** correspondiente.
    - **Las transacciones se firmarán con Metamask**.
    - **Se utilizarán eventos** para guiar al usuario final.
    - Se realizará la **implementación de librerías** que se ajusten a las necesidades del desarrollo.
    - Se implementarán **medidas de seguridad**. (Ej. emergency stop).
- **Creación de fronts para acceso y gestión (**amigables para el usuario final).
- **Desarrollo de smart contracts** con las siguientes relaciones:
    - Smart contract entre usuario y empresa de renting
    - Smart contract entre empresa de renting y entidad financiera
    - Smart contract entre usuario y entidad aseguradora
    - Los Smart Contracts serán sometidos a tests.

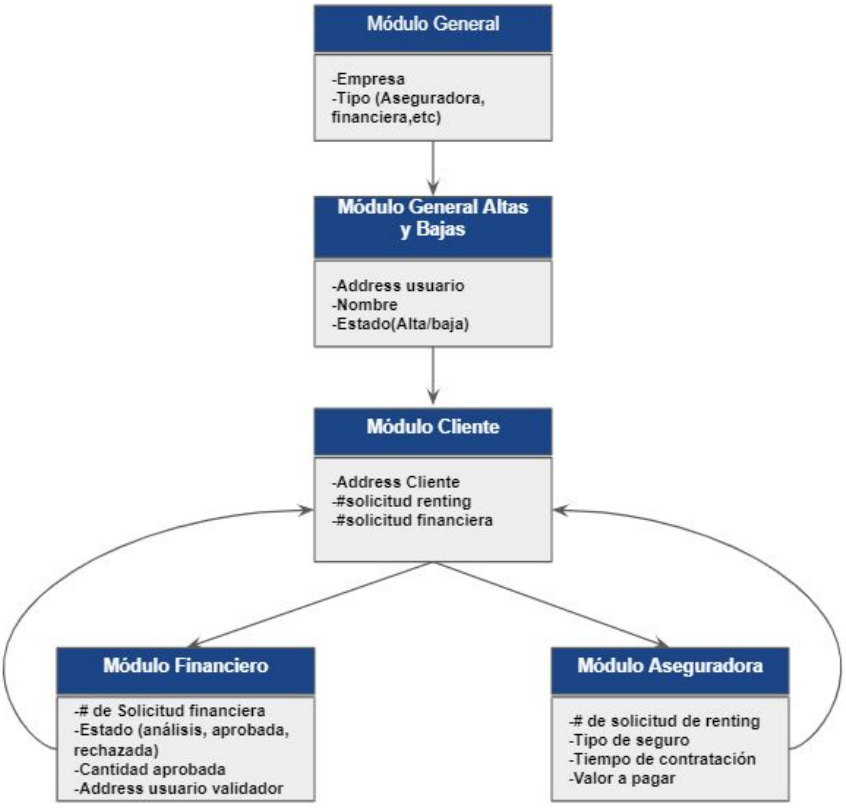
El desarrollo y consecución de los objetivos marcados, permitirá aportar el siguiente valor añadido:

- Creación de una DAPP novedosa (y con pocos ejemplos de implementación en el mercado actual).
- Análisis de la viabilidad de negocio de la solución.
- Implementación de medidas de seguridad (en el código) contra:
    - Race Conditions
    - Orden de las transacciones
    - Overflow’s
    - DoS
    - Forcibly sending
- Creación de un modelo de básico de riesgo del usuario.

1.1. Primera aproximación de la solución tentativa



Aproximación inicial: Modelo Inicial Entidad Relación



Aproximación inicial: Smart Contracts


Empresas
function altaEmpresa
function actualizarEmpresa
function altaUsuario
function actualizarUsuario
Empresa Financiera
function pagoMensual
function pagoFinal
function estadoFinanciación
Cliente
function altaCliente
function actualizarCliente
function altaFinanciacion
function actualizar financiación
function altaSeguro
function actualizarSeguro
function altarRecord
function actualizarRecord
Empresa Aseguradora
function pagoFinal
function límiteSeguro
function estadoSeguro

1.2. Módulos incluidos en el alcance del proyecto

Módulo General:

- Este módulo permitirá a los administradores de la Dapp realizar el alta de usuarios, de las empresas de seguros y empresas financieras.
- Es decir, es el módulo de administración donde los usuarios administradores podrán realizar todas las tareas de administración. En esta, primera fase:
    - Para cada uno de lo módulos, se implementará la gestión de perfiles. Esto permitirá garantizar que sólo aquellos usuarios pertenecientes a la empresa, puedan validar las operaciones de su respectiva empresa y no de cualquiera de las demás que participan en el flujo del proceso. Para cumplir con este objetivo se realizará una asignación de privilegios vinculado con el address de cada uno de usuarios.
    - Además, desde el módulo de administración, los usuarios con permisos de administración de la aplicación pueden realizar tareas de mantenimiento de contratos, vehículos, empresas, etc...

Módulo Financiero:

- Para permitir a los usuarios y empresas financieras desarrollar sus funciones dentro del flujo de renting, se desarrollará una pantalla o frontal, la cual permitirá registrar las solicitudes de financiación de los clientes. De esta forma de acuerdo con la información suministrada por el cliente y su histórico, se podrá proceder con el respectivo análisis de riesgo (mediante un modelo básico que tenga en cuenta el histórico del cliente, la información que se suministre por parte del cliente por pantalla, dando como resultado el scoring asociado a ese cliente) que devolverá el número máximo de tokens a solicitar prestados por parte del cliente. Una vez se ha definido el análisis de riesgo se realizará a través del mismo frontal la validación/aprobación de las solicitudes.

Módulo Cliente:

- Este módulo es de vital importancia para el funcionamiento del flujo del sistema. Para tener un control de los usuarios y un registro de sus acciones, se desarrollará una pantalla o frontal para realizar el alta del cliente.
- De igual forma una vez el cliente ya se ha registrado, se permitirá al mismo acceder al portafolio de productos de renting, así como la posibilidad de utilizar financiación y seleccionar el tipo de seguros que más le convenga. Para ello se desarrollará un frontal en el que se reúnan dichos productos y que permita al cliente realizar la solicitud de un coche, seleccionar el tipo de seguro y las condiciones del renting (se validará a través de smart contracts, que el usuario se encuentre registrado, cuente con un saldo suficiente y no tenga un histórico negativo).

IV. Parte Técnica

Repositorio Aplicación

En el siguiente enlace se encuentra el código fuente de la aplicación:

https://github.com/DappLeasingRenting/DappLeasingRenting.git

En el siguiente capítulo se procede a describir todos los aspectos técnicos del desarrollo de la aplicación:

V. Modelo Económico

Para el desarrollo y ejecución del siguiente proyecto, hemos considerado el siguiente escenario económico para poder llevarlo a cabo. Al igual que el alcance del propio proyecto, hemos considerado un modelo económico faseado. Es por ello:

1.3. Modelo Económico Fase I

Este modelo incluye las funcionalidades incluidas en la fase I y detallado en el apartado *"Módulos incluidos en el alcance del proyecto"* del presente documento:

Presupuesto de la fase de desarrollo

Esta fase contempla el desarrollo y construcción de la plataforma incluyendo la programación y codificación del programa. Para ello, se estima un equipo 2,5 FTEs y un plazo de estimado de un mes y medio para llevar a cabo todas las tareas de esta fase del proyecto, detallado de la siguiente manera[16]:

Recurso	Funciones	Horas estimadas	Coste hora	Importe total
Consultor Junior	• Programación • Análisis y resolución incidencia • Ejecución pruebas técnicas	210	54	11.340 €
Consultor Senior	• Programación • Definición plan de pruebas funcionales y técnicas • Ejecución pruebas técnicas • Análisis y resolución incidencia	210	81	17.010 €
Jefe Proyecto	• Gestión del proyecto • Ejecución pruebas funcionales	105	100	10.500 €
				38.850 € [17]

A estos costes de desarrollos, habría que añadir los **costes de implantación y uso**, los cuales son variables al depender del precio dinámico del coste del gas en Ethereum (la cual depende del uso de la red) y del valor de mercado de la criptomoneda Ether, la cual a modo ejemplo, durante el mes de Marzo de 2019 ha variado entre los 125 y 145 USD como se aprecia en el siguiente gráfico: [18]

[16] Costes estimados en base a propuestas de servicios ofertados con costes típicos de una consultora de servicios tecnológicos

[17] Coste IVA (21%) no incluido

[18] https://coinmarketcap.com/currencies/ethereum/

Pero al ser tan volátil como el resto de las criptomonedas, esta moneda también se ha visto expuesta a grandes picos y valles de valoración. Si vemos la evolución de la criptomoneda [19]:

Ethereum Statistics

Ethereum Price	€126,51 EUR
Ethereum ROI	4.918,07%
Market Rank	#2
Market Cap	€13.342.303.249 EUR
24 Hour Volume	€3.855.536.685 EUR
Circulating Supply	105.462.576 ETH
Total Supply	105.462.576 ETH
Max Supply	No Data
All Time High	€1.275,76 EUR
All Time Low	€0,374746 EUR

[19] https://coinmarketcap.com/currencies/ethereum/. Información obtenida a 31/03/2019

Por ello, vamos a plantear los costes en base a 3 escenarios de la criptomoneda:

- Escenario mínimo: precio actual de 126 euros/ether
- Escenario máximo: precio máximo obtenido por el Ehter, correspondiente a 1.275 euros/ether
- Escenario medio: precio medio, obtenido del promedio de los precios anteriormente citados. Es decir, 700 euros/ether.

Presupuesto de la fase de implantación y uso

De cara a estimar el presupuesto de estas fases, vamos a tener en cuenta las siguientes condiciones:

- Se realizará un traspaso de contratos actuales a smart contracts. Es decir, los contratos actuales físicos se mantiene hasta su fin de vida. No obstante, todas las nuevas operaciones ya se realizarán a través de la DAPP.
- Se creará una empresa, que será la empresa de renting y contará con un usuario administrador.
- La empresa de renting trabaja con una empresa asegurador única y una entidad financiera única
- Se estima una creación de 10 usuarios en la empresa de renting, y 5 usuarios para la entidad financiera y la entidad aseguradora.
- Estimamos una operativa de 100 smart contracts durante un año. Aunque si bien es cierto que un mismo usuario podría tener más de un contrato, vamos a estimar que un usuario por cada smart contract. Es decir, 100 usuarios.

Escenario	Coste Eth
Mínimos	126 €
Promedio	700 €
Máximos	1.275 €

PRESUPUESTO IMPLANTACIÓN				
TAREA	***COSTE UNITARIO***	***ESCENARIO MÍNIMO***	***ESCENARIO PROMEDIO***	***ESCENARIO MÁXIMO***
Desplegar contratos actuales en smart contract	0,16	20 €	112 €	204 €
Creación usuarios empresa renting (10)	0,01	13 €	70 €	128 €
Creación usuarios entidad financiera y aseguradora (10)	0,01	13 €	70 €	128 €

PRESUPUESTO USO ANUAL				
Creación usuarios (100)	0,005	63 €	350 €	638 €
Creación Smart Contracts (100)	0,48	6.048 €	33.600 €	61.200 €
Ejecución pago cuota mensual (12 cuotas anuales por 100 contratos)	0,001	151 €	840 €	1.530 €
TOTAL USO ANUAL		**6.262 €**	**34.790 €**	**63.368 €**

TOTAL DESARROLLO + IMPLANTACIÓN +USO ANUAL	**45.125 €**	**73.710 €**	**102.345 €**

VI. Conclusiones

Blockchain y resto de tecnologías disruptivas más actuales, están permitiendo transformar el mundo tal y como lo conocemos, haciendo que los distintos sectores, especialmente el financiero, están obligados a adaptarse y modificar sus procesos y operativas, así como modelos de negocio. Y esto es especialmente porque el usuario lo demanda. Ya no somos el usuario que para cualquier acción acudimos a la sucursal bancaria de confianza, por poner un ejemplo. Ahora queremos que sea omnicanal y en cualquier sitio por alejado que sea, que sea seguro, que sea confiable, que seamos nosotros los dueños y controlemos nuestro dinero y servicios...

Tampoco queremos movernos en base a las directrices marcadas por un tercero al que no conocemos, queremos ser parte de esos cambios.

VII. Trabajos futuros

Los módulos descritos a continuación, serían tenidos en cuenta para futuras fases del proyecto, considerando su importancia en el flujo de información y en el servicio de renting.

Módulo Aseguradora:

A futuro, en un escenario completo, el objetivo sería poder recabar información real (a partir de dispositivos IoT independientes) y que estos datos fueran leídos por el oráculo.

- Un modo de aseguramiento para el usuario, una solución Insutech llamada “Insurance as Service”, consistente en un modelo de renting donde se incluye un tipo de seguro que se adapte al uso de los vehículos por parte de los asegurados. en el cual el asegurado recibe coberturas y paga en consonancia al uso que le da al vehículo adquirido. De manera más detallada, a futuro se plantea conectar la información de una base de datos externa con el smart contract (el oráculo leería de esa base de datos), de cara a simular la utilización de los datos provenientes de un dispositivo IoT (kilómetros recorridos, velocidad, carreteras transitadas, tiempo de estacionamiento, etc..).
- Para cumplir con este objetivo, se utilizarían datos de la trazabilidad de vehículos, con el objetivo de simular un sistema de cobro más preciso (de acuerdo al desplazamiento y el modo de conducción del usuario).
- Se diferenciará dos tipos de información: dinámica (o información ficticia que simula el comportamiento en tiempo real de los vehículos) e información estática.
    - Del primer caso tendríamos: los kilómetros recorridos, la velocidad máxima, media, las carreteras transitadas, horas de conducción, tiempo de conducción seguida, etc
    - Respecto a información estática: se puede plantear la clasificación de riesgo de las carreteras, índice de accidentes por personas, sexo y edad, índice de siniestralidad en función de marca y tipo de automóvil…
- En base a toda la información, sería necesario así mismo definir las reglas de coberturas contratables. Es decir, en base a una serie de parámetros establecidos a partir de la información y datos que se disponen, ofrecer unas coberturas u otras, y adaptar el pago de los asegurados.
    - Por ejemplo: un conductor que conduce 10.000 kms al año, por autovías y siempre respetando los límites de velocidad, no debería pagar lo mismo que otro conductor que recorre más kilómetros, o que circula por carreteras convencionales o conduce de manera inapropiada.

Módulo taller

- El módulo de taller permitirá a empresas proveedoras de servicio de reparación, participar en los procesos de mantenimiento de los vehículos que han sufrido algún desperfecto o accidente. De esta forma se podrá registrar cualquier modificación o reparación en el coche. Para garantizar este proceso, se realizará, el desarrollo de un frontal, para la gestión del servicio de taller (para la reparación de los vehículos). En definitiva, se trata de simular el libro de mantenimiento de cualquier coche que se realiza a día de hoy de manera manual y en formato papel por lo general, asegurando la transparencia y la inmutabilidad de la información.
- La información del coste de los recambios quedará registrada y será transparente para el usuario final (de tal forma que el cliente pueda ver el coste del servicio aplicado por el taller).
- Adicionalmente, quedaría registrado componentes utilizados por cada vehículo permitiendo no poder alterar la información registrada y de este modo minimizar y asegurar la lucha contra el riesgo de fraude.

Módulo Compraventa

- Este módulo permitirá a la empresa de renting trabajar asociado a concesionarios dedicados a la compra/venta de vehículos. Así se pueden vender aquellos vehículos que los usuarios no deseen adquirir directamente.
- Se plantearía la posibilidad de registrar toda la información del ciclo de vida del vehículo, en combinación con el resto de módulos especialmente taller y proveedor, para asegurar que la información de cada vehículo sea 100% veraz y prevenir posibles fraudes.

Módulo Proveedor

- El módulo de proveedor gestionará las flotas de vehículos ofrecidas a la empresa de renting, registrando todo el proceso de fabricación del automóvil, desde la petición del mismo hasta su envío, y garantizando la transparencia de cara al usuario final, muy similar en su concepto a otras soluciones blockchain que se están realizando para asegurar todo el ciclo de vida de los procesos de supply chain de mercancías.

VIII. Bibliografía

Anexos

1. Manual de usuario