

|  |
| --- |
| **Universidad Internacional de La Rioja (UNIR)**  **Escuela Superior de Ingeniería y Tecnología**  **Grado en Ingeniería Informática** |
|  |
| PetChain: Dapp de gestión de mascotas |

**Ubicación del código fuente:**<https://github.com/cescari/tfg_project>

**Trabajo Fin de Grado**

**Presentado por:** Escario Bajo, Carlos

**Director/a:** Martinez Muñoz, Miriam.

Ciudad: San Lorenzo de El Escorial (Madrid)

Fecha: 05/06/2019

Resumen

El presente trabajo es una muestra de cómo es posible la realización de proyectos de gestión con Smartcontracts dentro de un ámbito corporativo o administrativo. La aplicación, bautizada como **PetChain**, pretende mostrar cómo es posible salvar la falta de comunicación existente en la actualidad, debido a la ausencia de interconexión entre los sistemas informáticos dentro del sector veterinario nacional, aprovechando las capacidades de confiabilidad e inmutabilidad que ofrece una red Blockchain y el sistema de ficheros IPFS.

PetChain es una aplicación “web clásica”, que permite la gestión de identidades de mascotas domésticas. Desarrollada como una Blockchain bajo una red *Ethereum*, funcionando en un entorno local en un servidor *Ganache* y con un frontal HTML, permite la gestión y administración de la información relacionada con las mascotas, los datos de sus dueños así como la distribución de los mismos, entre los profesionales veterinarios.

**Palabras clave**: Blockchain, web, Ethereum, Ganaché, Truffle, token, nodo, IPFS



Ilustración 1: PetChain logo

Summary

The current project is an example of how it is possible to carry out management projects with Smartcontracts within a corporate or administrative environment. The application, called **PetChain**, is inteded to show how it is possible to overcome the today’s lack of communication, due to the absence of interconnection among systems within the national veterinary sector, taking advantage of the capabilities of reliability and immutability offered by a Blockchain network and the IPFS file system.

PetChain is a "classic web" project, which allows the management of domestic pet identities. Developed as a Blockchain under an Ethereum network, working in a local environment on a *Ganache* server and with an HTML front end, it allows the management and administration of information regarding to pets, their owners' data as well as their distribution among veterinary professionals.

**Keywords**: Blockchain, web, Ethereum, Ganaché, Truffle, token, node, IPFS.

**Indice**

[Resumen 1](#_Toc10154852)

[Summary 1](#_Toc10154853)

[Índice de ilustraciones 4](#_Toc10154854)

[Índice de Tablas 5](#_Toc10154855)

[1. Introducción 6](#_Toc10154856)

[1.1. Presentación del problema 6](#_Toc10154857)

[1.2. La solución. 7](#_Toc10154858)

[1.1.1. API de servicios web. 8](#_Toc10154859)

[1.1.2. Blockchain 9](#_Toc10154860)

[2. Estado del arte. 10](#_Toc10154861)

[2.1. La Blockchain 10](#_Toc10154863)

[2.1.1. Características 10](#_Toc10154867)

[2.1.2. ¿Qué es un bloque? 10](#_Toc10154868)

[2.1.3. ¿Dónde están los bloques? 12](#_Toc10154869)

[2.1.4. Criptografía de clave pública 12](#_Toc10154870)

[3.1. IPFS 13](#_Toc10154871)

[3. PetChain. Descripción del proyecto 13](#_Toc10154872)

[4. Petchain. Especificación de requisitos. 14](#_Toc10154873)

[5.1. Propósito del documento 14](#_Toc10154876)

[5.2. Alcance del documento 14](#_Toc10154877)

[5.3. Participantes en el proyecto 15](#_Toc10154878)

[5.3.1. Presentación de participantes 15](#_Toc10154885)

[5.4. Organizaciones involucradas 16](#_Toc10154886)

[5.5. Descripción del sistema 16](#_Toc10154887)

[5.5.1. Perspectiva del producto 16](#_Toc10154890)

[5.5.2. Funciones del producto 16](#_Toc10154891)

[5.5.3. Características del usuario 17](#_Toc10154892)

[5.5.4. Restricciones 17](#_Toc10154893)

[5.6. Descripción técnica del sistema 17](#_Toc10154894)

[5.6.1. Front-End 17](#_Toc10154896)

[5.6.2. Seguridad 18](#_Toc10154897)

[5.6.3. Back-End 18](#_Toc10154898)

[5.6.4. Entorno de ejecución 18](#_Toc10154899)

[5.7. Objetivos del sistema 19](#_Toc10154900)

[5.8. Catálogo de requisitos del sistema. 23](#_Toc10154901)

[5.8.1. Requisitos de información 23](#_Toc10154904)

[5.8.2. Requisitos funcionales 26](#_Toc10154905)

[5.8.3. Requisitos no funcionales 29](#_Toc10154906)

[5.9. Matriz de rastreabilidad 32](#_Toc10154907)

[5.9.1. Matriz de rastreabilidad: Objetivos del sist. – Requisitos funcionales 32](#_Toc10154909)

[5.9.2. Matriz de rastreabilidad: Objetivos del sist. – Requisitos no funcionales 32](#_Toc10154910)

[5.10. Casos de uso 33](#_Toc10154911)

[5. PetChain. Descripción técnica 34](#_Toc10154912)

[6.1. NodeJS 35](#_Toc10154914)

[6.1.1. ExpressJS 35](#_Toc10154917)

[6.1.2. body-parser 35](#_Toc10154918)

[6.1.3. jsonwebtoken 36](#_Toc10154919)

[6.1.4. Generación del proyecto 36](#_Toc10154920)

[6.2. Truffle 37](#_Toc10154921)

[6.2.1. Instalación de Truffle 37](#_Toc10154924)

[6.2.2. Generación del proyecto 38](#_Toc10154925)

[6.3. Ganache 38](#_Toc10154926)

[6.3.1. Instalación de Ganache 39](#_Toc10154928)

[6.4. Web3.js 39](#_Toc10154929)

[6.4.1. Instalación de Web3.js 39](#_Toc10154931)

[6. Evaluación 40](#_Toc10154932)

[7. ¿Qué queda por hacer? Trabajo futuro. 40](#_Toc10154933)

[8. Bibliografía 40](#_Toc10154934)

[9. Glosario de términos 40](#_Toc10154935)

Índice de ilustraciones

[Ilustración 1: PetChain logo 1](#_Toc10148810)

[Ilustración 2: Representación de la cadena de bloques. 11](file:///C:\Users\Carolina\Google%20Drive\UNIR\GRADO%20INGENIERIA%20INFORMATICA\TFG\docs\TFG_Carlos_Escario_Bajo.docx#_Toc10148811)

[Ilustración 3: Ejemplo de bloque genesis.json 12](file:///C:\Users\Carolina\Google%20Drive\UNIR\GRADO%20INGENIERIA%20INFORMATICA\TFG\docs\TFG_Carlos_Escario_Bajo.docx#_Toc10148812)

[Ilustración 4: Bloque Genesis 12](file:///C:\Users\Carolina\Google%20Drive\UNIR\GRADO%20INGENIERIA%20INFORMATICA\TFG\docs\TFG_Carlos_Escario_Bajo.docx#_Toc10148813)

[Ilustración 5: Arquitectura de frameworks y herramientas utilizadas. 34](file:///C:\Users\Carolina\Google%20Drive\UNIR\GRADO%20INGENIERIA%20INFORMATICA\TFG\docs\TFG_Carlos_Escario_Bajo.docx#_Toc10148814)

[Ilustración 6: Comando instalación de ExpressJS 35](#_Toc10148815)

[Ilustración 7: Comando de instalación de body-parser 36](#_Toc10148816)

[Ilustración 8: Comando de instalación de jsonwebtoken 36](#_Toc10148817)

[Ilustración 9: Comandos de creación directorio del proyecto 36](#_Toc10148818)

[Ilustración 10: Inicialización del proyecto NodeJS 36](#_Toc10148819)

[Ilustración 11: Estructura del fichero package.json 37](#_Toc10148820)

[Ilustración 12: : Comando de instalación de Truffle 37](#_Toc10148821)

[Ilustración 13: Comando de inicialización de un proyecto Truffle 38](#_Toc10148822)

[Ilustración 14: Web de Truffle framework. 39](file:///C:\Users\Carolina\Google%20Drive\UNIR\GRADO%20INGENIERIA%20INFORMATICA\TFG\docs\TFG_Carlos_Escario_Bajo.docx#_Toc10148823)

[Ilustración 15: Comando de instalación de web3.js 39](#_Toc10148824)

Índice de Tablas

[Tabla 1: Dirección del proyecto 15](#_Toc10148835)

[Tabla 2: Analista y desarrollador del proyecto. 15](#_Toc10148836)

[Tabla 3: Colaborador del proyecto 15](#_Toc10148837)

[Tabla 4: Dirección facultativa y Veterinaria 15](#_Toc10148838)

[Tabla 5: Objetivos 001 19](#_Toc10148839)

[Tabla 6: Objetivos 002 19](#_Toc10148840)

# Introducción

¿Por qué Blockchain? ¿Si ya tiene más de 20 años, qué trae nuevo? ¿Por qué he de fiarme de algo que se califica a sí mismo como inmutable? ¿Pero es seguro? En la era de las APIs, ¿por qué debo de fiarme de un SmartContract? Pero y eso de un SmartContract, ¿qué es? ¿Necesito cambiar las competencias del equipo de desarrollo? Y además, ¿debo invertir en criptomonedas para poder hacer mi aplicación empresarial? Etc…

Estas cuestiones y otras muchas, son las que cualquier analista, jefe de proyecto, responsable de TI o incluso de negocio que se enfrenta a un nuevo desarrollo, podría llegar a hacerse si le planteasen la necesidad de diseñar e implementar un proyecto en una blockchain corporativa.

Se quiere ofrecer la visión de cómo es posible desarrollar una aplicación de gestión basado en un nuevo paradigma de desarrollo: **la Blockchain**. Observemos que se ha dicho “nuevo”, pues no es el objetivo de este proyecto, bajo ningún concepto, querer transmitir el concepto de “mejor”. Por otro lado, se quiere dejar claro que no es necesario saber invertir en criptomonedas, o cual es la cotización actual del Bitcoin o el Ether, para poder desarrollar una aplicación basada en una Blockchain.

## Presentación del problema

En la actualidad, la movilidad de las personas y las cosas han forzado que estemos viviendo en la era de la interconexión a todos los niveles, ya sea personal, empresarial o administrativa. La mayoría de los sectores, para realizar sus labores de negocio o de gestión, se ven obligados a consultar datos de otras fuentes. Las empresas y administraciones del territorio español, necesitan exponer y compartir sus datos para poder tener un control y ofrecer los servicios que los ciudadanos requieran. Es este flujo de información el que sirve de motor para gran parte sectores económicos en el mundo actual, y cuando éste se rompe, o simplemente no existe, notamos que todo se vuelve más lento e ineficiente.

Pues bien, este escenario, el de la falta de comunicación global, es el que en la actualidad se está produciendo en el sector veterinario español. Y este problema, además de los profesionales veterinarios, quien lo sufre son los usuarios del servicio, las personas y sus mascotas. ¿Pero y por qué? Pues debido a la movilidad de las personas y las familias que, junto con sus mascotas, se trasladan a otras residencias constantemente, y en cuestión de horas, por razones personales, de trabajo o de ocio.

En España, según datos de la web de profesionales del sector veterinario Petshopmagazine[[1]](#footnote-1), en el año 2018 había censados 5.147.000 perros y 2.265.000 gatos. Pues bien, es esta movilidad y la problemática administrativa que ella conlleva, en la que se quiere centrar el desarrollo del presente trabajo. Estos traslados familiares, ya sean ocasionales o permanentes, a nivel de mascotas también requieren de un registro y control administrativo por parte de los profesionales del sector veterinario. Éstas necesitan un control sanitario para su vacunación periódica, una atención puntual por algún tipo de enfermedad o el registro en sus nuevos domicilios. Este tipo de atención tiene como elemento angular de entrada el **Código de Identificación**, o lo que comúnmente se conoce como “**el chip**”. Este es un dispositivo electrónico, de un tamaño mayor al de un grano de arroz y compuesto por una electrónica miniaturizada encapsulada en plástico, que almacena un código alfanumérico de 15 posiciones único por cada dispositivo. Es el DNI del animal, el cual permite asociarlo al dueño y dotarle de un historial de domicilio, teléfono de contacto, historial veterinario, movimientos, etc.

La problemática surge debido a la ausencia de interconexión entre los diferentes servicios sanitarios veterinarios de las comunidades autónomas en España. Según el sistema SIACYL[[2]](#footnote-2), Sistema de Identificación Animal de Castilla y León, esta comunidad sólo tiene conexión con Castilla y La Mancha (SIACAM), Aragón (RIACA), Murcia (SIAMU) y Melilla (SIAMEL). Por ejemplo, se producen casos como los que ocurren con asiduidad, en alguno de los servicios veterinarios de la provincia de Ávila que se encuentran a escasos kilómetros de la Comunidad de Madrid, no tienen medios para localizar a los dueños de una mascota extraviada procedente de esta Comunidad mediante la consulta del chip identificativo. En estos casos, es necesario realizar una llamada telefónica a los servicios veterinarios de Madrid y en donde sólo existe atención telefónica en horario laboral y de Lunes a Viernes, con lo que se dan circunstancias en las que un animal que se extravía, y el si sábado por la mañana se intenta localizar al dueño, esto no sea posible hasta el Lunes siguiente, y sólo mediante una llamada de telefónica.

## La solución.

Entonces, ¿qué se puede hacer? Evidentemente, conectar los sistemas de cada una de las 17 comunidades autónomas. ¿Cómo? La respuesta a esta pregunta es que de múltiples maneras, pero en este punto nos vamos a centrar en lo más actual. Podremos hacerlo a través de una **API de servicios web** o a través de la creación de una **Blockchain**.

|  |
| --- |
| Es necesario resaltar la idea de que el objeto del presente trabajo no es reflejar las ventajas de un sistema sobre otro,si no el mostrar la existencia de un nuevo paradigma de generación de aplicaciones. |

### API de servicios web.

Ésta nos va a permitir el intercambio de información entre diferentes servicios web y una aplicación, usando para ello el protocolo http o https y empleando los dos formatos más extendidos: XML o JSON.

Normalmente entre los desarrolladores vamos a encontrar cuatro tipos de API para servicios web:

* **XML-RPC** (*Extensible Markup Language – Remote Procedure Call*): protocolo que permite la invocación de procedimientos o funciones alojadas en un sistema remoto. Con este mecanismo los desarrolladores pueden definir interfaces que pueden ser invocadas a través de la red.
  + Emplea protocolo http para la transmisión de información desde el cliente hasta el equipo servidor.
  + Especifica las llamadas a las funciones o procedimientos a través de XML.
  + Emplea un “vocabulario XML” muy limitado para realizar las llamadas (*requests*) y recibir las respuestas (*responses*).
  + El cliente XML-RPC especifica unos parámetros en la llamada y recibe del servidor una respuesta en formato XML o un error, en caso de producirse.
  + Las primeras definiciones del protocolo proceden del año 1998.
* **SOAP** (*Simple Object Access Protocol*): protocolo estándar para el intercambio de mensajes en formato XML entre dos objetos y diseñado para las comunicaciones vía Internet.
  + Es una aplicación de la especificación XML.
  + Permite el transporte de datos por los servicios web.
  + No está acoplado a ninguna plataforma o lenguaje de desarrollo.
  + Permite a las aplicaciones cliente conectarse de manera sencilla a servicios remotos e invocar métodos remotos.
* **JSON-RPC** (*Javascript Object Notation- Remote Procedure Call)*: concepto similar al XML-RPC, para la llamada a procedimientos o funciones remotas, pero realizados en formato JSON.
  + Emplea el protocolo http para la transmisión de información.
  + Paso de nombre del procedimiento o función y de los parámetros necesarios desde el cliente en un objeto con formato JSON y respuesta desde el servidor en un objeto con el mismo formato.
* **RESTful** (*Representational State Transfer*): Son servicios web basados en arquitectura REST.
  + Los servicios web RESTful se utilizan para la creación de APIs de aplicaciones basadas en web.
  + Se implementan sobre protocolo http.
  + Un servicio web RESTful define un URI, Uniform Resource Identifier un servicio, proporciona representación de recursos como JSON y un conjunto de métodos http (GET, POST, PUT, DELETE).
  + Independiente de la plataforma, sistema operativo y lenguaje de programación.

Con estos cuatro modelos de APIs podremos desarrollar diferentes capas de abstracción que permitan la interconexión de cada uno de los sistemas pertenecientes a cada comunidad autónoma.

### Blockchain

# Estado del arte.



## La Blockchain

¿Pero qué es Blockchain? La respuesta es, una red P2P (*peer-to-peer*) en la que se crean transacciones digitales, y que funciona con el mismo concepto que el de un libro mayor de contabilidad o *ledger*. En esta red la información se almacena en bloques, en donde cada uno de ellos contiene información relativa al bloque anterior, lo que permite ir formado una cadena. Información accesible pero inmutable.



### Características

Esta “cadena de bloques” posee las siguientes características:

* **Descentralizada** (*Trustless*): Todos los nodos son responsables de la gestión y modificación de la información al mismo tiempo. Esto significa que cualquier servicio o aplicación seguirá funcionando si un nodo o grupo de nodos deja de estar disponible, en este caso la información seguirá fluyendo al persistir en el resto de nodos de la red.
* **Distribuida** (*Many to many*)**:** Cualquier nodo perteneciente a la blockchain está conectado al resto de nodos de la red. Con la aplicación estricta de este concepto, en una Blockchain se hace casi imposible manipular los datos almacenados en ella, dado que todos los nodos tiene una copia de los mismos y los cambios no permitidos podrían ser rechazados al ser dados como *no válidos*.
* **Consistencia de datos** (*Proof of work*)**:** Tanto en **Bitcoin** como en **Ethereum** los nodos pertenecientes a la red verifican la validez de cada transacción realizada en ella, a través de un **algoritmo de consenso**. En el caso de estas dos redes, este algoritmo se denomina ***Proof of Work***. En capítulos posteriores, y después de haber introducido algunos conceptos de criptografía, profundizaremos en este concepto.
* **Inmutable** (*Ledger*)**:** Los datos almacenados en la red no pueden ser eliminados. Podrán ser modificados en posteriores operaciones, pero siempre existirá un registro histórico con todos los datos a través de la cadena de bloques.

### ¿Qué es un bloque?

Según se define en <https://www.sinergiablockchain.org/_/Doc/FAQ.pdf>:

*“Un bloque es un conjunto de transacciones confirmadas e información adicional que se ha incluido en la cadena de bloques. Cada bloque que forma parte de la cadena (excepto el bloque generatriz, que inicia la cadena) está formado por:*

* *Un código alfanumérico que enlaza con el bloque anterior.*
* *El “paquete” de transacciones que incluye (cuyo número viene determinado por diferentes factores).*
* *Otro código alfanumérico que enlazará con el siguiente bloque.”*

La imagen siguiente (*Ilustración 2*) muestra el concepto de una “cadena de bloques”.

Ilustración 2: Representación de la cadena de bloques.

**Block Hash: 0000078ecba1500**

**Previous Block Hash: 0000096effa4600**

**Block Hash: 0000011aee0534e**

**Previous Block Hash: 0000078ecba1500**

**Block Hash: 000056abff1189a**

**Previous Block Hash: 0000011aee0534e**

**Transaction Hash: 000aa76effa4133**

**Transaction Hash: aaf4000faee3a00**

**Bloque 76**

**Bloque 77**

**Bloque 78**

Pero como en todo siempre hay un principio, y la blockchain no es una excepción, existe un bloque generatriz denominado **Génesis**, a partir del cual se encadenan el resto. De modo que tendríamos la siguiente estructura (*Ilustración 3*). Este bloque se forma en el momento de la creación de la Blockchain.

Y está definido en un fichero en formato JSON que recibe el nombre de *genesis.json* (*Ilustración 4*).

Ilustración 3: Ejemplo de bloque genesis.json

|  |
| --- |
| { |

|  |
| --- |
| "config": { |

|  |
| --- |
| "chainId": 0, |

|  |
| --- |
| "homesteadBlock": 0, |

|  |
| --- |
| "eip155Block": 0, |

|  |
| --- |
| "eip158Block": 0 |

|  |
| --- |
| }, |

|  |
| --- |
| "alloc"   : {}, |

|  |
| --- |
| "coinbase"   : "0x0000000000000000000000000000000000000000", |

|  |
| --- |
| "difficulty" : "0x20000", |

|  |
| --- |
| "extraData"  : "", |

|  |
| --- |
| "gasLimit"   : "0x2fefd8", |

|  |
| --- |
| "nonce"   : "0x0000000000000042", |

|  |
| --- |
| "mixhash" : "0x0000000000000000000000000000000000000000000000000000000000000000", |

|  |
| --- |
| "parentHash" : "0x0000000000000000000000000000000000000000000000000000000000000000", |

|  |
| --- |
| "timestamp"  : "0x00" |

|  |
| --- |
| } |

### ¿Dónde están los bloques?

Los bloques se sitúan en los NODOS. Estos no son más que los ordenadores que componen la red, en donde reside un software, que se instala

**Block Hash: 00000aa11ba1500**

**Previous Block Hash: 0x0000**

**Block Hash: 0000011aee0534e**

**Previous Block Hash: 00000aa11ba1500**

**Transaction Hash: 000aa76effa4133**

**Transaction Hash: aaf4000faee3a00**

**Bloque 0**

**Bloque 1**

…

Ilustración 4: Bloque Genesis

### Criptografía de clave pública

## IPFS

IPFS es el acrónimo de Inter Planetary File System, y según consta en su web[[3]](#footnote-3)

# PetChain. Descripción del proyecto

# Petchain. Especificación de requisitos.



PetChain es un proyecto destinado al sector veterinario que permite la gestión de los sistemas de identificación de mascotas. La aplicación se basa en un desarrollo web tradicional, pero con la característica fundamental de estar implementada en una Blockchain bajo una red Ethereum.

PetChain gestiona de las identidades de las mascotas domésticas dando de alta, modificando los datos y gestionando la baja de los datos de los animales, bajo la ejecución de Smartcontracts creados en lenguaje Solidity.

## Propósito del documento

El presente documento pretende realizar una descripción de los requisitos informativos, funcionales y no funcionales de PetChain, con el fin de comprender y describir su funcionamiento, así como la enumeración de los participantes en el desarrollo, de cada una de sus partes y conseguir al final del mismo, una relación entre las partes y los creadores de las mismas.

Pretende ser una descripción de los requisitos informativos, funcionales, no funcionales del proyecto, con el objetivo de ofrecer a los lectores del documento del TFG una visión clara de la aplicación y las partes que lo componen.

## Alcance del documento

El presente documento tiene como alcance especificar:

* La declaración de los participantes en el proyecto.
* Definir de los objetivos de la aplicación.
* Proveer una descripción funcional del sistema que permita la mejor comprensión del mismo al equipo de evaluadores del proyecto TFG.
* Especificar de los requisitos informativos, funcionales y no funcionales que deberá cumplir la aplicación
* Establecer los límites de funcionales de PetChain.

## Participantes en el proyecto



### Presentación de participantes

|  |  |
| --- | --- |
| **Participante** | **Miriam Martínez Muñoz** |
| **Organización** | Universidad Internacional de la Rioja |
| **Rol** | Dirección de proyecto |
| **Es desarrollador** | Sí |
| **Es cliente** | No |
| **Es usuario** | No |
| **Comentarios** | Directora del proyecto de fin de grado. |

Tabla 1: Dirección del proyecto

|  |  |
| --- | --- |
| **Participante** | Carlos Escario Bajo |
| **Organización** | Universidad Internacional de la Rioja |
| **Rol** | Analista-Desarrollador |
| **Es desarrollador** | Sí |
| **Es cliente** | No |
| **Es usuario** | No |
| **Comentarios** | Ninguno |

Tabla 2: Analista y desarrollador del proyecto.

|  |  |
| --- | --- |
| **Participante** | **Pedro Escario Bajo** |
| **Organización** | Veterinaria García-Ochoa |
| **Rol** | Usuario |
| **Es desarrollador** | No |
| **Es cliente** | No |
| **Es usuario** | Sí |
| **Comentarios** | Trabajador en la Veterinaria García-Ochoa |

Tabla 3: Colaborador del proyecto

|  |  |
| --- | --- |
| **Participante** | **Iciar García-Ochoa** |
| **Organización** | Veterinaria García-Ochoa |
| **Rol** | Usuario |
| **Es desarrollador** | No |
| **Es cliente** | No |
| **Es usuario** | Sí |
| **Comentarios** | Propietaria de la Veterinaria García-Ochoa |

Tabla 4: Dirección facultativa y Veterinaria

## Organizaciones involucradas

|  |  |
| --- | --- |
| **Organización** | **Universidad Internacional de la Rioja** |
| **Dirección** | Av. de la Paz, 137, 26006 Logroño, La Rioja |
| **Teléfono** | N/A |
| **Fax** | N/A |
| **Comentarios** | [www.unir.net](http://www.unir.net/) |

|  |  |
| --- | --- |
| **Organización** | **Veterinaria García-Ochoa** |
| **Dirección** | Carretera de Casillas 6 local 3, 05420 Sotillo de la Adrada, Ávila |
| **Teléfono** | N/A |
| **Fax** | N/A |
| **Comentarios** | Ninguno |

## Descripción del sistema



### Perspectiva del producto

PetChain es una aplicación web, que tiene como objeto mostrar las capacidades que posee la Blockchain para el desarrollo de aplicaciones de gestión tradicionales. No es objeto de la misma ofrecer la visión de que el modelo que se presenta "es mejor" que cualquier desarrollo web tradicional, sino que como nuevo paradigma de desarrollo, es necesario tenerlo en cuenta como un futuro modelo para la generación de aplicaciones de gestión corporativas.

Su ejecución se realiza íntegramente en un entorno local, permitiendo este modelo, la visualización de cada una de las partes que componen el desarrollo. Esto es posible gracias al uso del framework Truffle, que con el servidor Ganache que lleva incorporado, ofrece la posiblidad de crear una red Ethereum y con ello poder desarrollar, desplegar y testear Smartcontracts desarrollados con lenguaje Solidity.

### Funciones del producto

PetChain es una aplicación que debe de permitir a los veterinarios:

* Identificar a las mascotas domesticas mediante un código alfanumérico único, así como asociarlas a una persona que actuará como dueño, y que estará identificado mediante DNI o Pasaporte y los datos personales (nombre, apellidos, domicilio, y teléfono de contacto).
* Modificar los datos sanitarios de vacunaciones,
* Modificar los datos personales del dueño de la mascota.
* Dar de baja a las mascotas del sistema.
* Mostrar un listado de mascotas.
* Visualizar el saldo en ethers y weis de cada uno de los veterinarios correspondientes a las transacciones realizadas.

### Características del usuario

Los usuarios de PetChain serán los veterinarios, que a nivel nacional, deben de realizar acciones de tipo administrativo a la hora de gestionar las identificaciones de animales de compañía.

Como perfil tecnológico, deben tener competencias a la hora de manejar formularios web, sin necesitar unos conocimientos técnicos profundos, pues el modelo visual no difiere de cualquier página web existente en el mercado.

Por otro lado el tipo de información que es necesaria cumplimentar en la web, está dentro del dominio del sector veterinario, con lo que su cumplimentación no debería presentar problemas para el colectivo que usará la aplicación.

### Restricciones

PetChain es un proyecto web que debe ser posible su visualización en toda clase de dispositivos, por lo tanto la estructura de las pantallas se debe de adaptar a la resolución de la pantalla en donde se ejecute, siendo el rango de estas desde dispositivos Smartphone, Tablets y PCs.

A nivel de seguridad, es necesario implementar características que permitan la autenticación y la autorización de los usuarios que intenten acceder a la aplicación, pero al ser una ejecución en un entorno local no es obligatorio el diseño de una base de datos SQL o NoSQL, que albergue sus credenciales de acceso.

## Descripción técnica del sistema



### Front-End

La web se desarrollará bajo el modelo de visualización responsive, por lo que su diseño se deberá adaptar al tipo de resolución de la pantalla desde la que se esté accediendo. Para conseguir este objetivo se empleará en su diseño el framework open source Twitter Bootstrap, ver. 4.3.1.

El desarrollo de las interfaces de usuario se realizará con HTML5 estándar, CSS3 y la programación de los scripts de cliente se realizará con JavaScript (ECMA Script 6) y el framework de cliente jQuery versión 3.1.1., siendo uno de los objetivos del desarrollo el de aprovechar al máximo el paradigma de programación MVC (Model View Controller).

### Seguridad

Como antes se indicaba, es necesario implementar un sistema que verifique la autenticación de los usuarios al sistema, así como la autorización para la realización de acciones asociadas al rol que tenga determinado. El sistema de credenciales empleado para el proyecto actual debe quedar preparado para poder implementar una conexión a una base de datos NoSQL en el caso de que PetChain se instale en un entono productivo. En el modelo de ejecución actual, sólo se exigirá que los usuarios estén definidos en un fichero JSON almacenado dentro de la estructura local de proyecto.

Aunque no se exija el almacenamiento de credenciales en una base de datos, si es necesario que la aplicación tenga implementados sistemas de protección de URL mediante JWT, así como la validación de usuarios mediante nombre de usuario y contraseña.

### Back-End

La aplicación se ejecutará en una Blockchain desplegada en un entorno local. La red estará funcionando desplegada en un servidor Ganache, el cual es un componente del framework de desarrollo y ejecución Truffle.

La conexión entre la capa de Back-End y el Front-End es posible mediante el uso del framework Web3.js. Este entorno, desarrollado íntegramente en Javascript, permite la interacción de Smartcontracts con el JavaScript alojado en el cliente y la ejecución de la lógica en ellos definida.

Por último la interacción de ambas capas permitirá la creación y modificación de uno o varios ficheros JSON, los cuales harán como soporte No SQL, el cual se implementará como un fichero físico en IPFS.

### Entorno de ejecución

La aplicación debe de ejecutarse en cualquier navegador estándar (IE11, Chrome o Firefox) en un servidor local o localhost.

Para la ejecución de funcionalidades como la seguridad, lectura y escritura de ficheros y paso de mensajes entre pantallas, es necesario la realización de solicitudes POST y GET, por lo la aplicación se va a desplegar con un servidor ExpressJS y bajo un entorno de ejecución NodeJS.

## Objetivos del sistema

|  |  |
| --- | --- |
| **OBJ-0001** | **Alta de mascotas** |
| **Versión** | 1.0 ( 04/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa * Pedro Escario Bajo |
| **Descripción** | El sistema deberá permitir el alta de una mascota en el sistema, asociándola a un código de chip. Este es un identificador con longitud fija de quince (15) caracteres alfanumérico. |
| **Sub-objetivos** | Ninguno |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

Tabla 5: Objetivos 001

|  |  |
| --- | --- |
| **OBJ-0002** | **Alta de dueños de mascotas.** |
| **Versión** | 1.0 ( 04/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa * Pedro Escario Bajo |
| **Descripción** | El sistema deberá permitir el dar de alta a una persona, asociándola a una mascota. |
| **Sub-objetivos** | Ninguno |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

Tabla 6: Objetivos 002

| **OBJ-0005** | **Modificación de datos** |
| --- | --- |
| **Versión** | 1.0 ( 04/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa * Pedro Escario Bajo |
| **Descripción** | El sistema deberá permitir modificar los datos asociados a las mascotas y a sus dueños. El veterinario modificador deberá pagar un canon fijo en weis al veterinario identificador. |
| **Sub-objetivos** | **[OBJ-0006] Modificación de datos de mascotas**: El sistema deberá permitir la modificación de los datos sanitarios de las mascotas, así como la inclusión de las vacunaciones periódicas obligatorias.  **[OBJ-0007] Modificación de datos de los dueños**: El sistema deberá permitir cambiar los datos correspondientes al dueño de la mascota, incluido el cambio a un nuevo propietario. |
| **Importancia** | importante |
| **Urgencia** | Inmediatamente |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0008** | **Baja de mascotas** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa |
| **Descripción** | El sistema deberá permitir dar de baja a una mascota del sistema, por motivos de defunción. |
| **Sub-objetivos** | Ninguno |
| **Importancia** | importante |
| **Urgencia** | **PD** |
| **Estado** | **PD** |
| **Estabilidad** | **PD** |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0009** | **Consulta de saldo** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Descripción** | El sistema deberá permitir consultar el saldo en ethers o weis que cada veterinario participante en el sistema, tiene por realizar acciones dentro del mismo. |
| **Sub-objetivos** | Ninguno |
| **Importancia** | Importante |
| **Urgencia** | Por definir |
| **Estado** | Por definir |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0011** | **Control de acceso** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Descripción** | El sistema deberá permitir el acceso al sistema a aquellos usuarios que estén incluidos en el fichero de usuarios creado. |
| **Sub-objetivos** | Ninguno |
| **Importancia** | Importante |
| **Urgencia** | Inmediatamente |
| **Estado** | Pendiente de validación |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0012** | **Visualización en múltiples dispositivos** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Descripción** | El sistema deberá estar diseñado para poder visualizarse en dispositivos del tipo Smartphone, Tablet y PC |
| **Sub-objetivos** | Ninguno |
| **Importancia** | Importante |
| **Urgencia** | Importante |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0014** | **Navegación por la aplicación** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Descripción** | El sistema deberá permitir la navegación entre las opciones de alta, modificación y baja de mascotas, así como la consulta del saldo de weis. |
| **Sub-objetivos** | Ninguno |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0013** | **Traspasar weis** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Descripción** | El sistema deberá *traspasar weis desde el veterinario modificador hasta el veterinario identificador, siempre y cuando el modificador realice un cambio en los datos de una mascota que ya exista en el sistema.* |
| **Sub-objetivos** | Ninguno |
| **Importancia** | importante |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **OBJ-0015** | **Gestión de sesiones** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Descripción** | El sistema deberá *ser capaz de manejar las sesiones de usuario y el correcto funcionamiento de los navegadores.* |
| **Sub-objetivos** | Ninguno |
| **Importancia** | Importante |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

## Catálogo de requisitos del sistema.



### Requisitos de información

Los requisitos de información son formas especializadas de requisitos que van a permitir la introducción de datos relativos a los actores que van a participar o componer el sistema.

|  |  |  |
| --- | --- | --- |
| **IRQ-0001** | **Datos de usuario veterinario** | |
| **Versión** | 1.0 ( 05/05/2019 ) | |
| **Autores** | * Carlos Escario Bajo | |
| **Fuentes** | * Iciar García-Ochoa | |
| **Dependencias** | * [FRQ-0001] Acceso al sistema | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a los usuarios veterinarios que usen el sistema. En concreto: | |
| **Datos específicos** | * Nombre de usuario * Contraseña del usuario * Rol * Número de colegiado * Colegio | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| Sesión de usuario | Sesión de usuario |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| Por definir | Por definir |
| **Importancia** | Vital | |
| **Urgencia** | Inmediatamente | |
| **Estado** | En construcción | |
| **Estabilidad** | Por definir | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0002** | **Datos de mascota** | |
| **Versión** | 1.0 ( 05/05/2019 ) | |
| **Autores** | * Carlos Escario Bajo | |
| **Fuentes** | * Iciar García-Ochoa * Pedro Escario Bajo | |
| **Dependencias** | Ninguno | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a *a las mascotas que se añaden al sistema.* En concreto: | |
| **Datos específicos** | * Nº de identificación * Fecha de implantación Nombre * Raza Peligrosa * Fecha de nacimiento * Capa * Pelo * Sexo * Pasaporte animal * Aptitud * Última vacunación antirrábica * Fecha de la última revisión * Número de colegiado última revisión * Cicatrices * Numero de certificado | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| Sesión de usuario | Sesión de usuario |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| Por definir | Por definir |
| **Importancia** | Importante | |
| **Urgencia** | Inmediatamente | |
| **Estado** | En construcción | |
| **Estabilidad** | Por definir | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0003** | **Datos del dueño** | |
| **Versión** | 1.0 ( 05/05/2019 ) | |
| **Autores** | * Carlos Escario Bajo | |
| **Fuentes** | * Iciar García-Ochoa * Pedro Escario Bajo | |
| **Dependencias** | Ninguno | |
| **Descripción** | El sistema deberá almacenar la información correspondiente al dueño de la mascota*.* En concreto: | |
| **Datos específicos** | * Nombre * Apellidos * Número de documento * Teléfono * Provincia * Municipio * Código Postal * País | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| Sesión de usuario | Sesión de usuario |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| Por definir | Por definir |
| **Importancia** | Importante | |
| **Urgencia** | Inmediatamente | |
| **Estado** | Por definir | |
| **Estabilidad** | Por definir | |
| **Comentarios** | Ninguno | |

|  |  |  |
| --- | --- | --- |
| **IRQ-0004** | **Saldo** | |
| **Versión** | 1.0 ( 05/05/2019 ) | |
| **Autores** | * Carlos Escario Bajo | |
| **Fuentes** | * Carlos Escario Bajo | |
| **Dependencias** | Ninguno | |
| **Descripción** | El sistema deberá almacenar la información correspondiente a *al saldo en ethers o weis correspondiente a los usuarios veterinarios que usen el sistema.* En concreto: | |
| **Datos específicos** | * Cuenta ethereum * Saldo en weis * Número de colegiado | |
| **Tiempo de vida** | **Medio** | **Máximo** |
| Ejecución smartcontract | Ejecución de smartcontract |
| **Ocurrencias simultáneas** | **Medio** | **Máximo** |
| Por definir | Por definir |
| **Importancia** | Importante | |
| **Urgencia** | Inmediatamente | |
| **Estado** | Por definir | |
| **Estabilidad** | Por definir | |
| **Comentarios** | Ninguno | |

### Requisitos funcionales

Ian Sommerville en su libro “Ingeniería de Software 9” define los requisitos funcionales como: “*enunciados acerca de servicios que el sistema debe proveer, de cómo debería reaccionar el sistema a entradas particulares y de cómo debería comportarse el sistema en situaciones específicas. En algunos casos, los requerimientos funcionales también explican lo que no debe hacer el sistema*” (Pearson Education, 2011, pags 84 - 85).

Estos requisitos nos darán una visión concreta de cuáles son los objetivos de funcionamiento de PetChain, y que además tienen su correspondencia con los Casos de uso descritos en la sección 5.10.

|  |  |
| --- | --- |
| **FRQ-0001** | **Acceso al sistema** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa * Pedro Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá permitir el acceso a los usuarios a través de un formulario en el que se debe introducir un nombre de usuario y una contraseña. Si los datos introducidos no son correctos, el sistema deberá mostrar en la pantalla un mensaje de error. |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **FRQ-0002** | **Identificación de veterinarios** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá mostrar el nombre del veterinario y el colegio en donde está inscrito, con solo introducir el número de Colegiado. |
| **Importancia** | Importante |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **FRQ-0003** | **Traspaso de weis** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá traspasar weis cuando se haga una modificación de los datos de una mascota, desde el veterinario modificador hasta el veterinario que dio de alta a la mascota. |
| **Importancia** | Importante |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **FRQ-0004** | **Navegación** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Pedro Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá permitir en todo momento la navegación por el sistema a través de las opciones que se muestren en la pantalla de inicio o en un menú situado en la cabecera de la aplicación. |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **FRQ-0005** | **Campos no modificables en la Modificación.** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá impedir en la opción de Modificación de datos de la mascota, que el usuario cambie los datos asociados al veterinario identificador y los datos de nacimiento correspondientes a la mascota sobre la cual se están realizando modificaciones. |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **FRQ-0006** | **Campos no modificables en la Baja de mascotas** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Iciar García-Ochoa |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá impedir en la opción de Baja de mascotas que el usuario cambie los datos asociados al veterinario identificador. |
| **Importancia** | Importante |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **FRQ-0007** | **Consultar weis disponibles** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá visualizar un listado con el saldo de weis que tiene cada veterinario, |
| **Importancia** | Importante |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **FRQ-0008** | **Validación de campos** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Pedro Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá mostrar en pantalla un mensaje que informa de aquellos campos que son obligatorios y no han sido rellenados en el momento de enviar el formulario. |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | Pendiente de verificación |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

### Requisitos no funcionales

Son aquellos requerimientos que no se refieren directamente a las funciones específicas que entrega el sistema, sino a las propiedades emergentes de éste como la fiabilidad, la respuesta en el tiempo y la capacidad de almacenamiento. De forma alternativa, definen las restricciones del sistema como la capacidad de los dispositivos de entrada/salida y la representación de datos que se utiliza en la interface del sistema, etc.

|  |  |
| --- | --- |
| **NFR-0001** | **Visualización** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá ajustar la visualización de las interfaces gráficas en función del modelo de desarrollo responsive. Es decir será el cliente quien detecte el tipo de dispositivo desde el que se está accediendo a la web. |
| **Importancia** | Quedaría bien |
| **Urgencia** | Puede esperar |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **NFR-0002** | **Moneda de pago** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá permitir el pago en weis, siendo la conversión en ethers de 1 ether = 1 e-18 wei. |
| **Importancia** | Importante |
| **Urgencia** | Por definir |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **NFR-0003** | **Tiempo de sesión** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá controlar que el tiempo que puede estar una sesión inactiva, será como máximo de 15 minutos. |
| **Importancia** | Importante |
| **Urgencia** | Puede esperar |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **NFR-0004** | **Usuarios autorizados** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá tener almacenados los usuarios de la aplicación en un fichero en formato JSON, en donde se indique su número de colegiado, nombre de usuario, contraseña y número de colegiado. |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | Pendiente de validación |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **NFR-0005** | **Número de cuentas** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá tener definidas por defecto al menos 100 cuentas en el servidor Ganaché. |
| **Importancia** | Vital |
| **Urgencia** | Inmediatamente |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

|  |  |
| --- | --- |
| **NFR-0006** | **Autenticación JWT** |
| **Versión** | 1.0 ( 05/05/2019 ) |
| **Autores** | * Carlos Escario Bajo |
| **Fuentes** | * Carlos Escario Bajo |
| **Dependencias** | Ninguno |
| **Descripción** | El sistema deberá tener un control de autenticación mediante JWT, que se almacena como variable en la SessionStorage. |
| **Importancia** | Importante |
| **Urgencia** | Puede esperar |
| **Estado** | En construcción |
| **Estabilidad** | Por definir |
| **Comentarios** | Ninguno |

## Matriz de rastreabilidad



### Matriz de rastreabilidad: Objetivos del sist. – Requisitos funcionales

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TRM- 001** | **FRQ-0001** | **FRQ-0002** | **FRQ-0003** | **FRQ-0004** | **FRQ-0005** | **FRQ-0006** | **FRQ-0007** | **FRQ-0008** |
| **OBJ-0001** | - |  | - | - | - | - | - |  |
| **OBJ-0002** | - | - | - | - | - | - | - |  |
| **OBJ-0005** | - |  |  | - |  | - |  |  |
| **OBJ-0006** | - | - | - | - | - | - | - |  |
| **OBJ-0007** | - | - | - | - | - | - | - |  |
| **OBJ-0008** | - | - | - | - | - |  | - |  |
| **OBJ-0009** | - | - | - | - | - | - |  | - |
| **OBJ-0011** |  | - | - | - | - | - | - | - |
| **OBJ-0012** | - | - | - | - | - | - | - | - |
| **OBJ-0013** | - | - |  | - | - | - | - | - |
| **OBJ-0014** | - | - | - |  | - | - | - | - |
| **OBJ-0015** | - | - | - | - | - | - | - | - |

### Matriz de rastreabilidad: Objetivos del sist. – Requisitos no funcionales

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TRM- 001** | **NFR-0001** | **NFR-0002** | **NFR-0003** | **NFR-0004** | **NFR-0005** | **NFR-0006** |
| **OBJ-0001** | - | - | - | - | - | - |
| **OBJ-0002** | - | - | - | - | - | - |
| **OBJ-0005** | - | - | - | - | - | - |
| **OBJ-0006** | - | - | - | - | - | - |
| **OBJ-0007** | - | - | - | - | - | - |
| **OBJ-0008** | - | - | - | - | - | - |
| **OBJ-0009** | - | - | - | - | - | - |
| **OBJ-0011** | - | - | - |  | - |  |
| **OBJ-0012** |  | - | - | - | - | - |
| **OBJ-0013** | - |  | - | - | - | - |
| **OBJ-0014** | - | - | - | - | - | - |
| **OBJ-0015** | - | - |  | - | - | - |

## Casos de uso

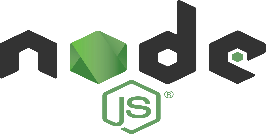
Esta sección mostrará, a través de diagramas UML, los diferentes requerimientos del sistema, permitiendo tener una visión más clara de los aspectos funcionales de la aplicación, los actores que intervienen y los sistemas externos a los que están conectados.

# PetChain. Descripción técnica

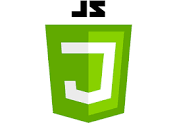
PetChain es una aplicación web que emplea para su ejecución una combinación de tecnologías, con el objetivo de conectar un frontal en HTML con un backend desarrollado con Smartcontracts.

Ilustración 5: Arquitectura de frameworks y herramientas utilizadas.

http



Ficheros estáticos



Scripts

Solidity



Compilador Solidity



Browser

**Express JS**

Web server

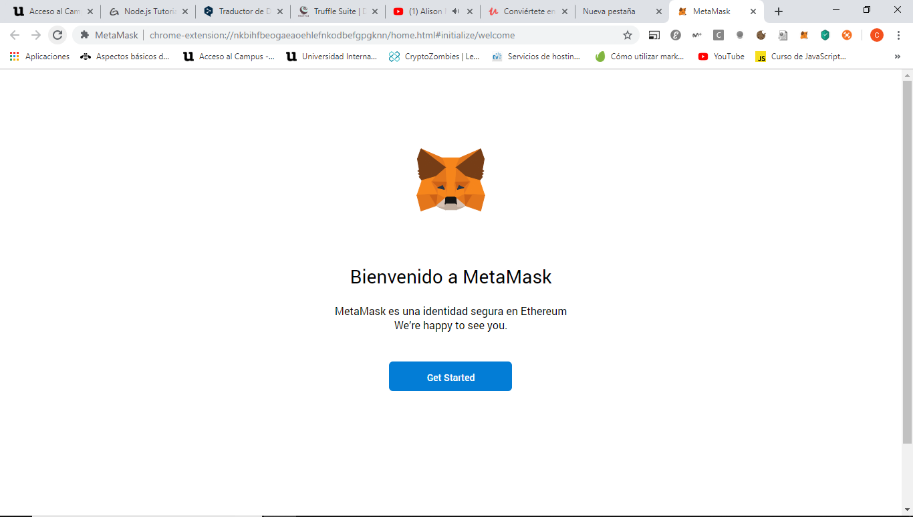
Blockchain server



Estilos css



Web3js



Metamask

En los próximos apartados se van a introducir y explicar con detalle, por orden de instalación, cada una de las tecnologías necesarias para el correcto funcionamiento de la aplicación.



## NodeJS

Node.js es un entorno multiplataforma de código abierto utilizado para la ejecución de JavaScript en el lado del servidor. Su funcionamiento se basa en la ejecución de eventos de manera asíncrona, esto significa que mientras NodeJS gestiona cualquier solicitud de I/O que le haya llegado y hasta que la petición finalice, ésta se estará ejecutando en segundo plano, y mientras el sistema podrá seguir realizando cualquier otra operación en primer plano.

Gran parte de su éxito se basa en la enorme cantidad de módulos existentes que permiten extender las funcionalidades del entorno. Para la instalación de dichos módulos se emplea un gestor de paquetes incluido en NodeJS llamado npm (Node Package Manager)[[4]](#footnote-4). PetChain para su ejecución necesita los paquetes descritos en las secciones siguientes.

|  |
| --- |
| **ATENCION**: Todas las instalaciones hechas vía **npm**, son realizadas con el parámetro **--save-dev**. Este parámetro indica que todos los módulos se deben instalar como una dependencia dentro del fichero **package.json**, en la lista de dependencias. Posteriormente, si se ejecuta el comando **npm install** en el directorio de la aplicación, los módulos se instalarán de manera automática en la lista de dependencias. |



### ExpressJS

Framework que permite la creación y ejecución de un servidor web dentro del entorno NodeJS.

|  |
| --- |
| **> npm install express -–save-dev** |

Ilustración 6: Comando instalación de ExpressJS

### body-parser

Módulo que permite la lectura de la cadena que se transmite en cualquier petición http entrante al servidor.

|  |
| --- |
| **> npm install body-parser –save-dev** |

Ilustración 7: Comando de instalación de body-parser

### jsonwebtoken

Estándar para la transmisión de información segura como un objeto JSON.

|  |
| --- |
| **> npm install express-jwt –save-dev** |

Ilustración 8: Comando de instalación de jsonwebtoken

### Generación del proyecto

La creación del proyecto NodeJS es un proceso sencillo, que no difiere del sistema operativo en el que se ejecute, y se realiza en los siguientes pasos.

|  |
| --- |
| **> mkdir tfg\_project**  **> cd tfg\_project** |

Ilustración 9: Comandos de creación directorio del proyecto

Creamos el fichero package.json, a través del comando npm init:

|  |
| --- |
| **> npm init** |

Ilustración 10: Inicialización del proyecto NodeJS

Al finalizar el proceso, se habrá creado un fichero package.json, que actuará como puerta de entrada para el proyecto. En nuestro caso, con las dependencias ya instaladas, éste archivo tendrá la siguiente estructura:

|  |
| --- |
| **{**  **"name": "tfg\_project",**  **"version": "1.0.0",**  **"description": "BlockChain para la gestión de un servicio de identificación de mascotas domésticas a nivel nacional.",**  **"main": "index.js",**  **"scripts": {**  **"test": "echo \"Error: no test specified\" && exit 1"**  **},**  **"repository": {**  **"type": "git",**  **"url": "git+https://github.com/cescari/tfg\_project.git"**  **},**  **"keywords": [**  **"tfg",**  **"blockchain",**  **"mascotas"**  **],**  **"author": "Carlos Escario Bajo",**  **"license": "SEE LICENSE IN ./license.html",**  **"bugs": {**  **"url": "https://github.com/cescari/tfg\_project/issues"**  **},**  **"homepage": "https://github.com/cescari/tfg\_project#readme",**  **"devDependencies": {**  **"body-parser": "^1.19.0",**  **"express": "^4.16.4",**  **"jsonwebtoken": "^8.5.1",**  **"nodemon": "^1.19.0",**  **"web3": "^1.0.0-beta.54"**  **},**  **"dependencies": {**  **"openurl": "^1.1.1"**  **}**  **}** |

Ilustración 11: Estructura del fichero package.json

## Truffle

Truffle[[5]](#footnote-5) es un framework que permite el desarrollo, compilación, despliegue y pruebas de Smartcontracts sobre redes Ethereum. Es una herramienta que se instala como módulo de NodeJS, v8.9.4 o superior, y está disponible para las plataformas Windows, Linux y Mac OS X. Las características que ofrece son:

* Scaffolding inicial del proyecto.
* Compilación de Smartcontracts y generación de archivos en formato JSON con la estructura del Smartcontract y su bytecode correspondiente.
* Despliegue sobre redes privadas y públicas.
* Generación y ejecución de test.

### Instalación de Truffle

Como se ha comentado anteriormente Truffle está disponible como un módulo del entorno de ejecución NodeJS, por lo tanto para su instalación haremos uso de npm (Node Package Manager). Ejecutamos entonces la sentencia siguiente:

|  |
| --- |
| **> npm install –g truffle –save-dev** |

Ilustración 12: : Comando de instalación de Truffle

Los parámetros de instalación son opcionales, pero permitirán una ejecución y actualización de las dependencias, en caso de actualizarse las versiones.

**-g**: permite la instalación a nivel global del sistema.

### Generación del proyecto

Dado que hemos realizado la instalación de Truffle con el parámetro –g, desde ahora vamos a tener disponible desde cualquier parte de la estructura de archivos de nuestra máquina los comandos ejecutables del framework, que permitirán su instalación y configuración desde la línea de comandos.

Para nuestro proyecto, ejecutaremos:

|  |
| --- |
| **> truffle init** |

Ilustración 13: Comando de inicialización de un proyecto Truffle

Este comando genera la estructura necesaria para el proyecto, que nos permitirá el almacenamiento de los ficheros solidity (\*.sol), su compilación y despliegue de binarios. Dicha estructura consta de los siguientes elementos.

* contracts/: directorio para el almacenamiento de ficheros solidity (\*.sol).
* test/: directorio para el almacenamiento de los test.
* migrations/: directorio para el almacenamiento de los scripts correspondientes a las migraciones de los archivos con extensión .sol a ficheros .js, y que contendrán la estructura del Smartcontract en formato JSON, así como en bytecode.
* truffle-config.js: fichero de configuración de Truffle para la definición de las redes de despliegue de los Smartcontracts.

|  |
| --- |
| **ATENCION**: Es necesario indicar que en la instalación de Truffle, se requiere **obligatoriamente** que la carpeta en donde se vaya a ejecutar el comando **truffle init**, esté completamente **vacía**. Si no se cumple esta premisa, el framework devolverá siempre un error indicando que no es posible su instalación para evitar sobre-escrituras a proyectos ya existentes. |

## Ganache

Ganache[[6]](#footnote-6) es un componente multiplataforma (Windows, Linux o Mac OS X), que forma parte del framework Truffle y su función es la servir como servidor de cuentas en una red Ethereum. Es el complemento ideal para el desarrollo de aplicaciones Blockchain en entornos cerrados, locales o corporativos, y está disponible para su ejecución como herramienta de escritorio o para invocarlo a través de línea de comandos (TestRPC).



### Instalación de Ganache

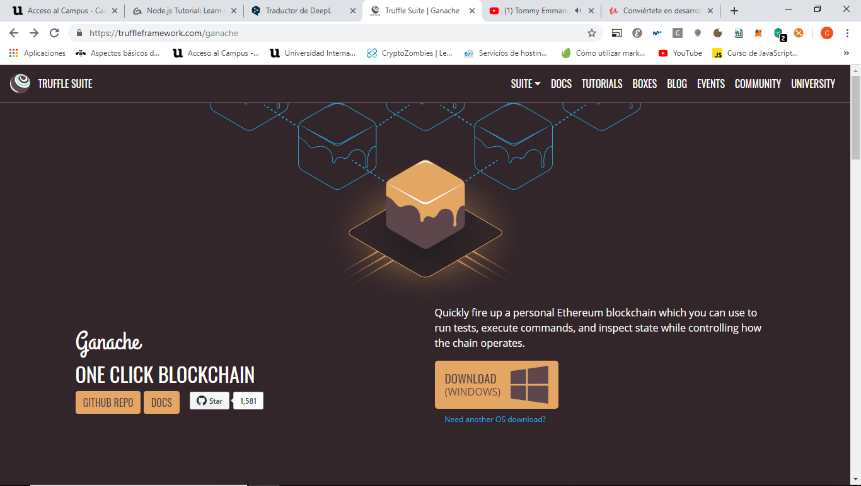
La instalación de Ganache es trivial y se realiza a través de un cásico “wizzard”. Para el presente proyecto se implementará como una herramienta de escritorio, tanto para un sistema Windows 10 y Linux Ubuntu 18.02, a través del instalador que se puede descargar desde la página web de Truffle.

Ilustración 14: Web de Truffle framework.

## Web3.js

Web3.js es la herramienta JavaScript, open source, multiplataforma e imprescindible para interactuar desde el navegador con Ethereum a través del protocolo http. Expone una API[[7]](#footnote-7) con gran cantidad de métodos con los que comunicar con el object provider, que en nuestro caso será el servidor de cuentas Ganache.



### Instalación de Web3.js

Esta librería está disponible de diversos métodos; es posible incorporarla a nuestro proyecto como un módulo de NodeJS a través del comando npm en la carpeta del proyecto:

|  |
| --- |
| **> npm install web3 -–save-dev** |

Ilustración 15: Comando de instalación de web3.js

Como se ha comentado anteriormente, con estos parámetros web3 se instalará como una dependencia del proyecto dentro del package.json de NodeJS.

Así mismo, es posible tener disponible la librería cuando se instala el framework de Truffle, dado que al

# Evaluación

# ¿Qué queda por hacer? Trabajo futuro.

# Bibliografía

# Glosario de términos

*A*

B

*C*

CSS3

Cascade Style Sheet ver.3 17

*D*

*E*

ECMA

European Computer Manufactures

Association 17

*F*

*G*

*H*

HTML5

Hiper Text Markup Language 17

*I*

*J*

JSON

Java Script Object Notation 4,7,8,

11,17,30,35

JWT

Javascript Web Token 17,30

*K*

*L*

*M*

MVC

Model View Controller 17

N

NoSQL

No Structured Query Language 16,17

O

P

Q

R

S

T

U

URL

Unifrom Resource Locator 17

V

X

Y

Z

1. [*http://petshopsmagazine.com/mascotas/censo-mascotas-espana/*](http://petshopsmagazine.com/mascotas/censo-mascotas-espana/) [↑](#footnote-ref-1)
2. *www.siacyl.org* [↑](#footnote-ref-2)
3. [*https://docs.ipfs.io/introduction/overview/*](https://docs.ipfs.io/introduction/overview/) [↑](#footnote-ref-3)
4. *npm web site:* [*https://www.npmjs.com/*](https://www.npmjs.com/) [↑](#footnote-ref-4)
5. *Truffle website: https://truffleframework.com* [↑](#footnote-ref-5)
6. *Ganache website:* [*https://truffleframework.com/ganache*](https://truffleframework.com/ganache) [↑](#footnote-ref-6)
7. [*https://github.com/ethereum/wiki/wiki/JavaScript-API#web3-javascript-app-api-for-02xx*](https://github.com/ethereum/wiki/wiki/JavaScript-API#web3-javascript-app-api-for-02xx) [↑](#footnote-ref-7)