Facultad de Estudios Estadísticos
Universidad Complutense de Madrid

ntic master
revolucionamos la comunicación

VERSION FINAL 15-9-2020

Blockchain & BigData Canino

MEMORIA

Autores:

Cristina Rodríguez Chamorro
Daniel Lanzas Pellico
Helena García Fernández
José Bennani Pareja
Juan José Lucas de la Fuente
Unai Ares Icaran

Tutor:
Sergio Torres Palomino

Documentación del TFM
Máster Blockchain y Big Data. *Curso 2019-2020*

ÍNDICE

Agradecimientos

A nuestras **familias**,
sin cuyo apoyo y paciencia este trabajo no habría llegado a su fin

A la Facultad de Estudios Estadísticos de la **UCM** de Madrid y
a **NTIC** Máster por haber hecho posible la realización de este Máster

A nuestro tutor, **Sergio Torres**, por haber aguantado
nuestras preguntas y haber resuelto nuestras dudas

Equipo y definición de tareas

Cristina Rodríguez Chamorro……Desarrollo aplicación Big Data
Daniel Lanzas Pellico…….... Desarrollo arquitectura Block Chain
Helena García Fernández…… Desarrollo aplicación Big Data
José Bennani Pareja……..…..... Desarrollo Web y API-REST
Juan José Lucas de la Fuente…….…… Desarrollo Web y API-REST
Unai Ares Icaran … Definición y desarrollo de algoritmos BD, Chaincodes y Estado del Arte

Estado del arte: Introducción al mundo canino

En la actualidad el mundo de las mascotas constituye un negocio multimillonario de aproximadamente 36.500 millones al año en toda Europa, donde hay 200 millones de mascotas en 80 millones de hogares. En España genera más de 1.000 millones anuales de negocio que generan más de 100.000 puestos de trabajo, entre indirectos y directos.

Según datos de la Red Española de Identificación de Animales de Compañía (REIAC) existen en el país más 13 millones de mascotas registradas, de las cuales más de la mitad corresponden a ejemplares caninos. La pureza de raza, la línea genealógica y los premios que han obtenido sus ancestros determinan mucho el precio, por lo que la verificación y certeza de estos datos son especialmente relevantes en este tipo de negocio donde existen muchos casos de personas que se aprovechan de la gente.

Actualmente existen multitud de organizaciones en diferentes países que gestiona las certificaciones del mundo canino, cada una encargándose de diferentes partes procesos (registros de afijos de criadores, camadas, propietarios, identificación canina, premios y títulos, ...) y en muchos casos de manera repetida, duplicando competencias, por no existir un registro unificado.

Con el fin de poder reunir a estos colectivos en un solo entorno compartido se plantea un desarrollo Blockchain que sirva para interactuar inicialmente entre:

- Criadores caninos
- Propietarios
- Veterinarios
- Federaciones caninas
- Jueces
- Sociedades y Clubes caninos

CONCEPTOS BÁSICOS DEL MUNDO CANINO

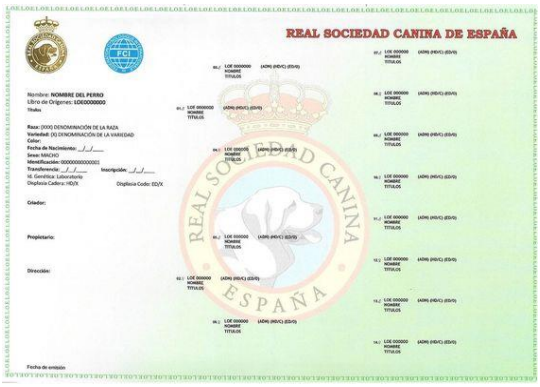
- Identificación canina

Este proceso lo realizan los veterinarios insertando un pequeño microchip subcutáneo del tamaño de un grano de arroz, en una capsula de cristal especial que contiene un transpondedor con un código único, siendo obligatorio en España con el objeto de evitar el abandono animal estando tipificado como delito en la Ley orgánica 1/2015.

Existe un registro gestionado por cada comunidad autónoma así como una Red Española de Identificación de Animales de Compañía (REIAC), que en muchos casos no está actualizado.

- Libro genealógico

Registro, fichero o sistema informático donde se inscribe los perros de raza pura, mencionando sus ascendentes y descendientes, gestionado por organizaciones reconocidas oficialmente a través de eventos.



Para su inscripción es necesario demostrar que las tres últimas generaciones del ejemplar se encuentran inscritas en un libro de origen de especies o si este hecho no pudiera ser demostrado, a través un reconocimiento de raza por un juez especialista de la organización.

- Federaciones caninas

Estas organizaciones se aseguran de que los pedigríes, los criadores y los jueces sean reconocidos mutuamente por todos los miembros que las integran. Organizan concursos y exposiciones de Morfología, Trabajo y disciplina, Rastreo y Agility, concediendo menciones y títulos a los mejores ejemplares, a través de jueces reconocidos por dichas organizaciones.

Existen numerosas federaciones a nivel nacional e internacional, por ejemplo:

- Fédération Cynologique Internationale (FCI)
- Real Sociedad Canina Española (RSCE)
- The Kennel Club (TKC)
- Alianz canine Worldwide (ACW)

Las sociedades y clubes de raza son organizaciones que colaboran con las federaciones para realizar diferentes gestiones a nivel local para el fomento de razas caninas o de alguna en especial. Preparan en coordinación con las federaciones concursos y exposiciones, por ejemplo:

- Sociedad Canina de Bizkaia
- Sociedad Canina Montañesa
- Sociedad valenciana para el fomento de razas caninas
- Sociedad Canina Gallega

- Afijos de criadores

Un afijo es una denominación o marca personal de un criador que lo registra a través de una sociedad o federación canina.

La concesión de un afijo autoriza a su titular o titulares a utilizarlo en la inscripción de camadas. Todos los titulares del afijo deben ser propietarios de la hembra, madre de la camada, para poder utilizar el afijo.

El afijo es propiedad exclusiva de la persona o colectividad que ha adquirido el derecho y es vitalicio. El propietario de un afijo puede aplicarlo a todos los ejemplares de cualquier raza de la que es criador. No puede aplicarse a un ejemplar un afijo diferente al de su criador. Nadie podrá ser titular de más de un afijo por raza.

Por ejemplo:

- Afijo: Coramonte
- Ejemplares: Vanessa de Coramonte, Gastón de Coramonte, ...

- Certificaciones

Es necesario estudiar el ciclo completo de registro de los perros desde el momento del nacimiento para detallar las certificaciones que debería proporcionar el proyecto blockchain a desarrollar, por ejemplo:

- Certificado de propietario de ejemplar y traspaso de propiedad
- Certificado de nacimiento de camadas
- Certificado de cesión temporal de hembra
- Certificado de afijo de criador
- Certificado de identificación canina (microchip)
- Certificado de la línea genealógica o pedigrí del ejemplar
- Certificado de reconocimiento de raza del ejemplar
- Certificado premios y títulos del ejemplar

- Procesos de registro

Los actuales procedimientos de las federaciones caninas se realizan mayoritariamente de manera presencial (ya que es necesario realizar pagos por las gestiones), lo que supone desplazarse hasta sus oficinas y pagar las correspondientes tasas.

La Blockchain permitirá certificar todos estos procesos puedan realizarse online, con una mayor seguridad desde cualquier punto del mundo, a cualquier hora.

FUNCIONALIDADES BÁSICAS A DESARROLLAR

- ## Blockchain canino

Las funcionalidades básicas a desarrollar en el proyecto Blockchian serán:

- Identificación y autenticación (Criadores caninos, propietarios, veterinarios, sociedades caninas, jueces, clubes caninos)
- Afijo de criador (alta, baja, modificación, certificación)
- Camadas (registro y certificación)
- Ejemplar (certificación propiedad y traspaso, pedigrí y defunción)
- Microchip (registro y modificación)
- Registro de vacunación
- Concursos y exposiciones (registro de premios y títulos)

En una puesta en producción, podría realizarse las siguientes ampliaciones:

- Identificación a través de ADN
- Registro de enfermedades

- ## Big Data Canino

Existen algunas ideas sobre las ampliaciones que se podrían realizar a partir de la Base de Datos ya generada con Blockchain y nuevos datos acumulados:

- Calidad estimada del cruce de razas a partir de los modelos obtenidos por las líneas genealógicas y los premios y títulos conseguidos.
- Estudio de características morfológicas a partir del ADN y detección de enfermedades

Para esta prueba de concepto se ha optado por la implementación de :

- Reconocimiento de razas a través de imágenes (Deep learnig)

CONCLUSIONES

El mundo canino esconde detrás una gran complejidad con múltiples participantes con intereses en algunas ocasiones en común y en otros particulares, sobre todo en cuanto comprendemos que detrás de las líneas genealógicas de los

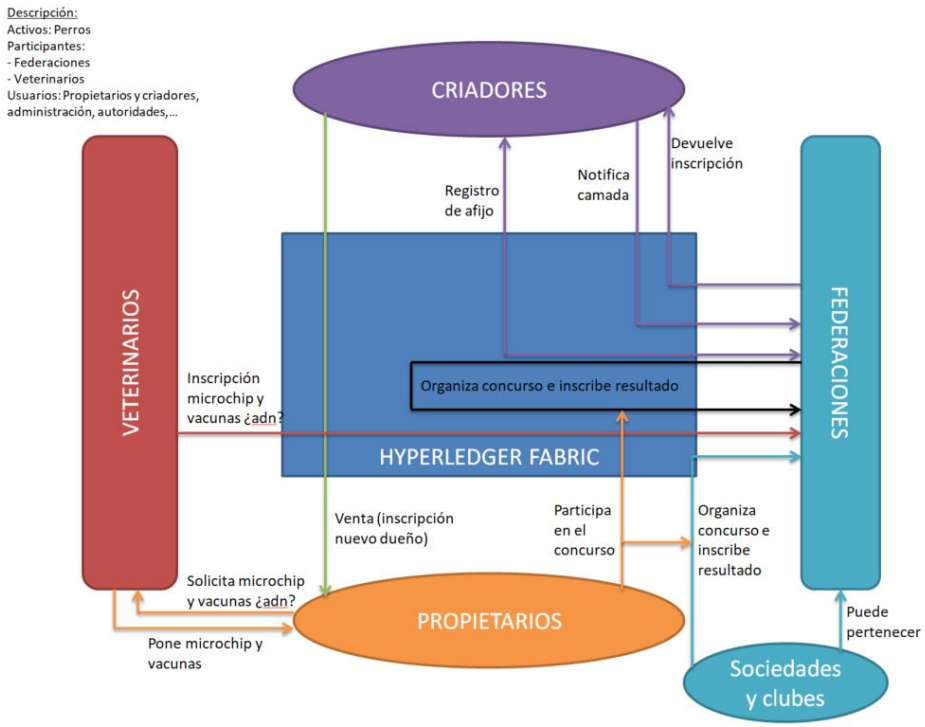
perros, el prestigio, los concursos y exposiciones se mueve mucho dinero, lo que puede hacer que cada organización se muestre recelosa, para compartir su información, produciéndose en algunos casos perdida de información, datos duplicados o no incongruentes por falta de actualización.

Por otro lado, existen los amigos de lo ajeno que intentan engañar y aprovecharse de personas, falseando datos y cometiendo fraudes, en contraposición con algunas asociaciones cuyo fin es el fomento de las razas caninas, pero se ven limitados por no disponer de los recursos necesarios para abordar un proyecto global. Es por ello, que un blockchain canino podría resolver muchos de los problemas citados.

Arquitectura del Proyecto: Descripción del Producto y Fundamentos Técnicos

En primer lugar, se decide el uso de la tecnología Blockchain para regir las relaciones entre las diferentes organizaciones, lo que redunda en que la actividad sea transparente para ambas y en que la información sea inmutable y no pueda ser modificada para realizar ningún tipo de fraude.

Por otra parte, dado que se trata de dos organizaciones privadas que deben interactuar sin llegar a tener confianza una en la otra y que los datos tienen una componente privada (siendo algunos de ellos sensibles y protegidos por el RGPD), se propone la utilización de una red Blockchain privada con la tecnología Hyperledger Fabric como base.



Los activos con los que contará la red son los perros, que tendrán un propietario que podrá cambiar, se les podrá poner el microchip y vacunas, participarán en concursos,...

Los participantes serán las Federaciones Caninas y los Colegios Veterinarios, que son los que ejecutarán las acciones sobre los perros.

Por otra parte que los usuarios serán las propias Federaciones, los Colegios Veterinarios, los propietarios, los veterinarios y las autoridades competentes (agentes de la autoridad, juzgados,...) a los que se permita el uso de la red.

ARQUITECTURA DEL PROYECTO

Dentro de Hyperledger Fabric se definen dos organizaciones con las siguientes características:

- Federaciones Caninas

  Se trata de las organizaciones que llevan a cabo el control de los afijos autorizados para la cría de perros, control de las características de las razas, pedigríes,...

  En este caso se tendrán en cuenta las cuatro mayores Federaciones existentes:

- FCI: Fédération Cynologique internationale
- RSCE: Real Sociedad Canina Española
- TKC: The Kennel Club
- ACW: Alianz Canine Worldwide

- Colegios Veterinarios

  Se trata de las organizaciones que llevan el control de todo lo relativo a la sanidad de los perros: colocación de microchip, vacunas, pasaporte sanitario, ...

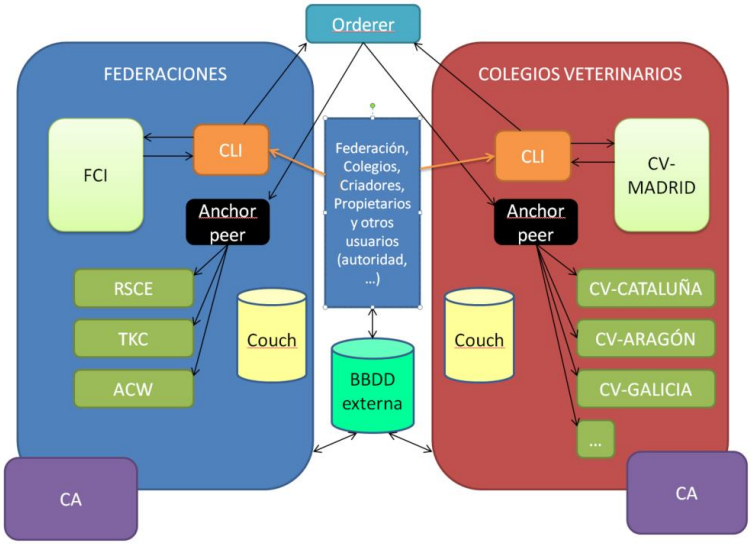
  Se tomarán los Colegios Veterinarios a nivel de Comunidad Autómoma, por lo que tendremos diecisiete Colegios Veterinarios

Se utilizará CouchDB en vez de levelDB para aumentar las posibilidades de consulta a la red y cada organización tendrá una autoridad de certificación (CA).

Además, se implementará una base de datos externa para guardar los datos sensibles y los destinados al uso por la aplicación de Big Data.

El tipo de consenso será "solo" para el desarrollo, aunque posteriormente debería implementarse "Kafka" en producción.

Una vez definidas las organizaciones la arquitectura será la siguiente:



Tras la instalación de Hyperledger Fabric en los servidores crearemos una red con la arquitectura descrita anteriormente, consistente en dos organizaciones (Federaciones y ColegiosVeterinarios), cuatro peers para la primera organización y diecisiete para la segunda, Orderer, CLI, CA´s y CouchDB. Instalaremos además Hyperledger Explorer para poder visualizar la información de la red en el navegador, accediendo también a la CouchDB desde el navegador.

Posteriormente añadiremos TLS a la red, generando una red más segura en la que será necesario proveer los certificados correspondientes al efectuar cualquier acción.

Por último desplegaremos la red entre dos servidores simulando la existencia real de dos las dos organizaciones.

SCRIPTS DE CONFIGURACIÓN

Tras definirse la estructuras de carpetas del proyecto se decide realizar una serie de scripts que levanten y paren el proyecto de manera automática, tanto en su despliegue en un servidor como en dos servidores, siendo los siguientes scripts:

- netcan_script.sh: En primer lugar limpia la instalación, a continuación accede al repositorio de Github, descarga las carpetas json, chaincode y scripts y sustituye las existentes por estas y posteriormente va lanzando el resto de scripts de configuración, ya sea para uno o dos servidores
- red_script.sh: Este script levanta la red hyperledger Fabric y copia los scripts necesarios al docker del CLI, donde luego habrá que realizar la configuración del proyecto

- Serv2_script.sh: Este script realiza la configuración en el servidor 2 en el caso de que se levante la red entre dos servidores
- config_script.sh: Este script se ejecuta dentro del docker del CLI y realiza la configuración del canal, los peers y los pares de anclaje, ya sea con TLS o sin TLS
- chaincode_script.sh: Este script también se ejecuta dentro del docker del CLI e instala e instancia los chaincodes desarrollados
- json_script: Este script copia los archivos de carga iniciales a los dockers de los chaincodes para realizar las cargas iniciales de datos a la blockchain
- carga_script.sh: Este script se ejecuta dentro del docker del CLI y realiza las cargas iniciales de datos a la blockchain
- stop_netcan_script: Por último este script para la red, borra los dockers levantados y borra los chaincodes instanciados

ARCHIVOS DE CONFIGURACIÓN

- configtx.yaml: En este archivo se realiza la configuración de las organizaciones y del canal y es el que servirá para la generación de los artefactos del proyecto.
- crypto-config.yaml: Define la arquitectura de la red con el orderer, las organizaciones y los peers para la generación del material criptográfico por medio de la herramienta de hyperledger fabric cryptogen
- docker-compose-cli.yaml: Es el archivo de configuración principal de Hyperledger Fabric. En él se define la estructura básica del proyecto.
- docker-compose-couch.yaml: Este archivo configura la red para el uso de CouchDB en vez de levelDB, lo que permite realizar índices y redunda en una mayor facilidad de uso y la posibilidad de realización de consultas más complejas.
- docker-compose-base.yaml: En este archivo se definen el orderer y los peers. En particular se establece que los peers extienden a su vez del archivo peer-base.yaml y el uso de TLS en el orderer pasando los certificados correspondientes en las variables
- peer-base.yaml: Establece la configuración común a todos los peers, incluido el uso de TLS y sus correspondientes certificados

PUESTA EN MARCHA DEL PROYECTO

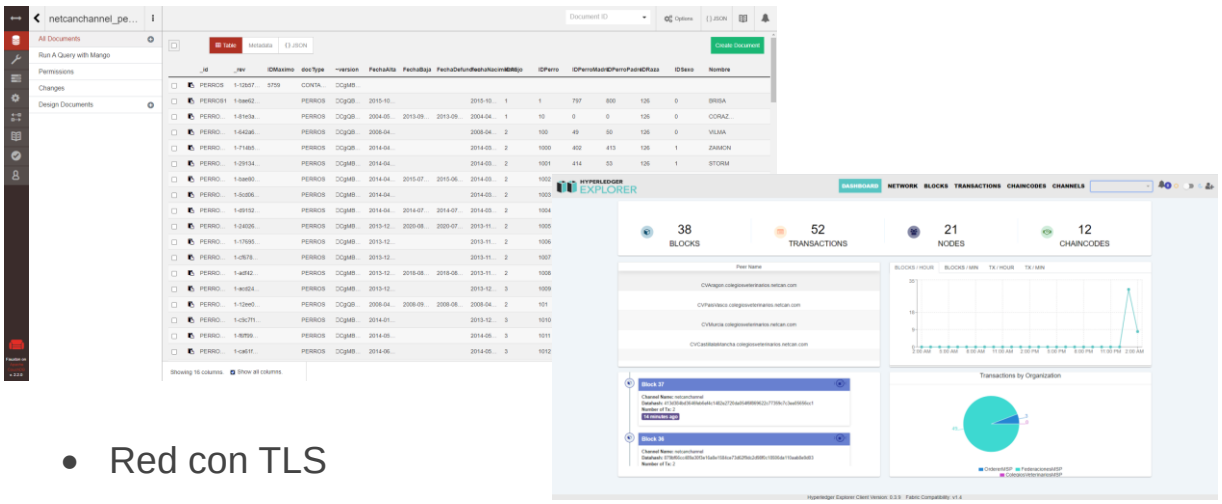
Se despliegan tres redes:

- Red inicial sin TLS

Los archivos de configuración pueden encontrarse en el repositorio Github https://github.com/DFLBB/TFM_archs en la carpeta Arquitectura bajo el nombre TFM_sin_TLS.tar.

Se trata de una copia completa del proyecto, encontrándose los scripts utilizados en la carpeta scripts2 del repositorio github.

Se procede a desplegar la red y se conecta desde el navegador a la CouchDB y a Hyperledger Explorer.



- Red con TLS

Los archivos de configuración pueden encontrarse en el repositorio Github https://github.com/DFLBB/TFM_archs en la carpeta Arquitectura bajo el nombre TFM_sin_TLS.tar.

Se trata de una copia completa del proyecto, encontrándose los scripts utilizados en la carpeta scripts del repositorio github.

Se modifica la red anterior para añadir TLS entre el CLI, el Orderer y los Peers. No se securizan las CA´s ya que según indicaciones del tutor supone más problemas que ventajas.

- Red creada entre dos servidores

Los archivos de configuración pueden encontrarse en el repositorio Github https://github.com/DFLBB/TFM_archs en la carpeta Arquitectura bajo el nombre TFM_dos_Servidores.tar.

Se trata de una copia completa del proyecto, encontrándose los scripts utilizados en la carpeta scripts3 del repositorio github.

Se parte de la red con TLS para simular una una situación más parecida a la realizada en la que cada servidor corresponde a una organización.

En primer lugar se crea una red Docker Swarm para conectar ambos servidores y posteriormente se modifican los archivos de configuración para dejar en cada servidor lo correspondiente a su organización así como los scripts para que lancen automáticamente la red entre ambos servidores.

Chaincodes y funcionalidades del sistema

CHAINCODES SEGÚN ORGANIZACIÓN

Los chaincodes utilizados por cada organización son los siguientes:

Federaciones Caninas

- Personas
- Perfil
- Perros
- Afijos
- Solicitudes
- Veterinarios
- Microchip
- Razas
- Exposiciones y concursos
- Título

Colegios de Veterinarios

- Personas
- Perfil
- Perros
- Veterinarios
- Vacunas
- Microchips
- Razas

FUNCIONES COMUNES DE LOS CONTRATOS

Existen un conjunto de funciones que se definen dentro de los contratos. A modo de ejemplo mostraremos algunas:

- ejecutarConsulta: Permite realizar consultas al sistema a través del lenguaje de consulta de Mango, que se expresa como un objeto JSON que describe los filtros de los documentos de interés que se desean consultar.
- asignarEstado
- borrarEstado
- consultarEstado
- consultarRangoEstados
- getQueryResultForQueryString: Devuelve en formato JSON el resultado de una consulta, donde el TipoEstado tendrá la definición especifica del estado consultado.

CHAINCODES

- ### PERSONAS

Contrato inteligente encargado de gestionar la identidad y sus datos personales de las personas que intervienen en las solicitudes que se lanzan contra el sistema. Actualmente gestiona los datos identificativos de:

- Criadores (propietarios de afijos)
- Propietarios de Perros

- Veterinarios
- Miembros de Federaciones

Está diseñado para admitir en el futuro ampliaciones de la blockchain, dando la posibilidad de albergar los datos de identificación de otro tipo de usuarios o datos asociados como jueces de certámenes caninos, miembros de Asociaciones caninas, miembros de Club de raza caninas y de grupos, miembros de laboratorios (para registros de ADN).

- AFIJOS

Contrato inteligente encargado de gestionar la identificación y propiedad de los afijos de criadores, denominación o marca personal registrada a través de una sociedad o federación canina que le autoriza a su titular o titulares a utilizarlo en la inscripción de camadas.

- PERROS

Contrato inteligente encargado de gestionar el registro de ejemplares canino, identificando su origen, pureza de raza, mencionando sus ascendentes y descendientes. Identfica la propiedad del ejemplar y sus cambios , asi como la defuncion del ejemplar.

- SOLICITUDES

Importante contrato inteligente dentro de la blockchain, encargado de gestionar las solicitudes de los usuarios cuando es necesario realizar la validación o autorización de la acción por más de una persona, por ejemplo, cuando se desea vender un perro y existe mas de un propietario, o cuando se quiere certificar un cruce de dos perros pertenecientes a diferentes propietarios.

- PERFILES

Contrato inteligente encargado de gestionar los roles de los usuarios del sistema. Su uso está restringido exclusivamente a usuarios Administradores y

permite definir perfiles de usuarios que permite el acceso a determinadas acciones y datos. Por ejemplo, solo un veterinario podrá poner un microchip o una vacuna.

- VETERINARIOS

Contrato inteligente encargado de gestionar los datos específicos de un veterinario como por ejemplo su número de colegiado.

- MICROCHIPS

Contrato inteligente encargado de registrar la identificación de microchip subcutáneo insertado por los veterinarios en el perro que contiene un transpondedor con un código único que permite identificar de manera univoca al ejemplar.

- VACUNAS

Contrato inteligente encargado de registrar el historial de las vacunas administradas por veterinarios y la duracion y tipo de proteccion de sus componentes.

- RAZAS

Contrato inteligente encargado de registrar gestiona el mantenimiento de los diferentes estándares de pureza de raza reconocidos, actualmente cerca de 346 razas, clasificadas en 10 grupos.

- Otros posibles contratos inteligentes

En un futuro podrían incorporarse con facilidad mas contratos a la Blockchain, como por ejemplo:

- TÍTULOS: Registra los títulos concedidos por federaciones, asociaciones y clubes por los méritos obtenidos por los ejemplares en exposiciones y/o concursos
- EXPOSICIONES Y CONCURSOS: Registra los resultados de los concursos y exposiciones de Morfología, Trabajo y disciplina, Rastreo y Agility que las diferentes federaciones, asociaciones y club realizan.
- ADN: Contrato que gestiona el registro de ADN. Facilitaría la certificación de autenticad de la linera genealógica y permitiría el estudio genético a partir de los datos obtenidos.
- ENFERMEDADES / TRATAMIENTOS: Contrato que gestiona el registro de las enfermedades y tratamientos que los veterinarios realizan sobre los perros, pudiéndose disponerse de un historial clínico para que cualquier veterinario pudiera consultarlo cuando llegue un ejemplar a su consulta.

API-REST

Desarrollo Big Data