kms.plus

Organización Descentralizada Autónoma
Autor: Alejandro Criado-Pérez
alejandro@criadoperez.com

Versión 0.35 - 27 de Septiembre de 2019

Blockchain de la automoción

"Creado entre todos y para todos"

Resumen ejecutivo

Vamos a capitalizar la información del sector del automóvil. Dándole valor a la información infrautilizada y aumentar el valor de la información ya capitalizada.

Para ello creamos un mercado de información para todos los actores del sector de la automoción, donde se consulta información, firman contratos nuevos, realizan pagos y entregan información de forma autónoma, bajo las condiciones preestablecidas por cada empresa. Los contratos entre las empresas tendrán validez legal.

Es de interés para cualquier entidad del sector automoción que utilice, compre y/o venda datos o disponga de los mismos y desee capitalizarlos de manera simple legal y automática.

Permite hacer negocios con todos los actores del sector, aunque no se conozcan entre ellos.

Descentraliza el poder de la información, devolviéndolo al creador de la misma.

¿Por qué la necesita el sector?

En el sector de la automoción, se generan multitud de datos de diferente naturaleza en multitud de empresas. Es muy habitual la compra y venta de datos entre ellas, sin embargo dichas transacciones se limitan a acuerdos 1-a-1 y no Todos-a-Todos.

Un blockchain de la automoción permite aumentar la facturación en las empresas que ya venden su información al ampliar su público, aumentar la cantidad de datos que podría vender y permitir que muchas entidades que generan información valiosa para el sector y no saben cómo venderla la pueda distribuir fácilmente.

Hace posible compartir información sin revelarla.

Usos potenciales

Los usos son variados y resulta imposible nombrarlos todos, pero destacando los más inmediatos y evidentes tenemos lo siguientes.

Para conductores

- Un comprador de un V.O. podría comprar un informe sobre el historial del vehículo del que está interesado, viendo desde los datos de fabricación, registro, número de transferencias, información de subastas, etc, garantizada y firmada por el origen del dato no por ningún intermediario, pudiendo así vender su vehículo a un valor más alto por tener un historial certificado.

Para fabricantes

- Los fabricantes ya venden datos por VIN a un número limitado de empresas. Ahora podrán vender los mismos datos con las tarifas que ellos quieran a cualquier interesado en el dato, desde un particular hasta una consultora que desea ver datos agrupados.

Para aseguradoras

- La aseguradora paga todas las piezas que reparan los vehículos de sus asegurados y el fabricante las vende. Diversos estudios demuestran una gran diferencia entre estos dos volúmenes, debido al enorme fraude que hay en el sector. Ahora el taller podrá demostrar a la aseguradora que realmente ha comprado dicha pieza, registrando una operación de compra a un vehículo.

Para empresas con flotas propia

- Con una sola llamada una empresa podría saber el activo del valor de mercado de toda su flota (valor agregado o individual a cada vehículo). Incluso podría pedir ser notificado si sufre cambios por encima de un valor.

Para renting

- Ahora una empresa de renting podrá comparar sus tarifas con los de la competencia sin revelarlas, ya que técnicamente se limita a que cada operador sólo podrá ver datos agrupados y no específicos. Ningún externo a la empresa de renting jamás

tendrá acceso a los datos de la misma. Solución que hasta ahora no era técnicamente posible.

Para consultoras

- Cualquier consultor o investigador podrá hacer consultas a la cadena que hasta ahora no eran posible, gracias a la nueva tecnología de datos agregados.

Equipo

Formado por desarrolladores de EOS y por personal del sector incluyendo fabricantes, aseguradoras, empresas dedicadas a la información del automóvil, renting, etc.

Porque ahora

En Junio 2018 nació EOS y el 26 de Febrero de 2019 nació la red Daap de LiquiApps. Hasta ahora no era técnicamente posible crear un infraestructura con las características requeridas por este proyecto.

Por otro lado, la tecnología para montar una DAC es muy reciente y que sepamos, a fecha de este escrito, no existe ninguna DAC empresarial constituida en España todavía.

Premisas que deberá cumplir la solución

1. **Código abierto**: Toda la infraestructura está basada en tecnologías de código abierto.
2. **Remuneración al origen del dato:** Se remunera a la fuente del dato sin intermediarios. Cada fuente podrá elegir qué datos compartir, con qué condiciones y a qué precio.
3. **Ricardian contracts:** Todos los smart contracts, tienen un contrato paralelo escrito en inglés que redacte la intención de dicho contrato. Si el código no se ejecuta como es debido por algún fallo, hay una vulnerabilidad o uso malintencionado, la parte afectada podrá solicitar un arbitraje donde predominará lo escrito en el Ricardian contract por encima del código, pudiendo si es necesario deshacer una transacción.

4. **Información descentralizada**: Los smartcontracts y el "listado" de la información disponible se almacena en la propia cadena (RAM). Sin embargo, la información en sí se almacenará en la vRAM de los DSPs. De esta manera toda la información está siempre disponible en sistemas descentralizados.

5. **GDPR**. Deberá cumplir con la GDPR (General Data Protection Regulation), y en particular el artículo de derecho al olvido. Por lo que será posible "eliminar" información.

6. **Desconfianza en los proveedores**. Un proveedor podría escribir un dato erróneo o que vulnera la GDPR, y luego desaparecer, contaminando la cadena. Por ello la red también debe de ser capaz de "bloquear" un dato que vulnere la constitución o el futuro EUA (EOS User Agreement) si es finalmente aprobado.

7. **Permisos**. Debido a la inmutabilidad del blockchain, ningún dato en formato bruto se escribirá en la cadena o en vRAM directamente. En vez, mediante una gestión de permisos se consultará antes de cada consulta si el acceso a dicha información sigue siendo válido. Si ha sido revocado, resultará imposible acceder a la misma.

8. **Local e Internacional**. La solución podrá ser utilizada por cualquier país, y todo el desarrollo es multipaís, sin embargo como cada mercado tiene sus particularidades, en el lanzamiento original se incluirán todas las particularidades del sector español, sin perjuicio de lo anterior.

9. **Ciclo completo**. Al proveedor de datos se le tiene que ofrecer la opción del ciclo completo del proceso. Es decir, desde el momento que el proveedor publica sus datos, la venta y el pago de la misma se realizará de forma automática.

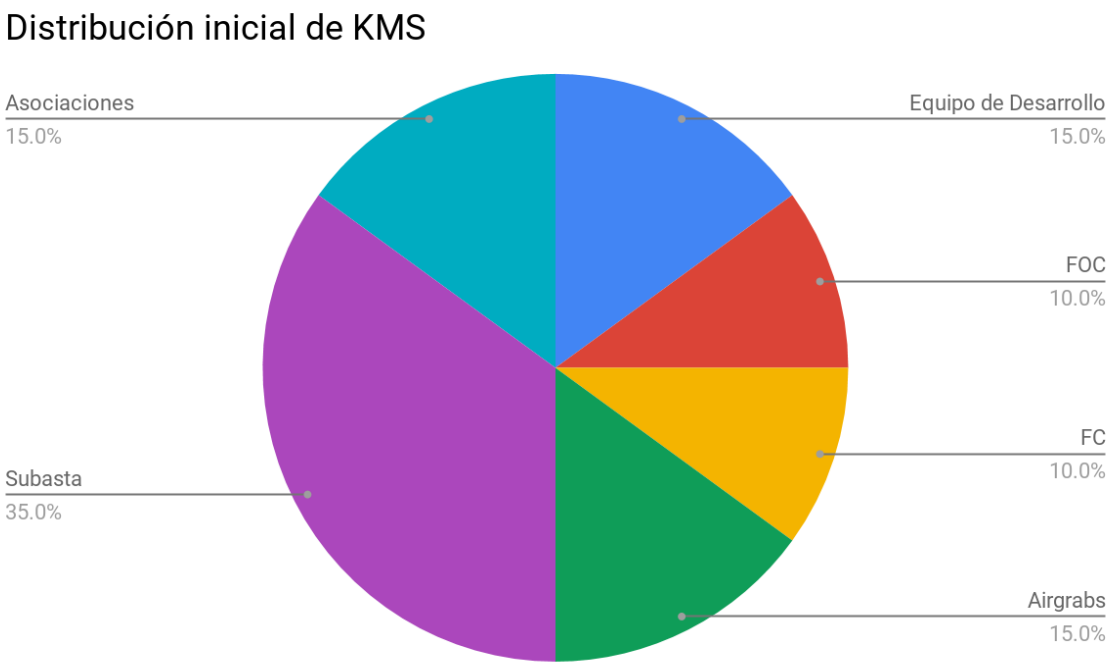
10. **Datos agrupados**. Se podrán consultar datos individuales de un vehículo o agrupados. Por ejemplo, ¿qué porcentaje de los vehículos diésel con tapicería de cuero son de 5 puertas?

11. **Datos gratuitos**. Cualquier proveedor podrá voluntariamente aportar información a la red sin coste para el consumidor.

12. **FIAT friendly**. Un proveedor de datos podrá establecer el precio de una información en diferentes FIATs (EUR, USD, etc) o en KMS.

Financiación y distribución de KMS

Habrá un ICO (“Initial Coin Offering”), de 100.000.000 de KMS.



La distribución será gradual y distribuida a lo largo de un periodo de 12 meses.

Se distribuirá entre los participantes del proyecto según su nivel de involucración y las empresas del sector según su peso en el mercado (detalles aún por definir).

Se plantean opciones como entregar los primeros tokens a fabricantes, aseguradores, y demás actores del sector, por su volumen en el mercado multiplicado por un factor variable según su implicación en el proyector durante el tiempo que dure la ICO.

Fase 1a - Airgrab

Durante los primeros 3 meses o los primeros 5000 usuarios (lo que sucedan antes) se entregarán 100KMS a cualquier usuario EOS que se registre gratuitamente (Airgrab de 500.000KMS).

Si no se consumieran todos los KMS al finalizar el periodo, los KMS restantes se destruirán.

Fase 1b - Subasta de financiación

De forma simultánea durante los primeros 12 meses se distribuirán 5.718.388 KMS mediante subastas mensuales (a último día del mes natural) y decrementales (cayendo un 15% cada mes), distribuidos de la siguiente manera:

Número de Subasta	KMS a distribuir	Porcentaje de la subasta
1	1.000.000	17.5%
2	850.000	14.9%
3	722.500	12.6%
4	614.125	10.7%
5	522.006	9.1%
6	443.705	7.8%
7	377.149	6.6%
8	320.577	5.6%
9	272.490	4.8%
10	231.616	4.1%
11	196.874	3.4%
12	167.343	2.9%
TOTAL	5.718.388	100%

Los KMS de la subasta mensual serán distribuidos entre todos los pagadores en función del porcentaje del pago total. Por ejemplo, si en un mes se reciben 100 EOS en pagos y un usuario ha realizado el pago de 5 EOS, dicho usuario recibirá el 5% (5 / 100) de los KMS distribuidos ese mes.

Fase 1C - Asociaciones

Durante los primeros 3 meses, se permitirá la creación de un cuenta gratuita a las diferentes asociaciones del sector (AER, AEGFA, GANVAM, FACONAUTO, etc).

A cada asociación se le entregará una cantidad de KMS bloqueados. Dichos KMS los podrán utilizar sólo para votar en la organización pero no los podrán transferir a nadie, excepto a sus asociados. Dispondrán de un periodo de 6 meses para transferirlos a sus respectivos asociados en la proporción que ellos consideren (normalmente por peso en la asociación o

de manera equívoca para todos). Los KMS que no sean transferidos a los asociados al finalizar el periodo de bloqueo serán transferidos al FOO. Cuando esto suceda, adicionalmente la asociación recibirá un 20% de los KMS totales que haya transferido satisfactoriamente (KMS ya desbloqueados).

Fase 2

En el caso de necesitar más recursos para poder operar se contempla la opción de hacer Stakemining (cuando usuarios EOS nos prestan temporalmente sus tokens para usarlos como CPU y NET a cambio de KMS).

Infraestructura técnica

La solución está creada en EOS donde se almacenan los contratos y DSPs donde se almacenará la información potencial a compartir.

Se plantea la opción de usar vRAM para el airdrop en vez de RAM (se estima un coste 6x menor).

Se plantea la opción de usar vAccounts para usuarios finales para reducir costes de creación de cuentas nuevos en EOS.

La plataforma de socios para gestionar la DAC está actualmente alojada en Google Cloud, concretamente en el Datacenter de Bruselas.

La web de cara al usuario (kms.plus) será colgada en un repositorio git y publicada en los servidores de manera automática (actualmente IONOS, en el Datacenter de Madrid).

Diseño general

Se utiliza una cadena de bloques pública, concretamente la mainnet de EOS.

Se utilizan los siguientes tokens:

- EOS. Para el el pago de RAM, CPU, “Bandwidth” , ejecución de código y almacenamiento de smart contracts.
- DAPPs. Para el pago de vRAM y vCPU en los diferentes DSPs.

- KMS. Token de cambio con el que se ejecutarán los contratos y se realizarán los pagos.
- bitEUR, bitUSD u otras smartcoins para almacenar el valor en diversas FIAT.

Cuando un usuario paga unos KMS para consultar cierta información, se distribuyen esos KMS entre todos los proveedores de datos que la hayan aportado.

Si un usuario ha establecido un precio fijo en euros para un dato en concreto, se le informa antes al comprador de su precio equivalente en KMS, así cuando el proveedor reciba los KMS se transformarán a una smart coin en euros como por ejemplo bitEUR.

Ejemplo de uso:

Un usuario particular quiere consultar la información disponible sobre un vehículo del cual sólo sabe su matrícula. Para ello, hace una llamada al sistema totalmente gratuita para ver qué información hay de ese vehículo. El sistema le responde con una lista de proveedores que han proporcionado datos de ese vehículo. Si después de ver el listado de la información disponible le interesa comprar el informe, puede comprarlo pagando en euros ó KMS, según su plataforma. En el caso de pagar en euros, estos son transformados a KMS inmediatamente para poder operar en la red.

ORGANIZACIÓN DE KMS.PLUS

kms.plus será una ODA, Organización Descentralizada Autónoma (DAC - Decentralized Autonomous Community).

Los detalles de la gobernabilidad de la organización serán redactados en la Constitución, pero de manera resumida son los siguientes.

Usuarios

Los usuarios del sistema tendrán KMS, equivalentes a acciones en una organización. Los KMS servirán como votos para la toma de decisiones en la organización. Los usuarios podrán votar ellos mismos o delegar sus votos a terceros (proxies).

Cualquier usuario podrá proponer cambios mediante referéndum.

Usuarios podrán proponer y realizar actividades (como asistir a eventos, realizar tareas y gestiones que necesita la organización, o realizar los cambios aprobados en los referéndum) con su compensación en KMS correspondiente.

Una vez aprobados, la cantidad correspondiente será bloqueada en el FOO y el usuario podrá realizar dicha actividad. Una vez terminada, el consejo podrá confirmar que el usuario ha realizado la actividad y liberar los fondos para pagar al usuario.

Financiación

La organización se financia generando inflación. Se permite que puntualmente un usuario añada por su cuenta un presupuesto adicional para realizar una tarea en concreto.

El primer año habrá un inflación del 20% para fomentar las primeras actividades, el segundo año una inflación del 10% y posteriores años habrá una inflación del 5% anual, aunque la cantidad final será votada, siendo un mínimo de 1% y un máximo de 7%. La inflación se ejecutará creando la proporción diaria correspondiente de KMS y distribuyendolos en la siguientes cuentas:

- FOO (fondo operativo de la organización). 85% de la inflación. Fondo para costear todas las operaciones de la organización
- FC (fondo para sueldos del comité). 5% de la inflación. Fondo para costear los sueldos del comité ejecutivo.
- FR (fondo de reservas). 10% de inflación. Fondo que puede utilizar el comité ejecutivo con un 51% de sus votos sin consultar previamente al resto de usuarios.

Comité ejecutivo

La organización será administrada por el comité ejecutivo formado por 5 usuarios (personas físicas o entidades), que son votados por los usuarios con KMS. Para que un usuario se presente al comité tendrá primero que “bloquear” una cantidad definida de KMS (50.000KMS) para garantizar que el candidato quiera defender los intereses generales de la organización.

El candidato también indicará la remuneración en KMS por ciclo que desea percibir a cambio de su labor, pero esta nunca podrá exceder el máximo indicado en la constitución.

Legalidad

Es importante anotar que una DAC aún no está reconocida como una organización en la legislación vigente, por lo que legalmente tener KMS no da derecho de propiedad en la organización. Simplemente permiten un formato de organización entre las partes.

Aunque no es necesario, se estudiará la posibilidad que KMS.PLUS se de alta como “Asociación” u otro tipo de entidad legal. Sólo se hará si dicha estructura se pueda adoptar con la gobernabilidad planteada en este documento.

KMS.plus se registrará a fecha 31 de diciembre el número total de KMS de cada usuario, así que el valor en euros equivalente, con el objetivo de facilitar a cada usuario registrar en Hacienda el valor de sus tokens a fin de ejercicio, cumpliendo así con la legislación vigente de criptomonedas en España.

Plataforma de socios

A través de una web (socios.kms.plus), los usuarios podrán realizar todas las tareas relacionadas con la gobernabilidad de la organización incluyendo:

- Firmar la constitución
- Presentarse como candidato y votar a candidatos
- Presentar propuestas de trabajo, referéndum y votar.
- Organizar reuniones audiovisuales

Sistema de votación

Cada ciclo del comité ejecutivo es de 15 días naturales. Al finalizar cada ciclo se realiza el pago a cada miembro por el ciclo y se recalculan los votos. De esta manera, automáticamente se mantiene el mismo comité o entran y salen candidatos.

Tipo de acciones del comité

Las acciones del comité pueden ser de tres tipos, según su riesgo y por ello tienen diferentes requisitos para su ejecución.

Riesgo alto

Para realizar una acción de riesgo alto es necesario la firma de todos los miembros del comité excepto de uno. Estar tareas son: (*pendiente de añadir más*)

- Realizar cambios en la constitución
- Expulsar a un miembro del consejo por motivos justificables o no.

Riesgo medio

Para realizar una acción de riesgo medio es necesario la firma la mayoría (>50%) del comité. Estas tareas son: (*pendiente de añadir más*)

- Cambiar la inflación para los siguientes ciclos
- Realizar pagos a terceros en euros o KMS (no usuarios)
- Asignar propuestas de trabajo a un usuario en concreto

Riesgo bajo

Para realizar una acción de riesgo bajo es necesario la firma de un sólo miembro del comité.

Estas tareas son: (*pendiente de añadir más*)

- Marca un trabajo como realizado. Acto que liberará los fondos reservados al mismo y realizará la transferencia correspondiente.

Gestión de permisos (borrador)

Diferenciamos entre el proveedor de un dato (el que lo proporciona) y el dueño de un dato, ya que no tiene porqué coincidir.

La cuenta kmseosguards tendrá los siguientes permisos:

- owner: Con un umbral requerido de 5
    - cuentadueño01@active (+1)
    - cuentadueño02@active (+1)
    - cuentadueño03@active (+1)
    - cuentadueño04@active (+1)
    - cuentadueño05@active (+1)
    - cuentadueño06@active (+1)
    - cuentadueño07@active (+1)
    - cuentadueño08@active (+1)
    - cuentadueño09@active (+1)
- active Con un umbral requerido de 5
    - kmseosguard@eosio.code (+5)
    - cuentadueño01@active (+1)
    - cuentadueño02@active (+1)
    - cuentadueño03@active (+1)

- cuentadueño04@active (+1)
- cuentadueño05@active (+1)
- cuentadueño06@active (+1)
- cuentadueño07@active (+1)
- cuentadueño08@active (+1)
- cuentadueño09@active (+1)

Se podrán escribir en la cadena registros de “revokedata”. El “revokedata” tendrá que estar firmado por el proveedor del dato o por el kmseosguard para ser válido.

Antes que poder acceder a cualquier dato kmseosguard tiene que verificar que no hay ningún registro de “revokedata” para ese dato. Si lo hay, no podrá realizar la transacción.

De esta manera para acceder a un dato será necesario tener el permiso del guardia y del proveedor de la información. Cualquiera de los dos puede “revocar” un acceso, con el objetivo de poder “eliminar” el acceso a un dato si el dueño lo solicita en un futuro.

Para prevenir ataques se pueden incluir retardos de pocos segundos antes de cualquier pago, para que los “Automated External Validators” pueda verificar que la transacción no es fraudulenta.

Fechas (borrador)

1. Q1

   Creación del grupo de trabajo que involucre a la mayor parte de participantes del sector posible, definir el diseño general, reglas a aplicar, y crear los primeros prototipos.

   Lanzamiento de la DAC a Jungletestnet

2. Q2

   Segunda fase de desarrollo. Lanzamiento a la Jungletestnet de EOS.

   Lanzamiento de la DAC a la mainnet.

3. Q3

   Lanzamiento a la mainnet de EOS e inicio de la ICO.