Uso de Smart Contracts e IPFS para la Gestión Segura de Datos de Acceso a Zonas Restringidas Vehiculares

Carles Anglés-Tafalla, Alexandre Viejo, Jordi Castellà-Roca
Universitat Rovira i Virgili, Departament d'Enginyeria Informàtica i Matemàtiques
Av. Països Catalans 26, E-43007 Tarragona, Spain
{carles.angles, alexandre.viejo, jordi.castella}@urv.cat

***Resumen*—En los últimos años, la implementación de áreas restringidas para vehículos (por ejemplo, Zonas de Bajas Emisiones o Zonas de Tarificación por Congestión) ha demostrado ser efectiva para abordar la congestión del tráfico urbano y la contaminación ambiental. No obstante, los sistemas que controlan dichas restricciones presentan problemas de privacidad, derivados del uso indiscriminado de cámaras, y dependencia en entidades centralizadas para procesos de tarificación y cobro. Aunque en la literatura han aparecido propuestas que descentralizan estas dependencias mientras se protege la privacidad de sus usuarios, el uso de herramientas como los *smart contracts* provoca que los datos de acceso de los usuarios se publiquen en un *public ledger* (i.e. blockchain) pudiendo dar pie a procesos de re-identificación. Siguiendo este paradigma descentralizado, en este artículo proponemos un sistema para la gestión de acceso vehicular a zonas restringidas que minimiza la cantidad de información que gestionan los *smart contracts*, reduciendo así los datos publicados en el blockchain, y complementado con un repositorio distribuido que almacena la extensión de estos datos garantizando su protección y control de acceso.**

***Index Terms*—Áreas restringidas vehiculares, Smart Contracts, IPFS, Privacidad, Seguridad.**

I. Introducción

Las Zonas de Bajas Emisiones (*LEZ*) y las Zonas de Tarificación por Congestión (*CCZ*), son áreas donde se aplican restricciones de acceso a vehículos en función de sus emisiones o de la densidad del tráfico, respectivamente. En los últimos años, estos mecanismos se han consolidado como esenciales para abordar la congestión del tráfico urbano y el impacto que esta ejerce sobre la contaminación ambiental en las grandes ciudades. La significativa proliferación de las LEZs y las CCZs en países europeos[1], junto con la intención de países como España[2] para legislar en su favor, constituye una prueba fehaciente de su impacto e importancia.

En este escenario, de acuerdo con la Transport Decarbonisation Alliance[3], la adopción controles de acceso automatizados, basados en redes de cámaras con reconocimiento automático de matrículas (ANPR), se ha convertido en el método preferido en los grandes núcleos urbanos para controlar el cumplimiento de las restricciones impuestas en este tipo de zonas. El funcionamiento de estos sistemas, ejemplificado en casos como los de Londres [1], Barcelona[4] o Estocolmo[5], se basa en fotografiar y reconocer indiscriminadamente las matrículas de los vehículos que circulan por el área restringida (*RA*), de modo que la entidad central que recibe los datos es capaz de determinar y cobrar las tarifas correspondientes.

Estos ejemplos muestran que las implementaciones actuales siguen un modelo intrusivo que permite a la entidad al control de la zona restringida identificar a los usuarios cada vez que sus vehículos se acercan alguna infraestructura del sistema. Este paradigma compromete la privacidad de aquellos que interactúan con el sistema y pone de manifiesto la necesidad de sistemas de control alternativos que gestionen los accesos de una manera más respetuosa con la privacidad sus usuarios.

En añadido a esta problemática, dichos sistemas también presentan una inherente centralización estructural de las entidades que controlan las infraestructuras, tarifican los accesos y cobran las tarifas. Estas entidades se convierten en un punto crítico de la arquitectura al constituir un *single point of failure* que pone en riesgo la seguridad y disponibilidad del sistema.

En la era emergente del *Internet-of-Vehicles (IoV)*, los vehículos de última generación se establecen como entidades inteligentes, equipados con sensores, cámaras, unidades de cómputo y comunicaciones *Vehicle-to-Everything* (V2X) [2]. Las nuevas capacidades de estos vehículos abren la puerta a la integración de tecnologías que permitan hacer frente los problemas de centralización identificados anteriormente.

Entre estas tecnologías, los *Smart Contracts* [3], junto con el subyacente *public digital ledger* descentralizado conocido como Blockchain, se han consolidado como herramientas esenciales para de diseñar nuevos modelos descentralizados que permiten el acuerdo de transacciones de recursos arbitrarios, tales como interacciones entre vehículos e infraestructuras, sin necesidad de entidades de confianza. Aplicadas a entornos vehiculares, y en particular a controles de acceso LEZ y CCZ, estas tecnologías podrían motivar el diseño de una solución descentralizada que de respuesta a los problemas de privacidad y estructurales identificados en la literatura.

I-A. Antecedentes

En la última década, se han realizado importantes esfuerzos de investigación en lo referente a los problemas de privacidad en controles de acceso a zonas restringidas vehiculares, como LEZs y CCZs. Inicialmente, las propuestas seguían la tendencia de trabajos como [4], [5], [6], [7], en los cuales el cálculo de tarifas depende de un Proveedor de Servicios (SP) centralizado que utiliza datos de localización recogidos

[1]Urban Access Regulations, http://urbanaccessregulations.eu/userhome/map
[2]Law on Climate Change and Energy Transition, https://www.boe.es/eli/es/l/2021/05/20/7
[3]Transport Decarbonisation Alliance (TDA), www.tda-mobility.org
[4]Barcelona Metropolitan Area - LEZ, https://www.zbe.barcelona/
[5]Stockholm charging scheme, https://miljobarometern.stockholm.se/trafik/

y enviados de forma segura y anónima por las Unidades a Bordo (OBUs) de los vehículos. No obstante, estas soluciones descuidan la privacidad en su sistema antifraude, que dota al SP de una red de checkpoints ANPR con el fin de cotejar los datos enviados por las OBUs. Sistema que solo es viable si la ubicación de los checkpoints es desconocida, resultando en un SP omnisciente si el número de checkpoints se incrementa para evitar que los vehículos los evadan intencionalmente [8].

La identificación de este problema de privacidad ha propiciado la consolidación de un nuevo enfoque más refinado, introducido inicialmente en [9] y luego adoptado por [10], [11], [12], que promueve la preservación de la privacidad de los usuarios por defecto, a menos que estos incurran en prácticas fraudulentas. Este planteamiento propone un proceso de autenticación mediante comunicación de corto alcance cada vez que un vehículo interactúa con las infraestructura del sistema, recurriendo al ANPR únicamente si el proceso no se completa o se omite. Estas propuestas protegen la privacidad de los usuarios durante el proceso de autenticación con diferentes planteamientos, tales como esquemas de firmas de grupo [9], seudónimos renovables [10], [11] o pruebas de conocimiento nulo [12]. No obstante, las anteriores propuestas presentan una fuerte dependencia en entidades centralizadas, habitualmente un SP, para gestionar partes críticas de sus sistemas, como validar pruebas de acceso, calcular las tarifas asociadas y gestionar los cobros. Esta dependencia supone un aspecto estructural común a mejorar, revelando un "single point of failure" que hace a estos sistemas más vulnerables a fallos y ataques, comprometiendo su seguridad y disponibilidad.

Con el fin de eliminar la centralización en estos elementos, [13] propone una mejora descentralizada sobre [10]. Dicha propuesta se basa en el uso de *Smart Contracts* para gestionar los accesos vehiculares como transacciones en el Blockchain, permitiendo determinar y cobrar las tarifas de los accesos de forma autónoma, sin intervención de terceros. Aunque esta propuesta aborda con éxito los problemas de centralización identificados en la literatura, el uso de un *public ledger* introduce nuevos retos de privacidad, ya que los datos de acceso/salida de los vehículos se publican pseudonimizados en el blockchain como *open data*, sin restricciones ni control sobre su acceso.

I-B. Contribuciones y plan del artículo

Teniendo en cuenta los problemas de centralización identificados en la literatura y considerando el potencial de los *smart contracts* junto con la tecnología de blockchain, en este artículo, siguiendo la línea marcada por [13], proponemos un nuevo sistema descentralizado para la gestión de acceso vehicular a zonas restringidas. Nuestra solución mejora el almacenamiento y la gestión de los datos de movilidad generados por los vehículos durante los accesos/salidas, optimizando así la privacidad y seguridad de los mismos.

Bajo esta premisa, nuestro sistema minimiza la cantidad de información usada por los *smart contracts* para el cálculo de tarifas, reduciendo así los datos publicados en el blockchain y con ello el riesgo a la reidentificación de los usuarios. Paralelamente, y como extensión de los datos de tarificación publicados en el blockchain, el sistema es capaz de generar datos precisos sobre los accesos y salidas de los vehículos, almacenándolos en un repositorio distribuido alternativo garantizando su protección y control de acceso.

En resumen, la propuesta ofrece las siguientes propiedades, no cubiertas simultáneamente en otras propuestas:

- El sistema descentraliza, mediante *smart contracts* y su red Blockchain, las entidades responsables de registrar los accesos de vehículos, calcular y cobrar las tarifas.
- El sistema preserva la privacidad de los usuarios a menos que estos no sigan el protocolo establecido, en cuyo caso pueden ser identificados y su anonimato revocado.
- El sistema captura y gestiona datos sobre las entradas y salidas de vehículos en zonas restringidas, asegurando su almacenamiento seguro en un repositorio distribuido. Gracias al soporte de blockchain, el sistema monitoriza y regula el acceso a estos datos de manera efectiva.

El resto del artículo está organizado de la siguiente manera. La sección II introduce la nueva propuesta. La sección III formaliza los protocolos que sustentan el sistema propuesto. Finalmente, la Sección IV recoge las conclusiones.

II. Modelo del Sistema

II-A. Actores

Nuestro sistema involucra a los siguientes actores: i) Administrador del Área Restringida (*RAA*); ii) Vehículo (*V*); iii) Punto de Control de Acceso (*ACP*); iv) Smart Contract de la Área Restringida (*SC*); v) Repositorio de datos (*DR*); y vi) Consumidor de datos (*DC*).

- Administrador del Área Restringida (*RAA*): Esta entidad gestiona la LEZ/CCZ y hace cumplir las restricciones impuestas a los vehículos. Entre sus funciones destacan la emisión de credenciales al resto de entidades, desplegar el *Smart Contract* que gestiona el área restringida y definir las categorías de emisión para los vehículos.
- Vehículo (*V*): Son las entidades que acceden y circulan por las áreas restringidas supervisadas por la RAA. Se asume que cada V está equipado con una Unidad de a Bordo (*OBU*) a prueba de manipulaciones con capacidades criptográficas, tecnología GPS, 4G y un sistema de comunicación de corto alcance (por ejemplo, Bluetooth, Zigbee o DSRC).
- Punto de Control de Acceso (*ACP*): Son infraestructuras físicas que controlan los accesos y salidas de la LEZ/CCZ. Para este propósito, están equipados con una cámara, GPS, comunicación de corto alcance y acceso a Internet. Cada ACP está bajo el control del Proveedor de Servicios (*SP*) a cargo de su configuración, despliegue y mantenimiento. Los múltiples ACPs de una área restringida pueden ser controlados por distintos SPs.
- Smart Contract (*SC*): es un protocolo de transacción programado para incluir datos de acceso a la LEZ/CCZ en el blockchain, permitiendo verificar, tarificar y pagar dichos accesos por medio de criptomonedas.
- Repositorio de datos (*DR*): Es un sistema de almacenaje de datos distribuido (i.e. IPFS) donde los ACPs suben datos sobre accesos de los Vs como extensión de los datos de tarificación publicados en el blockchain.
- Consumidor de datos (*DC*): Son entidades interesadas en acceder a la extensión de los datos almacenados en DR.

II-B. *Visión general del sistema*

La figura 1 ilustra el esquema general del sistema de control de acceso propuesto. En este escenario, al entrar o salir de la zona restringida, los Vs interactúan con los ACP a través de un sistema de comunicación de corto alcance (como DSRC, Zigbee or Bluetooth), completando un proceso de autenticación seguro. Con este proceso, ambas partes obtienen recíprocamente un recibo firmado digitalmente que contiene las pruebas de acceso o salida, según corresponda. Durante todo el proceso, se preserva el anonimato de V mediante el uso de un alias temporal, que puede cambiarse a voluntad para evitar que otras entidades vinculen los diferentes accesos realizados con un determinado alias. Por el contrario, si el proceso de autenticación se manipula o se omite debido al mal comportamiento de V, el ACP tomará una foto de la matrícula del V, permitiendo su identificación y pudiendo así reportar su comportamiento ante el RAA.

A modo de repositorio, en cada validación de salida, el ACP obtiene y recopila información sobre V (i.e. ID de acceso, timestamp de entrada y salida, localización de entrada y salida, categoría de emisiones, etc.). Estos datos son cifrados, para su securización y control de acceso, y almacenados en un repositorio descentralizado alternativo como IPFS.

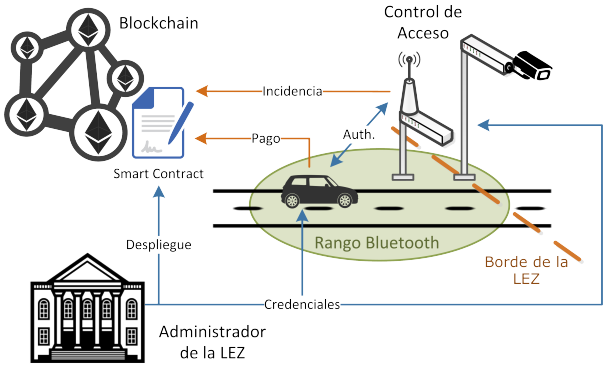

Figura 1. Esquema general del sistema

Al salir de la zona restringida, V dispone de un tiempo predeterminado (horas o incluso días) para abonar las tarifas de acceso asociadas. Para ello, V invoca el método de pago del SC usando los datos acordados con los ACPs durante la entrada y salida como parámetros. Para evitar publicar datos precisos sobre sus movimientos en la zona restringida, V solo envía el tiempo circulado, la franja horaria y su categoría de emisiones. Entonces, la lógica del SC realiza dos funciones clave: i) calcula el importe del pago a partir los datos proporcionados y los precios de acceso publicados en la blockchain; y ii) transfiere de manera autónoma el importe en criptomonedas desde la cartera digital de V a las carteras de los SPs que controlan los ACPs implicados en la entrada y salida de V.

Transcurrido el tiempo fijado por RAA para abonar las tasas, los ACPs implicados en el acceso o salida de V verifican, consultando el blockchain, si los datos de la transacción y el pago se han validado correctamente. Si se detecta alguna irregularidad, los ACPs pueden abrir una incidencia llamando al método del SC designado para ello, pudiendo publicar su copia de la prueba de acceso/salida firmada digitalmente por V. La lógica del SC impide la publicación de incidencias si no se ha agotado el tiempo para abonar las tasas. A través de la publicación de la prueba de acceso/salida en el blockchain, solo el RAA posee la capacidad de identificar al propietario de V e implementar medidas punitivas si fuera necesario.

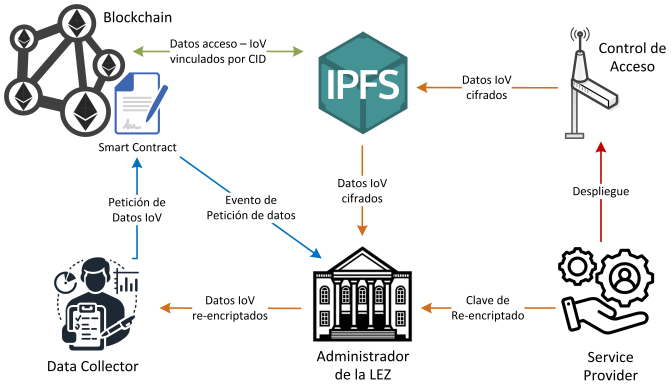

Figura 2. Esquema general del acceso a los datos extendidos

En la solución propuesta, los Vs publican en el blockchain la información mínima para tarificar sus accesos. Si en algún momento una entidad (DC), debidamente autorizada por RAA, desea obtener información extendida sobre esos datos (Figura 2), debe publicar una petición de acceso a datos en el blockchain por medio del correspondiente método del SC. Cuando la petición queda registrada, el RAA recopila todos los IDs de los accesos que solicita el DC consultando el blockchain, y descarga su versión extendida del repositorio en el IPFS. Entonces, por petición del RAA, los SPs implicados en dichos accesos generan claves de reencriptado para el DC que solicita los datos. Con esas claves de reencriptado en su poder, RAA reencripta los datos descargados del IPFS para DC sin tener acceso a los datos en claro. Finalmente, el DC puede descifrar los datos reencriptados usando su clave privada.

Cabe destacar que el sistema permite una gestión de roles que regula la cantidad y el nivel de generalización de los datos a los que un DC puede acceder. El RAA es el encargado de verificar si los datos solicitados están disponibles para el rol del DC que los solicita. Además, tanto la información relativa a los DCs como sus peticiones de acceso a datos quedan registradas en la blockchain, siendo accesibles para consulta pública.

III. Descripción del protocolo

Esta sección formaliza los protocolos que componen el sistema propuesto dando los detalles suficientes para su implementación. Estos protocolos son: *Configuración de la OBU*, *Adquisición de Tokens*, *Acceso/Salida*, *Pago*, *Verificación de Pago*, *Renovación del alias temporal*, y *Acceso al repositorio de datos*.

III-A. *Configuración de la OBU*

El primer protocolo configura las OBUs de los vehículos V, para obtener las credenciales necesarias para una interacción segura el resto de actores del sistema. Con este fin, la OBU

establece un canal seguro, i.e. TLS, con el RAA y proporciona la información de V, incluyendo el número de matrícula, el fabricante del coche, el modelo, etc. Se asume que la OBU no puede ser manipulada para enviar información falsa y que la RAA (como entidad gubernamental) puede verificar y obtener los datos de V y su propietario. Con esta información, RAA genera un alias pseudo-aleatorio temporal β y lo almacena vinculado con la información de V y su dueño. Seguidamente, RAA envía β al propietario de V por un canal alternativo, i.e. email, SMS o un sistema electrónico de autenticación público[6].

Una vez el propietario de V recibe β y lo introduce en la OBU, realiza los siguientes pasos:

a) V genera una pareja de claves (sk_V, pk_V).
b) V genera una solicitud de certificado $CSR(pk_V)$ para su clave pública, que incluye β.
c) V envía la petición de certificado $CSR(pk_V)$ a RAA.

Cuando RAA recibe un $CSR(pk^V)$ válido:

a) RAA verifica la validez de β en $CSR(pk_V)$.
b) RAA recupera los datos de V vinculados a β.
c) RAA emite un certificado $Cert(pk_V)$, incluyendo β en el campo *CommonName* y la categoría de emisiones del vehículo cat como extensión del certificado.
d) RAA envía el certificado $Cert(pk_V)$ a V.
e) V verifica la validez de $Cert(pk_V)$ con $Cert(pk_{RAA})$.
f) V almacena de forma segura $Cert(pk_V)$ y (sk_V, pk_V).

Finalmente, V genera una cartera digital W_V o, dependiendo de las preferencias en privacidad, un grupo de ellas $W_V^1, \ldots, W_V^n$, siguiendo las especificaciones de una red compatible con la Ethereum Virtual Machine (EVM).

III-B. Adquisición de Tokens para la cartera

A fin de pagar las tarifas de acceso y las comisiones de la red blockchain, los Vs deben adquirir criptomonedas, como divisa en el sistema propuesto. Para este propósito, los Vs hacen uso de servicios online[7] para realizar la compra y transferencia de criptomonedas a partir de mecanismos de pago clásicos (p. ej., tarjeta de crédito o transferencia bancaria). No obstante, este proceso puede incurrir en el riesgo de vincular las carteras digitales de los Vs a cuentas bancarias de sus propietarios, comprometiendo su privacidad.

Para evitar este riesgo, V puede generar una cartera temporal W_V^T en la que se transfieren las cripomonedas adquiridas. Luego, V solicita a un servicio de mixing[8] M que transfiera sus fondos en W_V^T a su grupo de carteras $W_V^1, \ldots, W_V^n$. Mediante el proceso de mixing, M ofusca el vinculo entre carteras origen y destino, evitando que el vendedor pueda asociar al comprador con sus transacciones en el blockchain.

III-C. Acceso

Este protocolo comienza en el momento que V accede en la zona restringida y establece un canal seguro con autenticación bilateral (p. ej., TLS) con el ACP a través del sistema de comunicación de corto alcance. Este proceso implica el intercambio de certificados, i.e. $Cert(pk_V)$ y $Cert(pk_{ACP})$. Entonces se realizan los siguientes pasos:

a) V genera un aleatorio de 64 bits δ_V como ID de acceso.
b) V prepara los datos de acceso $data_{in}$ = $\{\delta_V, \beta, t_V^{in}, pos_V^{in}\}$ y genera su firma digital $\sigma_V(data_{in})$. Siendo t_V^{in} el timestamp de entrada, y pos_V^{in} la posición de entrada.
c) V envía $data_{in}$ y $\sigma_V(data_{in})$ al ACP.
d) ACP recibe los datos de acceso, verifica la validez de $\sigma_V(data_{in})$ y si los datos en $data_{in}$ son correctos.
e) Si todo es correcto, ACP genera un aleatorio de 64 bits δ_{ACP} y calcula el ID de acceso δ_{in} = $\{\delta_V \| \delta_{ACP}\}$. En caso contrario, ACP hace una foto de la matrícula de V y detiene el protocolo.
f) ACP genera una prueba de acceso $proof_{in}$ = $\{SP_{in}, \delta_{in}, pos_V^{in}, t_V^{in}, \sigma_V(data_{in})\}$, donde SP_{in} es ID del SP propietario del ACP.
g) ACP envía $proof_{in}$ y su firma $\sigma_{ACP}(proof_{in})$ a V.
h) ACP almacena localmente $proof_{in}$, junto con la categoría de emisiones cat de V (contenida en $Cert(pk_V)$).
i) V recibe la prueba de acceso de ACP.
j) V verifica los datos de $proof_{in}$ y la firma $\sigma_{ACP}(proof_{in})$. Si es correcto, se almacena localmente hasta que se completa el protocolo de salida.

III-D. Salida

De forma similar al acceso, V debe formalizar su salida de la zona restringida. Para ello, V establece conexión segura con un ACP, que implica autenticación bilateral y obtención recíproca del certificado de la parte contraria:

a) V recupera $proof_{in}$ y $\sigma_{ACP}(proof_{in})$.
b) V prepara sus datos de salida $data_{out}$ = $\{proof_{in}, \sigma_{ACP}(proof_{in}), t_V^{out}, pos_V^{out}\}$ y computa su firma digital $\sigma_V(data_{out})$.
c) V envía $data_{out}$ y $\sigma_V(data_{out})$.
d) ACP recibe la petición de salida y, primero verifica las firmas $\sigma_V(data_{out})$ y $\sigma_{ACP}(proof_{in})$; seguidamente, verifica la validez de los datos en $data_{out}$.
e) Si alguna verificación falla, ACP detiene el protocolo y toma una foto de la matrícula de V cuando detecta su paso con el sensor de presencia. Luego, el ACP envía de manera segura la foto al RAA con fines punitivos, y acto seguido elimina la foto.
f) Si todas las verificaciones son correctas, el protocolo continua. ACP prepara los datos a almacenar en el IPFS, i.e. $data_{ipfs}$ = $\{\delta_{in}, t_V^{in}, t_V^{out}, pos_V^{in}, pos_V^{out}\}$.
g) ACP cifra $data_{ipfs}$ con la clave publica de su SP (pk_{SP}) de Proxy re-encryption [14], obteniendo $cdata_{ipfs}$ = $encrypt_{SP}(data_{ipfs})$.
h) ACP calcula localmente el ID de contenido (*CID*) donde se indexaran los datos en el IPFS[9], usándolo como ID de salida $\delta_{out} = hash_{ipfs}(cdata_{ipfs})$.
i) ACP prepara la prueba de salida $proof_{out}$ = $\{\delta_{out}, SP_{out}, data_{out}, \sigma_V(data_{out})\}$ y genera su firma digital $\sigma_{ACP}(proof_{out})$.
j) ACP almacena localmente $proof_{out}$, junto con la categoría de emisiones cat (contenida en $Cert(pk_V)$).
k) ACP envía $proof_{out}$ y $\sigma_{ACP}(proof_{out})$ a V como prueba de su tránsito por la zona restringida.
l) V verifica y almacena temporalmente la prueba de tránsito $proof_{out}$ y $\sigma_{ACP}(proof_{out})$.

[6] Cl@ve - Electronic Identity for the Administration - https://clave.gob.es
[7] My Ether Wallet - https://ccswap.myetherwallet.com/
[8] ETH-Mixer, https://ethereumixer.to/
[9] IPFS - CID local generator - https://github.com/alanshaw/ipfs-only-hash

Una vez finalizado el protocolo, el ACP sube los datos de tránsito cifrados $cdata_{ipfs}$ al servicio de almacenaje IPFS, coincidiendo el puntero CID recibido con el ID de salida δ_{out} calculado durante el protocolo. Los datos en $cdata_{ipfs}$, almacenados como repositorio, pueden subirse cifrados en bloques con diversos niveles de generalización, a fin de gestionar diversos grados de privacidad durante su divulgación.

III-E. Pago

Tras su salida, V dispone de un plazo de tiempo, desde horas a días, determinado por RAA para efectuar el proceso de pago. Este proceso está orquestado por smart contracts implementados sobre una red descentralizada de blockchain, eliminando la necesidad de cualquier autoridad centralizada.

Para iniciar el proceso de pago, V invoca el método *pay_access* del SC, subiendo como parámetros las ID de acceso y salida δ_{in} y δ_{out}, el dia, la franja horaria ID_t, el tiempo circulado t_V^f = (t_V^{out}-t_V^{in}), la categoría de V cat, SP_{in}, SP_{out} contenidos en $proof_{out}$ y en $Cert(pk_V)$. Con estos datos, el SC realiza las siguientes operaciones on-chain:

a) SC consulta los precios de la zona restringida publicados en el blockchain para la categoría de emisiones cat.
b) SC computa la tarifa de V acorde al t_V^f, la franja horaria ID_t y el dia para esa cat.
c) SC consulta en el blockchain la $address$ de las carteras digitales de los SPs propietarios de los ACPs implicados en la entrada y salida a partir de SP_{in} y SP_{out}.
d) SC transfiere la cantidad de criptomonedas correspondiente a la tarifa desde la cartera digital W_V a la W_{SP} de cada SP implicado. Si W_V no tiene fondos suficientes, se transfieren todos los fondos y se actualiza la deuda restante. V puede repetir el proceso, incluso con otras carteras, hasta subsanar la totalidad de la tarifa.
e) SC almacena los datos de la transacción, indexados por δ_{out}, junto con la deuda restante $debt$ y el resto de parámetros subidos. Independientemente del resultado del proceso, la transacción se registra en el blockchain.

Se debe matizar que el RAA dispone de permisos en un método específico del SC para actualizar la lista de precios de las tarifas de la zona restringida. Cabe destacar también que la información almacenada en IPFS queda vinculada a la transacción registrada en el blockchain, ya que CID = δ_{out}.

III-F. Verificación del Pago

Al expirar el plazo establecido por RAA para abonar las tarifas, los ACP implicados en el proceso verifican si V ha completado el protocolo de pago, verificando el estado del acceso δ_{out} en el blockchain (δ_{in} para el ACP de entrada):

a) ACP recupera $proof_{out}$ y la cat del acceso a verificar.
b) ACP verifica que la transacción con ID δ_{out} existe en el blockchain y obtiene su estado llamando al método *get_access* del SC.
c) ACP comprueba que el campo $debt$ es "0", y que los datos obtenidos son consistentes con los de su copia $proof_{out}$.
d) Si alguna de las condiciones anteriores no se cumple, ACP usa el método *open_incidence* del SC para reportar la incidencia. Con esa acción, la prueba de tránsito $proof_{out}$, que contiene la firma digital de V $\sigma_V(data_{out})$, se envía como parámetro.
e) ACP elimina su copia $proof_{out}$. En este punto la copia ya no es necesaria, bien porque el pago se ha completado correctamente o porque los datos del acceso de V se han publicado en el blockchain como incidencia.

A su vez, la lógica del SC verifica si se ha superado el plazo habilitado de pago par reportar una incidencia, usando t_V^{out} en $proof_{out}$ como referencia. Una vez publicados en el blockchain los datos de la prueba de tránsito $proof_{out}$, el RAA dispone de suficiente información para identificar al propietario del vehículo con alias β.

III-G. Renovación del alias temporal del vehículo

Aunque la identidad de V esta oculta tras su alias temporal β y la $address$ de su cartera digital, estos elementos puede llevar a la re-identificación del propietario de V si se usan reiteradamente. Para evitarlo, un V puede solicitar un nuevo alias β^* al RAA para prevenir que se puedan vincular subsiguientes accesos. El cambio del alias β implica nuevas claves criptográficas (sk_V, pk_V) y certificado $Cert(pk_V)$, ya que β se incluye en campo *CommonName*.

En caso de un V usando una única cartera digital para sus interacciones con el SC, es recomendable crear también una nueva cartera digital W_V^* con el fin de renovar la $address$ de la cartera en las transacciones que se publican en el blockchain. En caso de no haber agotado todos los fondos de su vieja cartera, V puede transferir los fondos de W_V a W_V^* haciendo uso de los servicios ofuscación de M, evitando que ambas *address* se puedan vincular.

III-H. Acceso al repositorio de datos

Al completar el protocolo de salida, los ACPs almacenan datos concretos sobre el tránsito de los vehículos en la zona restringida. Estos datos, extensión de los datos de tarificación publicados en el blockchain, i.e. tiempos y posiciones exactas de entradas y salidas, se encuentran almacenados en un repositorio descentralizado (i.e. IPFS) y protegidos mediante cifrado de accesos no autorizados.

Para obtener autorización, DC se registra como consumidor de datos en el sistema. En primer lugar, DC genera una pareja de claves (sk_{DC}, pk_{DC}) y una cartera digital W_{DC}. Luego, envía a RAA una solicitud, indicando los datos de la entidad, la clave pública pk_{DC} y la $address$ de W_{DC}. Entonces, RAA hace lo siguiente:

a) RAA verifica la entidad y asigna un rol en función de los datos y nivel de generalización al que tendrá acceso.
b) RAA publica en el blockchain los datos de DC, su rol y $address$. El SC dispone un método restringido para RAA con esta funcionalidad.
c) RAA emite un certificado $Cert(pk_{DC})$, que incluye $address$ y rol como extensiones.
d) Al recibir $Cert(pk_{DC})$, DC verifica su validez.

Para acceder a los datos una vez registrado, DC hace una petición llamando al método *get_data_by_date* del SC indicando como parámetro la fecha de los registros a obtener. SC puede disponer de otros métodos para búsquedas más específicas. Para este proceso se realizan los siguientes pasos:

a) SC verifica que la $address$ de DC está registrada y que su rol le permite acceder a los datos.
b) SC almacena la petición, quedando registrada en el blockchain, y emite un evento de acceso a datos.

c) Al captar el evento, RAA busca en el blockchain los accesos registrados en dicha fecha y obtiene sus IDs δ_{out}.
d) RAA consulta en el blockchain los SPs implicados en cada acceso δ_{out}.
e) RAA descarga del IPFS los datos cifrados $encrypt_{SP}(data_{ipfs})$ acordes a su rol, usando los δ_{out} como CIDs.
f) RAA solicita claves de reencriptado para DC a los SPs.
g) Cada SP implicado, genera una rk_{sp-dc} usando su clave privada sk_{SP} y la clave pública del DC pk_{DC}.
h) Al recibir las claves, RAA reencripta con rk_{sp-dc} cada set de datos cifrados, obteniendo $encrypt_{DC}(data_{ipfs})$ en cada caso.
i) Al recibir los datos de RA, DC puede descifrar los datos usando su clave privada sk_{DC}.

Debe tenerse en cuenta que el IPFS pueden almacenar los datos de tránsito en bloques y con distintos niveles de precisión. El sistema servir los datos de entradas y salidas de los vehículos más o menos generalizados en función de los permisos que otorga el rol del DC.

IV. Conclusiones

Los actuales controles de acceso a zonas restringidas vehiculares que preservan la privacidad de sus usuarios ponen de manifiesto una clara dependencia hacia entidades centralizadas en procesos críticos como la verificación de accesos, tarificación y cobro de tarifas. Aunque en los últimos años han aparecido propuestas cuyo objetivo se centra en abordar este problema estructural hacia un modelo descentralizado, la introducción de herramientas como *smart contracts*, implementadas sobre un *public ledger* descentralizado, provoca que los datos de acceso y salida de los vehículos sean visibles al resto de nodos, permitiendo procesos de re-identificación.

En este artículo se ha presentado una nueva solución autónoma para gestionar el control de acceso en áreas restringidas vehiculares basada en *smart contracts*, en línea con el modelo descentralizado establecido en la literatura. El sistema propuesto minimiza la cantidad de información que gestionan los *smart contracts* durante la tarificación y pago de tarifas, reduciendo los datos publicados en el blockchain, y lo complementa con un repositorio distribuido que almacena la extensión de dichos datos garantizando su seguridad y control de acceso.

Agradecimientos

This research is supported by Project PID2021-125962OB-C32 "SECURING/DATA' funded by MCIN/AEI/ 10.13039/501100011033 and by "ERDF A way of making Europe"; by Project HERMES funded by INCIBE and the European Union NextGenerationEU/PRTR; and by Grant SGR2021-00115 funded by AGAUR, Generalitat de Catalunya.

Referencias

[1] G. Santos, "Urban congestion charging: a comparison between london and singapore," *Transport Reviews*, vol. 25, no. 5, pp. 511–534, 2005.
[2] X. Shen, R. Fantacci, and S. Chen, "Internet of vehicles [scanning the issue]," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 242–245, 2020.
[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.
[4] R. A. Popa, H. Balakrishnan, and A. J. Blumberg, "Vpriv: Protecting privacy in location-based vehicular services," in *18th USENIX Security Symposium*. USENIX Association, 2009.
[5] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens, "Pretp: Privacy-preserving electronic toll pricing." in *USENIX Security Symposium*, vol. 10, 2010, pp. 63–78.
[6] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "A group signature based electronic toll pricing system," in *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE, 2012, pp. 85–93.
[7] F. D. Garcia, E. R. Verheul, and B. Jacobs, "Cell-based privacy-friendly roadpricing," *Computers & Mathematics with Applications*, vol. 65, no. 5, pp. 774–785, 2013.
[8] S. Meiklejohn, K. Mowery, S. Checkoway, and H. Shacham, "The phantom tollbooth: Privacy-preserving electronic toll collection in the presence of driver collusion." in *USENIX security symposium*, vol. 201, 2011, pp. 1–16.
[9] R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras, J. Castella-Roca, and A. Viejo, "Time-based low emission zones preserving drivers' privacy," *Future Generation Computer Systems*, vol. 80, pp. 558–571, 2018.
[10] C. Anglès-Tafalla, J. Castellà-Roca, M. Mut-Puigserver, M. M. Payeras-Capellà, and A. Viejo, "Secure and privacy-preserving lightweight access control system for low emission zones," *Computer Networks*, vol. 145, pp. 13–26, 2018.
[11] S. Bouchelaghem and M. Omar, "Reliable and secure distributed smart road pricing system for smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1592–1603, 2018.
[12] V. Fetzer, M. Hoffmann, M. Nagel, A. Rupp, and R. Schwerdt, "P4tc—provably-secure yet practical privacy-preserving toll collection," *Proceedings on Privacy Enhancing Technologies*, vol. 3, pp. 62–152, 2020.
[13] C. Anglés-Tafalla, A. Viejo, J. Castellà-Roca, M. Mut-Puigserver, and M. M. Payeras-Capellà, "Security and privacy in a blockchain-powered access control system for low emission zones," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 580–595, 2022.
[14] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," *IEEE Transactions on Services Computing*, 2016.