Seguridad y Privacidad en un Sistema de Control de Acceso Distribuido para Zonas de Bajas Emisiones

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

***Resumen*—Las Zonas de Bajas Emisiones (LEZ) son áreas donde se aplican restricciones al acceso de vehículos contaminantes. Estas soluciones se han convertido en los mecanismos principales para hacer frente a la contaminación ambiental y congestión vehicular en grandes zonas urbanas. Los sistemas desplegados actualmente para controlar dichas restricciones hacen uso de redes de cámaras para identificar los vehículos que circulan por la zona restringida, suponiendo un riesgo para la privacidad de sus usuarios. Aunque en la literatura han aparecido propuestas más respetuosas con la privacidad que hacen un uso mínimo de las cámaras, todas ellas presentan un problema estructural común: dependen de entidades centralizadas para desplegar la infraestructura, gestionar los accesos de los vehículos y cobrar las correspondientes tarifas. Estas entidades suponen un *single point of failure* en el sistema que pone en riesgo su seguridad y disponibilidad. Para hacer frente a esta problemática, en este artículo proponemos un nuevo sistema totalmente distribuido y autónomo para gestionar los accesos a LEZs, que hace uso de los sistemas avanzados de detección y comunicación de los vehículos de nueva generación para evitar el despliegue de infraestructuras de control. Esto, combinado con un sistema de gestión descentralizado basado en smart contracts que procesa los accesos como transacciones de Blockchain, elimina cualquier dependencia hacia *third parties* centralizadas con ánimo de lucro en el proceso de control de acceso a las LEZs.**

***Index Terms*—Low emission zones, Smart cities, Privacy, Security, Smart Contracts, Blockchain.**

I. Introducción

En los últimos años, las Zonas de Bajas Emisiones (*LEZ*) y de Cargo por Congestión (*CCZ*), es decir, áreas definidas donde se aplican restricciones a los vehículos contaminantes, se han convertido en mecanismos imprescindibles para hacer frente a la congestión del tráfico urbano y el impacto que esta ejerce sobre la contaminación ambiental. Prueba de ello es la gran proliferación de estas medidas en los países Europeos[1] o su intención de adoptarlas en los próximos años, como en el caso de España[2].

Ante este escenario, en las grandes áreas urbanas se han desplegado controles de acceso automatizados que permitan cumplir las restricciones que imponen estas zonas. El funcionamiento de dichos sistemas se basa en redes de cámaras, e.g. Barcelona, Estocolomo[3] o Londres [1], cuyo propósito consiste en fotografiar indiscriminadamente la matrícula de los vehículos que circulan por la zona restringida. Entonces, a partir de un sistema de reconocimiento de matrículas (ANPR), se identifica a los vehículos y se determina la tarifa que se debe abonar de acuerdo con la normativa o restricciones aplicables a la zona.

Tal como se infiere de los ejemplos citados, el uso de estas estrategias resulta muy invasivo, ya que todos los vehículos son identificados cada vez se aproximan a una infraestructura de control. Esta situación supone un riesgo para la privacidad de los usuarios y revela la necesidad de sistemas de control alternativos que gestionen el tránsito de las LEZ o CCZ de un modo más respetuoso con la privacidad de aquellos circulan por ellas.

Además de la amenaza en lo que a privacidad se refiere, se han detectado aspectos estructurales a mejorar en los actuales controles de acceso. Más concretamente, los actuales sistemas presentan una clara dependencia hacia las entidades centralizadas que despliegan las infraestructuras, calculan las tarifas y detectan a usuarios fraudulentos. 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.

Recientemente, han entrado en escena nuevos paradigmas que permiten acordar de manera descentralizada transacciones de recursos arbitrarios, tales como interacciones entre vehículos e infraestructuras, a través de un *public open ledger* verificable llamado Blockchain, sin necesidad de recurrir a entidades centralizadas o de confianza. Esta tecnología, combinada con los sistemas de detección, radar, cámaras y comunicación que incorporan los vehículos de nueva generación, abre la posibilidad a la concepción de soluciones distribuidas totalmente autónomas que no dependen de *third parties* centralizadas ni de la necesidad desplegar equipamiento adicional, eliminando los costes de implementación y mantenimiento que estos lleva asociados.

I-A. Antecedentes

En la última década, se ha publicado un gran número de artículos como respuesta a los problemas de privacidad en controles de acceso a zonas restringidas en entornos vehiculares, tales como Zonas de Bajas Emisiones (LEZ), Peaje por Congestión (CCZ) y Peaje Electrónico (ERP).

Inicialmente estas propuestas [2], [3], [4], [5], [6], [7] estaban basadas en la unidad de a bordo de los vehículos (OBU), recopilando datos relevantes para el cómputo de tarifas; una *third party* centralizada, i.e. Proveedor de Servicios (SP), que verifica todo el proceso y cobra las tarifas convenidas; y una red de puntos de control basada en cámaras que registra las matrículas de los vehículos para evitar el fraude. No obstante, tal como se destaca en [5], este planteamiento solo es viable si

[1] Urban Access Regulations, http://urbanaccessregulations.eu/userhome/map

[2] Ley de Cambio Climático y Transición Energética, https://www.miteco.gob.es/es/cambio-climatico/participacion-publica/marco-estrategico-energia-y-clima.aspx

[3] Stockholm charging scheme, http://www.stockholm.se/trangselskatt

la ubicación de los puntos de control es secreto, volviéndose especialmente invasivo y poco respetuoso con la privacidad de los usuarios si el número de puntos de control es elevado para prevenir que los vehículos los eviten intencionadamente.

Desde que se identificó dicha problemática, se ha ido consolidado un nuevo paradigma desde que fue presentado por primera vez en [8] y posteriormente adoptado por [9], [10], [11], [12], el cual promueve que siempre se preserve la privacidad de los usuarios a no ser que estos intenten cometer fraude. Este planteamiento propone un proceso de autenticación cada vez que el vehículo se encuentra con alguna de las infraestructuras del sistema, fotografiando la matrícula del vehículo únicamente en caso de no completar o omitir dicho proceso. Partiendo de este planteamiento, estas propuestas protegen la privacidad de los usuarios durante el proceso de autenticación por medio de distintos mecanismos, tales como esquemas de firmas de grupo [8], [9], seudónimos renovables [10], [11] o pruebas de conocimiento nulo [12]. No obstante, la dependencia de dichas propuestas en *third parties* centralizadas a cargo de validar las pruebas de acceso, computar las subsecuentes tarifas asociadas y cobrar dichas cantidades, supone un aspecto estructural común a mejorar, revelando un "single point of failure" que hace a estos sistemas más vulnerables a fallos y ataques, y compromete su seguridad y disponibilidad.

Con el fin de eliminar esta figura centralizada, en [13], [14] proponen una mejora descentralizada sobre [10] basada en el uso de Smart Contracts para gestionar los accesos a la LEZ como transacciones en el Blockchain, permitiendo determinar y cobrar el precio de los accesos sin intervención de *third parties*. Aunque la propuesta aborda con éxito los problemas de centralización y ofrece mecanismos para mitigar en cierto punto el monopolio en la gestión de las infraestructuras de acceso, el sistema sigue dependiendo de *third parties* con ánimo de lucro que desplieguen, gestionen y mantengan las infraestructuras de control de acceso y sus correspondientes gastos asociados.

I-B. Contribuciones y plan del artículo

Recientemente, la tecnología blockchain se ha convertido en la piedra angular a la hora de implementar ecosistemas de intercambio distribuidos de un modo fiable en un gran numero de dominios. Atendiendo a la dirección de la literatura actual, los escenarios de sistemas de transporte inteligente tales como LEZs o CCZs también dan muestras de adoptar esta tendencia.

Siguiendo esta dinámica descentralizada, y considerando los puntos de mejora identificados en los sistemas descentralizados en la literatura, en este artículo proponemos un nuevo sistema distribuido y totalmente autónomo para gestionar los accesos a LEZs, que hace uso de los sistemas de detección y comunicación avanzados de que disponen los vehículos de nueva generación, a cambio de incentivos, para evitar el despliegue y mantenimiento de infraestructuras de control. Además, el sistema, mediante el uso de smart contracts, permite procesar los accesos LEZ como transacciones de Blockchain y saldarlos descentralizadamente, eliminando de esta forma cualquier intervención de *third parties* centralizadas en el control, tarificación y cobro de los movimientos de los vehículos en la zona restringida.

En resumen, la propuesta ofrece los siguientes beneficios:

- *Anonimato revocable:* el sistema preserva la privacidad de los conductores que se comportan con honestidad pero es capaz de identificar a los usuarios deshonestos y sancionarlos.
- *Sistema descentralizado:* el sistema descentraliza las entidades responsables de los procesos generación, verificación, tarificación y cobro de los accesos de los vehículos a la LEZ; sustituyendo a las entidades responsables de dichos procesos por una red distribuida basada en Blockchain, combinada con el soporte de los sistemas de detección y comunicación avanzados de los vehículos de nueva generación que circulen por la LEZ.
- *Sin infraestructura:* el sistema no requiere el despliegue de infraestructuras de control de acceso gracias al uso de los sensores, cámaras y sistemas de comunicación de los vehículos, evitando los costes de implementación y mantenimiento y la dependencia hacia las entidades centralizadas que las gestionan.
- *Pago anónimo:* el sistema protege el anonimato de los usuarios durante el proceso de pago de tarifas por medio de la tecnología Blockchain y las medidas de preservación de privacidad aplicadas.

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 de la LEZ (*LA*); ii) Conductores (*D*); iii) Vehículo de control de Acceso (*ACV*); iv) Smart Contract de la LEZ (*SC*); y v) Servicio de Mixing de criptomonedas (*M*).

- Administrador de la LEZ (*LA*): es el encargado de dirigir la LEZ y establecer las restricciones que se aplican a los vehículos. Entre sus tareas destacan la emisión de certificados digitales para el resto de entidades, el despliegue del Smart Contract de la LEZ y la gestión de categorías de los vehículos.
- Conductores (*D*): son los usuarios potenciales, quienes, a través de las Unidades de a Bordo (*OBU*) de sus vehículos, interactúan con las infraestructuras del sistema. Las OBU*s* son dispositivos capaces de realizar operaciones criptográficas, equipados con tecnología GPS, 4G, sistema de comunicación de corto alcance (e.g. Bluetooth, Zigbee, IEEE 802.11p/DSRC, etc.) y un Secure Element (*SE*) en el cual una autoridad de confianza ha almacenado la matrícula del vehículo.
- Vehículo de control de Acceso (*ACV*): son vehículos que generan y verifican las pruebas de acceso de los vehículos que circulan por la zona restringida. Para desempeñar esta función, un vehículo ha de contar, además de las prestaciones de D, con un sistema avanzado de asistencia de conducción (*ADAS*), que incluya sensores de proximidad y cámaras en la sección trasera o delantera.
- Smart Contract (*SC*): es un protocolo de transacción especialmente programado para incluir los detalles de acceso a la LEZ en el blockchain, permitiendo verificar,

tarificar y pagar dichos accesos por medio de criptomonedas.

- Servicio de Mixing de Criptomonedas (*M*): es una entidad con ánimo de lucro capaz de ofuscar, a cambio de la pertinente tasa, la transferencia de fondos entre dos carteras digitales[4] [5].

II-B. Visión general del sistema

La figura 1 muestra el esquema general del sistema de control de acceso propuesto. En este escenario, al acceder a la LEZ, los vehículos con las capacidades para actuar como ACVs generan y verifican pruebas de acceso a los vehículos de su entorno cercano. Para ello, en el momento en que el sistema de sensores de un ACV detecta otro vehículo, este intenta establecer conexión con el D detectado mediante un sistema de comunicación inalámbrica de corto alcance. Dicho proceso de detección puede limitarse a las partes del vehículo que disponen de cámaras (trasera y/o delantera). Una vez ambos vehículos se han autenticado, ACV solicita, verifica y almacena la prueba de acceso de D, o la genera en caso que D no disponga de una. Si en algún momento, D intenta omitir o alterar este protocolo de alguna forma, ACV hace una foto de la matrícula del vehículo, pudiendo así reportar su comportamiento ante el LA.

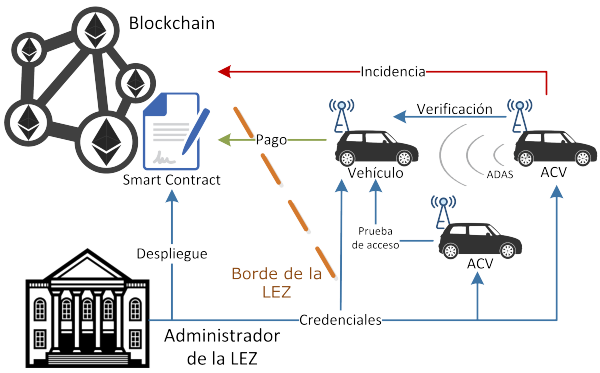


Figura 1. Esquema general del sistema

Una vez D ha abandonado la LEZ, puede iniciar el proceso de pago invocando al método de pago del SC de la LEZ, usando su recibo de acceso como parámetro. La lógica del SC utiliza los datos contenidos en dicho recibo para verificar su validez, calcular el importe de la tarifa y transferir las criptomonedas correspondientes desde cartera digital de D a las carteras de ACV y LA en la proporción pertinente.

Pasado un tiempo, fijado por la entidad que despliega el SC, los ACVs que hayan obtenido la prueba de acceso verifican si los datos de ese acceso han sido publicados en el Blockchain y dicha transacción aparece como pagada. En caso de encontrar alguna irregularidad, cualquiera de los ACV involucrados puede abrir una incidencia, publicando su copia almacenada de la prueba de acceso. Haciendo pública esta información, firmada por D, el LA dispone de todo lo necesario para resolver la incidencia, identificar al D fraudulento y recompensar al ACV si así se requiere.

[4]Tornado Cash, https://defirate.com/tornado-cash/
[5]ETH-Mixer, https://eth-mixer.com/

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 para la cartera*, *Generación prueba de acceso*, *Control del acceso*, *Pago*, *Verificación de Pago*, *Anti-Fraude* y *Renovación de seudónimos*.

III-A. Configuración de la OBU

Este protocolo inicial consiste en configurar la OBU de D para obtener las credenciales necesarias para interactuar con el resto de entidades del sistema. Con este fin, la OBU establece un canal seguro, vía TLS, con LA y proporciona la información de D (matrícula, marca, modelo, etc.). Se asume que la OBU no puede ser manipulada para proporcionar información falsa y que LA, como entidad gubernamental, puede verificar y obtener los datos de D. Entonces, LA realiza el proceso siguiente:

a) LA verifica los datos del vehículo y obtiene los datos del propietario (nombre, residencia, etc.).
b) LA genera un código de vehículo pseudoaleatorio β y lo vincula con D.
c) LA envía β como *One Time Password (OTS)* a D a través de un canal alternativo.

Una vez D recibe β:

a) D genera un par de claves (sk^D, pk^D).
b) D prepara una solicitud de certificado $CSR(pk^D)$ para la clave pública generada.
c) D envía β y $CSR(pk^D)$ a LA.

Cuando LA recibe un $CSR(pk^D)$ válido:

a) LA verifica la validez del código β.
b) LA recupera los datos de D vinculados a β.
c) LA emite el certificado Γ^D, incluyendo β en el campo *CommonName* y la categoría de emisiones del vehículo cat como extensión (X509 v3).
d) LA envía el certificado generado Γ^D a D.

Finalmente, D realiza las siguientes operaciones:

a) D verifica el certificado Γ^D a partir de Γ^{LA}. Si la verificación falla, se aborta el proceso; de lo contrario, sigue adelante.
b) D almacena de forma segura (sk^D, pk^D) y Γ^D.

Una vez obtenidas sus credenciales, D genera una cartera digital W_D compatible con Ethereum Virtual Machine (EVM) con el fin de poder interactuar con el SC que gestiona la LEZ. Con este fin, D genera una clave privada de 256-bits sk_D^W, una clave pública de 512 bits pk_D^W y su correspondiente *address*, de acuerdo con las especificaciones de la red compatible con EVM donde se despliegue el SC.

III-B. Adquisición de Tokens para la cartera

Con el fin de pagar su uso de la LEZ e interactuar con el SC de la LEZ, D debe a adquirir criptomonedas (i.e. elementos que actúan como divisa en nuestro sistema). Con este propósito, se espera que LA hospede un sitio web donde los usuarios puedan adquirir criptomonedas, que se transfieren directamente a sus carteras digitales[6], por medio de sistemas de pago clásicos (e.g. tarjeta de crédito, transferencia bancaria,

[6]My Ether Wallet - https://ccswap.myetherwallet.com/

etc.). Como este proceso podría permitir vincular la cartera digital de D a su cuenta bancaria, poniendo en riesgo su privacidad, D realiza los pasos siguientes para evitarlo:

a) D crea una cartera temporal W_D^T.
b) D al sitio web de LA y adquiere criptomonedas, que se transfieren a W_D^T.
c) D solicita al servicio de mixing M, que transfiera las monedas de W_D^T a la cartera real W_D de D.
d) M, mediante el mixing, ofusca el vínculo entre las carteras de origen y destino al transferir los fondos, evitando que LA pueda identificar las transacciones de D en el Blockchain.
e) D descarta la cartera temporal un vez las monedas han sido transferidas.

III-C. Generación prueba de acceso

Durante el tránsito por la zona restringida, un vehículo actuando como controlador de acceso (ACV) se ofrece a generar pruebas de acceso para otros Ds. Para ello, cuando los sensores delanteros o traseros del sistema ADAS detectan un vehículo D cercano, ACV intenta establecer conexión segura, involucrando autenticación bilateral, con D usando un sistema de comunicación de corto alcance (e.g.). Este proceso supone intercambio de certificados entre D y ACV.

a) D solicita una prueba de acceso para la zona donde transita ar = (N_D, loc, t_a, cat), siendo N_D un nonce, loc la ubicación, t_a una marca temporal y cat la categoría de emisiones del vehículo.
b) ACV verifica los datos de ar y genera el código de acceso $\delta = N_D \| N_{ACP}$.
c) ACV genera un recibo ρ = (δ, $zona_{id}$, t_a, cat) y su firma ρ'^{W}_{ACV}, generada con clave privada de su cartera digital para que el SC lo pueda verificar on-chain.
d) ACV prepara la prueba de acceso ap = (β, ρ, ρ'^{W}_{ACV}) y la firma digitalmente ap'_{ACV}. β se obtiene del certificado Γ^D.
e) D recibe ap y ap'_{ACV}. Verifica la firma ap'_{ACV}, comprueba que los datos contenidos en ap son correctos y la firma ρ'^{W}_{ACV} es válida.
f) D almacena la prueba de acceso ap, ap'_{ACV} y el certificado Γ^{ACV}.
g) D genera la respuesta rap = (t_b, β, ρ, ρ'^{W}_{ACV}, ap'_{ACV}) y su firma digital rap'_D, dónde t_b es el timestamp de la respuesta.
h) ACV recibe y almacena rap y rap'_D, una vez ha verificado la firma rap'_D y ha contrastado los datos contenidos en rap con los enviados ap.

Si en algún instante se interrumpe el proceso de generación, ACP inicia la fase anti-fraude para obtener evidencias de un posible D deshonesto.

III-D. Control del acceso

En el instante que un vehículo actuando como ACV detecta a otro D con los sensores ADAS, ACV puede iniciar un proceso de control. Para ello ACV establece conexión segura con autenticación bilateral con D e realiza los siguientes pasos:

a) D recupera su prueba de acceso ap, genera una respuesta rap = (ap, ap'_{ACV}, t_c) y la firma digitalmente rap'_D.
b) D envia rap y rap'_D y el certificado del ACV generador de ap.
c) ACV verifica las firmas rap'_D y ap'_{ACV}, y comprueba que la prueba tiene validez en el marco espacial y temporal actual.
d) ACV almacena rap y rap'_D como prueba. Si alguna verificación falla, ACV inicia la fase anti-fraude.

III-E. Pago

Obtenida la prueba de acceso, D puede abonar el coste de su acceso publicando el recibo ρ en el blockchain haciendo uso de la lógica de los smart contracts, y evitando así la intervención de entidades centralizadas. Con ese fin, D invoca al método *registrar_acceso* del SC usando los datos de acceso contenidos en ρ y su firma ρ'^{W}_{ACV} como parámetros. SC realiza las siguientes operaciones on-chain:

a) SC verifica la firma ρ'^{W}_{ACV} y obtiene la "address" de la cartera de ACV.
b) SC calcula la coste de acceso a partir de la $zona_{id}$ el t_a y cat, de acuerdo con las tasas publicadas en el blockchain por LA.
c) SC transfiere la cantidad de criptomonedas equivalentes al coste desde la cartera de D a las carteras de ACV y LA en la proporción pertinente.
d) SC actualiza el estado del acceso δ a "pagado". Si alguno de los pasos anteriores no se puede completar, se aborta el proceso y se revierten los cambios en el SC.

III-F. Verificación de Pago

LA, como responsable de la zona restringida y dueño del SC, fija el tiempo de que disponen los Ds para realizar sus pagos. Transcurrido ese tiempo los ACV pueden verificar y reportar los accesos impagados de los que hayan recogido pruebas:

a) ACV obtiene la información de la transacción δ publicada en el blockchain.
b) ACV verifica si el acceso está publicado, su estado es "pagado" y los datos coinciden con los de su copia rap.
c) Si no se cumplen estas condiciones, ACV invoca el método del Smart Contract *incidencia_pago* para publicar una incidencia, enviando rap y rap'_D como parámetros.
d) La lógica del SC comprueba si se cumplen las condiciones temporales para abrir una incidencia, verifica que el acceso δ no está pagado y, en caso contrario, comprueba que los datos en rap difieren de los publicados.
e) SC publica rap y rap'_D si se cumplen las anteriores condiciones. Con esta información publicada en el blockchain, LA dispone de las pruebas necesarias para identificar y sancionar la entidad fraudulenta y recompensar al vencedor de la disputa.

III-G. Anti-Fraude

Este mecanismo se ejecuta en paralelo en un ACV durante las fases de generación de prueba de acceso (Sección III-C) y control de acceso (Sección III-D), haciendo uso del sistema ADAS, i.e. la cámara/s del vehículo y los sensores de proximidad, para obtener información de los vehículos fraudulentos. Con el fin de simplificar este escenario, el proceso se puede restringir a los vehículos traseros y delanteros debido a la

mayor sensorización presente en dichas partes del vehículo. La idea general de este sistema fue inicialmente propuesta en [11] para sistemas ERP.

Durante las mencionadas fases del protocolo, los sensores del vehículo obtienen información precisa de la localización de otros Ds. Simultáneamente, ACV hace uso de un sistema indicador de intensidad de la señal recibida (e.g. RSSI [15]) durante la comunicación con D, para estimar la distancia entre ambos vehículos. Esta información, junto con la geolocalización enviada por D durante las fases de control, se combina para determinar si el D con el que se está comunicando es el detectado por los sensores, o se trata de un vehículo fraudulento con la OBU desconectada. De forma similar, la no respuesta por parte de un vehículo detectado por los sensores de ACV también indica la presencia de un D fraudulento. Ante esta situación la cámara del ACV hace una foto de la matrícula del infractor.

Una vez obtenida la evidencia, ACV envía la prueba, junto con una marca temporal y una geolocalización, firmada digitalmente a LA. LA recolecta las evidencias enviadas por los ACVs y, una vez dispone de una cierto número de pruebas emitidas por distintos ACVs, procede a identificar y sancionar al D en cuestión. Si la sanción prospera, i.e. D no aporta su prueba de acceso ap consecuentemente publicada en el Blockchain, los ACVs que hayan contribuido son debidamente remunerados.

III-H. Renovación de seudónimos

Aunque la identidad real de D está oculto tras el código de su vehículo β y la *address* de su cartera digital W_D, dichos elementos, si se usan en diversas interacciones, pueden llevar a la vinculación e incluso a la identificación de D.

Para evitarlo, un usuario D puede solicitar un nuevo código β^* para prevenir que se puedan vincular sus accesos. El cambio del código del vehículo β implica la generación de nuevas claves criptográficas (sk^D, pk^D) y certificado Γ^D, ya que incluye β en el campo *CommonName*, en un proceso similar al descrito en la sección III-A.

En lo referente a la *address* de W_D, D debe generar una nueva cartera digital W_D^*, descrito en III-A, con la que dispondrá de una nueva dirección para sus transacciones en el blockchain. En caso de no haber agotado todos los fondos de su vieja cartera, D puede transferirlos a la nueva por medio de los servicios ofuscación de M, evitando que ambas *address* puedan ser vinculadas.

IV. Conclusiones

Las actuales propuestas de control de acceso orientadas a la privacidad en escenarios LEZ, CCZ y ERP, presentan una dependencia clara hacia entidades centralizadas en sus principales cometidos, es decir, desplegar y mantener las infraestructuras de control, gestionar los accesos, determinar sus respectivas tarifas y promover sus cobros.

Aunque se han presentado propuestas para acabar con la estructura centralizada de algunas de estas operaciones, mediante el uso de la tecnología de los *smart contracts* y el subyacente paradigma descentralizado del Blockchain, dichas soluciones siguen dependiendo de *third parties* con ánimo de lucro que implementen, gestionen y mantengan las infraestructuras que controlan los accesos de los vehículos a la zona restringida. Siguiendo este planteamiento, en este artículo, hemos propuesto un control de acceso totalmente distribuido para escenarios LEZ que preserva privacidad de los usuarios honestos. De este modo, haciendo uso de los sistemas de detección, cámaras y comunicación avanzados que integran los vehículos de nueva generación, nuestra propuesta evita el despliegue de infraestructuras para gestionar el acceso de vehículos, evitando los subyacentes costes de despliegue y mantenimiento, y eliminando de la ecuación toda dependencia hacia entidades centralizadas.

Como trabajo futuro, se prevé implementar el sistema de control propuesto con el fin de verificar su viabilidad, así como llevar a cabo estudios basados en simulaciones que permitan determinar el umbral de ACVs honestos en circulación que nuestro sistema necesita para garantizar su correcto funcionamiento.

Agradecimientos

This research is supported by the European Union Regional Development Fund within the framework of the ERDF Operational Program of Catalonia 2014-2020 with a grant of 50 % of the total cost eligible, under the "FEM-IOT" project [001-P-001682]; by the EU's European Regional Development Fund (ERDF), through the "ERDF Catalonia Operational Programme 2014-2020, investment priority for the creation of jobs and sustainable growth", under the Territorial Specialisation and Competitiveness Project (PECT) "Cuidem el que ens uneix - Sensòrica" project [PR15-020174]; and by Grants RTI2018-095094-B-C21 "Consent" and PID2021-125962OB-C32 "SECURING/DATA" funded by MCIN/AEI/10.13039/501100011033 FEDER, UE.

Referencias

[1] G. Santos, "Urban congestion charging: a comparison between london and singapore," *Transport Reviews*, vol. 25, no. 5, pp. 511–534, 2005.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] J. Day, Y. Huang, E. Knapp, and I. Goldberg, "Spectre: spot-checked private ecash tolling at roadside," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, 2011, pp. 61–68.

[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] 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.

[9] R. Jardí-Cedó, J. Castellà, and A. Viejo, "Privacy-preserving electronic road pricing system for low emission zones with dynamic pricing," *Security and Communication Networks*, vol. 9, pp. 3197–3218, 2016.

[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. Anglès-Tafalla, S. Ricci, P. Dzurenda, J. Hajny, J. Castellà-Roca, and A. Viejo, "Decentralized privacy-preserving access for low emission zones," in *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - Volume 2: SECRYPT,*, INSTICC. SciTePress, 2019, pp. 485–491.

[14] C. Anglès-Tafalla, J. Castellà-Roca, and A. Viejo, "Privacy-preserving and secure decentralized access control system for low emission zones," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019.

[15] R. S. Yokoyama, B. Y. Kimura, L. A. Villas, and E. D. Moreira, "Measuring distances with rssi from vehicular short-range communications," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*. IEEE, 2015, pp. 100–107.