Control de Acceso Anónimo para Zonas de Bajas Emisiones basado en Smart Contracts

Carles Anglès-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*), áreas donde se aplican restricciones al tráfico rodado de acuerdo con su categoría de emisiones, es un mecanismo que en los últimos años ha tenido una gran proliferación en las grandes ciudades como medida para reducir la contaminación atmosférica. No obstante, los actuales sistemas de control propuestos para hacer cumplir dichas restricciones presentan problemas de privacidad, derivados del uso indiscriminado de cámaras, y de dependencia hacia entidades centralizadas en procesos de tarificación y cobro. Aunque en la literatura han aparecido propuestas que descentralizan las entidades responsables de estos procesos, mientras preservan la privacidad de los usuarios honestos, estas aún son poco flexibles respecto los parámetros que pueden tarificar. Siguiendo esta tendencia, en este artículo proponemos un sistema de control de acceso LEZ descentralizado más versátil que, por medio del uso de Smart Contracts y un esquema de firmas de grupo, permite tarificar en función del tiempo de tránsito en vez de solo por acceso, garantizando, a su vez, la privacidad, no-trazabilidad y no-vinculación de las acciones de los usuarios honestos.**

***Index Terms*—Ciudades Inteligentes, Zonas de Bajas Emisiones, Privacidad, Firmas de grupo, Smart Contracts.**

I. Introducción

Los altos niveles de contaminación que se registran en los grandes núcleos urbanos, debidos en gran parte a la congestión y atascos de vehículos, se han convertido en un grave problema para ciudades de todo el mundo. En estas áreas metropolitanas, los niveles de contaminación superan los límites establecidos por la Organización Mundial de la Salud [1], lo que representa un peligro para la salud de sus ciudadanos. La implementación de LEZ, es decir, áreas donde se aplican una serie de restricciones o recargos a los vehículos de acuerdo con su nivel de emisiones, es una de las medidas que más ha proliferado a la hora de abordar esta problemática. Esta tendencia puede verse reflejada en ciudades de países como Suecia, Italia, Holanda, Reino Unido y Alemania[1].

Ante esta predisposición, queda patente la necesidad de implementar sistemas de control para accesos a LEZ que permitan aplicar las restricciones que estas requieren. Actualmente, los sistemas automatizados existentes están basados en redes de cámaras, como los casos de Londres o Estocolmo [2], cuyo propósito es fotografiar indiscriminadamente la matrícula de los vehículos para, posteriormente verificar o calcular la tarifa que su propietario debe abonar de acuerdo con la categoría de emisiones de su vehículo.

Sistemas con una naturaleza tan invasiva como los mencionados anteriormente han fomentado la aparición de alternativas más respetuosas con la privacidad de sus usuarios. Estas propuestas se centran, principalmente, en recopilar pruebas de localización de forma anónima, generadas cuando los vehículos circulan por inmediaciones de las infraestructuras de acceso, para que, posteriormente, una entidad de confianza determine y cobre sus tarifas correspondientes. De este modo, sólo se registran las matrículas de los vehículos que alteran o omiten el protocolo requerido con la infraestructura. No obstante, esta forma de proceder implica una fuerte dependencia hacia las entidades centralizadas que controlan las infraestructuras, constituyendo un "single point of failure" en los procesos de verificación, tarificación y cobro de los accesos, y suponiendo un peligro para la seguridad y disponibilidad del sistema.

En los últimos años, ha adquirido especial relevancia el paradigma de los "Smart Contracts" [3], que permite acordar de manera descentralizada transacciones de recursos arbitrarios, como interacciones entre vehículos e infraestructuras LEZ, a través de un "public open ledger" verificable llamado Blockchain y sin necesidad de recurrir a entidades de confianza. Sin embargo, el uso de un "public ledger" suscita nuevos desafíos de privacidad, ya que las transacciones publicadas en él caen en el dominio público y, por lo tanto, cualquier información que contengan debe protegerse consecuentemente.

En vista a los problemas identificados en la literatura actual, la descentralización que estas tecnologías pueden aportar a los sistemas de control de LEZ, sin sacrificar o debilitar la privacidad de los usuarios en el proceso, debe ser tomada en serio y explorada en consecuencia.

I-A. Antecedentes

En la última década, una tendencia común ha prevalecido entre los sistemas de control para zonas restringidas [4], [5], [6]. En líneas generales, su funcionamiento consiste en utilizar la unidad de a bordo (OBU) de los vehículos con el fin de recopilar datos relevantes para el cómputo de su tarifa mientras estos circulan por el interior del área restringida. Más tarde, en base a estos datos, la OBU tarifica su tránsito en la LEZ y se envía a una tercera parte centralizada, generalmente un proveedor de servicios (SP), que valida todo el proceso y cobra la tarifa requerida. La privacidad de los usuarios es preservada al no revelar datos sensibles al SP y únicamente enviar datos anónimos o valores agregados.

No obstante, como estas propuestas solo recopilan datos en el extremo del vehículo, son necesarias medidas antifraude que eviten que los usuarios deshonestos alteren intencionalmente el comportamiento de la OBU para disminuir la distancia recorrida y, por ende, su tarifa (por ejemplo apagando la OBU o modificando su envío de datos). Para

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

este propósito, todas estas propuestas comparten un sistema antifraude basado en una red de "checkpoints" equipados con cámaras, en el que el SP recopila información sobre los vehículos fotografiando indiscriminadamente la matrícula de todos aquellos que circulan por la LEZ. Luego, los usuarios deben presentar pruebas criptográficas de su ruta que estén en consonancia con las fotografías registradas. No obstante, este planteamiento es muy invasivo y supone una amenaza para la privacidad de los usuarios del sistema, especialmente si el número de "checkpoints" es elevado para prevenir que los conductores los eviten intencionadamente.

En estos últimos años, un nuevo paradigma se ha consolidado desde que fue propuesto en [7] y luego adoptado en [8], [9], [10]. Este nuevo planteamiento promueve que la privacidad de los usuarios se preserve a menos que intenten cometer fraude. En este sentido, dichas propuestas solo fotografían las matrículas en caso de que no se complete o se omita un proceso de autenticación con las infraestructuras del sistema.

En [7], además de este nuevo paradigma anti-fraude, se propone un protocolo en el que las tarifas se calculan en base al tiempo de tránsito dentro de la LEZ. Posteriormente, en [8], el sistema se adaptó a un escenario LEZ multi-zona con precios dinámicos. Ambos sistemas hacen uso de firmas de grupo, requiriendo una regeneración periódica de credenciales, para mantener la privacidad de los usuarios cuando el SP verifica y tarifica todas las evidencias de acceso. La propuesta en descrita en [9] presenta un modelo de privacidad diferente, basado en seudónimos, con un protocolo más eficiente y ligero, que simplifica la gestión de evidencias durante la verificación y cálculo de tarifas de los accesos. Finalmente, en [10] se presenta un sistema basado en carteras criptográficas, en las que los usuarios acumulan deuda anónimamente cuando se encuentran con una infraestructura del sistema. Durante la fase de facturación, los usuarios liquidan la deuda de su cartera con el SP antes de que este les emita una nueva.

Tal como se puede apreciar, se pueden identificar puntos de mejora comunes en la arquitectura de las anteriores propuestas debido a la fuerte dependencia de estas hacia una entidad centralizada, generalmente un SP, para validar evidencias del acceso o tránsito de los vehículos, determinar las subsecuentes tarifas y cobrar sus correspondientes cantidades. Esta estructura centralizada propicia la presencia de un "single point of failure", haciendo a estos sistemas más vulnerables a fallos y ataques, y comprometiendo así su seguridad y disponibilidad.

Con el fin de eliminar la posición centralizada que ostentan los SPs en estos sistemas, en [11] se presenta una propuesta descentralizada basada en "smart contracts". Con esta tecnología, este sistema gestiona los accesos a la LEZ como transacciones de Blockchain, permitiéndole determinar y cobrar el precio de los accesos sin que intervengan terceras partes centralizadas. Aunque este trabajo aborda con éxito los problemas de centralización encontrados en la literatura, su propuesta es poco flexible en referente a los parámetros de tarificación, permitiendo cobrar únicamente por acceso y no atendiendo a otras variables como tiempo o distancia.

I-B. Contribución y organización del trabajo

Tal como se ha expuesto previamente, existe una clara dependencia hacia entidades centralizadas en la mayoría de propuestas de control de acceso a LEZs, y las alternativas descentralizadas presentes en la literatura actual todavía son poco flexibles en el tipo de parámetros que pueden controlar.

Bajo esta premisa, nuestro trabajo propone un sistema descentralizado de control de acceso a LEZs que otorga más flexibilidad al control de los vehículos, siendo capaz de tarificar a los usuarios de la LEZ en función de su tiempo de tránsito, mientras preserva la privacidad de los usuarios por medio de un esquema de firmas de grupo [12].

Nuestro sistema permite, gracias al uso de smart contracts, que los vehículos y las infraestructuras del sistema procesen los accesos y salidas de la LEZ como transacciones de Blockchain, sustituyendo a las terceras partes a cargo de verificar y cobrar el tiempo de estancia de cada vehículo por una red descentralizada que garantiza la verificabilidad, fiabilidad y transparencia de los eventos publicados.

En resumen, la propuesta ofrece los siguientes beneficios:

- *Sistema descentralizado:* el sistema descentraliza los procesos de verificación de evidencias, tarificación y cobro del tránsito de los vehículos por la LEZ; sustituyendo a las entidades responsables de dichos procesos por una red descentralizada basada en Blockchain y eliminando el "single point of failure" que estas suponen.
- *Más flexibilidad de tarificación:* El sistema es capaz de controlar y tarificar el tiempo que los vehículos pasan en la LEZ, a diferencia del resto de sistemas descentralizados actuales que solo son capaces de facturar por acceso.
- *Anonimato revocable:* El sistema siempre 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.
- *Privacidad sin trazabilidad* El sistema protege la privacidad de los usuarios por medio de un esquema de firmas de grupo, presentado en [12], que impide que las evidencias que estos generan puedan asociarse, evitando que sus distintos tránsitos por la LEZ se puedan vincular, sin la necesidad de regenerar sus credenciales.

El resto de este documento está organizado de la siguiente manera. La sección II introduce la nueva propuesta. La sección III detalla los los protocolos que de nuestro sistema. La sección IV analiza los requisitos de seguridad y privacidad del escenario propuesto. Finalmente, la Sección V 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) Infraestructura de control de acceso (*AC*); y iv) 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 para el esquema de firmas de grupo.
- Conductores (*D*): son los usuarios potenciales, quienes, a través de las Unidades de a Bordo (*OBU*) de sus vehícu-

los, interactúan con las infraestructuras del sistema. Las OBU*s* son dispositivos capaces de realizar operaciones criptográficas, equipados con tecnología GPS, 4G, Bluetooth y un Secure Element (*SE*) en el cual una autoridad de confianza ha almacenado la matrícula del vehículo.
- Control de acceso (*AC*): Son las infraestructuras que controlan el acceso y salida de la LEZ. Con ese fin, están equipadas con tecnología GPS, Bluetooth, acceso a Internet y una cámara. Pueden estar bajo el control de una o más entidades con ánimo de lucro, siempre y cuando LA no sea una de ellas.
- Servicion de Mixing de Criptomonedas (*M*): es una entidad independiente con la capacidad de ofuscar, a cambio de una tasa, las transacciones de Blockchain de manera que unos fondos transferidos no pueden rastrearse hasta la cartera digital originaria[2] [3].

II-B. Visión General

La figura 1 muestra una visión general de la propuesta junto con los actores involucrados en el proceso: Administrador de la LEZ (LA), Conductores (D), Infraestructura de control de acceso (AC) y el Smart Contract. En este escenario, con el fin de interactuar de forma segura con el resto de entidades, es necesario que la OBUs de los vehículos obtengan, del LA, credenciales válidas que acrediten su categoría de emisiones y generen una cartera digital que les permita pagar, mediante el uso de Smart Contracts, su tránsito por la LEZ.

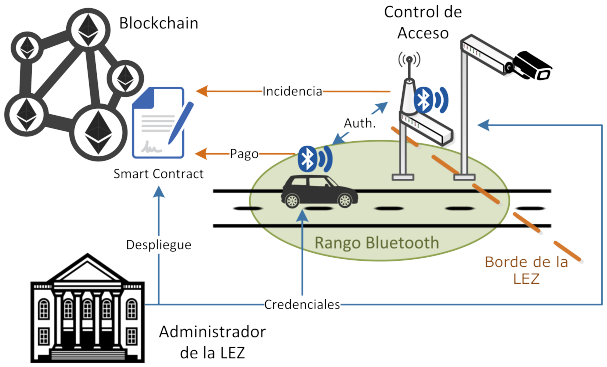

Figura 1. Arquitectura del sistema

El protocolo de acceso se inicia el momento en que D entra en la zona de interacción de AC (p.ej. alcance del Bluetooth) y su OBU se activa automáticamente. La detección de beacons *Bluetooth Low Energy* puede ser, por ejemplo, el detonante para iniciar este proceso sin la intervención de D. Al recibir esta señal, la OBU establece conexión segura con AC mediante una comunicación inalámbrica de corto alcance, permitiendo a D y AC acordar un recibo de acceso con los parámetros de entrada por medio de un proceso de autenticación. Todo este procedimiento es repetido durante la salida, obteniendo el subsecuente recibo de salida, que junto a su homónimo de entrada, conforma la prueba del tránsito del vehículo por la LEZ. Durante ambos procesos se preserva la privacidad de D, ya que toda evidencia que genera se firma anónimamente, gracias a un esquema de firmas de grupo, en nombre de la categoría de emisiones de su vehículo, siendo esa la única información que revela a AC. Si en algún momento, D intenta omitir o alterar este proceso de autenticación de alguna forma, AC hace una foto de la matrícula del vehículo, permitiendo así determinar su identidad.

Una vez D ha confirmado su salida, puede iniciar el proceso de pago de su tránsito por la LEZ. Para ello, D invoca remotamente el método de pago del Smart Contract de la LEZ, enviando su recibo de tránsito como parámetro. La lógica del Smart Contract utiliza los datos contenidos en dicho recibo para verificar su validez y calcular el importe de la tarifa a partir del tiempo transcurrido en la LEZ, la categoría del vehículo y la lista de precios publicada en el Blockchain vigente durante el acceso. Si el recibo es válido, se transfieren automáticamente los tokens LEZ correspondientes de la cartera digital de D a la de AC.

Después de un período de tiempo, los AC involucrados verifican si la transacción de tránsito de D se ha publicado en el Blockchain y si su estado figura como "pagado". En caso de encontrar alguna irregularidad, cualquiera de los AC involucrados puede abrir una incidencia. Para ello, interactúa con el Smart Contract y publica en el Blockchain su propia copia del recibo, que contiene la firma de grupo de D. Haciendo pública esta información, LA, como manager de los grupos, puede revelar la identidad de D a partir de su firma y revocar su anonimato.

III. 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*, *Acceso*, *Salida* y *Pago*.

III-A. Configuración de la OBU

El primer paso consiste en configurar la OBU del vehículo de un usuario D para obtener las credenciales necesarias para interactuar con las entidades del sistema. Con este fin, D establece un canal seguro, vía TLS, con LA y proporciona la información del vehículo (matrícula, marca, modelo, etc.). Se asume que la OBU no puede ser manipulada para proporcionar información falsa. Entonces, LA realiza lo siguiente:

- Comprueba si los datos del vehículo coinciden con la matrícula y obtiene los datos del propietario (nombre, residencia, etc.).
- Si es correcto, realiza los siguientes pasos: i) genera un código de vehículo β; ii) vincula el código β al propietario del vehículo D y; iii) envía β como "One Time Password" (OTS) a D a través de un canal alternativo.

Una vez D ha recibido β:

- Genera un par de claves (sk^D, pk^D) y prepara una solicitud de certificado $CSR(pk^D)$ para estas.
- Envía β y $CSR(pk^D)$ a LA.

LA realiza las siguientes operaciones con datos recibidos:

- Comprueba que: i) el código β existe y pertenece al usuario; ii) verifica que $CSR(pk^D)$ es válido.
- Emite el certificado Γ^D. El campo *CommonName* contiene el código del vehículo β en vez de información

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

personal. La categoría de emisiones del vehículo cat se incluye como extensión (X509 v3).
- Envía el certificado generado Γ^D a D.

Finalmente, D realiza las siguientes operaciones:
- Verifica la validez del certificado Γ^D.
- Si la verificación previa es correcta, Γ^D y (sk^D, pk^D) se almacenan de forma segura.

Con un certificado Γ^D emitido por LA, D puede autenticarse a las otras entidades del sistema. En base a esto, D establece un canal seguro con LA, con autenticación bidireccional, por el cual se negociaran las claves para la firma de grupos. D inicia este proceso haciendo lo siguiente:
- Prepara una solicitud de claves σ que contiene un identificador aleatorio id_D y una evidencia de la matrícula generada lp por el SE.
- Genera la firma digital de la solicitud σ'_D.
- Envía σ y σ'_D a LA.

Cuando LA recibe la solicitud de D:
- Verifica la firma σ'_D.
- Comprueba la validez de lp y si está asociada con el código del vehículo β contenido en el certificado Γ^D.
- Recupera la clave privada sk^{cat}_{LA} asociada a la categoría de emisiones cat del vehículo.
- Utiliza sk^{cat}_{LA} y id_D para generar la clave privada de grupo sk^G_D del usuario. En la sección $Register$ en [12] se definen los detalles este proceso.
- Genera la respuesta a la solicitud $r\sigma = (sk^G_D, \sigma, \sigma'_D)$ conteniendo la clave generada sk^G_D y la solicitud de D.
- Envía $r\sigma$ junto con su firma $r\sigma'_{LA}$.

En el otro extremo, D verifica la respuesta y la almacena como evidencia. La clave sk^G_D se almacena de forma segura en el SE de la OBU.

Una vez completado el proceso de generación de credenciales, D genera un grupo de carteras digitales Ethereum $W^1_D..W^n_D$, ya que es un requisito indispensable para publicar transacciones en el Blockchain y pagar los accesos a la LEZ mediante el uso de Smart Contracts. Con este propósito, por cada cartera, D genera una clave privada de 256 bits sk^W_D, una clave pública de 512 bits pk^W_D y su correspondiente dirección, de acuerdo con las especificaciones del protocolo Ethereum.

III-B. Adquisición de Tokens para la cartera

Como el sistema propuesto contempla el pago de tarifas mediante Smart Contracts, D debe adquirir tokens LEZ, es decir, elementos que actúan como moneda en el sistema, para sus transacciones. Para este propósito, LA dispone de un sitio web específico donde los usuarios pueden comprar tokens a cambio de dinero o criptomonedas. En este aspecto, se asume que las compras efectuadas con criptomonedas o modos de pago clásicos (p. ej. tarjeta de crédito) pueden plantear problemas de privacidad, ya que abren la posibilidad de vincular los datos del usuario (p. ej. su cuenta bancaria) con su cartera digital y, por lo tanto, con sus transacciones en el Blockchain.

Para evitar este vínculo, D crea una cartera temporal W^T_D en la que se transfieren los tokens comprados en la tienda online del LA. Luego, D solicita a M que transfiera cantidades de sus fondos en W^T_D a cada una de sus carteras $W^1_D..W^n_D$. M, mediante el proceso de mixing, ofusca el vínculo entre las carteras de origen y destino al transferir los fondos, evitando que LA pueda identificar las transacciones de Blockchain en las que está involucrado el comprador de los tokens.

La idea detrás de este procedimiento consiste en distribuir los fondos de D en pequeñas cantidades a múltiples carteras de un solo uso. De esta manera, D puede pagar sus tasas fraccionadamente usando distintas carteras y descartando las ya vacías.

III-C. Acceso

Cuando D accede a la LEZ, establece una comunicación de corto alcance con AC con el fin de validar los parámetros de su acceso. En el momento que D entra en el rango de interacción de AC, ambas entidades establecen una comunicación segura, TLS, que implica autenticación unidireccional por parte de AC. Entonces, la OBU de D realiza las siguientes operaciones:
- Genera un ID de acceso aleatorio δ que identificará la transacción en el Blockchain.
- Prepara ψ = (δ, N^e_{TLS}, pos_e, $fecha_e$, $hora_e$, cat), siendo N^e_{TLS} el nonce generado por AC del TLS handshake anterior y cat la categoría de emisiones de D.
- El SE de D firma ψ en nombre de su grupo de emisiones cat, obteniendo ψ'^G_D.
- Envía los datos de acceso ψ y su firma ψ'^G_D a AC.

Al recibir la solicitud de acceso, AC realiza lo siguiente:
- Comprueba si los datos contenidos en ψ son correctos.
- Verifica ψ'^G_D con la clave pública pk^{cat}_{LA} correspondiente al grupo cat de D.
- Si las verificaciones son correctas, AC prepara un recibo de acceso con los datos recibidos $r\psi$ = (id_{AC}, ψ ψ'^G_D).
- Envía $r\psi$ y su firma digital $r\psi'_{AC}$ como el recibo de acceso a D.
- Almacena localmente ψ y la firma de grupo de D ψ'^G_D hasta que la transacción de acceso sea publicada en el Blockchain.

Finalmente, D verifica los datos del recibo del acceso $r\psi$ y su firma $r\psi'_{AC}$. La prueba de acceso se almacena localmente como evidencia hasta que el proceso de pago se haya completado.

III-D. Salida

De forma parecida al acceso, D debe registrar su salida con una AC para conseguir su recibo de tránsito. Para ello, al abandonar la LEZ, ambas entidades establecen comunicación segura, con autenticación unidireccional por parte de AC. Entonces, D realiza las siguientes operaciones:
- Prepara los datos de salida ω = (N^s_{TLS}, pos_s, $fecha_s$, $hora_s$, $r\psi$, $r\psi'_{AC}$), siendo N^e_{TLS} el nonce del TLS handshake y $r\psi$ el recibo de acceso.
- El SE de D firma ω en nombre de su grupo de emisiones cat, obteniendo ω'^G_D.
- Envía los datos de salida ω y su firma ω'^G_D a AC.

Al recibir la solicitud de salida, AC realiza lo siguiente:
- Comprueba los datos en ω y la firma $r\psi'_{AC}$.
- Verifica ω'^G_D con la clave pública pk^{cat}_{LA} correspondiente al grupo cat de D.
- Comprueba el sensor de presencia y verifica si el vehículo detectado se ha autenticado. Si la verificación es incorrecta, AC fotografía la matrícula del vehículo.

- Si las verificaciones son correctas, AC prepara un recibo de tránsito ρ = (δ, $fecha_e$, $hora_e$, $fecha_s$, $hora_s$, cat, id_{AC}) y su firma ρ'^{W}_{AC}, generada con clave privada de la cartera digital de AC para que el Smart Contract pueda verificarlo on-chain.
- Envía el recibo de tránsito en la LEZ $r\omega$ = ($\rho, \rho'^{W}_{AC}, \omega, \omega'^{G}_{D}$) y su firma digital $r\omega'_{AC}$ a D como prueba de su interacción. El envío puede optimizarse eliminando los datos redundantes en ρ y ω.
- Almacena localmente ω y la firma de grupo de D ω'^{G}_{D} hasta que la transacción se publica en el Blockchain.

Finalmente, D verifica y almacena temporalmente la prueba de tránsito en la LEZ $r\omega$ y su firma $r\omega'_{AC}$.

III-E. Pago

Una vez obtenida la prueba de transito $r\omega$, D puede iniciar el proceso de pago interactuando con el Smart Contract de la LEZ. Para ello, D llama remotamente al método *registrar_acceso* con recibo de tránsito ρ y su firma ρ'^{W}_{AC}, contenidos en $r\omega$, como parámetros. Invocando este método, el Smart Contract realiza las siguientes operaciones on-chain:

- Comprueba si el acceso δ ya está publicada en el Blockchain. Si el estado de este acceso aparece como "pagado", no se realizan más acciones.
- Verifica la firma del recibo ρ'^{W}_{AC} y se revela la "address" de la cartera emisora, esta debe pertenecer a un AC registrado en el Blockchain. Si la verificación falla, el estado del acceso δ se actualiza a "firma inválida".
- En base al tiempo transcurrido $hora_s$-$hora_e$ y la categoría del vehículo cat contenidos en ρ, calcula la tarifa de D de acuerdo con los precios publicados en el Blockchain vigentes durante la fecha del recibo.
- Transfiere los tokens equivalentes a la tarifa desde la cartera digital de D a la de AC. En caso de fondos insuficientes, se transfieren todos los tokens y se actualiza la cantidad restante a pagar. D puede repetir este proceso con varias carteras hasta liquidar toda la deuda.
- Una vez saldada la deuda, actualiza el estado del acceso δ a "pagado".

Una vez transcurrido tiempo suficiente, cada AC involucrado comprueba el pago de D, verificando si la transacción de tránsito δ se ha publicado en el Blockchain:

- Obtiene la información de la transacción δ, invocando el método *ver_estado*.
- Verifica si la transacción δ existe y si su estado consta como "pagado".
- Si no se cumplen estas condiciones, el AC de entrada o salida puede publicar una incidencia invocando el método del Smart Contract *incidencia_pago*. Los datos de tránsito de D y su firma en nombre de su categoría de emisiones ω'^{G}_{D} se envían como parámetros.
- Una vez publicado, elimina su copia local del acceso.

La lógica del Smart contract, por su parte, verifica si se cumplen las condiciones temporales antes de publicar la incidencia y desvelar la firma de un usuario. LA, como dueño del Smart Contract, define y fija el tiempo que debe transcurrir antes de poder abrir una incidencia. Una vez publicados los datos de acceso y la firma de grupo del usuario ω'^{G}_{D}, LA tiene todos los medios para identificar a D.

Con este protocolo, los AC*s* involucrados en el acceso y la salida acumulan tokens en sus carteras digitales. LA, en cada período de facturación, recompensará económicamente a la entidad o entidades que gestionen los ACs en función de los tokens acumulados, obteniendo así beneficios por sus servicios.

IV. Security and privacy analysis

En esta sección se definen y analizan los requisitos de seguridad y privacidad que debe cumplir el sistema propuesto. Teniendo esto en cuenta, en primer lugar se presenta el modelo atacante, para, posteriormente, analizar uno por uno los requisitos de seguridad definidos.

El modelo de atacante previsto para la presente propuesta tiene en consideración tanto adversarios internos como externos. Se consideran atacantes internos a las AC*s* honestas pero curiosas y a los D*s* deshonestos que alteran el protocolo para cometer fraude. Por otra parte, cualquier entidad que omite los protocolos para cometer fraude es considerada un atacante externo. Finalmente, LA, que actúa como autoridad de certificación, se considera una entidad de confianza.

Considerando este modelo, las próximas secciones explican cómo se cumplen las siguientes propiedades de seguridad:

- *Anonimato revocable*: La privacidad de los usuarios se mantendrá siempre y cuando éstos sigan el protocolo estipulado. En caso contrario, el sistema debe ser capaz de identificar al usuario fraudulento aunque éste no disponga de credenciales o esté registrado al sistema.
- *No repudio e integridad de las acciones*: Sólo los usuarios correctamente registrados deben poder completar las interacciones con las infraestructuras del sistema. Las evidencias y pruebas generadas a partir de estas interacciones no se pueden negar, forjar ni falsificar.
- *Acciones no rastreables*: Las distintas acciones del usuario en la LEZ no han de poder vincularse o mapearse permitiendo un seguimiento.
- *Exculpabilidad*: Un usuario no puede ser falsamente acusado de fraude. En caso de una falsa acusación, la entidad implicada debe poder demostrar su inocencia con evidencias.

IV-A. Anonimato revocable

En los protocolos de acceso y salida de la LEZ, D preserva su anonimato en sus interacciones con AC al firmar sus mensajes en nombre su grupo. Como AC solo obtiene información de D a través de sus firmas, lo único que D revela a AC en este proceso es la categoría de emisiones de su vehículo. Solo LA, como gestor de grupos, puede desenmascarar a D a partir de su firma. En caso que D intente omitir o alterar los protocolos de acceso o salida, AC puede hacer una foto de la matrícula del vehículo, desvelando así la identidad de D.

Durante la fase de pago, D publica la información de tránsito en el Blockchain bajo la dirección de su cartera digital. Al no publicarse su firma de grupo en este proceso, ninguna entidad, interna o externa, es capaz de desvelar la identidad de D. En caso que D intente alterar u omitir la fase de pago, AC puede detectar estos indicios en el Blockchain y publicar su copia del recibo de tránsito con la firma de grupo de D. Con estos datos publicados, LA puede desvelar la identidad de D.

IV-B. No repudio e integridad de las acciones

Durante la fase de acceso o salida, tanto AC como D deben probar que disponen de credenciales válidas emitidas por LA. En el caso de AC, demuestra su identidad por medio de su certificado; y, en caso de D, demuestra que es un miembro válido de su grupo de emisiones firmando en su nombre.

Como resultado de las interacciones de acceso o salida, ambas entidades, AC y D, obtienen pruebas firmadas por la parte contraria; en el caso de D, firmada en nombre de su grupo de categoría de emisiones. En ambos casos, la validez de las firmas puede ser verificada por la parte contraria y, por tanto, se garantiza la integridad de las pruebas transmitidas. También en ambos casos, la identidad del emisor de la firma digital puede ser revelada, por medio de LA en el caso de D, evitando que dichas entidades puedan negar la emisión de las evidencias generadas.

IV-C. Acciones no rastreables

Durante sus interacciones en la LEZ, D sólo comparte sus datos de acceso y su firma de grupo aleatorizada con los AC*s* con los que se comunica. De esta manera, dichos AC*s*, incluso confabulándose, no disponen de medios para vincular las subsecuentes interacciones en accesos y salidas de D. De igual modo, la firma de grupo de D solo se hace pública en el Blockchain en caso de detectarse un intento de fraude, cosa que impide que LA, capaz de identificar a D a partir de su firma, pueda vincular sus acciones.

En el protocolo de pago, D hace uso de distintas carteras digitales, desechando las vacías, para desvincular su actividad de las transacciones previas registradas en el blockchain. De este modo, el resto de entidades no pueden enlazar las acciones de D a partir de la "address" de su cartera digital. La generación de carteras no supone una carga para el sistema al ser un proceso individual que no involucra a otras entidades.

Al adquirir fondos para nuevas carteras, D utiliza una cartera temporal, a la cual se transfieren los tokens adquiridos del vendedor. Posteriormente, estos tokens se transfieren de la cartera temporal a las carteras operativas usando los servicios de M, quien ofusca el rastro de dichas transacciones. De este modo, la entidad vendedora no puede vincular la información del comprador con las operaciones de su carteras digitales.

IV-D. Exculpabilidad

Para poder iniciar una incidencia por fraude contra D, un AC ha de publicar en el Blockchain su propia copia de recibo de tránsito con la firma de grupo de D. En ese aspecto, no es posible para ningún AC acusar falsamente a D, ya que una prueba válida para sostener una incidencia solo puede obtenerse completando correctamente los procesos de acceso y salida con la intervención de las entidades involucradas. De igual modo, D dispone de su propia evidencia, firmada por un AC, como defensa a cualquier acusación infundada.

V. Conclusiones y trabajo futuro

Los actuales sistemas de control de acceso a LEZs ponen de manifiesto una dependencia hacia entidades centralizadas en los procesos de verificación, tarificación y cobro de los accesos de los vehículos. Aunque se han hecho progresos para acabar con esta estructura centralizada y la problemática que la presencia de "single point of failure" conlleva, las actuales propuestas descentralizadas todavía presentan poca flexibilidad con respecto a los parámetros que pueden cuantificar.

El sistema de control de acceso a LEZ propuesto en este artículo adopta la tecnología de los "Smart Contracts", junto con el subyacente paradigma descentralizado del Blockchain, con el fin de eliminar las entidades centralizadas de los procesos de tarificación y cobro presentes en la literatura actual. A diferencia de otras propuestas descentralizadas, nuestro sistema presenta de una mayor flexibilidad a la hora parametrizar el tránsito de los vehículos en la LEZ, permitiendo tarificar no solo por acceso sino también en función del tiempo de su estancia. Durante todo el proceso, gracias al uso de esquema de firmas de grupo, el sistema preserva la privacidad de los usuarios y no permite su seguimiento ni la vinculación de sus accesos.

Como trabajo para el futuro, se prevé la implementación del sistema propuesto, poniendo especial interés en la fase de pago, con el fin de verificar la viabilidad, coste y consumo de Gas del Smart Contract propuesto.

Agradecimientos

The following funding sources are gratefully acknowledged: Governments of Catalonia (2017 SGR 705) and Spain (RTI2018-095094-B-C21). We also acknowledge the FEM-IOT project, co-financed by the European Union Regional Development Fund within the framework of ERDF Operational Program of Catalonia 2014-2020, granting the 50 % of total eligible cost. The authors' opinion in this work are their own and do not commit UNESCO Chair in Data Privacy.

Referencias

[1] World Health Organization and UNAIDS and others, *Air quality guidelines: global update 2005*. World Health Organization, 2006.

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

[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] M. Hoffmann, V. Fetzer, M. Nagel, A. Rupp, and R. Schwerdt, "P4TC - provably-secure yet practical privacy-preserving toll collection," *IACR Cryptology ePrint Archive*, vol. 2018, p. 1106, 2018.

[11] 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.

[12] J. Hajny., P. Dzurenda., L. Malina., and S. Ricci., "Anonymous data collection scheme from short group signatures," in *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications - Volume 1: SECRYPT,*, INSTICC. SciTePress, 2018, pp. 200–209.