Security and Privacy in a Blockchain-Powered Access Control System for Low Emission Zones

Carles Anglés-Tafalla*, Alexandre Viejo*, Jordi Castellà-Roca*,
Macià Mut-Puigserver†, M. Magdalena Payeras-Capellà†
*Departament d'Enginyeria Informàtica i Matemàtiques, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Av. Països Catalans 26, E-43007 Tarragona, Spain
E-mail: {carles.angles,alexandre.viejo,jordi.castella}@urv.cat
†Dpt. de Ciències Matemàtiques i Informàtica, Universitat de les Illes Balears, Ctra. de Valldemossa, km 7.5. E-07122 Palma de Mallorca, Spain
E-mail: {macia.mut, mpayeras}@uib.es

***Abstract*—Low Emission Zones (LEZ)s are areas where access restrictions to polluting vehicles are enforced. These infrastructures have become a main mechanism in large cities to deal with urban traffic and environmental pollution. A main problem of practical LEZs is that they generally depend on a camera network that identifies users and jeopardizes their privacy. In the literature, there are some privacy-preserving works that rely on camera-free approaches; however, they still suffer from a major issue: they depend on centralized entities to manage the vehicles' accesses/departures and their corresponding fee payment. Those centralized entities represent a critical single point of failure in the system, endangering its security and availability. In order to address this situation, this paper proposes a new scheme that decentralizes the LEZ management, dealing with vehicle accesses as blockchain transactions, and pricing and charging them using smart contracts. In order to validate the deployability of the new scheme in real scenarios, it has been implemented and tested in both a controlled environment and a low-traffic street. The evaluation of the smart contracts' costs in terms of gas has been included in the performed tests. The results obtained are satisfactory and show the feasibility of the new proposal.**

***Index Terms*—Low Emission Zones, Electronic Road Pricing, Smart cities, Privacy, Security, Blockchain.**

I. Introduction

In the last years, Low Emission Zones (*LEZ*)s (i.e. areas where access restrictions to polluting vehicles are enforced) have emerged as one of the most popular mechanisms in Intelligent Transportation Systems (ITS) to tackle urban traffic congestion and its subsequent impact on the environmental pollution. The rapid proliferation of LEZs through all Europe[1] confirms this assumption. In this way, central-Europe countries such as Germany, The Netherlands, Belgium, and the north of Italy have already implemented LEZs in some specially relevant areas as a way to honour the Paris Agreement[2]; while others, such as Spain, plan to deploy LEZs in all cities with more than 50,000 inhabitants[3].

In the view of that trend, the need to implement access control systems which enables compliance with LEZs' restrictions arises. In that matter, currently deployed automated approaches are based on camera networks, whose purpose is to indiscriminately photograph the license plates of all vehicles circulating the LEZ. Then, by means of an Automatic Number Plate Recognition (ANPR) system, those vehicles are identified and their accesses to the restricted area notified to a centralized entity which, in turn, proceeds by calculating and charging the corresponding access fees.

London [1] and Stockholm[4] are representative examples that implement this same approach but differing in their camera network layout. The London's network is composed by more than 1,000 cameras which are spread over the whole downtown's restricted area. On the other hand, in Stockholm, cameras are placed only at the entrance and exit points.

As the aforementioned examples reveal, these approaches are of an intrusive nature as users are identified each time they drive nearby a LEZ's infrastructure by means of the charging entity. This situation jeopardizes the privacy of those who interact with the system and reveals the need of alternative LEZ control systems that tackle the user's personal data in a more privacy-friendly way.

Besides these privacy threats, a structural issue has been also identified in the current LEZs' access control systems. In particular, current schemes strongly depend on centralized entities to manage the processes related to vehicles' access acknowledgment and fee payment. Those centralized entities represent a critical single point of failure in the whole system, endangering its security and availability.

Dealing with centralization issues is not a new topic in ITS. In the literature, several efforts have been made to bring decentralized coordination to vehicular scenarios, such as collision avoidance and intersection management [2]. The use of V2V communications to decentralize the coordination of autonomous vehicles has prevailed in this kind of scenarios to tackle bottleneck, lack of privacy, and fault tolerance problems.

Recently, the *Blockchain* (i.e., a public verifiable open ledger) has emerged as a promising tool to design and create

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

[2]Paris Agreement, https://unfccc.int/

[3]Strategic Framework of Energy and Climate, https://www.miteco.gob.es/es/cambio-climatico/participacion-publica/marco-estrategico-energia-y-clima.aspx

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

new decentralized paradigms that enable to securely settle arbitrary resource transactions, such as interactions between vehicles and infrastructures. This cutting-edge technology, when applied to ITS and, in particular, to LEZs' access control systems, may lead to design a decentralized solution that solves the privacy and structural issues identified in the literature.

A. Related Work

In the last years, considerable work has been published regarding the privacy issues related to LEZs' access control schemes, congestion charge (CCZ), and Electronic Road Pricing (ERP) control systems. Some relevant examples can be found in [3]–[13]. The main principle behind all these approaches lies in gathering fee-relevant vehicle data while circulating inside the restricted area to subsequently send it anonymously to a centralized third party, usually a Service Provider (SP), which validates the received data and determines the fee amount to pay. These systems rely on anti-fraud mechanisms based on the use of camera networks that collect vehicles' evidence for further analysis and punishment (if required) of those drivers that do not follow the protocol as expected.

Depending on the specific conditions under which those methods are using their camera networks to collect vehicles evidences, current published works can be classified into two main categories: i) *indiscriminate camera shooting*; and ii) *selective camera shooting*.

Proposals such as [3]–[8] fall into the *indiscriminate camera shooting* category. In these schemes, a SP gathers information of all vehicles' license plates driving through the LEZ by means of camera-based checkpoints. First, fee payment is computed by gathering anonymous location and time data from the vehicles' On Board Unit (OBU). Then, in order to detect fraudulent users trying to fake or alter their routes data, the information received from the OBUs is verified by means of a cryptographic protocol and the license plate recordings that have been gathered systematically.

A main shortcoming of the schemes that apply indiscriminate camera shooting is that they gather a lot of personal data from the drivers in a systematic way, regardless of whether the drivers are behaving in a dishonest way or not. This situation represents a major privacy issue for the involved users. As indicated in [6], another important shortcoming of this anti-fraud approach is that drivers can identify those checkpoints, or they can even collude to disclose their locations in order to deliberately avoid them and continue committing fraud. This misbehavior can only be solved by means of deploying more camera-based checkpoints which, in turn, will even gather more drivers' personal data, directly increasing the aforementioned privacy problem. In the end, this fraud measure poses a trade-off between user's privacy and fraud detection, as increasing the number of checkpoints results in more fraud detection but also in more vehicles' locations disclosure. In an extreme case, this method may result in the SP being able to fully track vehicles all by itself without needing the OBUs' anonymous data to estimate the users' fees.

Proposals belonging to the *selective camera shooting* category are more recent. In particular, the authors in [10] presented the first scheme aligned with this approach in 2016. After this preliminary solution, other works such as [11], [12], [14] have followed a similar path.

The main idea behind [10] is to complete an authentication process each time a vehicle meets a system infrastructure and to take photos only when the driver misbehaves by omitting or tampering with this process. By only taking evidences of dishonest drivers, the privacy of the honest ones is successfully preserved. The proposal presented in [11] is an enhancement of [10] that tackles a multi-fare LEZ scenario which dynamically changes the fare prices according to the traffic density. Both proposals share the same two shortcomings: i) they rely on group signatures to preserve the users' privacy when the SP is computing the access fees, however, the signature scheme in use requires generating new keys and certificates for each access to the LEZ which places an important burden on their efficiency; and ii) the existence of an untraceable e-payment scheme is assumed but left as out of the scope.

The scheme presented in [14] is a direct solution to the low efficiency of [10] and [11]. In particular, this work follows a different privacy-preserving approach based on pseudonyms which allows to simplify the vehicles' access data management when the SP is calculating fees during the payment step. Additionally, it also proposes using the driver's smartphone instead of the vehicle's embedded OBU as client device in pursuit of a greater deployability.

Finally, [12] is similar to [11] and it tackles an ERP multi-fare scenario as well; Nevertheless, in this case, the authors introduce an electronic payment system based on cryptographic debt-accumulation wallets, formally defining an aspect not covered in the aforementioned works. In this scheme, debt is anonymously accumulated, using Non-Interactive Zero-Knowledge (NIZK) proofs in the users' wallet during the access step. Then, at the end of the billing period, users are requested to settle their wallet's debt with the SP before it issues a new one.

Despite the category in which each of the aforementioned works fall, all of them share the same objective: they try to punish dishonest drivers while preserving the privacy of the honest users at their best. In addition to that, all of them also share a significant issue: they strongly depend on centralized entities (usually a SP) to perform their main procedures, i.e., acknowledging vehicles' access data, ascertaining their traffic fees, and charging the corresponding amount of money. The existence of centralized entities occupying a dominant position in the main protocols makes the whole system more vulnerable to technical failures and malicious attacks, threatening its security and availability.

B. Contribution and plan of this paper

In the last years, the blockchain technology has become a disruptive approach that has paved the way to support distributed and trusted sharing ecosystems in various domains. More specifically, the literature has already reported that exploiting this technology will allow the scientific community

to bring decentralized trust and transparency to intelligent transport systems scenarios such as the LEZs [15].

In order to address the centralization problems detected in the literature and taking into account the potential of the blockchain technology in intelligent transport systems, in this paper, we propose a new scheme that decentralizes the LEZ management, dealing with vehicle accesses as blockchain transactions, and pricing and charging them through the use of smart contracts.

Our new scheme is supported by a preliminary version presented in [16]. In particular, the new proposal extends the former one by means of the following points:

- A new more flexible approach in terms of fee calculation parameters is proposed.
- Security and privacy discussions are broadened in order to provide a formalized thorough analysis and meet the protocol extension's new claims.
- An extensive evaluation of the proposal is performed. This includes analyzing the performance of the designed smart contract's logic and its feasibility in a relevant scenario under the Technology Readiness Level 5 (TRL5) according to the European Commission [17].

Regarding the current literature, our new scheme achieves a set of properties that are not currently covered by the other works:

- *Non-probabilistic fraud control system:* Our system preserves the privacy of the drivers who behave honestly but it is capable of detecting dishonest users and punishing them.
- *Revocable anonymity:* The drivers' privacy is preserved as long as they follow the protocol in a trustworthy way; this is, the system is not able to disclose the identity of honest drivers who properly authenticate themselves, but it can identify those who try to commit fraud by skipping the system's procedure.
- *Decentralized system:* The proposed system decentralizes, by means of a blockchain-based distributed network, the entities responsible for registering vehicle accesses and pricing and charging fees. This improves the transparency of the system while preventing the entity that controls the LEZ infrastructure from introducing a single point of failure in the system, endangering its security and availability.
- *Anonymous payment:* The proposed system protects the anonymity of the users during the fee payment procedure by means of the smart contract technology and related privacy-preserving measures.

The rest of the paper is organized as follows. Section II introduces preliminaries. Section III formalizes the protocols that sustain the proposed scheme. Section IV analyzes the security and privacy guarantees of our approach. Section V analyzes the performance of the proposal, including its feasibility in a TRL5 scenario and the smart contract's logic gas consumption. Finally, Section VI reports the conclusions.

II. Our proposal

This section introduces the new scheme and its properties. First, it details the actors which are involved in; next it gives a general overview of how the proposed system works; then, it discusses how the blockchain is integrated into the scheme; finally, it depicts the security and privacy requirements which have been considered during its design.

A. Actors

The proposed system involves the following five actors:

- LEZ Administration (*LA*): This is the entity in charge of managing the LEZ. It is responsible for setting the access rules, the price, and deploying the smart contract that manages the accesses and payments of the system.
- Drivers (*D*s): They are the group of users whom the approach is addressed to. Ds's vehicle should be equipped with an on-board unit (*OBU*), which is assumed to be a tamper-proof device with cryptographic capabilities and equipped with GPS technology, 4G, and short range communications (e.g. Bluetooth, Zigbee, IEEE 802.11p/DSRC, etc.).
- Access Control Points (*ACP*s): They are physical infrastructures that control Ds' accesses to the LEZ. For this purpose, they are assumed to be equipped with a camera, GPS, short range communication, and Internet access. $ACPs$ may be under control of one or more for-profit entities but the LA cannot be one of them.
- Smart Contract (*SC*): This is a specific programmed transaction protocol to include the vehicular LEZ circulation details on the blockchain, so it can verify, price, and charge (in terms of digital currencies) the vehicles driving through the LEZ.
- Cryptocurrency Mixing Service (*M*): This is an independent for-profit entity (e.g., ETH-Mixer[5] or Tornado-Cash[6]) responsible for obfuscating the traceability of cryptocurrency transactions so that the transferred funds cannot be trailed back to the source digital wallet. The services of M are expected to be used when a user D is transferring digital currencies between two of her own wallets. This situation happens in the wallet renewal or in the temporary wallet relay process during crypto coins purchase.

B. General overview

Figure 1 depicts, in a general way, how the proposed scheme works along with the actors involved in the process.

Prior to the dialog between D and ACP, it is required that the D's OBU obtains from the LA valid credentials that certify D's emissions category; next, D's OBU must generate a set of digital wallets which will be used to interact with the restricted area's smart contract.

The proposed protocol starts when D is about to enter a LEZ and its OBU automatically awakes, triggered by the proximity detection signal of the communication technology in use. Once this signal is detected, the OBU establishes a secure connection via short-range wireless communication system with the ACP, permitting both parts to authenticate

[5]ETH-Mixer, https://eth-mixer.com/

[6]Tornado Cash, https://defirate.com/tornado-cash/

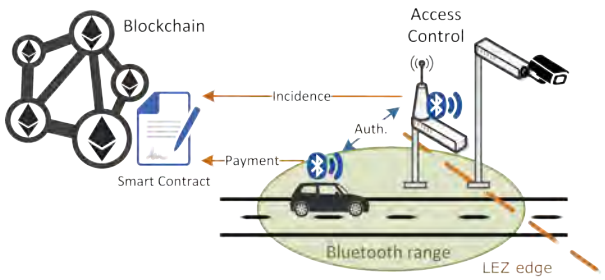


Fig. 1. System's general overview [16]

themselves, agree on the entrance parameters, and obtain an *access receipt* signed by their counterpart.

During the whole process, the user's anonymity is preserved through the use of a temporary alias, which can be changed at will in order to prevent other entities from binding the different accesses performed by means of a certain temporary alias. Conversely, if the authentication process is tampered with or it is somewhat skipped due to D's misbehavior, the ACP will take a photo of the vehicle's license plate, identifying the misbehaving driver and, hence, revoking her privacy.

When D is about to depart from the LEZ, a connection between the D's OBU and the ACP is established in a similar way as in the LEZ access step. However, in this case, both entities obtain a signed *exit receipt* instead. Both access and exit receipts constitute the *LEZ transit receipt*. Note that, this receipt contains a parameter to identify the linked transaction which is stored on the blockchain.

Once D completes the LEZ departure process, the corresponding payment must be done. To this effect, the D's OBU remotely calls the LEZ smart contract's payment method including, as parameters, some of the data stored in the *LEZ transit receipt*. By means of those parameters, the smart contract's logic: i) verifies their validity; ii) calculates the amount to pay according to the applicable prices published on the blockchain; and iii) automatically charges the corresponding amount, in terms of digital currencies, from D's to ACP's digital wallets.

Later in time, the $ACPs$ involved in the aforementioned access and departure processes may verify whether the transit transaction was correctly conducted and published on the blockchain.

In case of any irregularity, the $ACPs$ may open an incidence by calling the corresponding smart contract's method. In this procedure, the calling ACP will publish its own copy of the *LEZ transit receipt*, which contains the D's digital signature. By means of this information published on the blockchain, the LA can disclose the D's identity, revoking her anonymity, and it may then take any punitive measure.

C. Blockchain integration

The public ledger known as blockchain was originally designed as a mechanism to provide decentralization to financial transactions [18]. The principle behind this technology consists in granting equal decentralized trust to any node with the power of solving computational challenges, known as Proof-of-Work (PoW), and using it as a way to reach consensus. This concept was extended in [19] with Ethereum, whereby programmable logic programs (referred to as smart contracts) are run on the blockchain permitting to settle transactions of arbitrary resources in a decentralized way.

Design issues such as high PoW processing time, lack of scalability, or transactions fees payment do not fit well into heterogeneous scenarios, namely the Internet of things (IoT) or the Internet of Vehicles (IoV). In this way, researchers have proposed alternative consensus mechanisms to PoW in order to deal with those problems and integrate the Ethereum Virtual Machine (EVM) smart contracts' logic into these fields. Relevant examples of these efforts are the Proof-of-Stake (PoS) in Ethereum 2.0, where the nodes with the highest stake or deposit in the network are selected as block validators; and the Randomized Delegated Proof of Stake (Roll-DPoS) [20], a specialization of PoS for IoT scenarios which is used by the IoTeX[7] blockchain network. Conversely, IOTA [21] follows a different approach to solve the typical blockchain drawbacks in IoT scenarios. In particular, IOTA uses a Hash Directed Acyclic Graph (DAG) instead of the blockchain to process transactions in a parallel way. In the DAG, the Fast Probabilistic Consensus (FPC) protocol is used to reach consensus, combined with *Mana*, a delegated proof of token ownership used as a transferable reputation metric to avoid dishonest nodes from disturbing the validation process.

IoTeX and IOTA are IoT-specialized distributed ledgers compatible with EVM. This compatibility allows the deployment of native Ethereum smart contracts in those networks and gives access to the entire Ethereum development and testing ecosystem. This fact eases significantly the integration of the smart contract technology in IoT and IoV scenarios. In this way, the new scheme uses the programmable logic of EVM's smart contracts to include vehicle access details in blockchain transactions, and (on the basis of this data) automatically price and transfer the corresponding fees in terms of digital currencies. With this procedure, the nodes of the blockchain network are able to validate the vehicle access to the LEZ in a fully distributed way, enabling the system to run free of centralized third parties that oversee the whole process.

The blockchain paradigm requires network nodes (i.e., miners or validators depending on the network consensus mechanism in use) to contribute their resources to validate transactions and ensure a trustworthy advancement of the chain. In that regard, the proposed smart contract is expected to be deployed in a consolidated EVM-compatible network in order to get access to a well-established miners' ecosystem. In addition to this, we expect that the final users of the system (i.e., Ds) may act as miners/validators to compensate part of the money spent in driving through the LEZs. Also, we expect the for-profit entities that support the ACPs to hold significant resources that may be used to mine or validate and, thus, get an extra income.

[7]IoTeX, https://iotex.io/

D. Security and privacy requirements

The considered attack model is based on the following points: i) a driver D is dishonest if she follows the protocols partially or tampers with their data flow; ii) access control points (ACPs) are considered to be *honest-but-curious*, this is, they follow the proposed protocol as expected, but they may try to learn the Ds' personal data if they have the chance; iii) different ACPs may be controlled by different entities; iv) the LEZ Administration (LA) is a fully trusted entity; v) the LA and the ACPs are entities engaged in a commercial activity in which they collect data related to people, in this way, in EU countries, those entities are obliged to apply the principles of the General Data Protection Regulation (GDPR) [8] (i.e., data minimization, transparency, enforcing cyber-security measures, etc.); and vi) the computational power of the attackers do not permit them to break current computationally secure cryptosystems.

According to this adversary model, the proposed LEZ control system is designed to fulfill the following properties:

- *Revocable anonymity for dishonest drivers*. Ds' privacy is granted as long as they comply with the protocol. Otherwise, the proposed system is able to expose the identity of a dishonest driver, even if she does not hold any credentials.
- *Driver accesses to the LEZ are non-traceable*. The proposed system provides mechanisms that prevent adversaries from linking the different entrances and departures to and from the LEZ performed by a certain D, even when they are published on the blockchain.
- *Non-repudiation and integrity*. The evidences generated from the interaction between entities cannot be denied, forged or counterfeited.
- *Fraud avoidance (exculpability)*. D cannot be falsely accused of not paying their corresponding fees.

III. The proposed system in detail

The life-cycle of the proposed system is divided into seven protocols:

- *On-board unit set-up*: It describes the registration process that a D's OBU should complete with the LA to obtain the credentials which are required to successfully interact with the system.
- *Access control point set-up*: It defines the configuration process that a new ACP should perform to obtain its credentials and become operational.
- *Wallet filling*: It outlines the set of operations that a D should perform in order to anonymously purchase crypto coins (i.e., elements acting as native currency in our system) from the LA.
- *Access*: It describes the set of interactions between D and ACP which are required to agree with the parameters to access the LEZ.
- *Exit*: It describes the protocol between D and ACP which is run when D departs from the LEZ. As a result of this process, the departing D gets the *LEZ transit receipt*.
- *Payment*: It defines the steps that a D should follow in order to publish an agreed LEZ access on the blockchain and pay the corresponding fee by means of a smart contract interaction. This procedure includes the countermeasures that ACPs may apply against dishonest Ds who try to alter the protocol for their own profit.
- *Privacy Configuration*: It describes how a D's OBU renews the vehicle credentials and certificates as a measure to protect D's privacy.

In the following subsections, those seven protocols are formalized, giving enough detail to allow their implementation. Table I summarizes the notation of the most relevant elements used in those protocols.

A. On-board unit set-up

This initial protocol consists in configuring the D's OBU to obtain the required credentials that will be used to securely interact with the other system's entities. To this end, the OBU establishes a secure communication channel with the LA servers and provides the D's vehicle information (plate number, car maker, model, etc.). It is assumed that the OBU cannot be tampered with to provide false information. It is also assumed that the LA, as a governmental entity (e.g., the city council), is able to verify the correctness of the provided data and retrieve the vehicle's owner information from it. When the LA receives the vehicle's data, it performs the following operations:

a) LA checks whether the vehicle's data matches the plate number and, next, it obtains the owner's data (name, residence, etc.).
b) LA generates a pseudo-random temporary alias β.
c) LA binds the vehicle temporary alias β to the vehicle's owner.
d) LA sends β as One-Time-Secret (OTS) to D through an alternative channel.

Once D gathers the temporary alias β, she performs the following steps:

a) D generates a key pair (sk^D, pk^D).
b) D computes a certificate request $CSR(pk^D)$ for the generated public key, containing the temporary alias β in the *CommonName* field instead of the user's personal data.
c) D sends back the certificate request $CSR(pk^D)$ to LA.

When LA receives a valid $CSR(pk^D)$, it performs the following operations:

a) LA verifies the validity of the temporary alias β contained in $CSR(pk^D)$. If this verification fails, the vehicle registration is aborted; otherwise, the process continues.
b) LA gathers the vehicle's information bound to β.
c) LA issues the certificate Γ^D, including β in the *CommonName* field and the vehicle emissions category cat as a certificate extension. Note that, LA may include other extensions (e.g. a LEZ residence proof).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

TABLE I
NOTATION

Name	Description	Name	Description
pk^D	D's public key	$CSR(pk^D)$	D's certificate Request
sk^D	D's private key	Γ^D	D's certificate
W_D	D's digital wallet	β	Temporary alias
W_D^n	D's wallet #n	W_D^T	D's temporary wallet
pk^{ACP}	ACP's public key	$CSR(pk^{ACP})$	ACP's certificate Request
sk^{ACP}	ACP's private key	Γ^{ACP}	ACP's certificate
W_{ACP}	ACP's digital wallet	Γ^{LA}	LA's certificate
ϕ	ACP registration request	ϕ'_{ACP}	ϕ signed by ACP
δ	Access transaction ID	cat	Vehicle emissions category
ψ	Access information tuple	ψ'_D	ψ signed by D
$r\psi$	Access proof	$r\psi'_{ACP}$	$r\psi$ signed by ACP
ω	Departure data	ω'_D	ω signed by D
ρ	LEZ transit receip	$\rho'_{W_{ACP}}$	ρ signed by ACP's wallet
$r\omega$	Departure proof	$r\omega_{ACP}$	$r\omega$ signed by ACP
β^*	Renewed temporary alias	W_D^*	D's Renewed digital wallet

d) LA sends the generated certificate Γ^D to D.

Finally, in order to complete the registration process, D carries out the following operations:

a) D verifies the validity of the certificate Γ^D through Γ^{LA}. If this verification fails, the procedure is aborted; otherwise, it continues.
b) D securely stores Γ^D and (sk^D, pk^D).

Once the vehicle's credentials have been retrieved, D generates an *EVM digital wallet* W_D or, depending on her privacy preferences, a set of them $W_D^1 \dots W_D^n$. Next, the following steps are done:

a) D generates, for each wallet, a private key sk of 256-bit, a public key pk of 512-bit, and she derives its address according to the EVM key specs.
b) D securely stores the set of digital wallets $W_D^1 \dots W_D^n$.

B. Access control point set-up

When a new ACP infrastructure is deployed in the LEZ, a set of procedures are required for it to be operative. First, the entity implementing the ACP must formally request its deployment to the LA and provide the ACP's data: ACP_{id}, location coordinates, street, street direction, district, etc. Once the LA has verified and accepted the new infrastructure's setup, the ACP establishes a secure connection with LA's servers and generates its credentials following the next steps:

a) ACP generates a key pair (sk^{ACP}, pk^{ACP}).
b) ACP computes a certificate request $CSR(pk^{ACP})$ for the generated public key, containing the ACP_{id} in a certificate field.
c) ACP sends the certificate request $CSR(pk^{ACP})$ to LA.
d) LA receives the $CSR(pk^{ACP})$ and, first, it verifies that the certificate request information matches the one in the request. If this verification fails, the process is aborted; otherwise, it continues.
e) LA issues the certificate Γ^{ACP}.
f) LA sends the generated certificate Γ^{ACP} to ACP.
g) ACP receives Γ^{ACP} and verifies the validity of the certificate by means of Γ^{LA}. If this verification fails, the certificate is discarded and ACP should start over the process.
h) ACP securely stores Γ^{ACP} and (sk^{ACP}, pk^{ACP})
i) ACP creates a digital wallet W_{ACP} by generating a private key sk of 256-bit, a public key pk of 512-bit, and its address according to the EVM key specs.
j) ACP generates a registration request ϕ = $\{date, time, position, address\}$ and computes its digital signature ϕ'_{ACP}.
k) ACP sends ϕ and ϕ'_{ACP} to LA.
l) LA receives the registration request from ACP. LA then verifies the ACP's data in ϕ, and ϕ'_{ACP} by means of Γ^{ACP}. If everything is correct, it proceeds with the registration.
m) LA calls the SC method $regiter\_ACP$, only reachable for the SC's owner.
n) The SC adds the ACP_{id}, the W_{ACP} address and the ACP location in the authorized ACPs mapping, so they are published on the blockchain once the transaction is validated.

C. Wallet filling

In order to pay the use of the LEZ and the blockchain network's fees, Ds purchase crypto coins (i.e. elements acting as native currency in our system). For this specific purpose, LA is expected to host an Internet portal where Ds can buy crypto coins, which can then be directly transferred to their wallets[9] by means of classic payment mechanisms (e.g., credit card, wire transfer, or other cryptocurrencies). Purchasing coins may permit the binding of Ds' digital wallets to their respective bank accounts and, hence, it may jeopardize their privacy. To prevent this issue from happening, the next steps are followed:

a) D creates a temporary wallet W_D^T.
b) D accesses LA's Internet portal and purchases *crypto coins*. These coins are sent to the temporary wallet W_D^T.
c) D requests a *cryptocurrency mixing service*, M, to transfer the purchased crypto coins from the temporary wallet W_D^T to D's set of wallets $W_D^1 \dots W_D^n$. By means of a mixing process, M can cut the link between the source

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

and destination wallets when the funds are transferred, preventing the selling entity from binding any payment information with D's transactions on the blockchain.

d) Once the coins have been transferred, D discards the temporary wallet W_D^T.

After this process, the purchaser's identity cannot be linked to her wallet, however, the transactions in which a wallet is involved in can still be linked together through its address. Different strategies may be applied to address this problem. The simplest one would be that D uses only one wallet at a time, generating a new one each time she wants to cut the link between her transactions. Remaining funds in the old wallet can be transferred to the new one by means of M and the transaction obfuscation process that this entity provides.

D. Access

This protocol begins the moment D enters the ACP communication range. Then, both entities establish a secure communication via a secure channel (e.g., TLS). As a result of that, there is a strong bilateral authentication between both parties in which each one gets the counterpart's certificate (i.e. Γ^D and Γ^{ACP}). Then, they perform the following steps:

a) D generates a random 64-bits value δ_D, first half of the access ID that identifies the transaction on the blockchain.

b) D generates the access information tuple ψ=$\{\delta_D, pos_i, date_i, time_i, cat\}$. Next, it computes the corresponding digital signature $\psi_D^{'}$.

c) D sends ψ and its digital signature $\psi_D^{'}$ to ACP as receipt of the *access request*.

d) ACP receives the *access request* and, first, it verifies that Γ^D certificate is valid and has not expired; next, it verifies $\psi_D^{'}$ signature and checks if the data contained in ψ is correct. Note that the vehicle category cat is included in Γ^D.

e) If the previous verifications are correct, ACP generates a random 64-bits value δ_{AC} and calculates the access ID, $\delta = \{\delta_D \| \delta_{AC}\}$, which identifies the access transaction on the blockchain. Otherwise, ACP takes a photo of the vehicle's license plate and stops this procedure.

f) ACP prepares an access proof $r\psi = \{id_{ACP}, \delta, pos_i, date_i, time_i, cat, \psi_D^{'}\}$.

g) ACP sends the access data $r\psi$ and its corresponding digital signature $r\psi'_{ACP}$ to D as a proof of its access to the LEZ.

h) ACP stores $r\psi$ and ψ'_D until the payment of this access to the LEZ is completed and verified. These two elements are stored locally in the ACP and also, for backup purposes, in the cloud.

i) D receives the access data sent by ACP. D then verifies $r\psi$, along with the data contained in it, and $r\psi'_{ACP}$, by means of ACP's certificate Γ^{ACP}. Finally, D locally stores the proof of access until it leaves the LEZ by performing the exit protocol.

E. Exit

Similarly to the *Access protocol*, D must register her departure from the LEZ in order to obtain her *LEZ transit receipt*. To that end, when leaving the LEZ, D and the corresponding ACP establish a secure communication. This again implies performing a strong bilateral authentication and obtaining the counterpart's certificate. After that, they perform the following steps:

a) D prepares the departure data ω = ($r\psi$, $r\psi'_{ACP}$, pos_o, $date_o$, $time_o$), being $r\psi$ the receipt gathered during the access protocol. Next, it computes the corresponding digital signature ω'_D.

b) D sends ω and ω'_D to ACP.

c) ACP receives the exit request and, first, it verifies the signatures $\psi_D^{'}$ and $r\psi'_{ACP}$; next, it checks the validity of the data contained in ω. This validation process includes checking the vehicle's emissions category cat found in $r\psi$ with the one contained in Γ^D.

d) ACP checks the presence sensor and verifies whether the detected vehicle has been authenticated. If some verification fails, the system takes a photo of the vehicle's license plate. Then, ACP securely sends the photo to the LA for sanctioning purposes, and it immediately deletes it in order to comply with the data minimization principle of the GDPR.

e) If all the previous steps have been properly completed, D can exit the LEZ. For this purpose, ACP prepares a *LEZ transit receipt* ρ = (δ, $date_i$, $time_i$, $date_o$, $time_o$, cat, id_{ACP}) and its signature ρ'^W_{ACP}, signed with ACP's wallet private key, so it can be verified on-chain by the smart contract.

f) ACP sends the access data $r\omega$ = ($\rho, \rho'^W_{ACP}, \omega, \omega'_D$) and its corresponding digital signature $r\omega_{ACP}^{'}$ as a proof of their interaction. This sending could be optimized by omitting the redundant data in ρ and ω.

g) ACP locally stores ω and ω'_D until the payment process is completed and the transaction is published. Note that it also backups this data in the cloud for security purposes.

h) D verifies and temporally stores the *LEZ transit proof* $r\omega$ and its corresponding signature $r\omega'_{ACP}$ by means of Γ^{ACP}.

F. Payment

Once D obtains the *LEZ transit proof* and the corresponding *LEZ transit receipt*, she can start the payment process. This process is managed by means of a blockchain-based smart contract, without the intervention of any centralized entity (e.g., a service provider or the LA). Namely, D, using the signed *LEZ transit receipt* from ACP, interacts with the LEZ smart contract SC, which prices the use of the LEZ according to the agreed parameters and automatically transfers the corresponding amount in terms of digital coins. An overview of this process is shown in Figure 2.

First, as an individual step, LA, which is expected to be the smart contract's owner, has the authority to update the table of prices that SC inquires to determine the access fees. It is assumed that SC has a specific method for this purpose.

Once the *LEZ transit proof* $r\omega$ is obtained, D can start the payment process by calling the *register_access* method of the smart contract, uploading as parameters the *LEZ transit receipt*

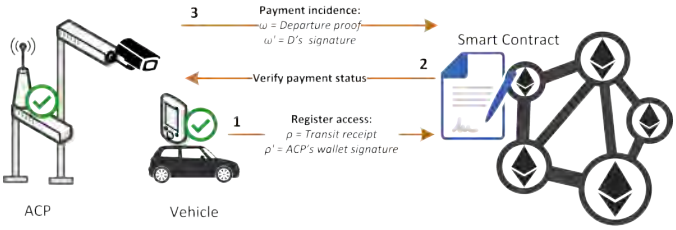


Fig. 2. Payment step

ρ and ACP's digital wallet signature ρ'^{W}_{ACP}. By calling this method, the following operations are processed on-chain by the SC's logic:

1) SC checks whether transaction δ is already published on the blockchain. In case it is registered and its status is set to "paid", no further action is taken. Otherwise, the LEZ access payment process continues.
2) SC verifies the receipt signature ρ'^{W}_{ACP} and discloses the address of the issuing wallet, which should belong to a registered ACP. If some verification is not correct, the status of transaction δ is updated to "invalid signature".
3) On the basis of elapsed time $time_o$-$time_i$ and the vehicle category cat contained in ρ, SC calculates the transit fee according to the applicable prices published on the blockchain at the access time.
4) SC transfers the corresponding fee amount in terms of crypto coins from D to ACP digital wallet. In case D's wallet does not have enough funds, all coins are transferred and the remaining amount to pay is updated. D can repeat the payment step with several wallets until the remaining debt is paid off, in which case the transaction status is set as "paid".
5) SC stores transaction δ with its attributes contained in ρ, the transaction status and the remaining debt. Regardless *register_access* execution result, the transaction is published on the blockchain.

Once enough time has elapsed for the transit transaction δ to be validated and published on the blockchain, the ACPs involved in the vehicle's access or exit verify the payment status by doing the following steps:

a) ACP gets the current transaction δ status by calling the *get_access_status* method.
b) ACP verifies whether the transaction with δ ID exists and if its current status is set as "paid". ACP also verifies if the published departure time $time_o$ is greater or equal to the one in its ω local copy.
c) If any of the previous conditions are not met, ACP publishes an incidence using the method *payment_incidence* of SC. In this process, the driver's temporary alias β, the transit data ω, and D's signature ω'_D are send as parameters.
d) In either case, in order to comply with the data minimization principle of the GDPR, ACP deletes the local and backup copies of the proofs of access/departure ψ or ω. Note that those proofs are no longer needed, either because the payment has been already completed, or because the access information has been published on the blockchain as an incidence.

SC, on its part, verifies whether the temporary constraints to publish an incidence are met by taking date and time in ω as reference to determine if enough time has been elapsed since the vehicle departure. LA, as the owner of the smart contract, is in charge of establishing the time that must be elapsed for an incidence to be opened. Once β, ω and ω'_D are published on the blockchain, LA could initiate sanctioning measures against any D who is linked to an incidence. This is possible because the temporary alias of D β is included in the access incidence information uploaded to the blockchain as well as D's signature, which only can be verified with D's certificate Γ^D. In this context, as LA knows the β-D relation, it is the only entity able to identify D.

By following the payment protocol, ACPs gather crypto coins in their wallets for every registered vehicle transit. It is assumed that LA, at each billing period, will monetarily reward the ACPs (in particular, the entities that support them) in accordance to the gathered amount, thereby getting profit from their services.

G. Temporary alias renewal

Even though the real identity of each D who uses the system is hidden behind a temporary alias β or an EVM wallet's address, those two elements, if used in different interactions, may be successfully linked and D's identity may be disclosed.

In order to prevent this issue, any D can ask for a new β^* to the LA in order to prevent other entities from binding her accesses. The change of a temporary alias β implies that a new pair of cryptographic keys (sk^D, pk^D) and a new certificate Γ^D have to be generated, due to the fact that β is embedded in the certificate's common name field.

Finally, when the protocol *Wallet filling* (see Section III-C) was discussed, the possibility of jeopardizing D' privacy by linking all her transactions that share the same wallet address was introduced, and it was suggested that D should use one wallet at a time as the simplest strategy to cut the link between her transactions. In this way, in order to securely renew her wallet, first, D must obtain a new wallet W^*_D by following the same operations stated in the protocol *OBU set-up* (see Section III-A). Next, D must anonymously transfer the funds between the old wallet W_D and the new one W^*_D by means of a mixing service M that obscures the relation between source and destination addresses.

IV. Security and Privacy Discussion

This section evaluates and discusses how the proposed access control system for LEZs fulfills the set of security properties stated in Section II-D according to the envisaged attack model (also introduced in Section II-D). These security properties are related to providing: i) revocable anonymity for dishonest drivers; ii) non-traceability of driver accesses; iii) non-repudiation; iv) integrity; and v) exculpability.

The evaluation and discussion of these security properties is grounded on four propositions. Each proposition is supported by a set of claims and their respective proofs.

Proposition 1. *The privacy of the drivers is granted as long as they comply with the protocol. Otherwise, the system is able to revoke the anonymity of a dishonest driver, even if she does not hold any credentials.*

Claim 1. *The proposed scheme guarantees the anonymity of honest drivers in the access protocol.*

Proof. In the bilateral authentication steps of the access/exit protocols, the ACP checks the driver's certificate, Γ^D. This certificate includes the emissions category, cat as a certificate extension, and includes β in the $CommonName$ field (the identity of each user D is hidden behind β), so no user's personal data is used in the authentication step. Moreover, although the ACP obtains the proof of access ψ with some information regarding the D's position in the authentication step, this element does not include any identifying information. □

Claim 2. *The proposed scheme guarantees the anonymity of honest drivers in the payment protocol.*

Proof. Once D has obtained the transit proof $r\omega$, she uses the smart contract to register the access and perform the payment. The parameters used in this procedure are the *LEZ transit receipt* ρ and ACP's digital wallet signature ρ'^{W}_{ACP}. No identifying information is present in these elements.

Next, the SC transfers the corresponding fee amount from D's wallet to ACP's wallet. D's wallet might be used to trace the identity of the user if the protocol was not well designed (purchasing coins may permit the binding of Ds' digital wallets to their respective bank accounts). In order to avoid this identification, the proposed protocol includes a method to manage D's wallets in a private way.

Temporary wallets are used to receive the crypto coins from LA's portal and, then, a mixing service is used to transfer the crypto coins from the temporary wallet to a set of wallets. By means of this mixing process, D's identity cannot be linked to the wallet used for publishing transactions on the blockchain. The use of different wallets allows to break the link between transactions. □

Claim 3. *The proposed system provides a method to revoke the anonymity of dishonest drivers with credentials.*

Proof. Although the new scheme provides anonymity to honest users, it also provides a method to identify dishonest drivers. In particular, once β, ω and ω'_D are published on the blockchain, LA could initiate sanctioning measures against dishonest drivers, that is, any D who is linked to an incidence.

In order to revoke D's anonymity, her temporary alias β plays a key role. In particular, β is included in the access incidence information published on the blockchain as well as D's signature, which can only be verified by means of D's certificate Γ^D. Only LA knows the relation between β and D, in this way, LA can reveal the identity of the dishonest driver who has used β. □

Claim 4. *The proposed system provides a method to revoke the anonymity of dishonest drivers without credentials.*

Proof. During the access protocol, ACP first receives an *access request* from D and it next verifies that Γ^D certificate is valid and it has not expired. If this verification fails because D's has no valid credentials, then ACP takes a photo of the vehicle's license plate and stops this procedure, revealing the identity of the user.

The exit protocol works in a similar way, and it also results in ACP taking a photo of the vehicle's license plate if any irregularity is encountered during the process. □

Proposition 2. *Drivers' accesses to the LEZ are not traceable.*

Claim 5. *Different entrances and departures performed by the same D are not linkable by means of the receipt. The temporary alias renewal protocol is used to provide unlinkability.*

Proof. Even when the accesses are anonymous, the reuse of certain elements in different accesses could be used to link some accesses done by the same D. In the proposed scheme, the real identity of each D is hidden by means of the use of a temporary alias β and a payment wallet. In this way, all accesses done under the same β could be linked, putting at risk the users' anonymity. In order to prevent this issue, any user D can ask at any time for a new temporary alias β^* to the LA (this implies that a new cryptographic key pair (sk^D, pk^D) and a new certificate Γ^D will be generated). Due to the fact that β^* is completely unrelated to the old β, different entrances and departures made with different βs will be unlinkable by an outsider too. □

Claim 6. *Different entrances and departures performed by the same D are not linkable when they are published on the blockchain.*

Proof. In the proposed scheme, the real identity of each D is hidden by means of a temporary alias β and a payment wallet. While the β is used to interact with the ACP when D enters and exits the LEZ, the payment wallet is used to interact with the blockchain-based SC and perform the payment of those entrances and departures. Different transactions published in the blockchain by means of the same wallet address will be linkable. In order to prevent this situation, D should generate a new EVM wallet W^*_D after each transaction, and she should use a mixing service M to transfer the remaining *crypto coins* from her old wallet to the new one, avoiding the traceability of the coins. □

Claim 7. *The only way for an external attacker to ascertain the accesses and departures performed by a certain D is to break the cyber-security measures applied by the LA and the ACPs to protect the gathered Ds' personal data (in order to comply with the GDPR). Even in this case, the window of opportunity for the attacker is limited due to the enforcement of the GDPR's data minimization principle.*

Proof. In the proposed scheme, the drivers' data is separated between the LA and the ACPs. This implies that the accesses/departures performed by a certain D can only be linked to her real identity if the LA and the ACPs share their data. The LA is fully trusted and the ACPs are *honest-but-curious*,

so they will not collude to achieve this purpose. As a result, an external attacker willing to get that personal data should be able to break the cyber-security measures applied by the LA and the ACPs and retrieve the required data. Even in this case, the ACPs follow the GDPR's data minimization principle and, hence, they delete any personal data linked to the drivers (i.e., access/departure proofs, license plate photos) as soon as this data is no longer needed (i.e., when the payment and sanctioning processes have been completed). □

Proposition 3. *The proposed system provides non-repudiation to the actors involved in the accesses to the LEZ.*

Claim 8. *D cannot deny having entered and/or departed the LEZ.*

Proof. At the entrance, D generates and digitally signs the access information item ψ. Then, at the exit, D generates and digitally signs the departure data ω. The cryptosystem in use to generate the signature provides the non-repudiation property to D's actions. The signatures generated by D can be verified by means of certificate Γ^D. In case of dispute and law enforcement, those signatures can be used to proof the entrance/departure of D in/from the LEZ. □

Claim 9. *ACP cannot deny its actions taken during a D's access to the LEZ.*

Proof. In the previous claim, we have discussed the fact that a D cannot deny having entered and/or departed the LEZ according to evidences ψ and ω. Regarding the ACP, which is the other party involved in the access/exit protocols, this entity also generates non-repudiation evidences for its counterpart. In particular, D gets the proofs $r\psi$ at the entrance point and $r\omega$ at the exit point. Both proofs are digitally signed by the respective access/exit ACPs (i.e., $r\psi'_{ACP}$ and $r\omega'_{ACP}$). The access/exit data (e.g., date/time and position) contained in $r\psi$ and $r\omega$ is linked to D by means of her digital signatures ψ'_D and ω'_D respectively included in the two aforementioned items. As a result of that, $r\psi'_{ACP}$ and $r\omega'_{ACP}$ unequivocally certify that a certain D has entered/departed in/from the LEZ under a certain set of conditions. In a posterior audit, D may use those proofs to prove its interactions with the involved ACPs, and these entities will not be able to deny them. □

Claim 10. *Access and exit receipts cannot be forged nor counterfeited.*

Proof. As it has been discussed in previous claims, access and exit receipts cannot be denied by their authors because they are digitally signed and work as a non-repudiation evidence. These digital signatures are assumed to be computed by means of a secure cryptosystem. In this way, they also provide the intrinsic properties of authentication and integrity. □

Claim 11. *Access and exit receipts cannot be reused.*

Proof. Access and exit proofs are linked by the same temporary alias δ. This item, in turn, is linked to an entry time and date by means of ψ and $r\psi$ and to a departure time and date by means of ω and $r\omega$. All these items are verified and digitally signed by D and ACP. In addition to that, ACP can check whether a certain transaction linked to δ has already been published on the blockchain in order to detect reused elements. In this way, if one entity reuses an old access/exit proof, then the other parties can be aware of that situation when they detect the reused δ value inside the exchanged items. Note that as the access/exit transaction identifier δ has two parts: the first one is chosen by D, and the second one is chosen by ACP. No entity is able to create a new transaction with the same identifier as an older one. □

Claim 12. *Payments have a timestamp.*

Proof. During the payment protocol, the SC calculates the transit fee according to the applicable prices based on the time that has passed between the entrance and the departure from the LEZ. This payment is then performed using crypto coins. Cryto coins are transferred from a D's wallet to ACP's wallet by means of a transaction published on the blockchain. Due to the fact that all transactions published on the blockchain are included in blocks that have a timestamp, the payments inherit the timestamp from the block in which they are published. □

Proposition 4. *The proposed system guarantees the exculpability of the honest drivers.*

Claim 13. *Drivers can prove their payments.*

Proof. The SC runs payments as blockchain transactions that transfer crypto coins from Ds' wallets to ACPs' wallets. The SC stores the transaction δ, the elements contained in the transit receipt ρ, and the transaction status (if the payment has been completed the status will be "paid"). Once the transaction is published on the blockchain, its payment status can be checked using the *get_access_status* method. Even though D can use different wallets to remain anonymous in the payment operation, she can prove by means of the blockchain that a certain transaction linked to δ exists and that its status is "paid". □

Claim 14. *Drivers cannot be falsely accused of not paying the access to the LEZ.*

Proof. ACPs are the entities in charge of verifying the payments. First, an ACP gets the status of a transaction δ by calling the *get_access_status* method. In this way, ACP verifies whether the transaction with δ ID exists and if its current status is stated as "paid". If a ACP wants to accuse D of not paying her access, the ACP must publish an incidence using the SC's method *payment_incidence*. In order to publish the incidence, the ACP must send D's temporary alias β, the transit data ω, and D's signature ω'_D. The incidence is then managed by the SC, which verifies whether the temporary constraints to publish an incidence are met. Once the incidence is published on the blockchain, LA can initiate the sanctioning process against D. However, if D has already paid for her access, when ACP tries to publish the incidence and reveals the value of ω, SC can then obtain the element δ and check the status of the transaction. If the status is "paid" then the incidence will be considered invalid and, hence, it will be discarded. □

V. Experimental Results

In this section, the feasibility of the proposed system is evaluated in a relevant scenario consistent under the Technology Readiness Level 5 according to the European Commission standards [17]. The purpose of this study is to ascertain the feasibility of the proposed system in a realistic setting.

A. Test Scenario

The life-cycle of the proposed system is divided into the seven protocols defined in Section III, but, for the sake of this study, we focus our analysis in three main points:

- Analysis of the protocols which are subjected to Real-Time Computing (RTC) constraints: the *Access* protocol (Section III-D) and the *Exit* protocol (Section III-E). Both procedures must respond according to certain time constraints while the vehicle is in the communication range of the system's infrastructure.
- Analysis of the performance of the decentralized fee calculation and payment processes during the *Payment* protocol (Section III-F).
- Analysis of the efficiency, in terms of gas, of the smart contract that manages the *Payment* protocol. The computational cost and storage requirements of this process have a direct impact on the system's feasibility.

In order to evaluate the feasibility of our system in a realistic environment, we have implemented two reduced-size prototypes to represent the entities involved in the *Access/Exit* steps: D and ACP. In particular, we have operated a handy stand-alone infrastructure to ease the deployment of the ACP on a street; and we have used a reduced LCD device, capable of communicating with the aforementioned infrastructure, as the D's OBU.

Focusing now on the communications between parties, it is worth mentioning that the proposed scheme is fully independent of the underneath communication technology, and it has been designed without assuming any specific communication feature. According to that, a wide range of short-range communication systems for vehicular networks such as Bluetooth, Zigbee or IEEE 802.11p/DSRC may be used. Among those options, we selected Bluetooth for our prototypes because it is a widespread general-purpose technology which can be easily found in the market and, in the last years, it has been systematically integrated into vehicles of all brands and price tags. Moreover, since this technology does not provide the advantages of more specialized vehicular communication technologies, using a more suited option should derive in better results than the ones achieved by means of Bluetooth.

Under this setting, two different lines of experiments have been run. First, a set of experiments have been conducted in a *controlled laboratory environment* in order to evaluate the performance of our system under optimal conditions. In this experiment, both D and ACP prototypes were placed, one next to the other, in a direct line of sight in an interference-free environment. We established a confidence interval of 20 exit protocol executions for this experiment.

The second line of experiments focused on validating the TRL5 level of maturity of our system. For this purpose, we deployed the ACP infrastructure in a *low traffic street*, in an industrial area, as shown in Figure 3. In this scenario we placed the OBU device inside a car at the co-driver's seat, and a BLE beacon-emitter wake module at 50 meters of the ACP in order to automatically awake the OBU's LEZ application. Under this setup, we drove through the ACP infrastructure at speeds of 20, 30, 40 and 50 km/h, running the exit protocol at each pass, in order to study the impact of the speed and the vehicle's body on the communication system. In this case, we ran the protocol 10 times for each proposed speed.

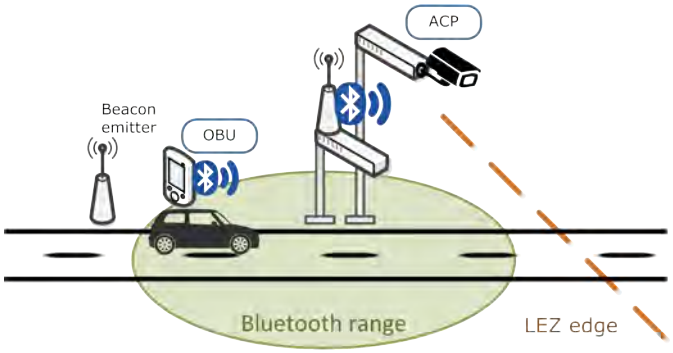


Fig. 3. Low traffic street deployment

The testbed configuration was the following:

- The ACP is running on a Raspberry Pi 3 with 1.2GHz quad-core ARM Cortex-A53 CPU, 1GB RAM, Bluetooth 4.1 Classic, Raspbian OS, supplied by AC-power. The ACP module also has a presence detector and a monochrome camera to detect and take photos of unauthenticated vehicles.
- The vehicle's OBU is implemented on a Raspberry Pi 3 with 1.2GHz quad-core ARM Cortex-A53 CPU, 1GB RAM, Bluetooth 4.1 Classic, Raspbian OS and equipped with a 3.5-inch LCD display to show the results. We also implemented an independent Wake Module running on a Raspberry Pi 1, simply equipped with a Bluetooth 4.0 device LM506/Class1, which periodically generates beacons to automatically wake up the OBU's application without any action from the driver.
- The protocol implementation running in the ACP and in the D's OBU was written in Java7 (openjdk-1.7) and the communication between both entities was established via Bluetooth, using its classic version 2.1 by means of Blucove Java library.
- The SC managing the *Payment step* is implemented by means of Solidity, an object-oriented programming language targeted on the EVM. Developing EVM smart contracts allows their deployment in any EVM compatible network like Ethereum, Binance Smart Chain, IoTeX, and IOTA. Among these options, we have used the Ethereum ecosystem in our experiments due to its maturity and its more advanced smart contract tools for testing, debugging, and doing performance analysis. In this way, the SC is deployed in the Ganache network, a personal blockchain used for Ethereum development,

which allows to evaluate better the performance of the smart contracts by avoiding the economic costs present in real operating networks such as the main Ethereum network.
- Signatures and encryptions were computed using the ECDSA cryptosystem with 256-bit key sizes. Furthermore, during *Access and Exit* protocols, the AES symmetric encryption scheme with 256-bit keys was used for managing the session keys.
- Regarding the digital wallets' cryptographic operations, they followed the Ethereum key specifications, this is, we used ECDSA with a 256-bit as private key and a point on the secp256k1 ECDSA curve (x,y point) as the corresponding public key. The public Ethereum address were the lower 160 bits of the Keccak-256 (aka SHA-3) digest of the public key.

It is worth mentioning that *Access* and *Exit* protocols share the same procedure and actors, so the performed experiments can be applicable to both of them. However, the latter performs some extra operations to verify the proofs obtained during the entrance, which makes it a little more costly in terms of computation and communication. For this reason, we focus the experiments on this step.

B. Performance evaluation in a laboratory environment

Table II depicts the results obtained in the tests performed in an interference-free environment. More specifically, the *Exit* protocol, from the instant the user-side application wakes up until it receives the signed interaction proof from the ACP, takes an average time of 1.46 seconds to be completed. This table also shows the fastest and the slowest protocol completion time, taking 1.047 and 1.790 seconds, respectively. The latter, representing the worst-case scenario, took 1.79 seconds, which, bearing in mind the vehicles' maximum speed limit of 50km/h in urban environments, results in a traveled distance close to 24.84 meters within that time interval.

TABLE II
CONTROLLED LABORATORY RESULTS (IN SECONDS)

Iteration	Time	Iteration	Time
1	1.489	11	1.514
2	1.790	12	1.558
3	1.144	13	1.490
4	1.047	14	1.327
5	1.413	15	1.624
6	1.326	16	1.481
7	1.462	17	1.720
8	1.073	18	1.599
9	1.536	19	1.759
10	1.402	20	1.555
Average	1.465	Deviation	.205

The total distance traveled in the worst case scenario (i.e., 24.84 meters) must be taken into account when deploying the system in a realistic setting, due to the fact that the ACP's communication technology range should cover at least that area in order to give the vehicles enough time to complete the *Access* and *Exit* protocols.

The run times shown in Table II cover all the processes performed in the *Access* and *Exit* protocols. It takes into account computation costs, communication overheads, and connection establishing time. Figure 4 broke down the times from Table II unveiling the average times of each relevant part of the *Access* and *Exit* protocols. As it can be appreciated, the connection establishment between the OBU's and ACP's Bluetooth devices consumes 0.903 seconds on average, representing the 61.7% of the step total run time. The remaining 0.562 seconds are entirely consumed during the protocol run, which includes: i) the ACP-side steps done by the system's infrastructure; ii) the user-side steps done by the vehicle's OBU; and iii) the communication overhead.

As shown in Figure 4, the ACP-side protocol and the OBU-side protocol take 0.081 and 0.380 seconds respectively, and the remaining 0.101 seconds are spent in transmitting 1788 bytes of data. It should be noted that the protocol run includes the costs of establishing an application-level strong bilateral authentication between the ACP and the OBU.

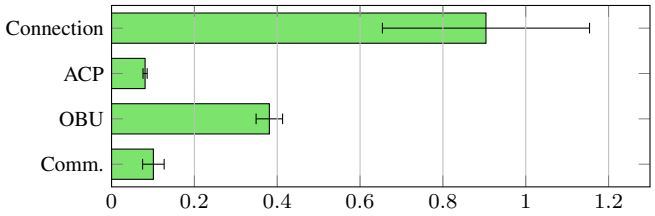


Fig. 4. Protocol execution and deviation time in seconds

The standard deviation shown in Figure 4 reveals that the completion times variability in Table II is mainly caused by communication issues, such as the Bluetooth connection establishment and the data transmission. Although, in relative terms, data transmission outlines a higher variability coefficient (i.e., 25.6%) than the Bluetooth connection process (i.e., 21.6%), in absolute terms the latter's variability has a lot more impact, this is 0.195 seconds, in the step total time than any other element of the protocol. In any case, it can be observed that, even in an interference-free scenario, the Bluetooth communication introduces a significant instability into the whole system's performance.

C. Performance evaluation in a low traffic street

In Section V-A, we defined a test scenario that validates the TRL5 level of maturity of our system. In particular, this setting is depicted in Figure 3.

We have conducted a set of performance tests in this environment and the results obtained are summarized in Figure 5. Those results show that the *Exit* protocol for vehicles circulating at speeds of 20, 30, 40 and 50 km/h requires, respectively, 2.69, 2.39, 2.09 and 1.90 seconds to be completed. These average times represent an increase between 0.44 and 1.22 seconds regarding the interference-free results obtained in the controlled laboratory setting. The time costs increase as expected due to the appearance of external factors inherent in any realistic vehicular scenario. Those factors are: signal

interference, vehicles' movement, and signal jamming because of the own vehicle's body.

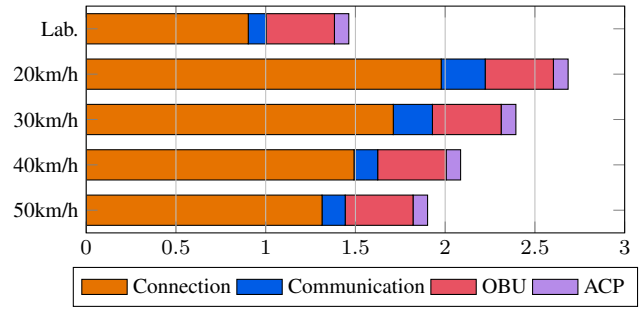


Fig. 5. Exit step average time completion at different speeds

Table III depicts those figures with deeper detail. In particular, it tackles the same protocol parts analyzed in the controlled laboratory tests and it shows that the protocol computation times at the OBU and ACP sides remain the same. This reveals that the scenario change has no influence in their execution environment and evinces that the upward time tendencies are caused by communication related processes. More specifically, the Bluetooth connection time show increases of 119%, 89%, 65%, and 45%, and data transfer overheads of 143%, 116%, 31%, and 28% for speeds of 20, 30, 40, and 50 km/h respectively. As we have already mentioned, several factors may be involved in these communication overheads: the own vehicle's body, the own vehicle's movement, the distance between ACP and the vehicle's OBU, or even external signal interferences.

Other conclusions can be drawn by focusing on the system response when vehicles are moving through at different speeds. In this way, as it can be appreciated in Figure 3, the Bluetooth connection time and, therefore, the total protocol run time, decreases as the vehicle circulates at higher speeds. Table III evinces this decreasing tendency regarding the communication operations. This behavior can be explained by the specificity of our low traffic street setting and by the distance between ACP and the vehicle's OBU at the moment of transferring data. Focusing on our setting, we placed a beacon-emitter wake up module 50 meters away from the ACP in order to automatically wake the user application up. Consequently, the application running in the vehicles' OBU approximately initiates, regardless of the vehicle speed, at this very distance, getting low signal strength at the beginning and improving it as the vehicle approaches the ACP. In this scenario, vehicles at higher speeds cover more distance and, thus, a major part of the protocol is done under better signal conditions, obtaining a better Bluetooth performance. For example, in the proposed scenario, two seconds after the app wakes up, a vehicle traveling at 20 km/h is still 43.8 meters away from the ACP. On the other hand, a vehicle at 50 km/h is only 22.1 meters away.

As a summary of the set of results obtained from the tests, it can be stated that factors such as the vehicle's body or the existence of external signal interference have an impact on the Bluetooth signal, as there is a general increase in the time

TABLE III
LOW TRAFFIC STREET RESULTS (IN SECONDS)

		Bluetooth Connection	Protocol execution time			Total
			Client	Server	Comm.	
20	Avg.	1.978	.380	.082	.245	2.685
	Dev.	.700	.019	.003	.126	.733
30	Avg.	1.711	.383	.082	.218	2.394
	Dev.	.744	.017	.003	.079	.751
40	Avg.	1.492	.381	.081	.132	2.086
	Dev.	.391	.022	.004	.022	.392
50	Avg.	1.314	.378	.081	.129	1.902
	Dev.	.351	.021	.003	.018	.359

costs of the proposed protocols in the outdoor scenario when compared with the figures obtained in the controlled laboratory environment. Nevertheless, these results also show that the most important factor affecting the Bluetooth performance (and, hence, the total time costs of the *Access* and *Exit* protocols) is the distance between the vehicle and the ACP. In any case, considering the 2.67, 2.39, 2.09, and 1.90 seconds to complete the *Exit step* for each speed, a vehicle would reach close to 14.84, 19.91, 23.22, and 26.39 meters for 20 to 50 km/h respectively. Those distances can be easily covered by the class1 Bluetooth adapter embedded in the ACP. This fact confirms the feasibility of the proposed system even when a non-specialized communication technology is being used. In this way, better results are expected if a V2X-dedicated technology such as IEEE 802.11p/DSRC is implemented instead.

In the light of these results, it can be stated that the proposed system is feasible in a relevant scenario consistent under the Technology Readiness Level 5 according to the European Commission standards.

D. Comparing our proposal with centralized alternatives

In the previous sections, we have proved that our proposal is lightweight enough to be feasible in a TRL 5 scenario. Nevertheless, the decentralized approach of our proposal requires additional cryptographic operations during the *Exit* protocol in order to decentrally acknowledge and charge on-chain, by means of the SC, the vehicle accesses during the *Payment step*. Under this premise, we compare our system with the centralized schemes in the literature in the following aspects: i) how demanding the adoption of a decentralized approach is; and ii) how much cost reduction is obtained at the system's entities due to the disposal of centralized third parties in the payment step.

In order to do that, we implemented and tested, under the same laboratory test-bed setting, schemes with similar privacy requirements and featuring RTC access or exit steps, i.e. [10], [11], [14]. In the same vein, we replicated the operations these works perform during the payment steps to determine the workload each one of them are facing for every registered vehicle access. It is worth mentioning that these schemes use a main centralized entity named *Service Provider* (SP) that leads their operations. In our tests, the SP used by those

TABLE IV
COMPUTATIONAL COSTS (SECONDS) IN THE EXIT STEP

	Client	Server	Total
Our scheme	.381	.081	.462
[10]	1.376	.153	1.529
[11]	1.393	.203	1.596
[14]	.312	.068	.379

proposals has been implemented on a PC Intel Core i7-4770S 3.10GHz with 12 GB of RAM and Windows10.

Table IV depicts the computational outcomes for each scheme's *Exit* protocol (*Access* protocol in the case of [11]). As it can be seen, our scheme achieves better time costs than [10] and [11], which were the first proposals to appear that applied *selective camera shooting*. In both cases, our system requires less computation time to complete the protocol in both ACP and D, however, it is worth mentioning the required time at D side in [10], [11], which takes around 1 more second to complete that step. This disparity is mainly caused by those schemes' privacy settings, which require that a smart card securely stores D's keys and generates its signatures. On the other hand, the lightweight protocol designed in [14] shows little better performance than our protocol in both ACP and D. The extra computational overrun that our proposal suffers is due to the generation of on-chain verifiable proofs which are used during the *Payment* protocol by the involved Ds.

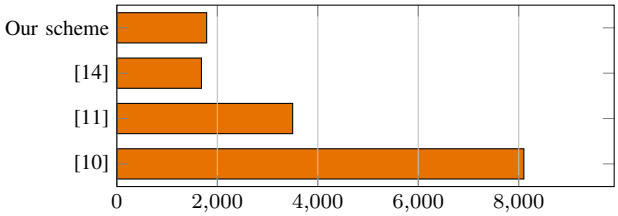


Fig. 6. Bytes transferred during the exit step

Focusing now on the communication costs, Figure 6 shows the amount of transferred data in the *Exit* protocol of each system. As it can be seen, [10] and [11] exchange 8,102 and 3,499 bytes of data between the ACP and D during the *Exit* protocol (*Access* protocol in the case of [11]). It should be noted that, in both cases, no secure channel at the application level is considered, leaving the channel securitization to the underneath communication technology. In this way, the related computational cost is not considered in this analysis. Compared to those systems, which incur in higher communication costs mainly caused due to price information transmission during the protocol steps, our scheme only sends 1788 bytes of data to validate a vehicle departure from the LEZ. This cost is 104 bytes higher than in the lightweight protocol proposed in [14], and it is caused by the additional on-chain verifiable proofs that the Ds of our protocol need when they interact with the SC to validate and pay their accesses to the LEZ.

As indicated above, the generation of on-chain verifiable proofs causes little extra costs in the *Exit* protocol. This situation is inherent to the use of the blockchain technology to decentralize the new proposal. Although decentralizing the system's architecture generates this extra cost, following this approach also brings significant advantages over the centralized works in the literature. In this way, Figure 7 and Figure 8 show the communication and computation costs that the entities of the centralized works being analyzed generate during the *Payment* step. As the charts show, all centralized schemes require relevant extra communication and computation efforts at their entities. These efforts mainly focus on sending access data to the SP and its later computation in order to determine the Ds' fees. As a result of that, while centralized schemes present from 469 to 2,155 bytes of additional communication costs and 6.32 to 109,87 milliseconds of additional computation overhead per access, the new proposal only needs Ds to send 134 bytes per access. There is no extra overhead at the other entities of the system.

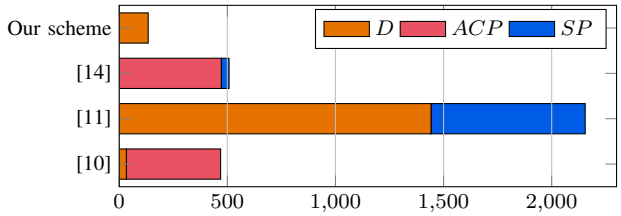


Fig. 7. Amount of bytes sent per access in the payment step

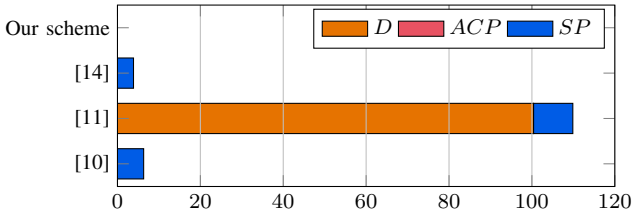


Fig. 8. Computation costs (miliseconds) per access in the payment step

In summary, our tests prove that: i) in the *Exit* protocol (which is equivalent to the *Access* protocol), our scheme outperforms some other similar works in the literature that follow a centralized approach; ii) also in the *Exit* protocol, the new proposal is aligned with one of the most lightweight centralized protocols in the literature, although our decentralized proposal achieves a certain additional overhead which is inherent to the use of the blockchain technology; and iii) in the *Payment* protocol, our decentralized proposal clearly outperforms all the centralized schemes by avoiding substantial communication and computation overheads arising from central management of fees calculation and its corresponding charges.

E. Smart Contract performance

As it has been already explained, the use of smart contracts is central within our proposal. In this way, in order to prove its viability and determine its efficiency, we conduct, in this section, a set of experiments to measure the cost in terms of gas of the smart contract that runs the LEZ.

In order to do that, we first implemented the LEZ smart contract mentioned in Section III, along with the most relevant methods required to carry out the *Payment* protocol detailed in Section III-F. The resulting system was next deployed in a *Ganache testing network*[10]. Regarding the experiments, their objective was specifically to evaluate: i) the *register_access* method used by Ds to validate, price, and pay their accesses to the LEZ; ii) the *payment_incidence* method orchestrated by the ACPs to open incidences against dishonest drivers; and iii) the smart contract deployment conducted by the LA.

Table V depicts, for the three aforementioned points, the gas cost and their monetary equivalent in dollars. This monetary translation was made considering the smart contract deployment in the Binance Smart Chain (BSC), a low-fee EVM-compatible Ethereum network replica, according to the recommended standard gas price[11] and the Binance Coin (BNB) exchange rate[12].

TABLE V
SMART CONTRACT OPERATION COSTS IN TERMS OF GAS AND ITS DOLLARS EQUIVALENCE.

Method	Gas	Binance Smart Chain
deploy	925,382	0.0046 bnb ($\simeq$1.94 $)
register_access	68,210	0.0003 bnb ($\simeq$0.14 $)
payment_incidence	138,788	0.0007 bnb ($\simeq$0.29 $)

As those figures show, deploying the smart contract is the costliest operation in terms of gas with a total amount of 925,382. Next, it comes the *payment_incidence* operation with a cost of 138,788, and, finally, the *register_access* method with a cost of 68,210. In order to put these costs into perspective, it should be noted that a basic transfer of Ether (ETH) or Binance coin (BNB) in their respective native networks consumes 21,000 gas. Those are special cases because they are Ethereum's and BSC's native assets and their gas consumption is expected to be the minimum. Thus, all smart contracts operations are expected to burn, at least, that amount of gas. According to that, it is stated that the smart contract operations performed by the new scheme, especially the user-end calls, are not expensive in terms of gas. Furthermore, it is worth mentioning that our implementation prioritizes the smart contract's autonomy by performing most of the operations on-chain. If reducing the gas consumption is preferred instead, it would be possible to easily achieve that by adapting the payment protocol to perform the most gas-burning operations (e.g., signature verification) off-chain.

The last column in Table V shows the gas consumption in dollars. Since the two more expensive operations, deployment and *payment_incidence*, are run by for-profit entities, those costs do not represent a significant burden to the system. On the other hand, the validation cost of the *register_access* is assumed by the drivers and, hence, it is a key aspect that requires especial attention. In this way, the *register_access* cost only represents a 0.14$ fee for standard priority, which we argue that it is affordable when deploying the proposed system in a real-world scenario. Following this point, it is important to mention that the proposed scheme does not require fast transaction validation times, due to the fact that the contract owner (i.e. the LA), can decide the specific amount of time that drivers have to publish their accesses to the blockchain. This flexibility brings two clear benefits to the drivers: i) they are able to offer low priority gas prices at the expense of higher validation times; and ii) they are not influenced by an occasional network congestion that may increase the cost of their operation. Both aspects allow the proposed system to keep low the cost that must be assumed by the drivers who use the LEZ.

[10]http://trufflesuite.com/ganache/

[11]BSC Average Gas Price - https://bscscan.com/chart/gasprice - 01/10/2021

[12]BNB price - https://coinmarketcap.com/es/currencies/binance-coin/ - 01/10/2021

VI. CONCLUSIONS

Low Emission Zones (LEZ)s have become an essential mechanism in large cities to deal with urban traffic and environmental pollution. All current privacy-preserving access control solutions being applied to LEZs rely on centralized entities to perform their main operations (e.g., vehicle accesses, charging fees...). Those centralized entities represent a crucial point of failure that deserves attention.

With the recent rise of the blockchain technology as a main approach to provide decentralized trust and transparency to various domains, in this paper, we have proposed a privacy-preserving LEZ access control alternative that uses the smart contracts logic and the underlying blockchain technology to decentralize the LEZ management.

The new scheme has been designed taking into account the requirements of revocable anonymity for dishonest drivers, non-traceability, non-repudiation, integrity, and exculpability. In order to show how the proposed system fulfills those requirements, a complete security and privacy analysis has been conducted.

Finally, to validate its deployability in real scenarios, the new scheme has been implemented and tested in both a controlled environment and a low-traffic street. The results obtained in those experiments show that the new decentralized proposal is lightweight and feasible in a relevant scenario consistent under the Technology Readiness Level 5 according to the European Commission standards. Regarding the cost introduced by the smart contract in use, our evaluation shows that the smart contract's cost in gas and the transactions' validation time have no impact on the whole system's feasibility when deployed in a low-fee platform like Binance Smart Chain.

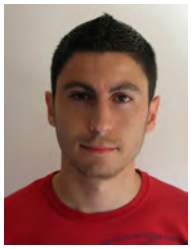
ACKNOWLEDGMENTS

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

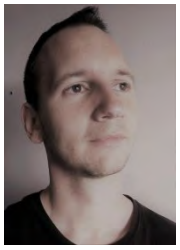
que ens uneix - Sensòrica" project [PR15-020174]; and by Grants RTI2018-095094-B-C21 "Consent", RTI2018-097763-B-I00 "Feltichain", PID2021-122394OB-I00 "Blobsec", and PID2021-125962OB-C32 "SECURING/DATA" funded by MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe".

REFERENCES

[1] G. Santos, Urban congestion charging: a comparison between london and singapore, Transport Reviews 25 (5) (2005) 511–534.
[2] S. El Hamdani, N. Benamar, A comprehensive study of intelligent transportation system architectures for road congestion avoidance, in: International Symposium on Ubiquitous Networking, Springer, 2017, pp. 95–106.
[3] R. A. Popa, H. Balakrishnan, A. J. Blumberg, Vpriv: Protecting privacy in location-based vehicular services, in: 18th USENIX Security Symposium, USENIX Association, 2009.
[4] X. Chen, G. Lenzini, S. Mauw, 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.
[5] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, C. Geuens, Pretp: Privacy-preserving electronic toll pricing., in: USENIX Security Symposium, Vol. 10, 2010, pp. 63–78.
[6] S. Meiklejohn, K. Mowery, S. Checkoway, 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.
[7] J. Day, Y. Huang, E. Knapp, 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.
[8] F. D. Garcia, E. R. Verheul, B. Jacobs, Cell-based privacy-friendly roadpricing, Computers & Mathematics with Applications 65 (5) (2013) 774–785.
[9] R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras-Capellà, J. Castellà-Roca, A. Viejo, Electronic road pricing system for low emission zones to preserve driver privacy, in: International Conference on Modeling Decisions for Artificial Intelligence, Springer, 2014, pp. 1–13.
[10] R. Jardí-Cedó, M. Mut-Puigserver, M. M. Payeras, J. Castella-Roca, A. Viejo, Time-based low emission zones preserving drivers' privacy, Future Generation Computer Systems 80 (2018) 558–571.
[11] R. Jardí-Cedó, J. Castellà, A. Viejo, Privacy-preserving electronic road pricing system for low emission zones with dynamic pricing, Security and Communication Networks 9 (2016) 3197–3218.
[12] V. Fetzer, M. Hoffmann, M. Nagel, A. Rupp, R. Schwerdt, P4tc—provably-secure yet practical privacy-preserving toll collection, Proceedings on Privacy Enhancing Technologies 3 (2020) 62–152.
[13] S. Bouchelaghem, M. Omar, Reliable and secure distributed smart road pricing system for smart cities, IEEE Transactions on Intelligent Transportation Systems 20 (5) (2018) 1592–1603.
[14] C. Anglès-Tafalla, J. Castellà-Roca, M. Mut-Puigserver, M. M. Payeras-Capellà, A. Viejo, Secure and privacy-preserving lightweight access control system for low emission zones, Computer Networks 145 (2018) 13–26.
[15] G. Baldini, J. L. Hernández-Ramos, G. Steri, R. Neisse, I. N. Fovino, A review on the application of distributed ledgers in the evolution of road transport, IEEE Internet Computing 24 (6) (2020) 27–36.
[16] C. Anglès-Tafalla, J. Castellà-Roca, 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.
[17] E. I. Delivered, The trl scale as a research & innovation policy tool, earto recommendations, Earto Impact Delivered (2014).
[18] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, [Online 2008], Available: https://bitcoin.org/bitcoin.pdf (2008).
[19] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, Ethereum project yellow paper 151 (2014) 1–32.
[20] X. Fan, Q. Chai, Roll-dpos: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems, in: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2018, pp. 482–484.
[21] S. Popov, H. Moog, D. Camargo, A. Capossele, V. Dimitrov, A. Gal, A. Greve, B. Kusmierz, S. Mueller, A. Penzkofer, et al., The coordicide, Accessed Jan (2020) 1–30.



Carles Anglés-Tafalla, Ph.D., is a postdoctoral researcher at the Rovira i Virgili University of Tarragona, Spain. He received his Ph.D. in Computer Science from the Universitat Rovira i Virgili in 2020. He has participated in several national funded research projects and authored several papers and conference contributions. His fields of activity are data privacy, data security and cryptographic protocols.



Alexandre Viejo, Ph.D., is an associate professor at Universitat Rovira i Virgili (Tarragona, Spain). He received his Ph.D. in Computer Science from the Universitat Rovira i Virgili in 2008. In 2009, he was a researcher at Humboldt-Universität zu Berlin (Germany). He has authored several papers and conference contributions. His fields of activity are data privacy, data security and cryptographic protocols.

Jordi Castellà-Roca (Menàrguens, Catalonia, 1975) is associate professor at Rovira i Virgili University. He got his Ph.D. in Computer Science from the Autonomous University of Barcelona in 2005. He has published over 70 works, is co-author of seven patents, and has participated in 36 research projects (main researcher in 19 of them). His research focuses on the fields of cryptography and privacy.

Macià Mut-Puigserver (Mallorca, 1966). He received his Ph. D. in 2006 from the University of the Balearic Islands (UIB). He is associate lecturer at the University of the Balearic Islands (UIB). As a researcher, he has been involved in several research projects and has an active pace of publications. His current research interests are: design of secure protocols, secure e-commerce, blockchain applications, privacy-preserving applications, and applied cryptography.

M. Magdalena Payeras-Capellà got her Ph. D. in Computer Science (2005) from the University of the Balearic Islands (UIB). She is associate professor at the University of the Balearic Islands (UIB). Her research focuses on security in communications networks, electronic payments, design of protocols for electronic commerce and secure and privacy-preserving applications. She has coauthored two patents and has participated in the creation of two spin-offs.