IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON BLOCKCHAIN TECHNOLOGY: PRINCIPLES AND APPLICATIONS

Received September 25, 2020, accepted October 11, 2020, date of publication October 28, 2020,
date of current version November 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3034299

Pay as You Go: A Generic Crypto Tolling Architecture

PAULO C. BARTOLOMEU[1], (Senior Member, IEEE), EMANUEL VIEIRA[2], AND JOAQUIM FERREIRA[3], (Senior Member, IEEE)

[1]Institute of Telecommunications, Department of Electronics, Telecommunications and Informatics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[2] Institute of Telecommunications, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[3]Institute of Telecommunications, Águeda School of Technology and Management, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

Corresponding author: Paulo C. Bartolomeu (bartolomeu@ua.pt)

This work was supported in part by the Fundação para a Ciência e a Tecnologia (FCT)/Ministério da Ciência, Tecnologia e Ensino Superior (MCTES) through National Funds, and in part by the European Union (EU) Funds under Project UIDB/50008/2020-UIDP/50008/2020.

ABSTRACT The imminent pervasive adoption of vehicular communication, either localized (ETSI ITS G5, IEEE WAVE or cellular D2D), long range (5G) or hybrid, will foster a richer service ecosystem for vehicular applications. The appearance of new cryptography-based solutions envisaging digital identity and currency exchange are set to stem new approaches for existing and future challenges. This article presents a novel tolling architecture that harnesses the availability of 5G C-V2X connectivity for open road tolling using smartphones, IOTA as the digital currency, and Hyperledger Indy for identity validation. An experimental feasibility analysis is used to validate the proposed architecture for secure, private, and convenient electronic toll payment.

INDEX TERMS
5G, blockchain, C-V2X, hyperledger indy, intelligent transportation systems, IOTA, open road tolling, self-sovereign identity, vehicular communications.

I. INTRODUCTION

Recent advances in wireless communications and crypto technologies are fostering the emergence of innovative solutions for cooperative connected and automated mobility (CCAM). In CCAM, the road infrastructure plays a central role in providing collaborative awareness data to connected and automated vehicles and other road users. Dependable vehicular communications are a cornerstone of CCAM. For more than ten years, research and development in this area have produced mature technology ready to be massively deployed, notably ETSI ITS G5 and IEEE WAVE, which share the same physical and MAC layers, initially adapted from IEEE 801.11. Recently, however, the emergence of the fifth generation of cellular mobile communications (5G) and other related cellular and device-to-device (D2D) technologies, notably cellular Vehicle to everything (C-V2X), have raised some doubts on which vehicular communication technology will prevail.

On the other side, recent advances in cryptography have also led to the appearance of new digital currencies and novel identity paradigms, all of which will be crucial for enabling the future of digital transactions among people, organizations and things.

An arena where such novelty combination will have a tremendous impact is on vehicular applications. The impending evolution of autonomous electric vehicles is expected to stem multiple services that will enhance the passengers' user experience and provide better returns for providers, as never before was possible. One service that can largely benefit from these innovations is the automatic free-flow tolling of vehicles, for which existing solutions are not able to meet stringent privacy requirements and provide real-time operation.

Road tolling, as a method of financing the transportation system, has long been in place all around the world. Since neither the drivers or the road operators want vehicles to stop or slow down to pay the toll, several technologies, collectively called Electronic Toll Collection (ETC), have been developed in the last 25 years, ranging from RFID sticker toll tags, to Dedicated Short Range Communications (DSRC) and to tolling systems based on an autonomous On Board Unit (OBU) using Global Navigation Satellite System/Cellular Network (GNSS/CN). Currently, Open Free-Flow Road Tolling (ORT), with all-electronic toll collection, is the preferred practice, as it is more environmentally

The associate editor coordinating the review of this manuscript and approving it for publication was Wenbing Zhao.

friendly, and safer than manual toll collection [1]. Electronic tolling is cheaper than a staffed booth, reducing the average cost per transaction. With electronic tolling one can also vary the amount of the toll, implement road congestion pricing, including for high-occupancy lanes, toll lanes that bypass congestion, and city-wide congestion charges.

Open road tolling systems need to classify vehicles, so different vehicles types can be charged different rates. Automated vehicle identification (AVI) systems use a variety of sensors for vehicle classification, including inductive loops to count the number of axles and light-curtain laser profilers to detect the shape of the vehicle, thus helping distinguishing trucks and trailers and to measure their height.

Violation enforcement systems need to be put in place together with open road tolling to minimize fraud and unpaid tolls. To this end, several technologies can be adopted, possibly including physical barriers or just automatic number plate recognition systems synchronized with the on board transponder detection.

Transaction processing, a core function of the electronic toll collection, is responsible for charging customer accounts. Customer accounts can be postpaid, where toll transactions are periodically billed to the customer, or prepaid, where the customer funds a balance in the account, which is then depleted as toll transactions occur. Depending on the country and on the adopted payment infrastructure, it can take several days to charge the customer account, for the case of the postpaid micro-payments.

Traditional open free-flow road tolling systems usually have a national or regional scope, making it cumbersome for unregistered drivers, e.g., tourists, to pay the toll, as there might not be toll booths with alternative payment methods. Additionally, these systems require the installation of a device in each vehicle, complex toll gantries and a centralized payment processing system.

In the last years a few solutions have been proposed to overcome these limitations. Harnessing the expected massive availability of ITS-G5 technology in new vehicles, different systems have been proposed to realize its full potential. An example is the precise vehicle location system aimed at improving Electronic Toll Collection proposed in [2]. In this work nearby vehicles' localization data (GPS and accelerometer) are collected from the Cooperative Awareness Messages (CAMs) received by a RoadSide Unit (RSU) installed at the toll gantry. An algorithm combining the principle of Differential-GPS with Kalman filtering is then applied obtaining an accurate localization estimation that ensures an efficient Electronic Toll Collection.

Another example is the work presented in [3], which investigates how to secure the tolling transactions performed with standard Cooperative Intelligent Transportation System (C-ITS) equipments. The proposed system relies on ITS components using the ITS-G5 technology with features specified by the European Telecommunication Standardization Institute (ETSI): RoadSide Unit (RSU) and On-Board Unit (OBU) and the standardized architecture of the Electronic Fee Collection by the International Organization for Standardization (ISO). In this case, the tolling server acts as a trusted party and a point-to-point communication is established between the RSU of the infrastructure (toll gantry) and the OBU embedded in the vehicle in order to enable the tolling transaction.

Although toll collection is an emerging use case for 5G communications as reported in [4] and [5], to the best of our knowledge there are currently no 5G based implementations reported in the literature. Nevertheless, the ubiquitous network connectivity ensured by the 5G technology brings along concerns about trust, security, and privacy [6], difficulting its adoption in supporting toll collection services.

This article proposes a privacy-preserving tolling architecture, leveraged by the IOTA cryptocurrency, to support decentralized feeless payments, the Hyperledger Indy for establishing trust using the Self-Sovereign Identity (SSI) paradigm, and C-V2X for providing connectivity with the road side infrastructure. The proposed solution introduces multiple innovations bringing comfort and value to drivers and road operators in a holistic way.

The adoption of 5G C-V2X communications makes it possible to enable open-flow tolling directly with smartphones, not requiring the installation of specialized devices in vehicles for identification. As communications built upon the SSI paradigm are established among trusted entities (users and operator), which have to make a direct cryptographic proof of their identities, interactions are not only highly secure and anonymous but are also quickly established and performed. Since a third party authorization authority is not required, there is minimal network latency in the process (i.e., only local Device-to-Device communications are conducted). Furthermore, as the adopted identity framework is decentralized and has a global reach, it is not bound to a specific country or operator, providing a seamless operation for users traveling between different regions or countries. This, not only occurs due to the identity framework but, also, to the proposed crypto payment system, which provides each user and operator with its own wallet that can be debited or credited according to the service usage or provision, respectively. The availability of a digital cryptocurrency wallet allows for both users and operators to check their transactions in almost real-time, also something that existing systems do not support. The evolution of toll charging towards decentralization advocated in this proposal carries a number of benefits as discussed above. An additional one is the absence of a Single Point of Failure (SPoF), leading to a high security and availability. To the best of our knowledge, there is currently no comparable tolling system combining the presented technologies and benefits.

The rest of the paper is organized as follows: section II provides a brief overview of the key technologies required to build the new tolling system, while section III presents the novel tolling architecture, whose feasibility is experimentally evaluated in section IV. Section V presents an overview of related work in the area of secure 5G communications and, finally, section VI summarizes the contributions of the paper.

II. KEY EMERGING TECHNOLOGIES

The future of open road tolling systems will be shaped by emerging technologies such as 5G communications, new crypto currencies and distributed ledger identity networks. This section presents a brief overview of selected technologies and their potential impact on electronic tolling systems. Although it is possible to use ETSI ITS G5 or IEEE WAVE communications to convey the tolling transactions between vehicles and the road side infrastructure, the crypto tolling architecture proposed in this article considers the use of C-V2X communications [8], mainly to allow the use of smartphones instead of specialized devices installed in the vehicles, a change that brings several advantages and key benefits for both users and road operators. The replacement of the standalone (RFID, DSRC, etc.) identifier in ORT systems by an *App* running on a smartphone provides a much easier path for software update and service improvement, offering a much higher security control to the operator and a better user experience for toll payers that access improved versions of the *App* in a seamless way.

In this approach users also benefit of not having to acquire a device that represents an additional cost and the hassle of having to periodically take it for battery service. On the operator perspective it is one less product requiring physical life-cycle management (inventory, maintenance, disposal, etc.).

Business users, especially those with large fleets of vehicles traveling across different countries, will profit the most with the proposed system, since its integration on a toll expenditure management platform can contribute to significantly reduce the toll expense tracking burden while simultaneously provide a faster and easier driving experience for their professionals. Moreover, a given user can use her *App* with different vehicles in a seamless way. There is no need to change the physical identifier between different vehicles, operators or countries.

A. C-V2X COMMUNICATIONS

Connectivity is the touchstone of the Internet of Things (IoT) era. The 5G promise of pervasive high bandwidth and low-cost wireless communications suggests a bright future for IoT, as an heterogeneous range of applications will emerge under this umbrella. Scenarios where services are enabled by the occurrence of direct (and automated) interactions among ''things'' represent one of the most interesting opportunities for the 5G Device-to-Device technology. Indeed, such scenarios allow alleviating the traffic load from base stations by taking advantage of the proximity among devices, which not only contributes to improve parameters such as throughput, latency and power usage, but also increases the overall capacity of the network [7] and its reliability.

The 3GPP Release 14 introduced the C-V2X standard [8], also known as LTE-V or LTE-V2X, that uses the LTE PC5 interface for vehicle-to-vehicle (V2V) communications. This standard, designed to support both cooperative traffic safety and efficiency applications, includes two modes of operation, namely C-V2X mode 3 and C-V2X mode 4. In C-V2X mode 3, scheduling and interference management of V2V traffic are assisted by eNBs via control signaling, while in C-V2X mode 4 scheduling and interference management of V2V traffic are based on distributed algorithms implemented between User Equipments (UEs). C-V2X mode 3, can thus be used for long-range network communications (V2N), relying on the conventional mobile network to enable a vehicle to receive cooperative perception data originated beyond the vehicle's line of sight. On the other side, C-V2X mode 4 is used for short-range direct communications between vehicles (V2V), between vehicles and infrastructure (V2I), and vehicles and other road users (V2P), such as cyclists and pedestrians. C-V2X mode 4 works independently of the cellular networks in dedicated ITS 5.9GHz spectrum.

Considering an open road tolling system as the target application, this article proposes the use of C-V2X mode 4, as it can support safety applications in the absence of coverage from the cellular infrastructure, which might not be present in remote areas. In this scenario, a compatible user smartphone will actively seek connectivity with *Toll Gantries* in their range using the C-V2X mode 4 to conduct the associated toll payments. The smartphone can still use 5G cellular connectivity to support any other running applications.

Concerning the security aspects of C-V2X, the 3GPP R14 specification [8] states that no security and privacy is applied for the PC5 broadcast communication by setting the fields related to group security to 0. In this way, messages exchanged among UEs have no standard security mechanisms in place. Application layer security is outside the scope of 3GPP, but it is suggested that credentials should be periodically refreshed to avoid UE tracking. Security and privacy mechanisms for C-V2X mode 4 need to be defined by regulators and operators. As for authentication, traditional LTE authentication mechanisms can be employed and enforced in C-V2X mode 3. But, since an operator may not be present in mode 4, proper authentication has to rely on other schemes. The security and privacy support for the proposed automatic tolling solution relies on the authentication and encryption mechanisms provided by the instatiation of the Self-Sovereign Identity paradigm in the Hiperledger Indy platform.

Recently, the 5G NR-V2X (New Radio) [9] was introduced as the third phase of the 3GPP V2X and it is backward compatible, at the upper layers, with LTE-V2X. To meet the low latency and reliability requirements for the advanced V2X use cases, NR-V2X is designed to support 5G Ultra-Reliable Low-Latency Communications (URLLC). 5G NR-V2X also defines two types of sidelink communication modes: mode 1 and mode 2. The NR-V2X mode 1 defines the mechanisms that allow direct vehicular communications, with the support of the cellular network' base station that allocates radio resources to the vehicle through the Uu interface. Mode 2, on the other hand, supports direct vehicular communications, via PC5 interface,

whenever a vehicle is out of the coverage of the cellular network.

The C-V2X and 5G NR form a new connectivity ecosystem that is compatible with the proposed tolling architecture using both technologies: LTE-V2X mode 4 and NR-V2X mode 2. While it is still not clear if future smartphones will massively support C-V2X or 5G NR-V2X, the proposed architecture can be easily adapted to work with both on existing On-Board Units (OBUs). Starting in early 2021, smartphone chipsets supporting 3GPP release 16 will integrate C-V2X 5G NR, fostering pervasive D2D communications.

B. IOTA

IOTA is a cryptocurrency that was created with a focus on IoT to solve the problems of scalability, control centralization, transaction fees and post-quantum security that characterizes other cryptocurrencies employing the blockchain technology [10]. The *Tangle* is its key contribution and builds on the concept of Directed Acyclic Graphs (DAGs) as a substitute for blockchains.

In the *Tangle* every vertex is a transaction. To add a transaction to the *Tangle* two other transactions must be approved. This approval can be represented by an outgoing edge, meaning that the outdegree of every vertex is equal to 2. The indegree is not limited, a transaction can be approved by any number of transactions. Transactions which are currently not approved by any others are called tips. Similarly to blockchains, for a transaction to be appended to the *Tangle*, some ''proof-of-work'' (PoW) must be executed, mainly to avoid spam attacks.

C. HYPERLEDGER INDY

The Hyperledger Indy is a distributed ledger built for decentralized identities. It uses a blockchain as a ledger and employs a permissioned protocol where only trusted elements can add transactions to the ledger. The trust factor removes the need for users to do any PoW, shortening the time required to add a transaction. Whenever a transaction needs to be updated, a new updated one is added to the ledger. The older transaction, whilst still existing in the ledger, is simply ignored in future queries.

Hyperledger Indy is mostly known for its main implementer, the Sovrin Foundation. Sovrin is a global trust network that provides the legal and trust foundation for self-sovereign identities (SSI) [11]. Four roles with specific scopes and permissions are defined: Trustees, Stewards, Trust Anchors and Identity Owners. In Hyperledger Indy any user is able to issue its own credentials. An issued credential is stored in the user's wallet and can be provided to prove certain attributes to a proof requester, also called *Verifier*. Every created proof is signed by the credential *Issuer*. If the *Verifier* trusts the *Issuer* then he can also trust the created proof.

III. CRYPTO TOLLING

The proposed open road tolling architecture arises from the opportunity to adopt a decentralized approach for identification and payment that ensures adequate anonymity and, at the same time, provides accountability and traceability. The modern smartphone is established at the center of the ''Pay as You Go'' architecture. This device has the required computational power to run blockchain wallets, connectivity to communicate via 5G D2D and a GPS to monitor its physical location and assist in the validation of toll payments.

There are several motivations to adopt a distributed SSI mechanism enabling devices to prove their identities directly to each other without a central authority involved. Devices are closer to each other during information exchange (identity validation) making the process typically faster. Because the data exposure is set to the minimum required to fulfill a given function, personal data has an higher level of protection. The information controlability is also higher because the user/device is in control of the information that it shares. Because the identity information is distributed among wallets located in devices that can be mobile (e.g., smartphones) there is also an higher level of portability.

The adoption of a decentralized payment approach was driven by several factors. IOTA has ultra low fees (or no fees at all) applicable to transactions, which is a strong enabler for micro payment systems, such as open road tolling. Because IOTA is a globally available cryptocurrency it can be traded worldwide without control of central authorities/governments. Finally, when compared to other cryptocurrencies such as Bitcoin, IOTA transactions are confirmed much faster, thus allowing payments to be available to the receiving party much earlier.

Although the use case presented in this article specifically addresses the open road toll payment use case, the proposed architecture and its operation can be easily generalized to other automatic service or product payments that can work under similar requirements.

A. ARCHITECTURE

The ''Pay as You Go'' architecture comprehends several stakeholders: *Road Operator*, *Toll Gantry*, *Vehicle* and *User*. The *Operator* is generally the company who has the concession of a given highway and charges the *Vehicle*'s owner for its use. The *Operator* does so by employing automatic *Toll Gantries* that are used to register information about *Vehicles* that pass by. This information is then used to either automatically collect payment from the *Vehicles*' owners bank account or to provide mechanisms for posterior enforcing of voluntary or forceful charging. In both cases, images of the vehicle are recorded for traceability. *Vehicles* have distinct physical attributes (licence plate, toll class, etc.) which allow their identification in an unambiguous way. Finally, *Users* that possess a valid driving licence are allowed to drive their *Vehicles* on roads covered by *Toll Gantries*, whereas the driver' smartphone is the center element for paying the toll service.

As depicted in Fig. 1, all stakeholders are interconnected. it is assumed that the *User* smartphone is equipped with 5G and communicates with the *Toll Gantries* using C-V2X mode 4. The *Road Operator* can communicate with the *Toll*

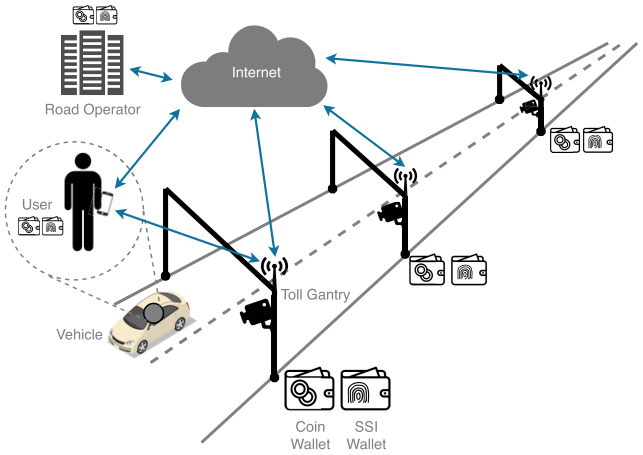


FIGURE 1. "Pay as You Go" architecture.

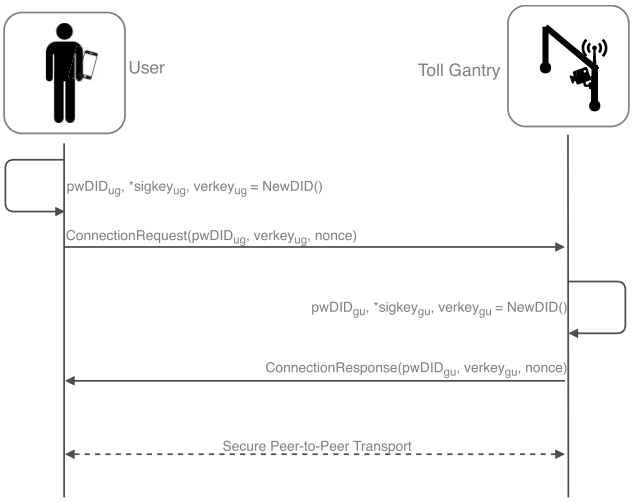


FIGURE 2. Establishing a pairwise DID transport.

Gantries via a wired/fiber backhaul connection to the Internet or, also, via 5G.

Each of the participating entities possesses a set of unique identifications saved in a SSI wallet that is used to authenticate them and prove their veracity. Besides the identity wallet, entities will have coin wallets which are used to make and receive IOTA payments.

B. OPERATION

The proposed crypto architecture relies on three key elements: 5G C-V2X mode 4 connections between the *User*'s smartphone and the tolling infrastructure, Hyperledger Indy for identity management/validation and IOTA currency to conduct the tolling service micro payments.

In the context of this article, it is assumed that 5G C-V2X mode 4 communications will be seamlessly established between the *User*'s smartphone and the *Toll Gantries*. In this sense, the trigger mechanism for initiating a new 5G C-V2X connection is implemented in the smartphone *App* that listens to specific announcements broadcasted by the *Toll Gantries* and, when such a request is detected, an "in-band" connection to the *Toll Gantry* is initiated.

The smartphone *App* will perform an early check to evaluate if there is a previous ongoing digital relationship with the *Toll Gantry* in range before attempting to create a new pairwise Decentralized Identifier (DID) for the relation. This evaluation can be realized by storing in the *App* the relationship between known *Toll Gantry* DIDs and their geographical location (as perceived in previous interactions). In this case, when a new interaction is about to begin, the smartphone App reads its geographical localization from the GPS and filters the list of possible DIDs, selecting the one that is closer (minimal localization error). Then, the smartphone *App* (re)establishes the pairwise DID connection by echoing a request and receiving a response from the *Toll Gantry*.

The creation of verinyms (DIDs) associated with the identities of the *User*, *Toll Gantry*, *Operator*, etc. is beyond the scope of this article. The considered scenario assumes that the edge wallets of the *User* and *Toll Gantry* have already been populated with the necessary credentials generated by third party trusted organizations or authorities that are recognized to provide them. In this context, it is also assumed that both parties have already created their *Master Secrets* allowing to guarantee that a given credential uniquely applies to them.

1) PAIRWISE DID CREATION

If the connection is successfully re-established, then a new exchange and validation of credentials can begin. Otherwise, a new pairwise DID relation is required to be established following the diagram of Fig. 2. As documented, the *User* agent running in the smartphone begins by creating a DID and associated keys and storing them in its local wallet. This new DID will be used only in the context of the interactions with this unique *Toll Gantry*. The impossibility of reading the signing (private) key ($sigkey_{ug}$) stored in the wallet is distinguishable by the use of an asterisk in its notation.

Subsequently, the *User* agent sends a connection request to the *Toll Gantry* agent encompassing the created DID ($pwDID_{ug}$), verification key ($verkey_{ug}$) and nonce. The verification key allows the *Toll Gantry* to check the authenticity of the message, i.e., that it was sent by the *User*. The nonce is used by the initiating party (in this case the *User* agent) to correlate the response with the request.

Upon receiving the connection request, the *Toll Gantry* agent also creates a new DID ($pwDID_{gu}$) to be used in the context of this unique digital (*Toll Gantry* to *User*) relationship. Afterward, it sends an encrypted connection response using the *User*'s verification key (*verkey*) that encompasses the newly created DID ($pwDID_{gu}$), verification key ($verkey_{gu}$) and the nonce originally received from the *User* agent. Because messages in both directions can now be encrypted using the verkeys of the target party, a unique secure peer-to-peer transport is established between *User* and *Toll Gantry*.

2) CREDENTIAL VALIDATION

The credentials validation phase is stemmed by the *User* edge agent that sends a *Tolling Charge* proof request to the *Toll Gantry* in order to collect verifiable proof that its attributes

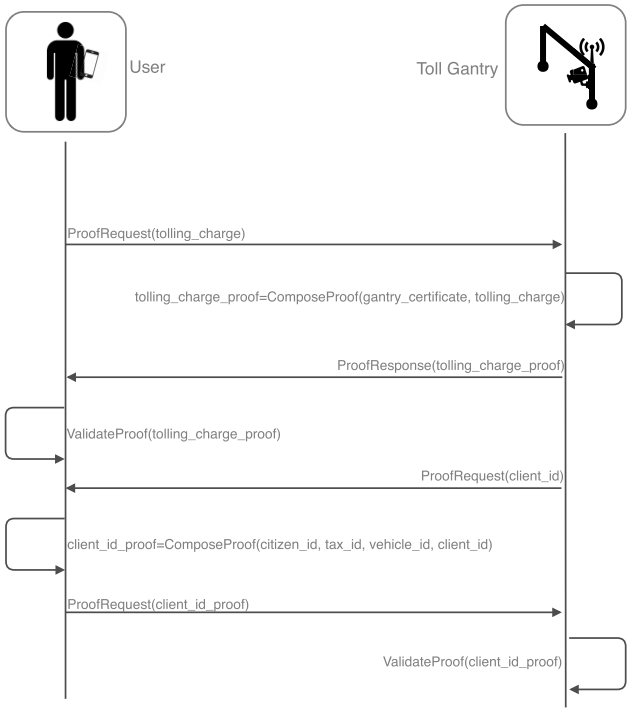


FIGURE 3. ***User*** **and** ***Toll Gantry*** **identity validation.**

meet specific criteria. In this case, the *Tolling Charge* requires a name, localization and unique identifier code. All of these credential parameters must be formally asserted by a tolling operator. As depicted in Fig. 3, the *Toll Gantry* agent then composes a proof based on the received proof request and on the *Toll Gantry* certificate that is stored on its wallet.

On the opposite direction, the *Toll Gantry* agent sends a *Client Identification* proof request requiring the *User*'s name, VAT number and vehicle plate number. This information is exposed according to the settings defined by the *User* in the smartphone App. These settings are established upon completing the App installation and can be updated at any time. For example, if the *User* has selected requiring an invoice tied to its tax identity for business purposes, the App provides the associated information during this phase. Otherwise, personal identity information is not shared.

It is worth noting that this information exchange is conducted solely between the *User* App (agent) and the *Toll Gantry* agent, without involvement of the actual *User*.

The direction of the vehicle passage can easily be detected by the cameras of the enforcement system that capture its passage.

3) PAYMENT

After the *User* and *Toll Gantry* identities are validated, the *Toll Gantry* sends the payment request to the *User*'s smartphone. This request contains the due amount, the IOTA address to transfer IOTAs to, and a nonce for the *User* to use as a reference. This bill will be sent encrypted using the pairwise Decentralized Identifier (DID) created by the *User*.

The tolling App can then use this information to proceed with the IOTA transaction transferring the due amount to the designated address. If the payment with the specific nonce and value is not received within a pre-defined interval in the designated address, the operator may trigger a legal process using the information collected by the enforcement system (license plate number, vehicle characteristics, photos, etc.) and, if available, information obtained during identity validation.

IV. FEASIBILITY EVALUATION

This section evaluates the feasibility of implementing the proposed payment architecture with the constrains imposed by its operation. For this analysis a C-V2X mode 4 line of sight communication range of 600 meters [12] and a maximum speed of 130 Km/h were considered. The speed corresponds to the legal limit that covers most of the countries around the world. The identity ''handshake'' between the *User*'s smartphone and the *Toll Gantry* plus the IOTA value transaction registration into the *Tangle* needs to be completed during the period in which the smartphone is in range of the *Toll Gantry*, i.e., 33.2 seconds considering a coverage of 1.2 Km (twice the communication range).

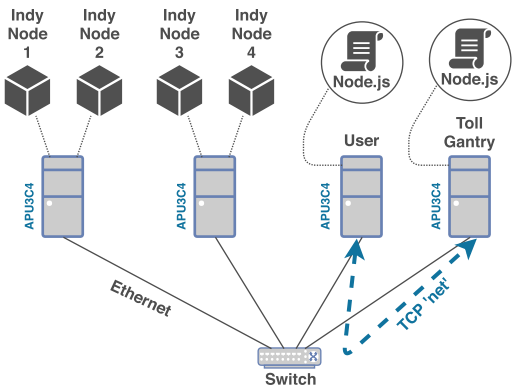
The evaluation is focused on assessing the overall identity validation and IOTA toll transaction timeliness under network conditions that can mimic a 5G C-V2X mode 4 connection. An experimental testbed was built encompassing four embedded PCs portraying the computing power characteristic of typical RoadSide Units (RSUs). Provided the unavailability of 5G smartphones supporting the 5G C-V2X mode 4, a 10/100 Ethernet network was employed to emulate the C-V2X mode 4 communication between *User* device and *Toll Gantry*. Although widely different technologies, with respect to the physical medium (wired vs. wireless) and medium access methods (*Carrier-Sense Multiple Access with Collision Avoidance* vs. *Sensing-based Semi-Persistent Scheduling*), their bandwidth and end-to-end latency can still be comparable. As reported in [14], considering a 5G C-V2X communication scenario, with a small number of devices (10), a latency of 24 ms is attainable. Thus, the results from the proof of concept testbed on timeliness and latency shall hold, even for an experimental setup based on C-V2X mode 4 communications.

In the following subsections, the setup and timing results obtained for both *Credential Validation* and *IOTA Payment* are presented and discussed.

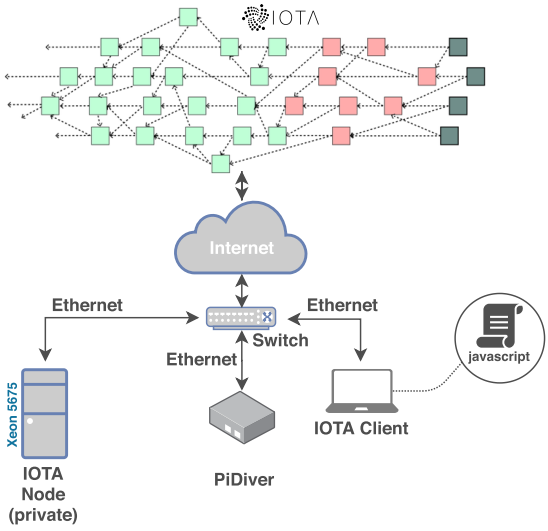
A. CREDENTIAL VALIDATION

The experimental setup shown in Fig. 4 was realized to evaluate the credential validations between *User* and *Toll Gantry*. For this purpose a set of four APU3C4 embedded PCs running Arch Linux was used. Each PC encompasses a quadcore AMD Jaguar processor clocked at 1 GHz and 4 GB of RAM memory. Two PCs were configured to run a total of four Hyperledger Indy nodes while the other two were used as Identity Owners, one representing the *User* and the other one acting as the *Toll Gantry*.

The Indy node pool was setup using Docker together with version 1.6.78 of the Hyperledger Indy. On the Identity



(a) Hyperlegder Indy evaluation setup.



(b) IOTA evaluation setup.

FIGURE 4. Experimental setups used to evaluate the latency of performing credential validations with the Hyperledger Indy framework and conducting digital money transactions through the IOTA network.

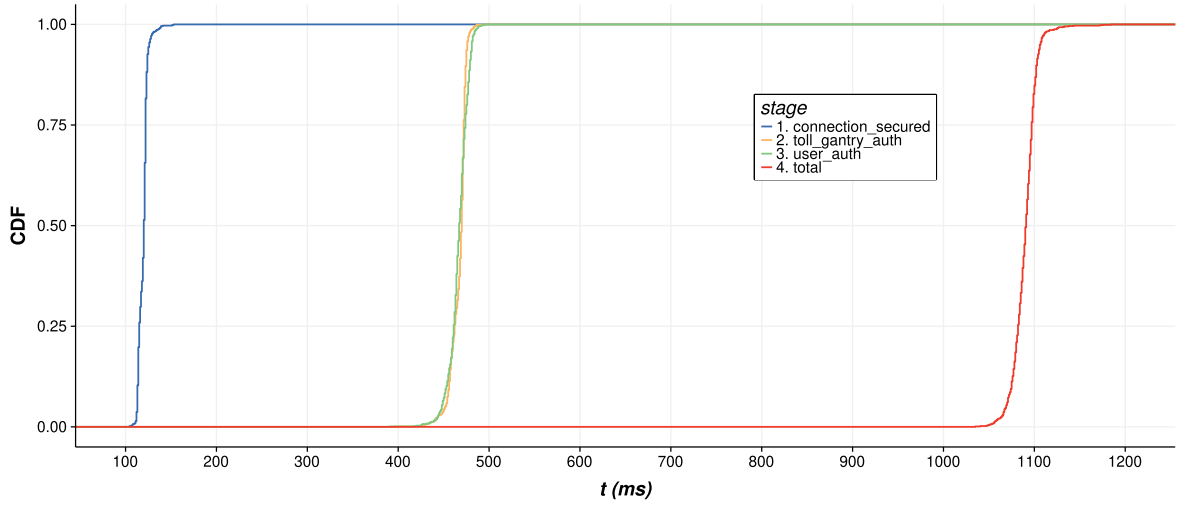


FIGURE 5. CDF of the latency experienced to establish a secure communication channel through the exchange of the on-spot created pairwise DIDs and both-ways authentication achieved through the exchange and validation of proofs.

Owner side, the Node.js wrapper for the Indy SDK version 1.6.7 was employed. The *Toll Gantry* and *User* interaction was simulated with two different Node.js scripts built upon the TCP 'net' module. A basic communication performance test with the mentioned 'net' module allowed to conclude that the average round trip delay between *Toll Gantry* and *User* PC was 70 ms.

In order to assess the time required to validate the identities of the *Toll Gantry* and of the *User* in an Hyperledger Indy setup, following the interaction sequences depicted in Figs. 2 and 3, a set of 1000 latency measurements were conducted for the process of establishing a pairwise Decentralized Identifier (DID) transport plus *User* and *Toll Gantry* identity validation.

The results of this assessment are documented in the Cumulative Distribution Function (CDF) illustrated in Fig. 5. The average elapsed time for establishing a secure channel and validate the credentials of both parties (*User* and *Toll Gantry*) is 1090.3 ms. In average, establishing a secure pairwise DID connection took 119.4 ms, while the credential validation of the *Toll Gantry* and *User* lasted 467.0 ms and 465.9 ms, respectively.

An aspect that is worth mentioning is the latency determinism in all stages of the credential validation. The steep CDF latency curves indicate that the delays are concentrated around average values with little dispersion around them.

B. IOTA PAYMENT

In order to evaluate the *Tangle* transaction attachment latency, which represents the amount of time taken to conduct a toll payment, a test setup employing a personal computer, a IOTA node and a "Proof-of-Work" (PoW) accelerator

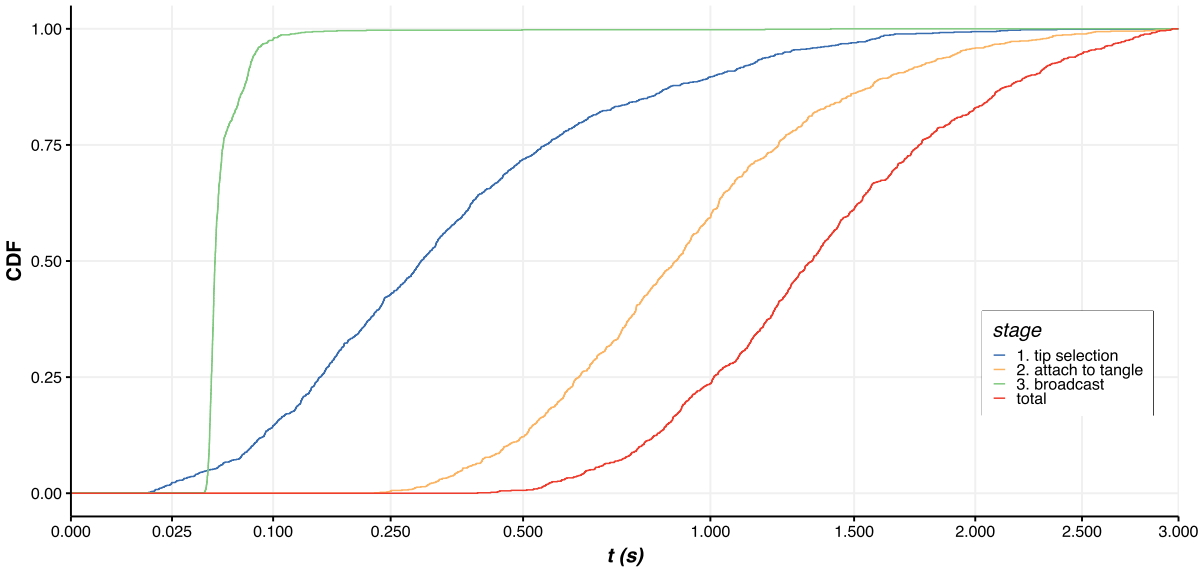


FIGURE 6. CDF of the latency experienced during the multiple phases of issuing a value transfer to the *Tangle* (three signed transactions).

encompassing an FPGA where used. The test setup is illustrated in Fig. 4b. The personal computer employs a i7-3630QM CPU, operating at 3.40 GHz with 8GB RAM memory. The IOTA node is implemented on a four-core virtual machine running on a Xeon X5675 processor operating at 3.46 GHz with 12GB RAM memory. This node is connected to the IOTA network and runs IRI version 1.5.5 (IOTA's node software) while exposing its API through HTTP. The PoW accelerator is a Cyclone 10 LP FPGA, named PiDiver [13], connected through its GPIO pins to a Raspberry Pi 3B running a HTTP server. In Fig. 4b the PiDiver plus Raspberry Pi is represented as a single entity named PiDiver.

Using IOTA's JavaScript library, *iota.js*, value transactions (bundle of three transactions) were added to the *Tangle* in order to simulate effective toll payments. This bundle includes in the transactions' message field (*signatureMessageFragment*) the nonce related to the toll payment request issued by the *Toll Gantry*. The bundle also holds information about the sender and receiver addresses as well as the value transferred between the two.

The process of attaching a value transaction to the *Tangle* can be divided in three stages: selection of two transactions to be approved (tip selection), execution of the PoW (attach to Tangle), and network broadcast of the transaction (broadcast). The processing work related to these three stages was outsourced through HTTP requests by the personal computer to the other local network elements, the IOTA node and PiDiver. Hence, the processing power of the client (PC) has a negligible impact on the overall transaction latency since the core computational effort is conducted by the PiDiver. The motivation for using a PC as the IOTA client is the availability of mature test and development tools, which contrast with those available for Android or iOS used for creating the actual toll payment App.

In the first stage, the tip selection algorithm is run two times, a process which was outsourced to the IOTA node as it requires an up-to-date ledger. In the second stage the Proof-of-Work is computed, a process which was outsourced to the PiDiver in order to shorten the time required to find a valid nonce. The third stage corresponds to the diffusion of the transaction in the *Tangle*, a process which was outsourced to the IOTA node as it is connected to the IOTA network. The Cumulative Distribution Functions (CDF) of a 1000 iterations of the latency experienced in these three phases is plotted in Fig. 6.

As shown, the duration of the PoW has a high variance due to the randomness of finding a suitable nonce. The step with the higher impact in the overall latency is the "attach to tangle" component corresponding to the "proof-of-work" that needs to be carried out for each transaction. The average latency is 1.02 s in this case. The second most significant contribution is the "tip selection", averaging at 0.43 s. The message broadcast averages around 0.06 s. Overall, the global latency of adding a value transaction to the *Tangle* using our setup is 1.51 seconds in average.

After a transaction is added to the *Tangle*, and before it can be considered complete, it must be *confirmed* in the *Tangle*. Although this process is carried without the involvement of the *User* smartphone, it does implicate that the transaction cannot be deemed concluded until it is *confirmed*. Indeed, the longer it takes for the transaction to be *confirmed* the less probable it is to be. This is where *reattach* and *promote* techniques can be employed to foster its confirmation. This process is beyond the scope of this article as it can be later executed by the *Road Operator* or by the *Toll Gantry*.

C. DISCUSSION

Results for credential validation show that this process takes a short amount of time and it is highly deterministic when compared to attaching a *Tangle* transaction. Although the amount of information used in the credential validation is adequate

for the envisaged purpose, it may not fit other applications requiring more parameters in the credentials.

The results for the latency of a IOTA value transfer are, approximately, 40% higher than those of the credential validation. To make that worse, a IOTA exchange among parties results not in one transaction added to the *Tangle*, but in multiple transactions. These transactions are grouped into a so-called *bundle* that represents an atomic transfer item in the *Tangle*. The ''tip selection'' and ''broadcast'' are the same as for appending a single transaction. However, the PoW (''attach to tangle'') must be carried out individually for each of the embedded transactions in the *bundle*. At the recommended level of security for low-value transactions (level 2 - 256 bit signature) three transactions will be embedded in the bundle: debit, credit and debit signature. This number of transactions occurs when exchanging IOTAs only between two addresses/''accounts'': one belonging to the *User* and the the other to the *Toll Gantry*.

The overall latency of conducting the credential validation and performing the IOTA value exchange between *User* and *Toll Gantry* is demonstrated to last 2.6 seconds in average for the realized test setup. This result shows that an open road toll collection system solely based on the proposed architecture and operation can perform all steps within a bounded time window of 33.2 s, thus making the solution feasible and providing enough slack to handle higher vehicle speeds and support reduced communication ranges, for example.

As the trials were conducted in a very controlled communication environment, it is expected that common wireless phenomenons such as multi-path fading and interference will degrade the performance of the electronic tolling system, but without compromising its operation.

V. RELATED WORK

Vehicle-to-everything (V2X) services will benefit from the enhanced performance of 5G systems, such as ultra-low latency, higher data rates, reliability and other features such as network slicing [15]. Moreover, high speed data rate and low latency timings are expected to be accompanied with efficient authentication procedures.

Legacy cellular networks provide a high level of security to its users. Traffic is encrypted and the User Equipment (UE) and base station (BS) are mutually authenticated. However the new networking paradigms created by 5G advanced features require new security mechanisms. In 5G, not only the UE and BS are authenticated mutually but the authenticity of third party services needs to be verified [16].

Traffic is expected to be largely offloaded to D2D connections between user equipment in order to decrease the computational burden on base stations. This allows a more efficient spectrum use but also gives rise to certain problems such as increased interference.

New attack vectors are expected to arise due to the more advanced services that 5G is capable of supporting. The multitude of services supported by 5G makes it very difficult to create a one-fits-all security architecture. Such architecture should be capable of sustaining DDoS and man-in-the-middle attacks, as well as jamming due to device interference and third party eavesdropping.

Vuk Marojevic discussed in [17] possible threat scenarios for C-V2X concluding that, despite the safety-critical nature of C-V2X, only a few mechanisms and procedures have been specified to secure it. In fact, the 3GPP R14 specification for C-V2X explicitly states that no security is applied for the C-V2X broadcast type communication, i.e., messages exchanged among UEs have no standard security mechanisms in place.

In [6], Lu *et al*, present a comprehensive survey on the security of 5G V2X services together with an in-depth analysis of the state-of-the-art strategies for securing 5G V2X services, discussing how to achieve trust, security, or privacy protection in each strategy.

According to Qualcomm [18], as security over PC5 mode 4 relies on application layer security, there will be no difference in the privacy and security for the C-V2X when compared to IEEE 802.11p based solutions. This means that application-level security defined in IEEE WAVE (1609.2) and ETSI ITS G5 can be transparently used in C-V2X. Despite this possibility, for the use case considered in this article, that would imply using a centralized public key infrastructure [19] and a significant bandwidth penalty on the wireless medium [20].

Yang *et al* discuss the process of securing 5G wireless communications using the physical layer in [21]. Physical layers security techniques use the characteristics of the wireless channel, multiple antennas, modulation and coding in order to avoid eavesdropping. These techniques have two major advantages: they don't require any considerable computational complexity, meaning that powerful unauthorized devices can't disturb the network security, and they have a high scalability, avoiding the need of a sometimes difficult to implement cryptographic key distribution system where devices constantly join and leave network cells.

Key management in small network cell can be difficult where users constantly join and leave access points. The increased latency caused by the frequent handovers between cells can also impact the efficiency of the authentication processes. In order to leverage the benefits of SDN, a fast authentication method is presented in [22]. The proposed method is considered to be hard to be compromised due to the use of several physical layer attributes used as user fingerprints in the authentication process. User location is also predicted in order to prepare the next relevant cells.

5G is put forward as a potential candidate for vehicular networks (VANETs) in [23]. A system architecture is proposed featuring real-time video services with emphasis on reliable, secure and privacy-aware communications. The architecture is composed by a mobile core network (MCN), a trusted authority (TA), a department of motor vehicles (DMV), and a law enforcement agency (LEA). D2D and mmWave procedures are used in the communications. The proposed cryptographic mechanisms include a pseudonymous authentica-

tion scheme, a public key encryption with keyword search, a ciphertext-policy attribute-based encryption, and threshold schemes based on secret sharing.

In device-to-device (D2D) communications, devices can communicate with each other without going through base stations. A secure data sharing protocol (SeDS) for D2D communication in 4G LTE-Advanced is proposed in [24]. The described method achieves various security requirements through the use of digital signatures and symmetric encryption without adding extra load to the network. The proposed method can detect free-riding attacks by keeping records of the current user equipments in the network.

In [25] the authors propose a secret key sharing method between two devices without the need of prior knowledge between both in order to achieve secure D2D communications. This is achieved with a low computational cost and small mutual authentication overhead. The proposed method was implemented using two smartphones and the Wi-Fi Direct protocol, demonstrating the efficiency and usability of the proposal.

The physical layer can also be used to secure D2D communications. In [26], the authors propose the use of a beam forming technique that uses physical layer coding to secure information as it passes through a relay. Results show that the algorithm converges fast and D2D performance is degraded as the number of eavesdroppers rise.

D2D nodes in proximity can share sensitive information relative to their users identity and personal details [27]. A eavesdropper con exploit D2D communication weaknesses and use the stolen information for illegal purposes. Contributing to D2D security, in [28], the concept of continuous authenticity and a security scoring system (SeS) for measuring security is proposed. Legitimacy patterns, which are sequence of bits inserted in the transmitted packets continuously are introduced to give an advantage over the attackers. In order to measure the security, the security scoring system is based on the violation of the legitimacy patterns. Simulation results show an efficient detection of attacks without requiring intensive computations at higher layers of the software stack.

VI. CONCLUSION

The deployment of 5G C-V2X technology will foster a richer service ecosystem for vehicular applications. The emergence of new cryptography based technologies for digital identity and currency will stem new solutions that will meet existing and future challenges. This article proposes a crypto tolling architecture that harnesses 5G C-V2X connectivity between *User* and *Toll Gantry* devices in order to establish a secure, private and convenient tolling system. Besides describing the architecture and operation of the envisaged solution, the paper also documents a feasibility analysis conducted using an experimental setup. Results show that an open road tolling system can be realized using the IOTA framework for payments and the Hyperledger Indy for Self-Sovereign Identity validation. Results also show that the use of dedicated GPU hardware can ensure the execution of IOTA's PoW in a timely fashion.

REFERENCES

[1] K. Persad, C. Michael Walton, and S. Hussain, "Toll collection technology and best practices," Center Transp. Res., Univ. Texas Austin, Austin, TX, USA, Tech. Rep. 0-5217-P1, 2007.

[2] M. Randriamasy, A. Cabani, H. Chafouk, and G. Fremont, "Reliable vehicle location in electronic toll collection service with cooperative intelligent transportation systems," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, 2017, pp. 1–7.

[3] M. Randriamasy, A. Cabani, H. Chafouk, and G. Fremont, "Formally validated of novel tolling service with the ITS-G5," *IEEE Access*, vol. 7, pp. 41133–41144, 2019.

[4] F. Camacho, C. Cárdenas, and D. Muñoz, "Emerging technologies and research challenges for intelligent transportation systems: 5G, HetNets, and SDN," *Int. J. Interact. Des. Manuf. (IJIDeM)*, vol. 12, no. 1, pp. 327–335, Feb. 2018.

[5] H. Ullah, N. Gopalakrishnan Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5G communication: An overview of Vehicle-to-everything, drones, and healthcare use-cases," *IEEE Access*, vol. 7, pp. 37251–37268, 2019.

[6] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G Vehicle-to-Everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.

[7] C. Vlachos and V. Friderikos, "MOCA: Multiobjective cell association for Device-to-Device communications," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9313–9327, Oct. 2017.

[8] *E-UTRA and EUTRAN; Overall description; Stage 2 (v14.8.0, Release 14)*, document TS 36.300, 3rd Generation Partnership Project, Oct. 2018.

[9] *Technical Specification Group Services and System Aspects; Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services (V16.3.0, Release 16)*, document TS 23.287, 3rd Generation Partnership Project, Jul. 2020.

[10] S. Popov. (Oct. 2017). *The Tangle*. Accessed: Nov. 2, 2020. [Online]. Available: http://iotatoken.com/IOTA_Whitepaper.pdf

[11] Sovrin Foundation. (Jan. 2018). *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust*. Accessed: Jan. 26, 2020. [Online]. Available: https://sovrin.org/library/sovrin-protocol-and-token-white-paper/

[12] *Addendum to V2X Functional and Performance Test Report; Test Procedures and Results for 20-MHz Deployment in CH183*, 5GAA Automotive Association, Munich Germany, May 2019.

[13] T. Pototschnig. (Apr. 2018). *IOTA PoW Hardware Accelerator FPGA for Raspberry Pi (und USB)*. Accessed: Jan. 26, 2020. [Online]. Available: https://microengineer.eu/2018/04/25/iota-pearl-diver-fpga/

[14] A. K. Gulia, "A simulation study on the performance comparison of the V2X communication systems: ITSG5 and C-V2X," M.S. thesis, ICT Innov., KTH Roy. Inst. Technol., Stockholm, Sweden, Feb. 2020.

[15] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Veh. Commun.*, vol. 12, pp. 50–65, May 2018, doi: 10.1016/j.vehcom.2018.01.008.

[16] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018, doi: 10.1109/access.2017.2779146.

[17] V. Marojevic, "C-V2X security requirements and procedures: Survey and research directions," 2018, *arXiv:1807.09338*. [Online]. Available: http://arxiv.org/abs/1807.09338

[18] *C-V2X Technical Performance Frequently Asked Questions*, Qualcomm, San Diego, CA, USA, Oct. 2019.

[19] B. Fernandes, J. Rufino, M. Alam, and J. Ferreira, "Implementation and analysis of IEEE and ETSI security standards for vehicular communications," *Mobile Netw. Appl.*, vol. 23, pp. 469–478, Feb. 2018, doi: 10.1007/s11036-018-1019-x.

[20] J. Rufino, L. Silva, B. Fernandes, J. Almeida, and J. Ferreira, "Overhead of V2X secured messages: An analysis," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5, doi: 10.1109/VTC-Spring.2019.8746479.

[21] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015, doi: 10.1109/mcom.2015.7081071.

[22] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6, doi: 10.1109/icc.2016.7510994.
[23] M. Hashem Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Oct. 2016, doi: 10.1109/tvt.2016.2541862.
[24] A. Zhang, J. Chen, R. Q. Hu and Y. Qian, SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks, *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659–2672, Apr. 2016, doi: 10.1109/TVT.2015.2416002.
[25] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, "Secure key establishment for Device-to-Device communications," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 336–340, doi: 10.1109/glocom.2014.7036830.
[26] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-aho, "Physical layer security for relay assisted MIMO D2D communication," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 651–656, doi: 10.1109/iccw.2015.7247255.
[27] R. I. Ansari, C. Chrysostomou, S. A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, and J. J. P. C. Rodrigues, "5G D2D networks: Techniques, challenges, and future prospects," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3970–3984, Dec. 2018, doi: 10.1109/jsyst.2017.2773633.
[28] I. Abualhaol and S. Muegge, "Securing D2D wireless links by continuous authenticity with legitimacy patterns," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, doi: 10.1109/hicss.2016.713.

PAULO C. BARTOLOMEU (Senior Member, IEEE) received the Ph.D. degree in informatics engineering from the University of Aveiro, Portugal, in 2014. He has participated in several research and development projects at the academia (ARMONIO and CAMBADA) and in the industry (CIRaF, DHT-Mesh, BikeEmotion, LUL, and SheepIT). He is the author of two patents and more than 40 scientific publications, including papers in conferences, journals, and book chapters. His research interests include the IoT, real-time communications, networked embedded systems, decentralized identity, and blockchain.

EMANUEL VIEIRA received the master's degree in engineering physics from the University of Aveiro, Portugal, in 2017. His research interests include machine learning and blockchain technologies.

JOAQUIM FERREIRA (Senior Member, IEEE) received the Ph.D. degree in informatics engineering from the University of Aveiro, Portugal, in 2005. He is currently an Adjunct Professor with the School of Technology and Management, University of Aveiro, and a Researcher with the Telecommunications Institute. He has been involved in several international and national research projects. His research interests include dependable distributed systems, fault-tolerant real-time communications, wireless vehicular communications, cooperative ITS systems, and medium access control protocols. He is the author of several scientific articles and book chapters in his areas of expertise. He has served on several conferences scientific committees.