I. Agudo, M. Montenegro-Gómez, and J. Lopez, "A Blockchain Approach for Decentralized V2X (D-V2X)", *IEEE Transactions on Vehicular Technology*, 2020.
http://doi.org/10.1109/TVT.2020.3046640
NICS Lab. Publications: https://www.nics.uma.es/publications

A Blockchain Approach for Decentralized V2X (D-V2X)

Isaac Agudo, Manuel Montenegro-Gómez, Javier Lopez
Network, Information and Computer Security Lab
University of Malaga
Malaga, Spain
{isaac,mmg, jlm}@lcc.uma.es

***Abstract*—New mobility paradigms have appeared in recent years, and everything suggests that some more are coming. This fact makes apparent the necessity of modernizing the road infrastructure, the signalling elements and the traffic management systems. Many initiatives have emerged around the term Intelligent Transport System (ITS) in order to define new scenarios and requirements for this kind of applications. We even have two main competing technologies for implementing Vehicular communication protocols (V2X), C-V2X and 802.11p, but neither of them is widely deployed yet.**

One of the main barriers for the massive adoption of those technologies is governance. Current solutions rely on the use of a public key infrastructure that enables secure collaboration between the different entities in the V2X ecosystem, but given its global scope, managing such infrastructure requires reaching agreements between many parties, with conflicts of interest between automakers and telecommunication operators. As a result, there are plenty of use cases available and two mature communication technologies, but the complexity at the business layer is stopping the drivers from taking advantage of ITS applications.

Blockchain technologies are defining a new decentralized paradigm for most traditional applications, where smart contracts provide a straightforward mechanism for decentralized governance. In this work, we propose an approach for decentralized V2X (D-V2X) that does not require any trusted authority and can be implemented on top of any communication protocol. We also define a proof-of-concept technical architecture on top of a cheap and highly secure System-on-Chip (SoC) that could allow for massive adoption of D-V2X.

***Index Terms*—Intelligent Transport Systems, Blockchain, Security, Privacy, Identity, Bluetooth Low Energy.**

I. Introduction

In the next few years there will be a lot of changes in the automotive sector among with new mobility services and offers, as a consequence of the profound technological transformations of these sectors, but in the meanwhile the driver is the sole actor responsible for the decisions made in the vehicle. There is a diversity of Connected Vehicle (CV) environments and options [1]: V2V (vehicle-to-vehicle); V2I (vehicle-to-infrastructure); I2V (infrastructure-to-vehicle); V2P (vehicle-to-pedestrian); and V2X (vehicle-to-anything). Whereas the current V2X technologies, i.e. C-V2X and 802.11p, are a requirement for advanced autonomous driving, there will be human drivers in the road for many years. Driving is essentially a decentralized process, the infrastructure gives some guidance but ultimately drivers engage with each other to make everything work. As V2X technologies reach the market, drivers would be able to benefit from all the available information, an this will result in an increased road safety and driving efficiency.

Typical V2X communication is performed in broadcast, where some infrastructure elements or vehicles broadcast relevant information to nearby vehicles. In those scenarios there are different security requirements that might be relevant [2]: authentication, message integrity, access control, message confidentiality, availability, privacy and anonymity. The two main security services that any ITS infrastructure needs to provide are authentication and message integrity. Vehicles need to authenticate the sender of the received messages and be sure that their integrity is preserved before using any of the information in those messages.

Confidentiality is not that relevant for ITS communications as information is usually of interest to any neighboring vehicle, but privacy is very relevant when vehicles share their position. Current ITS standards use pseudonyms to make it difficult for external entities to track the location of a vehicle and to protect its identity. Vehicles are issued multiple "unlinkable" pseudonymous certificates that, under certain circumstances, e.g., misbehaving vehicles, can be revoked as a whole with the help of some additional information. Whereas using those pseudonymous certificates is necessary to protect privacy, it is not enough: all other protocol identifiers—e.g., MAC address, sequence numbers, IP addresses, ports, etc.—need to be changed accordingly too. Moreover, there is still the issue of RF fingerprint [3] that could identify the radio emitter even if all identifiers are removed.

The increase of information in next generation vehicles would also require new mechanisms to ensure the integrity and authenticity of all vehicular data, but also that privacy requirements are met. The decentralized nature of this information and the fact that driving is based mainly on publicly available data provide some foundations for a blockchain approach to ITS, with the aim of providing an open, transparent and secure decentralized ITS platform.

One of the first works tackling ITS issues with blockchain technologies dates back to 2016. In [4], the authors present a preliminary study of blockchain-based ITS. The work is mainly conceptual, although they present a case study for blockchain-based real-time ride-sharing services. Other au-

thors in [5] try to combine Vehicular Ad-hoc Networks (VANETs) and Ethereum's blockchain-based application concepts to enable transparent, self-managed and decentralized ITS services, without the need of a central managing authority. This work focuses mainly on traffic regulation, vehicle tax and vehicle insurance applications. In [6] blockchain is used to prevent odometer fraud while preserving privacy principles. Records are kept encrypted in a back-end storage, while the blockchain is used to prevent tampering with the encrypted records. Odometer fraud prevention is a typical blockchain use case [7] and has been the base for different Proof-of-Concept prototypes [8]. There is already a solution in this line in the market: VinChain[1]. In [9], the authors propose the use of blockchain to implement an insurance record system that can include all aspects of insurance transactions. In [10], the authors propose the use of a consortium blockchain technology to form a vehicular blockchain, which performs distributed data storage and secure data sharing. However, this approach is not dealing with the network governance, the real challenge for ITS deployments.

Recently, there have been proposals to use blockchain for data sharing in the Internet of Vehicles (IoV) paradigm. In [11], the authors propose a hybrid blockchain architecture and federated learning for node selection. In [12], the use of Deep Reinforcement Learning is proposed to implement intelligent data caching using blockchain in Vehicular Edge Computing (VEC).

A common challenge for all ITS approaches is how to enable V2X communications. Different technologies can be used depending on the application, as not all of them share the same time critical profile. For example, a connected traffic light information service has a maximum latency requirement more relaxed than V2V applications such as cooperative collision mitigation or avoidance or adaptive cruise control, were a few extra milliseconds can be the difference between suffering a car crash or avoiding it. As a rule of thumb, it is said they are not time-critical when they can be implemented using regular 4G/LTE networks [13], i.e., maximum latency above 100 ms. Some automakers are already providing ITS services using cellular network communications instead of direct I2V communication. For example, Audi launched the Audi Traffic Light Information in Las Vegas in 2016 and started testing it in Europe in 2019 with the goal to implement Time-to-Green and Green Light Optimized Speed Advisory (GLOSA) in all their cars. In order to access this service, you must have an Audi car compatible with their subscription service, whereas, when using direct communications instead, any car close enough will get the information. By using direct communications, the system does not depend exclusively on the cellular network. On the other hand, direct communications according to current ITS standards would require the installation of a dedicated equipment in the vehicle.

In order to reach a massive adoption of V2X communications, we need a technology that is widely deployed and affordable. There is the promise of 5G as a V2X enabler, but until 5G is widely deployed globally its cost will be a hindrance. If we try to find a short-range communication technology that is already widely deployed with an affordable cost, and where any device can talk to any device in its proximity, Bluetooth Low Energy is the only choice. According to the Bluetooth Market Update in 2019 [14] more than 3 billion Bluetooth devices were shipped with support for Bluetooth Low Energy. All smartphones shipped in 2019 included Bluetooth, most of them with Bluetooth Low Energy. Regarding operating systems, the most representative ones, i.e., iOS and Android, support Bluetooth Low Energy since 2013 and have been including new functionalities in each new version. Bluetooth Low Energy is expanding Bluetooth usage scenarios, from location-based services [15] to IoT [16]. Some authors have even analyzed suitability of BLE for Time-Critical Industrial IoT Application [17]. Although there has been a previous attempt to implement ITS services over Bluetooth Low Energy [18], it relies on a reduced security model due to the limitation imposed in BLE 4.0 for broadcasting messages, i.e., 31 bytes.

In this work, we propose an approach for Decentralized V2X that provides similar integrity, authentication, confidentiality and privacy features compared to IEEE 1609.2, but uses a distributed governance model. We also provide a conceptual architecture and evaluate how to materialize it using an affordable BLE SoC.

The paper is organized as follows. In section II we analyze security mechanisms in both ETSI ITS and IEEE 1609 ITS standards. In section III we review recent efforts to define Decentralized Public Key Infrastructures (D-PKI). Section IV analyzes the challenges arising from applying D-PKI concepts to vehicular networks and provides alternatives for a security level equivalent to VPKI. This section is setting the principles for a Decentralized Vehicular PKI (D-VPKI). Section V describes a Proof-of-Concept technical architecture to materialize all D-V2X concepts and evaluates some hardware components that could be used to implement it. Finally, section VI presents some conclusions.

II. Security of Intelligent Transport Systems Protocols

There are different initiatives for ITS standardization around the globe. The working group with a longer trajectory in this field is the IEEE 1609 DSRC WG from the United States (US), that is behind the WAVE standard. The IEEE 1609.2 [19] standard defines the security data structures and message formats. It proposes the use of a vehicular public key infrastructure (VPKI) supporting ECDSA signatures [20] and ECIES encryption [21]. In the IEEE 1609.2 standard there is also a recommendation to protect the devices themselves by using hardware-backed private keys. Ideally, the device should use some kind of trusted execution environment to protect all sensible cryptographic material. In Europe, the ETSI ITS Working Group 5 is responsible for all aspects related to security, data protection and privacy of ITS standards. A

[1]https://vinchain.io

detailed review of the different European standards for ITS can be found in [22]. In [23], the authors present a detailed comparative analysis of security aspects for both U.S. and Europe ITS protocol stacks and standardization activities.

In the European side, security requirements are specified in the technical report ETSI TR 102 893 and are very in line with the IEEE 1609.2 standard. Those protocols were originally designed to work on top of the IEEE 802.11p standard [24] in the 5.9 GHz frequency band but are also compatible with LTE based technologies, i.e., C-V2X. The VPKI behind ITS protocols needs to offer specialized security services. It needs to protect privacy in vehicles and at the same time it needs to avoid overhead for time critical use cases.

The US government has developed a prototype pilot for a Security Credential Management System (SCMS) [25], a VPKI designed to provision PKI certificates to vehicles and infrastructure. This pilot aimed at the following provision model:

- Certificate validity period: 1 week
- Certificates valid simultaneously: minimum 20
- Overall covered time span: 1-3 years

In this work, they use Butterfly keys in order to avoid the generation and independent certification of thousands of public keys per vehicle. This technique can be used to securely request an arbitrary number of certificates per vehicle, by using a single request to the SCMS, based on only one signing public key seed, one encryption public key seed, and two expansion functions. A diagram showing the interactions between the entities involved in the pseudonymous certificates provisioning is shown in Figure 1.

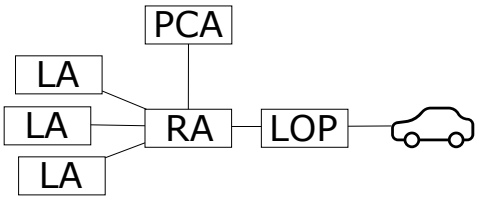

Fig. 1. Interactions in pseudonymous certificates provisioning

The four entities in the diagram are the following:

- **LOP**. This is the Location Obscurer Proxy. Its role is to hide the location of the requesting device from the RA.
- **RA**. This is the Registration Authority. Its role is to validate and process certificate requests. When using Butterfly keys, it recreates all the certificate requests from the same seed and send them to the PCA individually, unordered and mixed with other requests from different vehicles in order to make it difficult for the PCA to link requests derived from the same seed.
- **PCA**. This is the Pseudonym CA. Its role is to issue short-term pseudonymous certificates.
- **LA**. These are the Linkage Authorities. Their role is to generate information that can help link pseudonymous certificates, in case they need to be revoked. By requiring more than one LA to work collaboratively, no single entity would be able to link certificates.

Some of the mechanisms implemented in the SCMS pilot for the pseudonymous certificates are inspired in the ideas introduced by David Chaum in [26] but adapted to the security requirements of ITS. In [27], there is a detailed step-by-step explanation of the provisioning and revocation of pseudonymous certificates, as well as a security analysis of how Butterfly keys work. In [28], authors analyze the main security challenges for a VPKI, mainly the trust model and the management of pseudonyms, and propose their own solution validated with mobility data from previous research studies.

Apart from trust and privacy related issues, there is also the challenge of optimizing messages length in order to reduce latency in ITS use cases. The IEEE 1609.2 standard, uses elliptic curve cryptography in order to reduce the size of the digital signatures and the key material. In particular, the specification uses the ECDSA algorithm [29], but there are already some experts [30] that recommend the inclusion of faster elliptic curve signatures such as Ed25519 [31].

Messages are encoded using the SignedData structure (Figure 2). This structure is divided in four parts:

- **HashAlgorithm**. Identifies the hash algorithm used in the message.
- **ToBeSignedData**. Includes both a payload and a header info. The payload can be a basic safety message (BSM) [32] in the U.S. standard, including core state information about the transmitting vehicle such as position, dynamics, status, etc. In the ETSI standard it could be a periodic cooperative awareness message (CAM) [33] or an (event-driven) decentralized environmental notification message (DENM) [34]. BSM messages can also be periodic or event-driven. The header info includes among other fields the generation time and location.
- **SignedIdentifier**. It could be an 8 bytes digest of the sender certificate, in order to save bandwidth, or the sender certificate itself.
- **Signature**. It contains the signature of the message.

Fig. 2. Signed Data Structure

As we have mentioned before, there are different options for the signer identifier that have a direct implication both in the length of the messages and in the processing time, i.e., latency.

The straightforward solution would be to include a compact certificate as defined in the IEEE 1609.2 specification, that already saves approximately 50% of the space compared to traditional X.509 certificates. These certificates are denoted as explicit certificates in the standards. The recipient of the message first needs to verify the validity of the certificate using the root CA public key and then extract the public key from

the certificate in order to check the signature of the message. The fields of the certificate are the following:

- Certificate version.
- Device ID of the certificate signer.
- Information about the target device.
- Public key of the signature.
- Digital signature encoded as a couple of curve points.

In case an 8 bytes digest is included in the signer identifier, the recipient needs to find the certificate in its local cache but there is no need to check the validity of the certificate in real time, as the cache could implement an asynchronous mechanism to validate certificates at inclusion and remove expired certificates. The first message might incur in a higher overhead than in the former case, but for bursts of messages the second and following messages would be processed similarly or even faster. In any case, a compact certificate needs to be received from time to time in order to feed the local cache.

The IEEE 1609.2 specification also allows for the use of implicit certificates [35], although this option is not available in the ETSI specification. Implicit certificates are even more compact than explicit certificates, as the public key is derived from the rest of fields of the certificate plus some public information and do not require the inclusion of the signature from the CA. However, there is an overhead for the derivation of the public key in the first message, although for the second and following messages a cache mechanism similar to the one mentioned in the aforementioned case could help mitigating it.

Table I contains some data from a Certicom study in 2005 [36] where they compared certificate sizes between RSA, ECDSA and ECQV, i.e., implicit certificates. Certificate size is estimated as the size of the public key and its signature, all other metadata are excluded from the comparison as they will largely depend on the application.

TABLE I
PUBLIC KEY PLUS SIGNATURE SIZE FOR DIFFERENT SECURITY LEVELS

Security Level	ECQV	ECDSA	RSA
112	225	673	4096
128	257	769	6144
192	385	1153	15360

Another challenge on maintaining a VPKI is certificate revocation. Real time revocation mechanisms such as OCSP would create a bottleneck in the system and cannot be used as a standalone solution for VPKI [37]. On the other hand, mechanisms such as CRL also have deficiencies. Depending on the number of pseudonyms used by the vehicles, the size of the CRL may grow very quickly. In [38], the authors analyze the parameters that determine the sizes of CRLs and propose adding a "valid after" field to the IEEE 1609.2 certificates in order to reduce CRL size.

III. DECENTRALIZED PKI (D-PKI)

One of the main challenges of PKIs is trust. In the Internet ecosystem, trusting root CAs is hard. Modern web browsers include a curated list of trusted root CAs, but even those CAs might be compromised. In the ITS ecosystem, there are even more entities that need to be trusted.

The world is moving towards decentralization in many ways. A first step towards decentralization of trust is Certificate Transparency[2], that provides an open framework for monitoring and auditing TLS certificates in nearly real time. The central piece of this framework is the Certificate log, that maintain a *cryptographically assured, publicly auditable, append-only record of certificates*. Using this framework, the owner of a domain or any interested party, would be able to check all certificates issued for this particular domain, in order to detect malicious or erroneous certificates. Still, the system depends on a reduced number of certificate logs that could be compromised.

The first approach to implement a fully decentralized PKI, using Blokchain technologies was Certcoin [39] in 2014. Certcoin had no central authority; instead, it made use of a secure distributed dictionary for key lookup. The concept of Decentralized Public Key Infrastructure (DPKI) was analyzed in detail in the first Rebooting Web of Trust workshop (RWOT-I), that took place in San Francisco in 2015. As a result, a white paper [40] was produced elaborating on the requirements for a successful deployment of a DPKI following the steps of Certcoin. Those ideas were later materialized in a formal model for a smart-contract-based DPKI [41]. In this work, the authors use the Universal Composability (UC) framework to perform a security analysis under the strong RSA assumption in the Random Oracle model. The RWOT-I white paper mentions two design principles for DPKIs:

- *Each principal must be in complete control of their current identifier/public-key binding.* Based on that, an attacker who wants to affect a particular identifier/public-key binding would need to compromise the principal owning it. In traditional PKIs, compromising a CA allows the attacker to affect many identifier/public-key bindings at once with no extra effort.
- *The system must make all-or-nothing forward progress: either every principal must witness every other principal's updates to their identifier/public-key bindings, or else no one may observe any updates.* This would prevent isolation attacks, forcing the attacker to target the whole network at once.

One of the challenges for DPKIs is the decentralized registration of identifiers. The white paper mentions some principles for registration:

- *Identifiers cannot be destroyed*. Only the principal who registered the identifier would be able to delete it, although registrations may have an expiration date.
- *Registering rules must be transparent*. Those rules should be easy to understand. For example, registration could be implemented on a first-come-first-serve basis or as a decentralized auction.

[2]http://www.certificate-transparency.org/

- *Registering rules cannot be altered once set*. If these rules were modified after some principals register an identifier, the principals might lose control over their identifiers without their consent.
- *Identifiers management must support a peer-to-peer mechanism*. That would ensure that a single entity cannot prevent identifiers from being updated or renewed.

Instead of using digitally signed certificates, a DPKI uses a decentralized database. As we can see in Figure 3, the common practice for DPKIs is that Principals first register their identifiers in the DPKI using a *master key* and afterwards, they can submit arbitrary entries to this decentralized database, linking their identifiers to *public keys* under their control. Those public keys, or subkeys, would serve the same purpose as the public keys included in X.509 end-entities certificates.

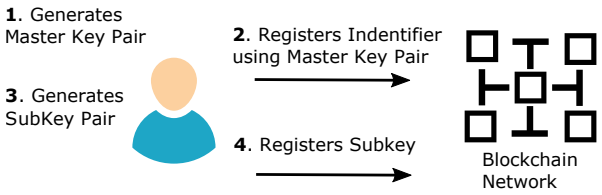

Fig. 3. DPKI Identifier and public keys registration

Directly storing the public keys in the blockchain might not scale well; that is why in 2017 the Decentralized Identity Foundation (DIF) started working on a scalable solution to this problem, the Sidetree protocol [42]. Sidetree is a "Layer 2" protocol that can help creating a scalable DPKI on top of any existing Blockchain without the need for centralized authorities or secondary consensus mechanisms (Figure 4). The Sidetree protocol is run by independent nodes that maintain a consistent view of all public keys in the system, anchoring all the operations over them in the base blockchain.

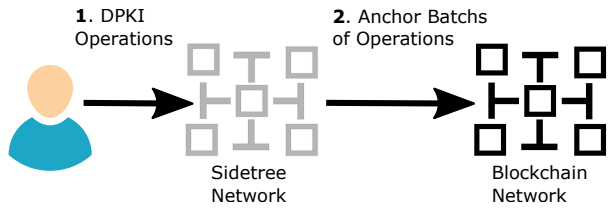

Fig. 4. DPKI using the Sidetree protocol

There are currently two implementations of the Sidetree protocol:

- **ION**, a Sidetree implementation in the Bitcoin blockchain.
- **Element**, a Sidetree implementation in the Ethereum blockchain.

Microsoft is the leading force behind ION, although it is also collaborating with Transmute and ConsenSys in the Element implementation. Both efforts use IPFS [43] as the underlying Content Addressable Storage [44] (CAS), where all DPKI operations are stored and replicated among members of the Sidetree network.

The protocol makes use of W3C Decentralized Identifiers (DIDs) [45], a type of identifiers that enables verifiable, decentralized digital identity. DIDs are URLs that associate a subject with a DID document containing cryptographic material that can help the subject, or a third party, to prove control over the DID, e.g., a public key whose corresponding private key is owned. The DID specification separates the roles of the *DID subject*, the entity identified by it, and the *DID controller*, the entity that can make changes to the DID document associated to the DID, although both roles could be assumed by the same entity.

Another complementing technology to DID, in some way analogous to the Attribute Certificates in the X.509 standard, is W3C Verifiable Credentials (VCs) [46]. A verifiable credential is *a tamper-evident credential that has authorship that can be cryptographically verified*. There are different actors in the VC ecosystem:

- **Issuer**. Asserts claims about subjects, creating verifiable credentials from these claims.
- **Subject**. The entity about which claims are made.
- **Holder**. Possesses verifiable credentials and generates verifiable presentations from them.
- **Verifier**. Receives and processes verifiable credentials, optionally inside a verifiable presentation.

All operations related to verifiable credentials are managed over a Verifiable Data Registry. This could be implemented in different ways, being one of them distributed ledgers. In Figure 5 there is a representation of the different actors in the VC ecosystem.

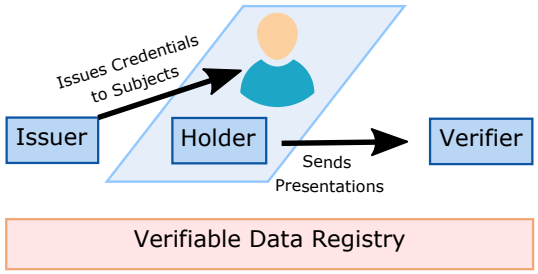

Fig. 5. Verifiable Credentials

Verifiable presentations allows for the verification of claims using privacy-enhancing technologies, e.g., Zero-Knowledge Proofs (ZKP). That would allow the holder to disclose only part of the credentials to the verifier in a secure way.

IV. Decentralized Vehicular PKI (D-VPKI)

The Decentralized Vehicular PKI (D-VPKI) would be the core of D-V2X, the same way as VPKI is the core of V2X. We need to pay attention to the requirements imposed by ITS applications and try to find the most suitable and most decentralized solution for any of the following requirements:

A. Identifiers

In vehicular networks, the prime candidate for identifier would be the Vehicle Identification Number (VIN) [47], a standard for a world-wide uniform identification numbering system for road vehicles. In 2019, the MOBI alliance presented a standard for blockchain-based Vehicle Identification (VID) [48] in an attempt to augment VIN and adapt it to the blockchain ecosystem. The first draft of the VID specification was launched in 2019 and is only available to MOBI members, but, based on the information publicly available, the concept of VID must rely on the DID specification.

There are different ways to link the VIN to the vehicle using a blockchain, all of them assuming we have some trusted hardware in the vehicle where we can implement a crypto wallet.

- The vehicle would generate the master key to register its VIN as the identifier to the D-VPKI. The vehicle would also be the controller, being in charge of any change to the identifier. That would require a very secure wallet to prevent the car owner from tampering with the keys and modifying the VIN
- The vehicle would generate the master key to register its VIN as the identifier to the D-VPKI, but the Original Equipment Manufacturer (OEM) would be the controller, being in charge of any change to the identifier. That would soften the security requirements for the vehicle.
- The vehicle would generate a master key and register a random DID into the D-VPKI. Later on, the OEM would issue a VC to the vehicle DID containing the VIN number and any other relevant information. The vehicle would be the subject of the VC, but the OEM would remain the Holder. Anytime the vehicle needs to prove its VIN, the OEM would need to engage in a verification protocol.
- The same as before, but the vehicle would be the Holder and the subject of the VC. Anytime the vehicle needs to prove that its DID is associated with its VIN, it would need to engage in a VC verification protocol. This gives the vehicle more control and better privacy properties but at the same time requires a more secure environment.

Given the nature of the identifier and the immutability of the D-VPKI, the preferred options would be the last two, as they allow for the replacement of the vehicle crypto wallet in case on malfunctioning by simple issuing a new VC to the new DID. The last one is the most decentralized, giving the vehicle full responsibility over the VC.

B. Pseudonyms

Privacy is also a relevant aspect for D-VPKIs that needs to be balanced with regard to Transparency. When implementing a general purpose DPKI in a public blockchain, the link between identifiers and public keys is completely transparent: anyone can inspect those links. However, there are situations where this link needs to be kept private, as, for example, in vehicular networks.

In [49], the authors propose a Privacy-aware Blockchain-based PKI (PB-PKI) as an adaptation of the Certcoin DPKI. The authors adapt the key updating process of CertCoin in order to avoid any public link between the updated public key and their identity or the previous public key. They make use of a hidden link in the form of an offline key pair, that needs to be generated for each key update. This key pair can be used later to trace back to an initially posted identity. This key pair is shared using a secret sharing scheme among a majority of network members, so that the network can link the identity in case of misbehavior. For each update, a linking evidence to the previous key is also secretly shared with a neighbor group of network members, in this case by encrypting a signature of a nonce included in the update with their public keys. The neighbor group can link to the previous key but not to the original identity—it can attest the new key is indeed linked to an existing key. The same authors revise privacy requirements for vehicular networks using Blockchain [50] to conclude that "linkability properties based on distance may be more fitting than time-based ones", but how to manage proximity groups in a decentralized way remains an open problem.

In a VPKI, the Registration Authority (RA), the Pseudonym CA (PCA) and the Linkage Authorities (LAs) implement a three-party protocol where none of the participants can trace back the identity of pseudonymous certificates individually, but, when collaborating, the link between them can be established. In a D-VPKI, there is no registration authority, as the vehicle itself is in charge of registering its identifier. There is also no PCA, as public keys are not certified by any trusted third party. However, the role of LAs is still relevant.

We have different options in order to implement a privacy preserving mechanism that allows vehicles to use unlinkable pseudonyms in a D-VPKI. Using the PB-PKI approach, the OEMs could designate some trusted LAs under their control that will participate in the registration of pseudonyms. The neighbor group would still be formed by vehicles in the proximity but, instead of secret-sharing the offline keys with a majority of the network, it would share them only with the LAs network. In case of misbehavior, the LAs could reconstruct the offline keys and trace back to the master key in order to revoke this identifier.

Another option would be to use privacy enhanced Verifiable Credentials (VCs). In this case, the vehicle will register many different DIDs, and the OEM will issue ZKP-enabled VCs for all of them, to link them to the master DID in a privacy-friendly way. This process will be performed in a secure environment and the OEM will remove the VC once issued. Another solution would be to use a Secure Multiparty Computation [51] to create the VC, preventing the OEM from learning the original DID to which the pseudonyms are linked. Later on, when the vehicle wants to use a new pseudonym, it will create two verifiable presentations: one showing that the new pseudonym and the previous one belong to the same master DID and a second one showing that the master DID is not revoked, in both cases without disclosing the master DID. The first presentation will be secret-shared with a different subset of LAs each time, whereas the second will be sent to the whole network. In case of misbehavior, the LAs could

trace back all the pseudonyms to the original DID, so that it could be revoked. We assume LAs are honest but curious and will not collude in order to trace back the master DID for the pseudonym. As a variant, LAs could be implemented as smart contracts providing a fully decentralized Linkage Authority.

Recently, the authors in [52] proposed a cooperative authentication mechanism that provides cooperative privacy preservation in vehicular networks based on proxy group authentication.

C. Proof of Location

Another relevant service that is currently outside of the ITS standards is secure location. Currently, ITS protocols assume location and time are received by the vehicle using GPS and then broadcasted using the ITS protocol. This approach has certain limitations: on the one hand, it is susceptible of GPS Spoofing attacks [53] and on the other hand, neighbors have no means to check the accuracy of the received GPS coordinates. Although there are some proposals that try to overcome those limitations [54], [55], current standards assume that the on-board unit (OBU) can be trusted to send accurate GPS coordinates.

There have been some recent works that implement Proof of Location (PoL) based on Blockchain [56], [57]. Currently, there are two main independent initiatives working on actual use cases for Proof of Location in Blockchain:

- FOAM[3] aims at providing tools for crowdsourced mapping and decentralized location services. FOAM concept for location bases services is based on a permissionless and autonomous network of radio-enabled devices that offer secure location services without the need of globally trusted sources like GPS.
- XYO[4] is a decentralized network of devices that anonymously collects and validates geospatial data. The ecosystem incentives location validators using their own ERC20 Token.

In a D-VPKI, all infrastructure elements could act as anchors for PoL. Any device could prove its location by showing what infrastructure elements are nearby. In practice this could be implemented by having the infrastructure elements issue privacy enhanced VCs including their location. For example, traffic lights will issue a VC for any DID that passes nearby. Later on, the vehicle could create presentations at different granularity levels. That would enable to implement proximity groups using smart contracts that verify all VCs and group vehicles according to their location in a privacy friendly way.

D. Revocation

There have been some recent works that try to implement certificate revocation in a blockchain. In [58], the authors implement and evaluate a prototype certificate blockchain to publish certificates and maintain their state. Their result shows that the miners of this certificate blockchain should store around 100Gb of data. In [59], the authors propose the use of Blockchain to keep track of certificate status in vehicular networks, removing the need for sharing CRLs in ITS. This is a relevant problem that has been approached from different angles. In [60], the authors propose the use of Edge computing to assist in the revocation of certificates for vehicular networks.

Another approach would be to use Certificate Issuance and Revocation Transparency (CIRT) [61], that aims at producing proof of currency for certificates using two Merkle trees that keep track of both issued certificates and their state. The complexity of the proofs is $O(\log n)$ both in time and space. There is another proposal in the same direction that aims at providing constant size proofs, but at the cost of using bilinear-map accumulators [62].

Revocation is usually triggered when a misbehaving entity is detected. Detecting misbehaving entities is also a relevant challenge in vehicular networks, which is somehow inherited from the early days of Wireless Sensor Networks [63]. In [64], a credibility system for IoT devices is implemented on top of a Blockchain in a decentralized way. This idea has also been analyzed in the automotive ecosystem [65], [66]. Smart contracts could help define a transparent mechanism to detect and report misbehaving vehicles.

E. Governance

In a fully decentralized setup, governance is one of the main challenges. Decentralized governance requires a complete change of paradigm that might create tensions with currently established practices. It is very difficult to balance this tension in areas that require a strong regulation, such as intelligent transport systems. On the other hand, the more transparent the system is, the easier it is to make it decentralized. One would expect that a fair and transparent system would have no problem transitioning to a fully decentralized setup.

In order to fully understand the governance of a decentralized system, we need to look at different layers [67]. In this work, the authors define three layers, represented in Figure 7.

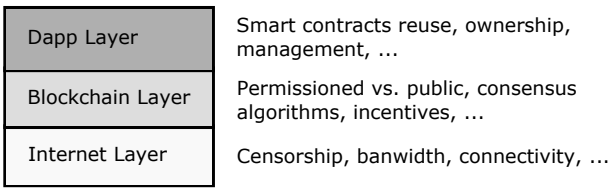

Fig. 6. Governance layers

First, there is the Internet protocols layer that govern how devices can talk to each other. If some country decides to block some kind of traffic it will break decentralization. Second is the blockchain network layer: Ethereum governance is not the same as Bitcoin; using Proof-of-Work (PoW) consensus is not the same as using Proof-of-Authority (PoA) or Proof-of-Stake (PoS); governance is also different between public blockchain and permissioned blockchains. The last layer is the decentralized application layer (Dapp) that could be implemented directly to the blockchain or use some existing Dapp

[3]https://foam.space
[4]https://xyo.network

framework, i.e., a set of supporting smart contracts. In this layer there are different aspects that affect governance, but in particular there is still the issue of who creates those smart contracts and, more importantly, who can manage them in case they need to be fixed and updated. If only a designated set of entities can do it, the network will be effectively under their control, losing their decentralized essence.

A balanced approach for D-VPKI would be to use some form of permissioned blockchain, an approach that has been successfully applied to other critical environments, such as Smart Grids [68].

F. Blockchain access

Another limitation of blockchain-based PKIs is the need to have a fully synchronized node. Depending on the size of the blockchain, validation might require a significant amount of time in case the node lost sync. In [69] the authors propose a modification to the Bitcoin protocol that allows for the creation of proofs of proof-of-work with sublinear complexity in the length of the chain. These proofs can help verify the last k blocks of the blockchain without having to examine the whole blockchain. This approach has some limitations in presence of adversaries and with variable block difficulty. FlyClient [70] tries to overcome those limitations using an optimal probabilistic block sampling protocol and Merkle Mountain Range (MMR) commitments that highly reduce the storage requirements. Another work in the same direction is BlockQuick [71] that claim to require less data for validation than existing approaches.

There are also Internet of Things (IoT) oriented Blockchains that try to reduce complexity of verification and increase its performance. In particular, IOTA [72] is a blockchain specifically targeted to the IoT with a focus on scalability and performance. This system was developed with the aim of creating trust between IoT devices without the need for a monetary incentive [73].

In Figure 7 we can see the different modalities to integrate vehicles with blockchains.

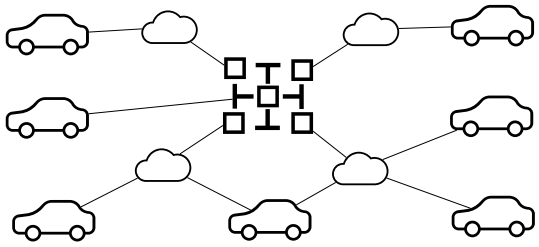

Fig. 7. Integrating the vehicle into the Blockchain

- Vehicle as a node. In this situation the vehicle itself is a node in the Blockchain. This requires the vehicle to be in sync with other nodes at all times. Loss of connectivity can derive in a loss of sync and depending on its duration, this could make some services unavailable. Also, syncing the node may have a significant impact on storage and communication, depending on the type of blockchain used. According to [70], even using a simplified validation, an Ethereum [74] node needs to download and store about 4 GB of data.
- Virtual Vehicle Node. In this situation each vehicle is paired with a Virtual Vehicle Node (VVN), that is a node of a blockchain. Storage and communication requirements due to the syncing process no longer affect the vehicle. VVN will stay in sync even if the vehicle loss connectivity, but some applications might become unavailable until connection is reestablished. We can have three sub-cases:
  - 1-1: In this case there is a 1 to 1 mapping between VVN and vehicles. This situation would be very in line with the Digital Twin concept [75].
  - 1-N: In this case a VVN can handle more than one vehicle. Vehicles could be organized in fleets, so that a single VVN serves a whole fleet. VVN could also be open to any vehicle, very in line with Blockchain Edge Computing architectures [76].
  - N-M: That would be the most general case, where any vehicle can be paired with any number of VVNs in order to make the system more resilient.

If we consider how ITS infrastructures are currently planned, the best fit would be to deploy VVNs in the Edge, either in 5G antennas or roadside units, and allow any vehicle in their proximity to join them. This would help ensuring that vehicles connected to the same VVN have the same view of the blockchain, simplifying DID resolution and many other processes.

V. Proof-of-Concept Technical Architecture for Decentralized V2X (D-V2X)

Blockchain integration in V2X requires the inclusion of new functionality in the vehicle. In Figure 8 we can see five conceptual modules that would need to be included in a D-V2X device.

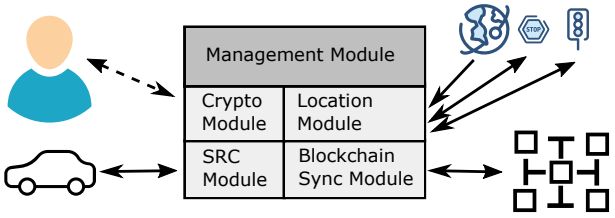

Fig. 8. Conceptual architecture for D-V2X

The *Blockchain Sync Module* will be in charge of connecting the vehicle to the blockchain or any other decentralized network, e.g., Sidetree, required for the operation of ITS services. The module could act as a full node, something that will require more processing and storage capabilities in the device, or just connect to a online service that gives access to the blockchain, e.g., Infura. The main role for this module would be to maintain a list of valid DIDs from neighbor devices and associated public keys that can be used to verify the authenticity of received messages.

The *Short-Range Communication (SRC) Module* will work as a traditional DSRC module. Instead of working on a commercial ITS stack, we have opted for a more open environment, implementing our own simplified ITS stack over Bluetooth Low Energy so that anyone could experiment with it. This will allow the inclusion of smartphones in the D-V2X ecosystem, democratizing ITS services.

The *Cryptographic Module* will be in charge of protecting all DID associated keys, acting as a car wallet. All cryptographic operations that involve some private key will occur inside this module. Other operations, such as signature verification, could be performed in other modules, e.g., SRC Module. This module could also be used for crypto payments, e.g., electronic tolls.

The *Location Module* will be in charge of calculating the GPS position of the vehicle and receive privacy enhanced VC including Proof of Location from nearby infrastructure elements, e.g., traffic lights and signs. For that, the module might need to engage in a security protocol with the road elements.

Lastly, the *Management Module* will be in charge of implementing ITS services on top of the above-mentioned modules. For example, in a traffic light, the logic to keep track of state changes would be run in this module. Also remote management to adjust their cycles and adapt to traffic conditions or to give way to emergency vehicles when they are near could be performed by this module.

As mentioned before, any modern smartphone would fit this conceptual design. The 5G network will surely allow more and more use cases to be implemented over cellular networks instead of direct communications and we foresee the smartphone might end up being the center of Decentralized V2X. However, the current smartphone ecosystem faces some difficulties, as there is no standardized trusted execution across platforms and the Bluetooth Low Energy (BLE) API does not always expose all functionality.

We have evaluated different hardware platforms that could fit this conceptual architecture. After our test, we have concluded that the nRF52840 System on Chip (SoC) from Nordic Semiconductor[5] is a perfect candidate for a Proof-of-Concept, taking into account both technical and economic aspects. This particular SoC is relatively cheap and is widely used, e.g., most modern Arduino BLE boards include it. Also, it includes an ARM TrustZone® CryptoCell cryptographic unit that allows the execution of cryptographic operations with high efficiency; independently of the CPU and at the same time protecting the cryptographic keys from the rest of the code, acting like a Hardware Security Module (HSM). Another important aspect is that it implements both the extended advertisement extension and the long-range extension of BLE 5.0, that allows much longer payloads for broadcast messages than traditional BLE.

Another positive aspect of the nRF52840 is that the Software Development Kit (SDK) provided by Nordic Semiconductor, simplifies the use of the cryptographic standards supported by ARM CryptoCell 310 subsystem, including Elliptic Curve Cryptography (ECC). Many elliptic curves are supported by this module, such as NIST FIPS 186-4 (NIST P-192, NIST P-256...), SEC 2 curves (secp192r1, secp256r1, secp521r1...), Koblitz curves (secp256k1, secp192k1...) and Edwards/Montgomery curves (d25519 and Curve25519) [77]. This would allow us to create blockchain transactions securely and without a noticeable overhead. In fact, the nRF52840 has been already chosen by some manufactures to implement crypto wallets[6].

We have implemented a prototype, which is still under heavy development, for a Secure Smart Traffic Light[7] using the nRF52840 as the core component. This particular prototype is not making use of blockchain yet because it is only a broadcasting device. However, this prototype has been used to validate a minimal overhead for the generation and verification of digital signatures in the CC310. We have defined in this prototype a security layer for V2X messages over extended advertisement BLE messages. The device broadcasts a single advertisement which includes the message payload digitally signed in order to provide authenticity. In our prototype, the payload contains the traffic light unique identifier (1 byte length), the GPS location coordinates (8 bytes), the inbound direction (4 bytes), the outbound direction (4 bytes), the current phase (1 byte), and time remaining (1 byte). Privacy issues are not addressed either at this stage of the prototype, given that the payload contains no sensitive information.

Regarding Internet connectivity, we have already tested two LPWAN technologies: LTE Cat-M1 (shortened as LTE-M) and NB-IoT. Both standards were developed by the 3GPP, and their specifications were frozen in the 3GPP Release 13. In general terms, LTE-M is optimized for higher bandwidth and mobile connections: uplink and downlink speed is much higher than NB-IoT, and it has support for roaming devices and for voice communication. On the other hand, NB-IoT technology allows more connections per cell, a better indoor and underground penetration, and a lower cost of hardware modules. We have developed a library to evaluate the NB-IoT network[8].

The main advantage of LTE-M over NB-IoT is its lower latency—50 to 100ms of latency instead of the 1.5 to 10 seconds of NB-IoT technology—, which makes it the best solution for vehicular networks. Also, the possibility of making voice calls would allow the direct implementation of emergency calls using this device. The nRF52840 SoC is also included in the Nordic Thingy:91[9], an easy-to-use battery-operated prototyping platform including a cellular IoT modem for LTE-M and NB-IoT networks (nRF9160 SiP) and a GPS receiver. That is the target platform for the next stage of the prototype as it would allow us to test the whole D-V2X functionality in a single device, using an unify SDK.

[5]https://bit.ly/2WkgQhe

[6]https://bit.ly/307TfBl

[7]https://github.com/nicslabdev/MOTAM-nRF52_Beacons

[8]https://github.com/nicslabdev/BG96-NB-IoT-Arduino-Library/

[9]https://bit.ly/2Op6gRH

VI. Conclusions and future work

The technology for D-V2X is ready to be applied and there are already hardware platforms capable of running it. D-V2X might not substitute industry standards in the short term, but, as part of a community effort, some complementary services can be implemented over D-V2X. In particular, platforms such as Waze could be implemented in a fully decentralized way, redistributing profit to the community, instead of centralizing it. Technologies such as DID and VC can enable a fully decentralized identity infrastructure for ITS applications.

In order to have a fully decentralized environment, anyone should be able to access this technology. We need to remove technological barriers and this is why we have also shown that some ITS use cases can be implemented using BLE, a widely deployed technology already present in all current smartphones and vehicles. The main challenge we are facing right now is how to optimize the connection with blockchains for both vehicles and road users.

As future work, we plan to extend our traffic light prototype to a vehicle prototype that makes uses of privacy enhanced VC. We also intend to implement a second prototype as an Android application, showing interoperability between both prototypes.

References

[1] S. E. Shladover, "Connected and automated vehicle systems: Introduction and overview," *Journal of Intelligent Transportation Systems*, vol. 22, no. 3, pp. 190–200, 2018.

[2] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A Survey," *Computer Networks*, vol. 169, no. 107093, pp. 1–20, 2020.

[3] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, Dec. 2012.

[4] Y. Yuan and F. Wang, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, 2016, pp. 2663–2668.

[5] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, ser. UbiComp '16. New York, NY, USA: Association for Computing Machinery, 2016, pp. 137–140.

[6] M. Chanson, A. Bogner, F. Wortmann, and E. Fleisch, "Blockchain as a privacy enabler: An odometer fraud prevention system," in *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*, ser. UbiComp '17. New York, NY, USA: Association for Computing Machinery, 2017, pp. 13—-16.

[7] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17 578–17 598, 2019.

[8] L. R. Abbade, F. M. Ribeiro, M. H. d. Silva, A. F. P. Morais, E. S. d. Morais, E. M. Lopes, A. M. Alberti, and J. J. P. C. Rodrigues, "Blockchain applied to vehicular odometers," *IEEE Network*, vol. 34, no. 1, pp. 62–68, 2020.

[9] M. Demir, O. Turetken, and A. Ferworn, "Blockchain based transparent vehicle insurance management," in *2019 Sixth International Conference on Software Defined Systems (SDS)*, 2019, pp. 213–220.

[10] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019.

[11] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 2020.

[12] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4312–4324, 2020.

[13] Z. Xu, X. Li, X. Zhao, M. Zhang, and Z. Wang, "Dsrc versus 4g-lte for connected vehicle applications: A study on field experiments of vehicular communication performance," *Journal of advanced transportation*, vol. 435, Aug. 2017.

[14] Bluetooth SIG, Inc., "Bluetooth market update 2019," 2019, https://www.bluetooth.com/bluetooth-resources/2019-bluetooth-market-update/.

[15] R. Faragher and R. Harle, "Location fingerprinting with bluetooth low energy beacons," *IEEE journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2418–2428, 2015.

[16] J. Fürst, K. Chen, H.-S. Kim, and P. Bonnet, "Evaluating bluetooth low energy for IoT," in *2018 IEEE Workshop on Benchmarking Cyber-Physical Networks and Systems (CPSBench)*. IEEE, 2018, pp. 1–6.

[17] R. Rondón, M. Gidlund, and K. Landernäs, "Evaluating bluetooth low energy suitability for time-critical industrial IoT applications," *International Journal of Wireless Information Networks*, vol. 24, no. 3, pp. 278–290, 2017.

[18] K. Thomas, H. Fouchal, S. Cormier, and F. Rousseaux, "Intelligent transport system based on bluetooth," in *International Workshop on Communication Technologies for Vehicles*. Springer, 2019, pp. 50–59.

[19] "IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pp. 1–240, 2016.

[20] "IEEE Standard Specifications for Public-Key Cryptography," *IEEE Std 1363-2000*, pp. 1–228, 2000.

[21] "IEEE Standard Specifications for Public-Key Cryptography—Amendment 1: Additional Techniques," *IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000)*, pp. 1–167, 2004.

[22] B. Lonc and P. Cincilla, "Cooperative ITS security framework: Standards and implementations progress in Europe," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2016, pp. 1–6.

[23] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Transactions on Intelligent Vehicles*, pp. 1–1, 2020.

[24] "IEEE Standard for Information Technology—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802.11p-2010*, pp. 1–51, 2010.

[25] T. Weil, "VPKI hits the highway: Secure communication for the connected vehicle program," *IT Professional*, vol. 19, no. 1, pp. 59–63, 2017.

[26] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84—-90, Feb. 1981.

[27] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for V2X communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[28] M. Khodaei, H. Jin, and P. Papadimitratos, "Secmace: Scalable and robust identity and credential management infrastructure in vehicular communication systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 5, pp. 1430–1444, 2018.

[29] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[30] W. Whyte, "IEEE 1609.2 and connected vehicle security: Standards making in a pocket universe," Dec. 2016.

[31] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang, "High-speed high-security signatures," *Journal of cryptographic engineering*, vol. 2, no. 2, pp. 77–89, 2012.

[32] "On-Board System Requirements for V2V Safety Communications," *SAE J2945/1 Standard*, 2020.

[33] "302 637-2 V1.4.1-Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," *ETSI*, 2019.

[34] "302 637-3 V1.3.1-Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," *ETSI*, 2019.

[35] N. M. Rabadi, "Implicit certificates support in IEEE 1609 security services for wireless access in vehicular environment (WAVE)," in *The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010)*, 2010, pp. 531–537.

[36] Certicom, "Explaining implicit certificates," *Code and Cipher*, vol. 2, no. 2, pp. 5–6, 2005.

[37] M. Khodaei and P. Papadimitratos, "Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in VANETs," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec 18)*. New York, NY, USA: Association for Computing Machinery, 2018, pp. 172—183.

[38] M. E. Nowatkowski, J. E. Wolfgang, C. McManus, and H. L. Owen, "The effects of limited lifetime pseudonyms on certificate revocation list size in VANETs," in *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*. IEEE, 2010, pp. 380–383.

[39] S. Y. Conner Fromknecht, Dragos Velicanu, "A decentralized public key infrastructure with identity retention," Cryptology ePrint Archive, Report 2014/803, 2014, https://eprint.iacr.org/2014/803.

[40] C. Allen, A. Brock, V. Buterin, J. Callas, D. Dorje, C. Lundkvist, P. Kravchenko, J. Nelson, D. Reed, M. Sabadello *et al.*, "Decentralized public key infrastructure," in *Rebooting the Web of Trust I: San Francisco*, 2015.

[41] C. Patsonakis, K. Samari, M. Roussopoulos, and A. Kiayias, "Towards a smart contract-based, decentralized, public-key infrastructure," in *International Conference on Cryptology and Network Security*. Springer, 2017, pp. 299–321.

[42] Decentralized Identity Foundation, "Sidetree protocol," https://identity.foundation/sidetree/spec/.

[43] J. Benet, "IPFS—Content Addressed, Versioned, P2P File System," *arXiv preprint arXiv:1407.3561*, 2014.

[44] N. Tolia, M. Kozuch, M. Satyanarayanan, B. Karp, T. C. Bressoud, and A. Perrig, "Opportunistic use of content addressable storage for distributed file systems." in *USENIX Annual Technical Conference, General Track*, vol. 3, 2003, pp. 127–140.

[45] World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0—Core architecture, data model, and representations," https://www.w3.org/TR/did-core/.

[46] ——, "Verifiable Credentials Data Model 1.0—Expressing verifiable information on the web," https://www.w3.org/TR/vc-data-model/.

[47] "Road vehicles—Vehicle Identification Number (VIN)—Content and structure," International Organization for Standardization, Geneva, CH, Standard ISO/TC 22 3779:2009(en), Oct. 2009.

[48] VID Working Group, "Vehicle Identity Standard," Mobility Open Blockchain Initiative, Standard, 2019.

[49] L. Axon. and M. Goldsmith., "PB-PKI: A Privacy-aware Blockchain-based PKI," in *14th International Joint Conference on e-Business and Telecommunications (ICETE 2017), SECRYPT*, 2017, pp. 311–318.

[50] L. Axon, M. Goldsmith, and S. Creese, "Chapter eight—privacy requirements in cybersecurity applications of blockchain," in *Blockchain Technology: Platforms, Tools and Use Cases*, ser. Advances in Computers. Elsevier, 2018, vol. 111, pp. 229 – 278.

[51] A. C. Yao, "Protocols for secure computations," in *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)*. IEEE, 1982, pp. 160–164.

[52] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4221–4232, 2020.

[53] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, and B. Eissfeller, "Emerging attacks on VANET security based on GPS Time Spoofing," in *2015 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2015, pp. 344–352.

[54] Y. Zhang, C. C. Tan, F. Xu, H. Han, and Q. Li, "Vproof: Lightweight privacy-preserving vehicle location proofs," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 1, pp. 378–385, 2014.

[55] T. Tithi, B. Deka, R. M. Gerdes, C. Winstead, M. Li, and K. Heaslip, "Analysis of friendly jamming for secure location verification of vehicles for intelligent highways," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7437–7449, 2018.

[56] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, "Blockchain-based proof of location," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2018, pp. 146–153.

[57] M. R. Nosouhi, S. Yu, W. Zhou, M. Grobler, and H. Keshtiar, "Blockchain for secure location verification," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 40–51, 2020.

[58] Z. Wang, J. Lin, Q. Cai, Q. Wang, J. Jing, and D. Zha, "Blockchain-based certificate transparency and revocation transparency," in *Financial Cryptography and Data Security*, 2019, pp. 144–162.

[59] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, 2018, pp. 674–679.

[60] J. A. Onieva, R. Rios, R. Roman, and J. Lopez, "Edge-assisted vehicular networks security," *IEEE Internet of Things Journal*, vol. 6, pp. 8038–8045, Oct. 2019.

[61] M. D. Ryan, "Enhanced certificate transparency and end-to-end encrypted mail," in *NDSS*, 2014, pp. 1–14.

[62] A. Singh, B. Sengupta, and S. Ruj, "Certificate transparency with enhancements and short proofs," in *Information Security and Privacy*. Cham: Springer International Publishing, 2017, pp. 381–389.

[63] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," *Computer Communications*, vol. 33, no. 9, 2010.

[64] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Security and Communication Networks*, no. 7817614, 2018.

[65] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–5.

[66] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[67] P. De Filippi and G. McMullen, "Governance of blockchain systems: Governance of and by distributed infrastructure," in *Blockchain Research Institute and COALA*, 2018.

[68] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992–8004, 2019.

[69] A. Kiayias, N. Lamprou, and A.-P. Stouka, "Proofs of proofs of work with sublinear complexity," in *Financial Cryptography and Data Security*, 2016, pp. 61–78.

[70] B. Bünz, L. Kiffer, L. Luu, and M. Zamani, "FlyClient: Super-light clients for cryptocurrencies," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, May 2020, pp. 1059–1077.

[71] L. Exosite, "Blockquick: Super-light client protocol for blockchain validation on constrained devices," 2019.

[72] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "Iota feasibility and perspectives for enabling vehicular applications," in *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2018, pp. 1–7.

[73] S. Popov, "Iota: Feeless and free," *IEEE Blockchain Technical Briefs*, 2019.

[74] V. Buterin, "Ethereum whitepaper," 2013, https://ethereum.org/en/whitepaper/.

[75] S. Boschert and R. Rosen, *Digital Twin—The Simulation Aspect*. Cham: Springer International Publishing, 2016, pp. 59–74.

[76] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[77] N. Semi, "Arm trustzone cryptocell 310 on nrf52840 module documentation." https://infocenter.nordicsemi.com/topic/ps_nrf52840/cryptocell.html?cp=4_0_0_5_5.