Towards a Blockchain-based Identity and Trust Management Framework for the IoV Ecosystem

Anastasia Theodouli, Konstantinos Moschou
Konstantinos Votis, Dimitrios Tzovaras
CERTH / ITI
Thessaloniki, Greece
anastath, konsmosc, kvotis, tzovaras@iti.gr

Jan Lauinger, Sebastian Steinhorst
Embedded Systems and Internet of Things
Technical University of Munich, TUM
Munich, Germany
jan.lauinger, sebastian.steinhorst@tum.de

***Abstract*—The past decade has seen a huge growth not only in the Internet of Things (IoT) but also in the Internet of Vehicles (IoV) from both academia and industry. Autonomous Vehicles (AVs) combine a variety of sensors, IoT devices, control units, gateways, etc. Therefore, the software of the different sensors and IoT devices needs to be updated to the latest version by the Software Vendors. This paper proposes a blockchain-based identity and trust management framework for the IoV ecosystem, that aims to provide secure software updates. The proposed framework consists of two processes: the identification and registration of the entities of the ecosystem, and the authentication of the entities which relies on established W3C standards for defining verifiable credential presentation, verification, and revocation. We illustrate the feasibility of our approach in a case study.**

***Keywords*-blockchain; Self-Sovereign Identity(SSI); Decentralized Identifiers(DIDs); Verifiable Credentials(VC); software update; Autonomous Vehicles; identity management; Internet of Things(IoT); Internet of Vehicles(IoV)**

I. Introduction & Motivation

The IoV ecosystem allows the establishment of a communication channel among vehicles so that they can exchange information. This information exchange has numerous benefits such as increasing road safety, and better traffic control. However, in the IoV ecosystems, there are several vulnerabilities that can be exploited which can have detrimental effects, such as provoking accidents. As such, it is necessary to ensure the authenticity of the data exchanged in the established communication channel. To this end, we present our first contribution, which is an Identity and Trust Management Framework that allows the identification and authentication of the stakeholders of the IoV ecosystem and secures their communication. The framework leverages the Blockchain technology to save the Identifiers of the stakeholders in a decentralised way which eliminates the single point of failure while increasing availability and at the same time it overcomes the necessity of having a trusted third party, centralised Certificate Authority (CA) for managing the identifiers. The centralised approach is more prone to the single point of failure as it allows for easier data breaches in case that the server hosting the certificates is compromised. It's worth noting that the proposed framework follows the proposed World Wide Web Consortium (W3C) standards for Decentralised Identifiers (DIDs) [1]. Furthermore, it uses Verifiable Credentials (VCs) so as to build Trust among the stakeholders of the IoV ecosystem. Credentials are sets of claims (or statements), made by one entity, i.e. the Issuer, (normally) for another entity, i.e. the Holder (or Prover). VCs wrap the claims mentioned above with a set of metadata and digital proofs (digital signature is the most usual type of digital proof) which cryptographically prove who is the Issuer of the Credentials [2],[3]. Vehicles are equipped with sensors, control units, and IoT devices; the maintenance of these devices must be done by authorised services over a secure communication channel. To this end, we present our second contribution which is the application of the Identity and Trust Management Framework mentioned above to an important use case in the IoT domain, i.e. the software update of the IoT devices embedded in the vehicle, in a secure and private way.

The remainder of this paper is structured as follows. In Section II, we present background on blockchain technology and similar works. Section III contrasts our choice of a Distributed Ledger Technology (DLT) framework for Identity Management (IdM) with respect to other DLT frameworks and IoV specific Public Key Infrastructure (PKI)s. In Section IV, we present our proposed Framework, by outlining, (i) the blockchain platform that will be used after assessing its suitability for our IoV ecosystem necessities and comparing it with other candidate blockchain platforms, (ii) its stakeholders and their roles, and (iii) its processes. Finally, in Section V, we conclude the paper and define the next steps for this work.

II. Background & Related Work

A. Blockchain Technology

In blockchain technology, cryptography and, essentially, hash functions bind data blocks together and enable data integrity checks. Consensus protocols, timely consecutive cryptography, and a decentralized network design extend

978-1-7281-6728-2/20/$31.00

the data linking concept to establish the attractive guarantees. Ledger data immutability (tamper resistance), integrity, traceability, transparency, and availability count to the guarantees that enable secure and reliable bookkeeping of data.

One of the branches that originated from blockchain research is the consortium-based DLT [4]. Compared to public blockchains, the most distinctive characteristic of consortium-based DLT is that only authorized nodes participate in the network [5]. This restriction enables the network to utilize voting based consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) which increase the scalability of the network. As a result, consortium blockchains achieve faster transaction finality and low-delay verification times of transactions.

IdM in the IoV is a potential concept that profits of DLT [6]. Moreover, DLT for this purpose should follow a consortium-based DLT approach. The reason for this is that consortium controlled DLT concepts enable the implementation of voting concepts that may eliminate central authority roles. Additionally, the IoV comes with infrastructure participants such as vehicle insurance and compliance companies. These authorities can only provide trusted services in form of trusted technical inspections, license registrations and vehicle admission, if they are part of the consortium. This means that the ledger between the authorities depends on input from multiple authorized sources. External input in form of transactions from authorized participants should pass a fair consortium decision to lower trust boundaries between consortium partners [7]. Afterwards, the tamper-proof bookkeeping property of DLT excludes the third party that manages bookkeeping between stakeholders.

External input verification among closed environment DLT frameworks is state-of-the-art research and requires explicit examination during application design [8]. Further, the focus on privacy preserving techniques [9], scalability solutions, and blockchain types (public, private and consortium blockchain networks) [10] drive distributed ledger framework development to tailored design choices. Different DLT architectures address the aforementioned problems differently and introduce different pros and cons. Hence, the right selection of a DLT framework is important with the goal to design IdM. In our case, IoV-specific requirements as well as the Self-Sovereign Identity (SSI) [6] IdM approach dominate our framework selection in section III.

B. Related Work

In this section, we mention existing work which focuses on (i) addressing security in software/firmware updates on Internet of Things (IoT) and related environments, and (ii) IdM using the Blockchain technology.

In [11], the authors present works related with the over-the-air (OTA) software updates in the IoV ecosystem focusing on the security challenges; blockchain based techniques are also presented among others. In [12], the authors introduce a consortium blockchain-based solution among the Autonomous Vehicles (AVs) manufacturers using smart contracts to ensure authenticity and integrity firmware updates tailored for AVs. In [13], Gelenbe at al. present an approach to secure the network communications in smart mobile ecosystem using virtualised honeypots. Using this approach, installation of mobile malware which could occur during software updates of devices is mitigated. In [14], Lee and Lee et al. propose a blockchain-based solution to ensure the integrity of firmware updates on embedded IoT devices instead of depending on a centralized vendor network. For the distribution of updates, a peer-to-peer file sharing network such as BitTorrent is proposed to ensure integrity and versions tractability of updates. In [15], Yohan and Lo et al. propose a blockchain-based framework that aims to provide secure verification on the firmware released by the device manufacturer.

In Ockam network [16], a decentralized blockchain IdM platform that enables interoperability, security, privacy, trust and reliability among IoT devices is developed. It is implemented with open standards developed by the W3C and the Decentralized Identity Foundation (DIF) for DIDs and VCs to ensure interoperability of identities.

As regards the works mentioned above, we differ in that (i) we focus on the IoV ecosystem, (ii) we require/combine identity management as a necessity for our secure software update use case, (iii) we also address the issue of revocation of the credentials which is important in advanced identity management solutions, and (iv) we map the stakeholders of our framework to the standardization registration paradigms of the European Union (EU).

III. Blockchain Platform Evaluation

As stated in section II-A, the IoV scenario requires a privacy-aware and consortium-based DLT solution with scalability and real-time capabilities to handle location and velocity dynamics that occur in the IoV. The framework investigation and comparison indicates *Indy* as a promising solution to solve the secure communication scenarios in respect of IoV characteristics. We evaluate *Indy* based on the following criteria.

- Coverage of necessary identity management concepts and performance
- Existence of privacy preserving techniques
- Framework architecture comparison

The Hyperledger *Indy* framework follows a client and processor transaction design. The *Indy* client System Development Kit (SDK) represents the transaction client that creates, bundles, signs, and submits predefined transaction requests that the processor validates. *Indy* ledger transactions cover all important ledger interactions around Decentralized Identifier (DID) management. DID creation and querying,

key rotation, credential schema creation, credential definition creation, etc belong to the *Indy* transaction repertoire [17].

Additionally, the *Indy* SDK supports local credential management with the help of wallets. Wallets have the ability to cache and store VCs and cryptographic key pairs. Regarding the consensus algorithm, *Indy* relies on PBFT which allows high transaction throughput [4]. Performance results of [18] prove that *Indy* meets global scale criteria with regard to ledger query speed. Querying the ledger for VCs information happens at least twice during mutual authentication of the initial secure communication scenario.

Regarding privacy, the *Indy* IdM framework stores explicitly public information on chain. VCs with private information can be kept entirely local which respects privacy requirements during VCs lifetime. In general, VCs features enable to bind multiple private credentials to public credential definitions and credential schemata. The Credential Schemata of public authorities in this case sign Credential Definitions which in turn sign VCs which creates cryptographically sealed trust connections. With that, it is possible to implement trusted IdM procedures such as registration, authentication, authorization, and revocation between clients that do not store their DIDs in a publicly accessible ledger.

Compared recent PKI architecture design such as the US Security Credential Management System (SCMS) [19] and European Cooperative Intelligent Transport Systems (C-ITS) [20] approach, the DLT *Indy* IdM framework does not require the construct of Enrollment Authorities (EAs) and Pseudonym Certificate Authorities (PCAs)/Authorization Authorities (AAs) to create pseudonym key pairs using processes such as butterfly key expansion. VCs with the properties that enable to create Credential Presentations (CPs) and verification through Zero Knowledge Proofs (ZKPs) support privacy requirements out of the box.

When comparing Sovrin's *Indy* IdM to other DLT IdM frameworks such as Jolocom, uPort, ShoCard, Blockstack and Namecoin, the work of [21] highlights the following distinctions between all solutions. All DLT IdM solutions build on public blockchains except Sovrin's *Indy*, ShoCard and Blockstack who are not bound to the underlying blockchain. ShoCard, Blockstack and Namecoin do not offer out of the box support for DIDs. Even though Blockstack meets the critera to manage self-sovereign DIDs, the description of the implementation is missing. The uPort and Namecoin identity scheme publish identity attributes which affects privacy guarantees. Among similarities in usage, verification, and purpose, *Indy* differentiates in respect of development status and incentives. There is no requirement for incentives when it comes to permissioned DLT. Moreover, the *Von Network* [22] which implements *Indy* pool nodes as well as the Hyperledger *Aries* client [23] which adopts DIDs and *Indy* IdM schema compatibility indicate further adoption of Sovrin's IdM design.

IV. Proposed Identity & Trust Management Framework

In this section, we present the identified stakeholders of the system and their role. Identified identities are then mapped to authority roles of *Indy*. This approach represents the prerequisite to determine the logical process of the IdM use case for secure communication.

As regards the registration of the vehicles to the system, we have followed the paradigm provided by the European Union [24] in order to identify the stakeholders involved. The list of the identified stakeholders appears in Table I below. The Table I marks the stakeholders, that are involved in the use case that we describe in Figure 1 below, with bold. Although we followed the European Union paradigm mentioned above to identify the stakeholders of our system in a concrete and realistic way, in the rest of this Section, we will elaborate only on the role of the stakeholders who participate in the Use Case presented in the Figure 1 below.

Table I
Framework Stakeholders

Stakeholder	**Hyperledger Indy Role**	**Ecosystem Role**
-	Trustee	Steward creator
-	Steward	Trust Anchors Creator
Government	Trust Anchor	Issuer of Credential Schemas
Vehicle manufacturer	Trust Anchor	Issuer of Credential Definition
Pre-market device software vendor	Trust Anchor	Issuer of Credential Definition
Pre-market device software vendor API	User	Prover/Verifier
Post-market device software vendor	Trust Anchor	Issuer of Credential Definition
Post-market device software vendor API	User	Prover/Verifier
Vehicle Owner or Transportation Authority (Vehicle Operator)	Trust Anchor	Issuer of Credential Definition
Vehicle Registration Certificate Authority	Trust Anchor	Issuer of Credential Definition
Insurance Company	Trust Anchor	Issuer of Credential Definition
VAT payee / tax office	Trust Anchor	Issuer of Credential Definition
Roadworthiness Provider Authority	Trust Anchor	Issuer of Credential Definition
Vehicle	User	Prover/Verifier

A. Role of the Trustee and the Steward

In Hyperledger Indy, Trustees and Stewards are specific roles given to users who play an important role in building the trust in the network [1]. However, in the paradigm that we

[1]https://medium.com/@kctheservant/exploring-hyperledger-indy-through-indy-dev-example-10075d2547/

follow [2] Trustees and Stewards are created programmatically within a set of pre-defined transactions, the so-called domain genesis transactions; the bootstrapping of the system by assigning/binding the roles of Trustees and Stewards to real users who can truly build trust to the system due to their inherent properties, is a matter of future work. Trustees create users assigned the Role of Stewards and Stewards create users assigned the role of Trust Anchors [3]; the latter, are entitled to write transactions to the Ledger, e.g. for publishing to the Ledger Decentralised Identifiers and for creating and publishing to the Ledger Credential Schemas and Credential Definitions. Note that each Steward is also a Trust Anchor.

In the following, we assume that a Trustee has created a user in the system assigned the role of Steward who is responsible for onboarding to the System, by assigning the Role of Trust Anchor to the Government, the Pre-market device software vendors, and the post-market device software vendors. To do this, first, a secure communication is established between the Steward and each of the aforementioned stakeholders. This involves the creation of unique pairwise DIDs, one for the Steward and one for the each Stakeholder, respectively. Along with the DIDs an associated verification key and signing key are also created. These pairwise DIDs are private data stored locally within software applications which are controlled by the Steward and the Stakeholders, the so-called 'wallets'.

For the establishment of the secure communication, a mutual authentication process is done during which both parties should prove to each other that they hold the signing keys corresponding to the pairwise DIDs. After the successful completion of the mutual authentication, the messages exchanged are encrypted with the verification keys of the two parties to ensure the confidentiality of the exchanged messages. Then, the Government issues a DID and sends it to the Steward along with its verification key, the Steward publishes the DID and the verification key to the ledger and assigns to the Government the role of Trust Anchor. All data published to the Ledger are available to all users of the network who have at least read access; also, they are considered to be trusted by all the users of the network. The same procedure will occur for the pre-market and post-market device software vendors. In the rest of this paper, we will refer to the process of (i) the secure connection establishment between a Trust Anchor and a new user, (ii) the subsequent write of the DID and verification key to the ledger by the Trust Anchor, and (iii) the assignment of a role to the new User as *Registration* of the user to the system. Furthermore, the process of creating unique DIDs (along with the corresponding verification and signing keys) is considered to be the process of *Identification* [4]. A list of the processes of the system is displayed in Table II below.

Table II
FRAMEWORK PROCESSES

Process ID (PID)	Process Name
1	Identification and Registration
2	Authentication (VC Presentation, VC Verification, VC Revocation)

B. Role of the Government

The Government should be first registered in the System by a Steward (or Trust Anchor) having the role of Trust Anchor. Then, it issues and publishes to the Ledger Credential Schemas which can be used as 'standards' for the Issuance of Credentials by the pre-market and post-market device software vendors.

Per default, *Indy* initializes administration authorities such as the Steward role which remain central if a single steward is deployed. It is possible to circumvent such design choices. One way is to run multiple steward roles. Another way to eliminate central authority roles is to leverage *Indy* Plugins. *Indy* Plugins let developers create customized transactions and transaction validation rules. One way to eliminate transaction acceptance of single authorities could look like this. Custom validation smart contracts could be triggered upon ledger interactions to collect votes of consortium members to prevent central authority power. Ledger members that need to vote on new Credential Schema transactions benefit of the human readable JSON-LD data structure of VCs. Such dynamic validations which let consortium members actively interact during transaction processing provides consortium based verification of transaction data and, thereby, consortium-only control.

C. Role of Pre-market and Post-market device software vendor

Pre-market and post-market device software vendors are the designers and manufacturers of devices such as video camera, lidar, radar, odometers, Global Positioning System (GPS), inertial measurement unit (IMUs), and embedded electronics like Electronic Control Units (ECUs) that are embedded to the vehicle before or after its transfer to an Owner or Operator, respectively. They are both responsible for the regular updates of the software that is installed within the devices.

The Pre-market and Post-market device software vendors issue Credential Definitions for the Pre-market and Post-market device software vendor APIs, respectively. These

[2]https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md

[3]Note that the 'Trust Anchor' role has been renamed to 'Endorser'.

[4]We consider this process as Identification of the user, since it encompasses the creation of the unique identifiers of the user. Note though, that in the generic case, one user can have multiple DIDs to avoid identity correlation.

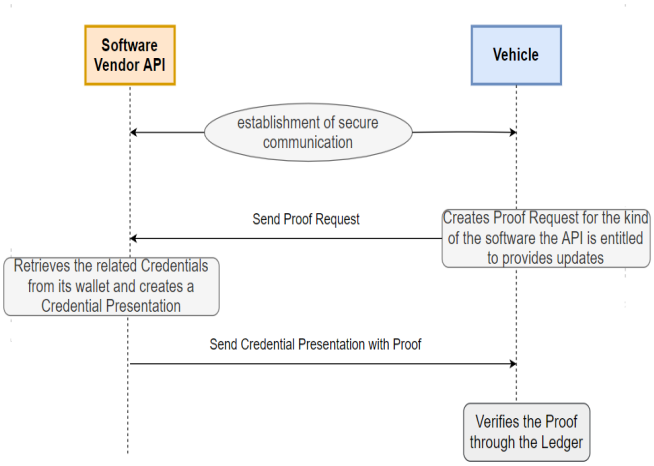

Figure 1. Authentication of the Software Vendor API by the Vehicle

Credentials Definitions are based on the Credential Schemas that were published to the Ledger by the Government.

D. Role of Pre-market and Post-market device software vendor API

The Pre-market device software vendor APIs are APIs located at the Cloud that contain services and endpoints for the provision of the device software updates. The steps of the process for the authentication of the API by the Vehicle are the following:

1) The API first establishes a secure communication with the Vehicle.
2) The Vehicle sends a Proof Request for the Credentials regarding the kind of software the API is entitled to provide updates for.
3) The API retrieves the related Credentials from its wallet, and creates a Credential Presentation including a Proof that the Credentials were issued to them by the device software vendor and sends the Presentation to the Vehicle.
4) The Vehicle verifies through the Ledger the Proof included in the Credential Presentation regarding the Issuer of the Credentials, i.e the Software Vendor.

The process is displayed in Figure 1 below. The above process is only the half of the mutual authentication; the authentication is mutual, so the Vehicle will have also to present Credentials to the API that prove that the device to be updated is among the devices that have been manufactured by the Software Vendor who performs the update. The Issuer of these Credentials is the software Vendor. The API verifies through the Ledger the Proof included in the Credentials regarding the Issuer of the Credentials, i.e the Software Vendor. The Software Vendor is trusted by both entities since its DID and verification are published and resolvable from the Ledger by a Trusted Anchor.

After successfully completing the mutual authentication, the API should present to the Vehicle requested Credentials containing the digital fingerprint (e.g. a hash) of the Code corresponding to the latest update of the software to be installed within the device. The Issuer of this Credentials will be the device software vendor. The Vehicle will verify the Credentials proof by querying the Ledger and then check the Integrity of the code that is sent to it by following a procedure similar to the verification of digital signatures.

In case that software code Integrity verification fails, it means that there was a tampering of the code or the code does not belong to the Pre-market Software Vendor. The Vehicle will not install the software update. Then, a secure communication between the Vehicle and the Software Vendor will be initiated so that the Credentials of the API are revocated. [5]. The role of the Post-market device software vendor API is similar to the role of the Pre-market device software vendor API.

V. Conclusions & Future Work

Our choice of a DLT framework for the IdM in the IoV ecosystem selects Hyperledger *Indy* due to the availability of advanced IdM concepts of SSI, framework expandability, and privacy preserving techniques. With the IdM capabilities of *Indy*, it is possible to design DID issuance and management among infrastructure stakeholders of the IoV. For stakeholder identification, the secure software update scenario between a vehicle and a cloud API defines specific ecosystem roles. Additionally, standardization formalities of vehicles introduce required authorities for a legitimate IdM design. The incorporation of all identities to the DID credential design establishes DLT-based credential connections of identities that are bound to PKI keypairs. Mutual authentication of credentials and connected PKI keypairs enables secure communication of software updates. The scenario of software integrity checking as a mechanism to provoke revocation covers maintenance procedures of IdM.

Future work remains in the form of bootstrapping DIDs of Trust Anchor and Steward roles and to correct adjustments that emerge during the implementation. Additionally, the ledger requires a consortium controlled design of input verification of transactions. Addressing *Indy* plugins indicates the potential to enhance transaction verification of the ledger. Another issue that needs to be solved in the future is the acceptance of a revocation transaction. The reason therefore is the case of a vehicle which detects compromised software, but cannot verify whether the API or the vehicle itself caused the derogation. As a result, the decision of the Trust Anchor who submits the revocation transaction requires an extended revocation design.

[5]Note that in case that the tampering of the code is done in-vehicle, we need to devise a different revocation strategy as it is mentioned in the future work section

ACKNOWLEDGMENT

Authors acknowledge support from the European Union's Horizon 2020 innovation action programme under grant agreement No 833742 (nIoVe).

With the support of the Technische Universität München - Institute for Advanced Study, funded by the German Excellence Initiative and the European Union Seventh Framework Programme under grant agreement No 291763.

REFERENCES

[1] "Decentralized Identifiers (DIDs) v1.0," https://www.w3.org/TR/did-core/, 2020, [Online; accessed 28-February-2020].

[2] "Verifiable Credentials Data Model 1.0," https://www.w3.org/TR/vc-data-model/, 2019, [Online; accessed 28-February-2020].

[3] D. Tzovaras, N. Karagiannis, and M. G. Strintzis, "Robust image watermarking in the subband or discrete cosine transform domain," in *9th European Signal Processing Conference (EUSIPCO 1998)*. IEEE, 1998, pp. 1–4.

[4] F. Masood and A. R. Faridi, "Distributed ledger technology for closed environment," in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2019, pp. 1151–1156.

[5] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2017, pp. 466–473.

[6] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: a survey," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4-2, p. 1735, 2018.

[7] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[8] B. Curran and J. Richards, "What are oracles," *Smart Contracts, Chainlink & "The Oracle Problem". Accessed*, vol. 15, 2019.

[9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[10] J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, *Blockchain and Applications: International Congress*. Springer, 2019, vol. 1010.

[11] S. Halder, A. Ghosal, and M. Conti, "Secure ota software updates in connected vehicles: A survey," *arXiv preprint arXiv:1904.00685*, 2019.

[12] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," *2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco*, pp. 1–7, 2019.

[13] E. Gelenbe, G. Görbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Nemesys: Enhanced network security for seamless service provisioning in the smart mobile ecosystem," in *Information Sciences and Systems 2013*. Springer, 2013, pp. 369–378.

[14] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.

[15] A. Yohan and N.-W. Lo, "An over-the-blockchain firmware update framework for iot devices," *2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan*, pp. 1–8, 2018.

[16] "Ockam," https://www.ockam.io/, 2017, [Online; accessed 05-March-2020].

[17] T. L. Foundation, "Hyperledger Indy Project," https://www.hyperledger.org/projects/hyperledger-indy, [Online; accessed 27-February-2020].

[18] Z. A. Lux, F. Beierle, S. Zickau, and S. Göndör, "Full-text search for verifiable credential metadata on distributed ledgers," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, 2019, pp. 519–528.

[19] J. Kolleda, L. Frank, S. Andrews, T. Poling, D. Fitzpatrick, J. Marousek, and B. A. Hamilton, "National security credential management system (scms) deployment support: Scms baseline summary report," United States. Dept. of Transportation. ITS Joint Program Office, Tech. Rep., 2018.

[20] C. Platform, "Certificate policy for deployment and operation of european cooperative intelligent transport systems (c-its)," *European Commission*, 2017.

[21] J. Roos, "Identity management on the blockchain," *Network*, vol. 105, 2018.

[22] bcgov/von network, "A portable development level Indy Node network," https://github.com/bcgov/von-network, [Online; accessed 28-April-2020].

[23] N. George, "Cto, sovrin foundation, sponsor and hyperledger aries, sponsor and contributor, 2019. announcing hyperledger aries, infrastructure supporting interoperable identity solutions."

[24] "Car registration documents and formalities," https://europa.eu/youreurope/citizens/vehicles/registration/formalities/index_en.htm, 2019, [Online; accessed 05-March-2020].