Blockchain-based Self-Sovereign Identity Solution for Vehicular Networks

Engin Zeydan*, Josep Mangues*, Suayb Arslan†, Yekta Turk◇
*Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain, 08860.
† Massachusetts Institute of Technology, MA, USA, 02139.
◇Mobile Network Architect, Istanbul, Turkey, 34396.
[engin.zeydan, josep.mangues]@cttc.cat, sarslan@mit.edu, yektaturk@gmail.com

***Abstract*—Identity and access management frameworks address data governance and system access rights for users, organizations, and vendors. Emerging identity management models such as Self-Sovereign Identity (SSI) that is based on Distributed Ledger Technology (DLT) technology, have emerged to address the challenges associated with centralized authority. The main goal of SSI is to help users self-manage their data shared with services. In this paper, we explore a possible application of the SSI concept to vehicular networks. We propose a new methodology, that is alternative to the conventional blockchain-based SSI, which ensures confidentiality, authentication, and integrity of vehicle users identity and their data. At the end of the paper, we also compare SSI-based and Non-fungible token (NFT)-based blockchain solutions, the challenges and future directions of SSI solutions in the context of vehicular networks.**

Keywords*—*self-sovereign, digital identity, blockchain, vehicular networks.

I. Introduction

The number of devices used in the network infrastructure to connect to various services is increasing. At the same time, it is becoming increasingly difficult for service providers to identify and authenticate the devices used for specific services. Therefore, increasing the level of security and privacy becomes an additional challenge when many devices are connected to different services offered by operators/service providers [1], [2]. Almost all web-based applications on the Internet today leverage digital identity services today. However, most user identity and access management systems today are based on single sign-on solutions and multi-factor authentication which may introduce additional risks (such as identity theft and fake users) to their trustworthiness due to centralized platforms.

Self-Sovereign Identity (SSI) has emerged as a new digital identity model based on Blockchain Network (BCN), cloud and mobile computing technologies [3]. SSI can also help to promote transparency and trust [4]. For example, during the process of data sharing, individuals can make informed decisions about sharing of their data with others to ensure privacy and security. One of the main principles of SSI is to ensure that only the necessary information for a service is collected. Sharing partial digital identities for each service can also help prevent re-identification and correlation of data. In parallel, the next generation Connected and Automated Mobility (CAM) applications in vehicular networks need to leverage advanced registration mechanisms to improve security and privacy, including authentication. As vehicles move through different regions (either within country or between countries), a true mobility scheme must support advanced authentication methods. In cross-border situations, roaming procedures between operators need to be established and vehicle authentication, integrity and confidentiality of vehicle data must be ensured.

II. Related Work and Contributions

The use of BCN to create transactions based on interactions between nodes has been studied in many relevant areas of telecommunication networks [5]. In vehicular networks, vehicular data such as location, route, data transfer, money transfer, Global Positioning System (GPS) speed, engine control unit info, obstacles detected, etc., as described in [6] can also be committed to BCN as transactions (similar to for example the service orchestration logs committed to BCNs in [5]). For authenticating users via BCNs, a cloud-based authentication scheme

978-1-6654-7598-3/23/$31.00 ©2023 IEEE

using blockchain for Internet of Things (IoT) devices is studied in [2]. In [1] it was shown that blockchain-based authentication system can reduce communication latency compared to existing protocols for 5G-Enabled IoT.

At the same time, there have been some attempts to design blockchain-based SSI systems. A public blockchain-based system is proposed in [7] in the context of the European Union (EU) General Data Protection Regulation (GDPR). The European Union Agency for Cybersecurity (ENISA) and European Telecommunications Standards Institute (ETSI) are collaborating to define requirements for remote identity proof[1]. Verifiable credentials [8] and Decentralized identifiers (DIDs) [9] have been described in W3C standards. The OpenID foundation[2] enables, protects, and promotes OpenID technologies. Decentralized Identity Foundation (DIF)[3] develops an open ecosystem for DID and ensures interoperability. The implementation of BCN-based decentralized identity solutions is growing rapidly. Zebra is the first zksnark-based anonymous credential for on-chain verification [10]. A permissionless decentralized digitized passport is implemented in [11].

In the area of vehicular networks, there are several cross-border projects supported by H2020 projects to develop CAM applications. The 5G-ROUTES project[4], the 5GCroCo project[5], the 5G-CARMEN project[6] and the 5G-MOBIX project[7] seek to validate various CAM use cases in 5G cross-border situations. However, scalable and resilient authentication of vehicle users is still an ongoing process and not well studied as a use case. Furthermore, the desired level of confidentiality, authentication, and integrity is still an ongoing research process.

In this paper, we propose a new method to enable blockchain-based SSI technology for vehicular networks. Unlike the traditional blockchain-based SSI method, which lacks integrity and confidentiality, the proposed method enables integrity and confidentiality in addition to authentication. In the proposed method, confidentiality is ensured by preventing an outsider from accessing vehicle data transactions during the block commit phase of permissioned BCN by obtaining authorization from SSI BCN. Integrity is satisfied by using permissioned BCN for vehicle data. Authentication is guaranteed through the interaction between permissioned BCN for vehicle data and the SSI permissionless BCN.

III. Key Control Points in Web 3.0 for identity management

Identity management modeling has been evolving from the simplest model to newer models [12]. In traditional *centralized identity*, user is authenticated with several applications and services separately. This is the most common model that is used today which has high security and privacy risks due to multiple copies of data in the databases of service providers. In the case of *federated identity*, user is only authenticated with identity provider once (with just one set of credentials) and redirected to access various applications and services of service providers. Although federated identity approach simplifies the user experience, it still possess risks since it requires a trusted identity provider. In SSI, user is authenticated with applications via BCNs by using verifiable credentials (received directly from the issuers of credentials in the form of a cryptographic hash of the transaction) that can be disclosed by users selectively.

To control data usage, several reliable data and system maintenance technologies are being used: **Federated learning** enables to train Artificial Intelligence (AI) models without explicit data sharing across different participating parties, while **Secure computing** is used to enable confidentiality, availability and integrity. Several techniques such as Fully Homomorphic Encryption (FHE) (allowing arbitrary computation on encrypted data), secure hardware (that relies on tamper-resistance chips or other hardware-based security techniques), Multi Party Computation (MPC) (which allows multiple parties to compute a function using their inputs without revealing their inputs to each other), **Distributed Ledger Technology (DLT)** allows users in different sites to propose and validate transactions and update them in a synchronized way over the network, **Differential privacy** allows public data sharing while protecting information about individuals.

In comparison to web 2.0, in web 3.0 users control data usage without relying on centralized control or intermediary. Three key control points are available for this as described in the next three subsections.

[1] Online: https://www.etsi.org/newsroom/news/2067-2022-05-enisa-and-etsi-joint-workshop-tackles-challenges-for-european-identity-proofing, Available: December 2022.

[2] Online: https://openid.net/, Available: December 2022.

[3] Online: https://identity.foundation/, Available: December 2022.

[4] Online: https://www.5g-routes.eu/, Available: December 2022.

[5] Online: https://5gcroco.eu/, Available: December 2022.

[6] Online: https://5gcarmen.eu/, Available: December 2022.

[7] Online: https://www.5g-mobix.com/, Available: December 2022.

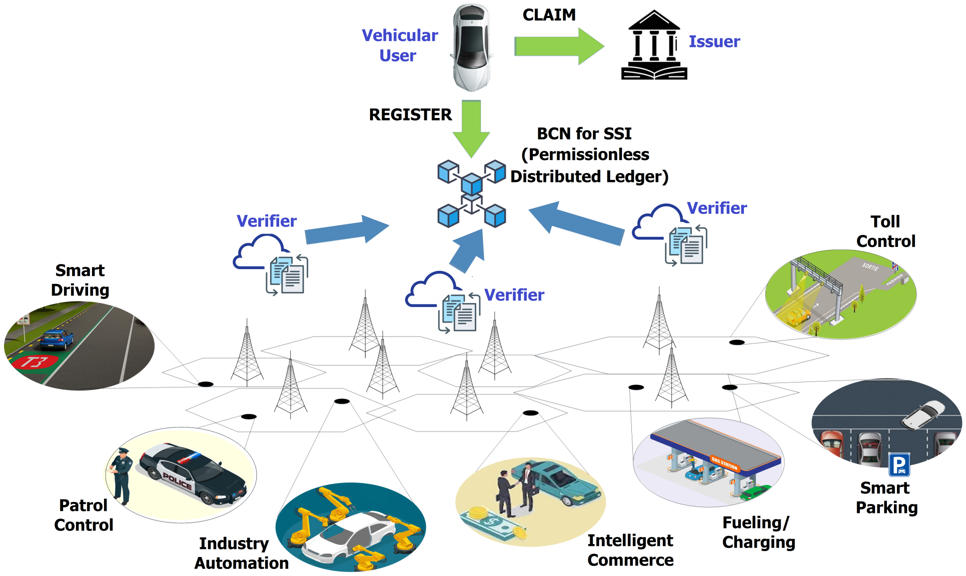


Fig. 1: Blockchain-based SSI architecture and interactions of vehicular user with different usage areas.

A. Decentralized Identity

Attributes and identifiers are used to identify an individual or object in a specific role or context. This is for identities to access resources and a basic building block of a decentralized Public Key Infrastructure (PKI). In DID, no central authority or certified registry is present. Instead, a DLT or BCNs are used to verify the information. DID can refer to any subject, such as a person, vehicle, organization, data model, etc. In SSI-based systems, DIDs represent the cryptographically verifiable credential issued by authorities and is stored in BCNs. In addition to holding a vehicular node's basic identity, SSI can be used to verify any identity-related information or verify potential other types of information needed for transactions such as for assessing risks, doing compliance checks, checking insurance status or vehicular device health data.

B. Decentralized Access Control

This is used for access control to data. In this method, users are authenticated automatically without relying on trusted and powerful centralized servers that enforce access. The main mechanism used here is to separate authorization and access via access policies and dissemination of secrets. Therefore, authorization and access are co-designed. By possessing the identity's private keys, a vehicle may demonstrate its authority over the identity.

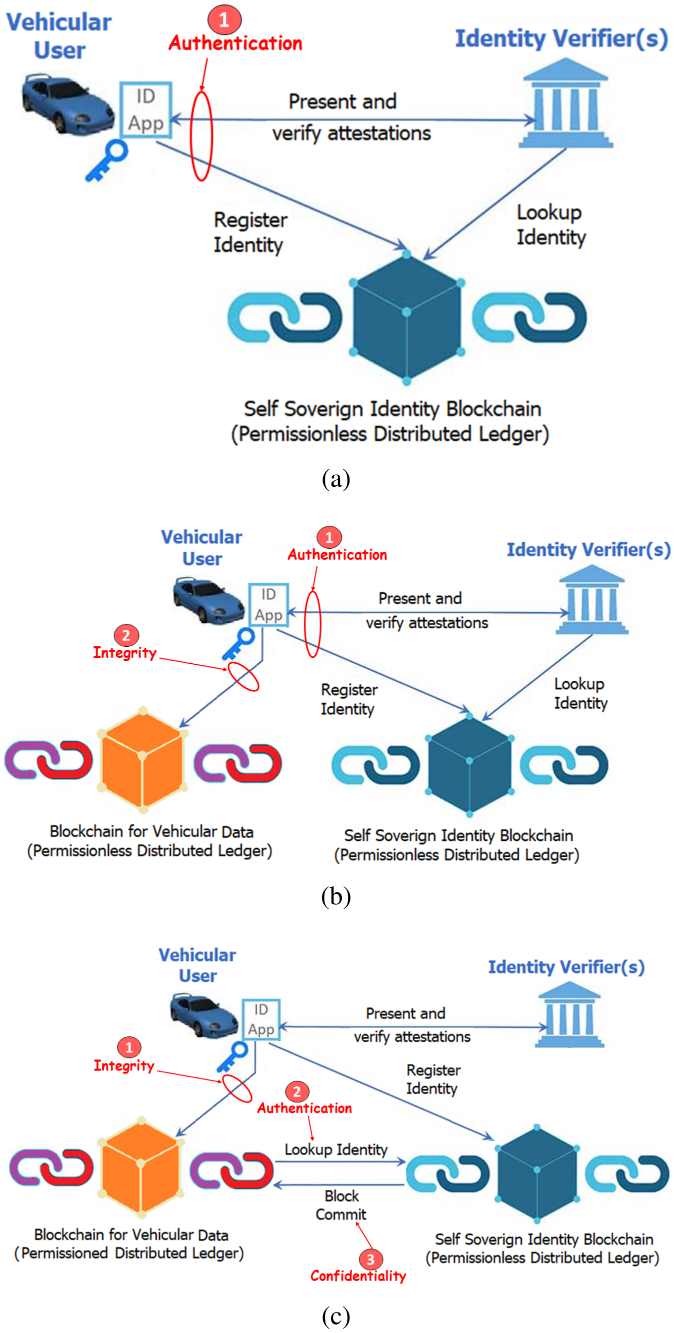
The DLT is used as a policy decision point to authorize data consumers via immutable transactions. After the approval of data access from BCN, the data consumer only receives the decryption key. Some key applications are policy-based data sharing between organizations, multiple application access to user consent data, managing access to IoT devices and systems, manage and tracking access to critical resources and information.

C. Decentralized Computation (policy-compliant)

This is used for data usage control and computation of data without a central authority. The computation of data is performed in a way that is compliant with a specific set of rules or policies. Using this technique, computation is performed in a more secure, private, fair, and transparent manner. One prominent examples is the secure multi-party computation with verifiable secret-sharing schemes [13] in which an external blockchain is used to control the network, handle identities and access control, and act as a tamper-proof log of events.

IV. Self-Sovereign Identity Platform for Reliable Vehicular Networks

Figure 1 shows the blockchain-based SSI architecture and interactions of the vehicular user with different usage areas. In this figure, several application usage areas of the BCN-based SSI platform are available such as smart driving, patrol control, industrial automation, intelligent commerce, fueling/charging, smart parking, and toll control for vehicular networks. The verification of the vehicle users in these different scenarios is done via BCN-based SSI solution which uses a permissionless DLT approach to register user identities.


Vehicular User
1
Authentication
Identity Verifier(s)
ID App
Present and verify attestations
Register Identity
Lookup Identity
Self Soverign Identity Blockchain (Permissionless Distributed Ledger)
Vehicular User
1
Authentication
Identity Verifier(s)
ID App
Present and verify attestations
2
Integrity
Register Identity
Lookup Identity
Blockchain for Vehicular Data (Permissionless Distributed Ledger)
Self Soverign Identity Blockchain (Permissionless Distributed Ledger)
Vehicular User
Identity Verifier(s)
ID App
Present and verify attestations
1
Integrity
Register Identity
2
Authentication
Lookup Identity
Block Commit
3
Confidentiality
Blockchain for Vehicular Data (Permissioned Distributed Ledger)
Self Soverign Identity Blockchain (Permissionless Distributed Ledger)

(a)

(b)

(c)

Fig. 2: Various approaches for blockchain-based SSI solutions in vehicular networks (a) Authentication, (b) Integrity and Authentication, and (c) Confidentiality, Integrity and Authentication.

A. *Blockchain based Secure Architecture Alternatives*

Fig. 2 shows three methods of network security and privacy for vehicular users achieved by using BCN. Fig. 2a shows the method for authentication only, Fig. 2b for both integrity and authentication, and Fig. 2c shows the proposed method for confidentiality, authentication, and integrity. As shown in Fig. 2a for a classical BCN-based SSI, the verification of the credentials provided by the vehicle user is performed by checking the DID in a permissionless BCN. This process can be done immediately without relying on the issuer. Moreover, during this authentication process, vehicle users can control which attributes can be disclosed or kept private.

Fig. 2b, on the other hand, is a further development of Fig. 2a and includes another permissionless BCN for the permanent, transparent, and immutable recording of other relevant vehicular data. Suppose that two vehicle users want to communicate with each other. First, both vehicle users verify their own digital identity information by presenting certificates and verifying attestations with the identity verifier. Note that there are two separate transactions at this stage which is very time-consuming. After the digital identities are presented and attestations are verified, vehicle users commit data into the BCN that can be shared with other vehicle users. This in turn increases the reliability and integrity of the overall system. Note that these vehicle users also have an account number generated in the BCN. In this case, during communication, we have the possibility to match the vehicle user's ID with the account ID number. This situation violates confidentiality.

Fig. 2c ensures the authentication, integrity, and confidentiality of the system. The principle of operation is as follows: After the first step of integrity assurance via the permissioned BCN, where vehicle data is passed to the BCN, the permissioned BCN instead asks the permissionless BCN-based SSI for approval as shown in Fig. 2c whether blocks may be created for transactions owned by these users and whether they are valid users. If the users in the block are verified in the SSI blockchain, the block is created and the vehicle data is committed to the BCN in the approval phase. As can be seen, in this scenario, the vehicle user does not perform any authentication process. Hence, confidential information, such as matching the digital ID with the blockchain account ID of the vehicle user, cannot be performed or disclosed. This ensures confidentiality. Moreover, this approach is faster than Fig. 2c approach since the vehicle user only commits its data to the BCN and no further authentication is required by the vehicle user in this dynamic and mobile environment.

B. Data Format of Vehicle Digital Identity

In this section, we present an example of a digital identifier format. Note that if vehicle ownership or any of the related features changes, only that attribute will be updated. There is no need to create and register a new digital identity from scratch. A sample vehicle identity can be as follows:

```
{
  "id": "Vehicle_Did",
  "value": "0x123456789101112",
  "Owner_Id": "Text",
  "Owner_Type": "Private/Company",
  "Issue_Date": "Date",
  "Issuer": "Value",
    "Did_Items": [
      {"Vehicle_Type": "Value"},
      {"Vehicle_Model": "Value"},
      {"Gearbox_Type": "Value"},
      {"Colour": "Value"},
      {"Fuel": "Value"},
      {"Engine_Capacity": "Value"}
      {"Traffic_Release_Date": "Date"}
      {"Engine_Chassis_Number": "Date
         "}
    ]
  }
```

C. A Cross Border Use Case

One concrete example of the application of the proposed BCN-based SSI architecture is for CAM applications in cross-border scenarios. Authenticating vehicles while protecting their privacy in a scalable and reliable manner is a challenging issue due to the need for a central authority that manages and identifies the identities. In Fig. 3, a use case scenario of CAM for a cross-border scenario is presented. Proposed BCN-based SSI architecture can help vehicles to securely and efficiently identify themselves while sharing their information with other vehicles or relevant authorities (e.g., customs or border control). This potentially benefits the automation process of crossing international borders.

V. Comparisons, Challenges & Future Directions

A. SSI-based vs. NFT-based Solutions

The concept of the digital asset was introduced with Non-Fungible Tokens (NFTs). Therefore, a solution based on NFT can also be used to store identity information in a BCN. For example, an NFT can be created for a particular vehicle user, and the NFT ownership may be assigned to the corresponding vehicle user. This can also be considered a similar structure to the SSI architecture. However, there are some fundamental differences between the SSI architecture and NFT within the BCN. First of all, NFTs is used to digitally sign a digital asset. SSI and NFT concepts can be compared as follows: NFTs allow a user to show what is possessed, while SSI allows to prove the digital identity. From this perspective, NFTs are mostly used for objects that are physical, such as artwork. However, for moving vehicles that are in constant communication with their environment, SSI-based authentication is required. Table I provides a comparison of BCN-based NFT and SSI technologies applied to vehicular network identify a solution.

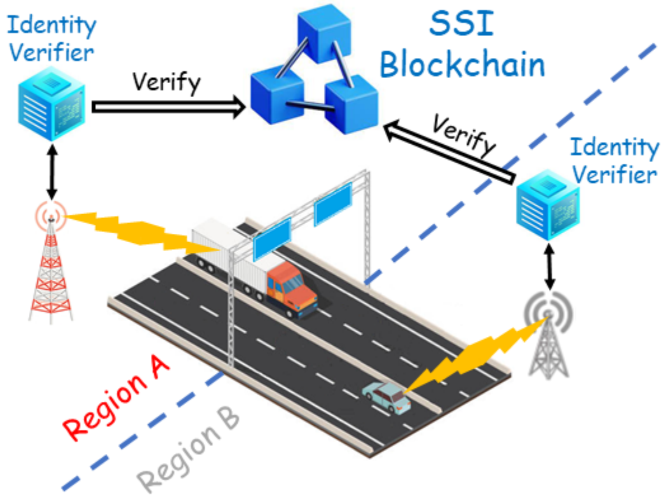


Fig. 3: Vehicle Identities are verified by using the blockchain-based SSI network in a connected and automated cross-border use case.

B. Challenges

Key Management: Since SSI management models give the responsibility to users, key management is a significant challenge in BCN-based SSI architectures.

Lack of Implementation and Standardization Details: The development of appropriate technology and infrastructure to achieve security and interoperability of such BCN-based SSI architecture with clear guidelines and standards is still an ongoing study in the ecosystem. Note that identity verification processes must be updated for each transaction. If using a man-in-the-middle attack

TABLE I
COMPARISONS OF BCN-BASED NFT AND SSI TECHNOLOGIES FOR VEHICULAR NETWORK IDENTITY MANAGEMENT PROBLEM.

Solution	Characteristics	Advantages	Disadvantages
NFT based Identity	— Allows tokenization of things like art, collectibles, etc. — Directly links a unique identifier to one blockchain address. — Used to certify ownership. — Confer licensing rights to use the Fixed asset. — Cannot be copied, substituted, or subdivided. — Contains references to digital assets.	— Introduced in a ERC-721 standard format. — The ERC-1155 standard offers semi-fungibility. that can represent a class of assets. — Wide industry implementation experience.	— Digital representations of Fixed assets on a blockchain. — Proving the ownership of a certain asset but not the rights to commercial usage. — Legal issues in financial interactions. — Removes the transparency and traceability of who the current owner is. — Can be created by anybody.
Self-Soverign Identity	— Addresses establishing trust in a dynamically interacting vehicle environment. — Gives individual vehicles control over the information they use. — Digital vehicle identities are managed in a decentralized manner.	— Provides great flexibility for dynamically interacting assets. — Presents an overall architecture with issuers and verifiers. — The class of the vehicle can be indicated in the identity proof.	— Lack of implementation experience in industry for DiDComm. — Unmature, but developing standardization aspects.

DID belonging to a vehicular user can be obtained by the malicious user if the verification process is not performed on every transaction. However, verifying identity with every transaction has an impact on transaction time.

Validation of New Identity Verifier: It is a challenge to select new verifiers and integrate them into the system. If a node needs to be added to the system, who gives that identity verifier node authority in the system? For example, when new countries are added to the EU, their motor vehicle institutions should also be added to the system as a node. As a solution to this challenge, the process of inclusion in the system can be performed by the node that has the authority to record.

Interoperability for Secure Communication: Interoperability between different networks is a big challenge where transportation. In the studies related to SSI, for secure communication between the user and the identity verifier, the implementation of the messaging protocol DID Communications (DIDComm) [8] is on the agenda. This protocol is customized for DID messages. However, from a security point of view, the Transport Layer Security (TLS) protocol is now more widely used in the industry, and knowledge of it is at a higher level. In this regard, the development of middleware between TLS and SSI blockchain could be a sufficient solution to provide DIDComm features.

Performance Issues of Blockchain Platforms: If the blockchain technologies currently in use are investigated, even in the best cases Transactions per Second (TPS) values are around 3000 TPS. However, if it would be necessary to use BCN when multiple vehicle users need DID proof processes at the same time, this may cause problems. For example, there are about 250 million vehicles in the EU. As a workaround, messaging queuing services such as Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP) can be used before data is transferred into blockchain networks. However, in this case, the need for real-time tasks may be affected. Another solution, still preliminary, would be to prioritize vehicle users according to their service types at DID proof processes. For this reason, an advanced blockchain platform with faster sharding capabilities should be created for such scenarios.

C. Future Directions

Post Quantum Cryptography (PQC) has emerged as a new security layer to protect against quantum computers which need to be adapted to telecommunication networks as well [14]. Especially, BCNs can suffer from quantum attacks during block commit phase [15], [16]. Therefore,

[8] Online: https://identity.foundation/didcomm-messaging/spec/, Available: December 2022

blockchain-based SSI solutions need to adapt to evolving architectural and algorithmic developments in the post-quantum era. **SSI as a Service** can work in a robust and scalable way with the blockchain platform, which is actually based on a cloud-native architecture. This requires the underlying blockchain platform of SSI to be provided as a service. In this way, the roles of the verifier and issuer can be provided as a service more quickly. **Homomorphic encryption** as a service can be added to a SSI system in the cloud to ensure the necessary confidentiality of executed transactions. **DIDComm Messaging** needs to support data formats other than JavaScript Object Notation (JSON), which is currently the only format available. Moreover, the addition of forward and backward secrecy in DIDComm messaging needs to be considered. **Open API** can actually open DID services to external environments and create an environment where service providers for vehicles can be integrated. DIDComm integration does not have to be done by each service provider individually. Therefore, SSI can be easily accessed with REST Application Programming Interface (API) calls. This makes it easy to enable various services for vehicles.

VI. Conclusions

This paper proposes a new approach to BCN-based SSI solution that enables integrity, confidentiality, and authentication for vehicular user identity and data sharing for CAM applications. After describing the key control points and enablers for identity management in Web 3.0, we present different architectural options for SSI platform designed for vehicular networks including the proposed technique. At the end of the paper, we also compare SSI-based and NFT-based solutions to enable authentication services for vehicular networks and present challenges and future directions of BCN-based SSI solutions.

Acknowledgment

This work was partially funded by "ERDF A way of making Europe" project under grant PID2021-126431OB-I00 and Spanish MINECO - Program UNICO I+D (grants TSI-063000-2021-54 and -55) Grant PID2021-126431OB-I00 funded by MCIN/AEI/10.13039/501100011033.

References

[1] B. Goswami and H. Choudhury, "A blockchain-based authentication scheme for 5g-enabled iot," *Journal of Network and Systems Management*, vol. 30, no. 4, pp. 1–33, 2022.

[2] K. Albalawi and M. M. A. Azim, "Cloud-based iot device authentication scheme using blockchain," in *2019 IEEE Global Conference on Internet of Things (GCIoT)*, pp. 1–7, IEEE, 2019.

[3] A. Preukschat and D. Reed, *Self-sovereign identity*. Manning Publications, 2021.

[4] Katharina Koerner, "Self-sovereign identity as future privacy by design solution in digital identity?," *White Paper*, 2022. Available: https://bit.ly/3UFsM8s, [Online; accessed December-2022].

[5] E. Zeydan, J. Baranda, J. Mangues-Bafalluy, Y. Turk, and S. B. Ozturk, "Blockchain-based service orchestration for 5G vertical industries in multi-cloud environment," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2022.

[6] P. H. Rettore, G. Maia, L. A. Villas, and A. A. Loureiro, "Vehicular data space: The data point of view," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2392–2418, 2019.

[7] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the gdpr," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pp. 342–345, 2020.

[8] World Wide Web Consortium, "Verifiable Credentials Data Model v1.1," 2022. Available: https://www.w3.org/TR/vc-data-model/, [Online; accessed December-2022].

[9] World Wide Web Consortium, "Decentralized Identifiers (DIDs) v1.0, Core architecture, data model, and representations," 2022. Available: https://www.w3.org/TR/did-core/, [Online; accessed December-2022].

[10] D. Rathee, G. V. Policharla, T. Xie, R. Cottone, and D. Song, "Zebra: Anonymous credentials with practical on-chain verification and applications to kyc in defi," *Cryptology ePrint Archive*, 2022.

[11] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, pp. 1336–1342, IEEE, 2018.

[12] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019.

[13] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *arXiv preprint arXiv:1506.03471*, 2015.

[14] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent advances in post-quantum cryptography for networks: A survey," in *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*, pp. 1–8, 2022.

[15] E. Zeydan, Y. Turk, S. B. Ozturk, H. Mutlu, and A. A. Dundar, "Post-quantum blockchain-based data sharing for iot service providers," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 96–101, 2022.

[16] E. Zeydan, J. Baranda, and J. Mangues-Bafalluy, "Post-quantum blockchain-based secure service orchestration in multi-cloud networks," *IEEE Access*, vol. 10, pp. 129520–129530, 2022.