BEAT-Traffic: a Blockchain-Enabled infrastructure for Anonymous-yet-Traceable Traffic reporting

Marina Dehez Clementi, Jean-Christophe Deneuville, Emmanuel Lochin, Jérôme Lacan

BEAT-Traffic: a Blockchain-Enabled infrastructure for Anonymous-yet-Traceable Traffic reporting

Marina DEHEZ-CLEMENTI[1], Jean-Christophe DENEUVILLE[2], Emmanuel LOCHIN[2], Jérôme LACAN[1]
[1]*ISAE-SUPAERO, Université de Toulouse* Toulouse, France
[2]*École Nationale de l'Aviation Civile, Université de Toulouse* Toulouse, France
name.surname@{isae-supaero.fr;enac.fr}

***Abstract*—Intelligent Transportation Systems (ITS) have become increasingly popular in recent years, and are viewed as the future of transportation. These systems rely heavily on open communication networks to ensure road safety and efficiency. However, the rapid and secure sharing of information over large-scale cyber-physical systems such as ITS poses significant challenges, including data lineage, data consistency, access rights management, and privacy preservation. In this paper, we propose a solution to improve the sharing of sensitive data over ITS using blockchains and distributed cryptography. We demonstrate how these technologies can be applied to the reporting of Road Hazard Warnings, creating a blockchain-based data collection system that ensures the dissemination and security of reported messages. Our approach combines blockchains and group signatures to achieve the necessary security properties, including privacy preservation and censorship resistance, while maintaining performance levels comparable to existing literature. We provide a theoretical analysis of the solution's security properties and expected performance characteristics. Our results demonstrate the potential of blockchain-based solutions for addressing the challenges of secure and efficient information sharing in ITS. We believe that our work will contribute to the development of secure and privacy-preserving ITS systems, and encourage further exploration of blockchain-based solutions in the field of intelligent transportation.**

***Index Terms*—Intelligent Transportation Systems, open communication networks, road safety, secure information sharing**

I. Introduction

Intelligent Transportation Systems (ITS) have become increasingly popular in recent years due to their ability to improve road safety and traffic efficiency. The use of vehicular communications in ITS to spread information about the position of vehicles [1] and to infer the state of traffic [2] has become essential for the development of smart transportation systems. However, the sharing of information in an open setting like ITS poses significant challenges due to the heterogeneous nature of its components. Additionally, there are additional security concerns that must be addressed, especially since Denial of Service (DoS) attacks or modification/fabrication attacks can have a tremendous impact on the safety of road users.

Since 2015 and the Jeep hack [3], cyber security vulnerabilities in vehicular environments have been increasingly reported. The threat model on vehicular communications in ITS can be separated into two levels: data level and service level. Tampering with data can lead to unwanted hazardous events; therefore, having a message authentication process is essential. However, collecting authenticated data allows malicious entities to track users. On the service level, having a centralized authority in decision making makes the system vulnerable to denial of service, either from a malicious origin (censorship-vulnerable as there is a single decision-maker), or failure (similar to centralization issues in databases).

These issues can partly be solved by using a blockchain [4]. The distributed nature of this technology maps the ITS and delegates the central authority to authenticated peers, even if not trusted, hindering DoS and censorship attacks. However, additional work must be done to solve the privacy issues. By nature, blockchains are transparent, and tracking a user is still possible if not easier. Yet, anonymizing the traffic and messages, while possible, is not an option as road users must be accountable for their actions on the road both in regards to the law and insurance requirements.

In this paper, we propose the full description of a distributed Traffic Reporting service that guarantees censorship-resistance, anonymity of the users, and yet holds them accountable for their actions. The proposed system will use blockchain technology to decentralize the decision-making process while maintaining user accountability. Additionally, the system will incorporate a privacy-preserving mechanism to ensure the anonymity of the users while maintaining the transparency of the data. We believe that this proposed system will contribute significantly to the development of secure and privacy-preserving ITS systems and encourage further exploration of blockchain-based solutions in the field of intelligent transportation.

The article is organized as follows: Section II provides an overview of ITS in relation to Vehicular Ad-hoc Networks (VANET). Section III covers the background on blockchains. Section IV discusses relevant related works, which are compared to our results in Section VIII. Section V describes the methodology used to build our Traffic Reporting service, which is presented in Section VI; and finally, Section VII summarizes our security argument, which justifies that we have achieved our initial goals.

II. An overview of VANETs

Intelligent Transportation Systems (ITS) leverage sensing, analysis, control, and communication technologies to improve the safety, mobility, and efficiency of ground transportation, and are integral to smart cities. Vehicular Ad-hoc Networks

(VANETs) [5], self-configuring networks that integrate mobile nodes such as vehicles equipped with On-Board Units (OBU) and static infrastructure nodes like Roadside Units (RSU), are a key communication mode in ITS. VANETs provide vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication links through the 802.11p (WAVE) standard [6], specifically designed for VANETs.

A. Infrastructure

The European Telecommunications Standards Institute (ETSI) is the authority responsible for defining communication standards for ITS in Europe, with a specific focus on Cooperative-ITS. The Cooperative-ITS standardization axis contributes to the definition of information and communication technologies intended to increase travel safety, minimize environmental impact, and improve traffic management. The Basic Set of Applications (BSA) [7], defined by ETSI, guides early developments in ITS by regrouping applications and use cases related to active road safety applications, traffic efficiency applications, and other applications enabling cost-effective deployments.

In this paper, we focus on active road safety applications, use cases, and underlying communications. Active road safety applications can be divided into two categories: Cooperative Awareness and Road Hazard Warning.

B. Communication standards and security

Cooperative Awareness applications involve informing road users and roadside infrastructure nodes in real-time about each other's position, dynamic, and attributes through the periodic exchange of Cooperative Awareness Messages (CAM) [1]. Road Hazard Warning (RHW) applications handle road safety and improve traffic efficiency by sharing data through Decentralized Environmental Notification Messages (DENM) [2], which contain information about road hazards or abnormal traffic conditions that can lead to the identification of unwanted events.

Security is crucial for V2X communications, particularly for the propagation of CAMs and DENMs. ETSI released a report in 2021 that specifies the security architecture for ITS communication [8]. The three mandatory security properties for CAMs and DENMs are authenticity, integrity, and authorization. Confidentiality is ignored as per se everyone needs to access the content of CAMs (for safety purpose). The issue of privacy is also studied in the report and applies to both types of messages. To this end, the document suggests the use of temporary identifiers in ITS messages while protecting the vehicle's canonical identifier. These two measures aim at:

1) Restricting the access to the unique identifier of vehicles (known as the *canonical identifier*) to a single entitled authority called the Enrollment Authority;
2) Providing hierarchical ITS-station management;
3) Reducing message linkability.

In this paper, we focus on this privacy requirement and describe a framework that aims at supporting all three aforementioned desired properties.

Blockchain technology, popularized by Bitcoin in 2009 [4], has found its place in various industries besides DeFi, such as supply chain [9], space and aeronautics [10], [11], healthcare [12]. Thus, in addition, we propose to use a blockchain to develop a traffic reporting service that provides reliable, scalable, secure, and privacy-preserving data collection for DENMs in ITS. In the following section, we present blockchains and justify their plus-value in tackling the observed challenges.

III. Background on blockchains

Blockchains have indeed gained in popularity since the advent of Bitcoin, the cryptocurrency developed by Satoshi Nakamoto [4]. In his working paper, the author defines the technology's essential concepts, including: the *transactions*, i.e. the way to distribute a piece of information; the *timestamp server* which ensures the synchronization of the network; the *proof-of-work* also known as the *consensus* algorithm; the *P2P network* which guarantees decentralization; and finally, the notion of *incentive*, under the form of a reward given to nodes that behave honestly and contribute to the network.

Blockchains are different from distributed databases and Distributed Ledger Technologies (DLT) in that there is no central authority that manages the authentication of the peers nor the verification of the records' validity. Instead, the nodes form the network and together execute a protocol known as the *consensus algorithm*. They also check whether the new transactions should be added to the previous ones. Blockchains are exceptionally famous because they are resilient in the presence of Sybil nodes (a feature known as *fault tolerance*) and prevent the deletion of the records (the *immutability* property).

The *consensus algorithm* is the core mechanism that deals with selfish, faulty or malicious nodes (the aforementioned Sybil nodes). It ensures the system's resilience to node failures, network partitioning, delayed, dropped or compromised messages, among others. The design of this algorithm is inherently tied to the type and the application context of the blockchain solution. For instance, Bitcoin is widely adopted by a large community and completely open (no central entity monitors the participants). Thus, the consensus algorithm should rely on a resource that is common to all participants and fairly distributed, *i.e.* the computational power of their devices. On the other hand, private blockchain implementations often rely on a smaller P2P network of which authorization policies and authentication mechanisms control the access. Hence, in these cases, the consensus algorithm would privilege a reputation-based mechanism that weights the votes of the peers according to their reputation in the network [13].

A. Key properties

Blockchain technology is desirable for its key properties of *decentralization*, fighting by design censorship and single points of failure; *transparence* and *open-sourceness*, rising against proprietary software from its conception. In addition, records are *immutable* and cannot be changed unless the

adversary takes control of more than 51% of the network's discriminating resource (which is highly unlikely). Thus, blockchains provide a great and valuable tool for system audits.

B. Smart contracts

In the context of blockchains, "a smart contract is an executable code that runs automatically on the blockchain by consensus nodes without any trusted third party" [14]. It embeds a protocol that facilitates, verifies, or enforces the negotiation or performance of a specified contract. Similarly to traditional blockchain transactions, calls and results given by a smart contract are traceable, irreversible and stored inside the distributed ledger; the contract itself, once deployed, is immutable. Therefore, it can be considered as a computer program that is running at the top of blockchain. For their ability to execute according a specific set of rules, smart contracts enable users to run complex programs and perform non-numerical exchanges while benefiting from the distribution and security of a blockchain infrastructure. As such, they can be used to build evolved decentralized applications that can be monitored via the transparency of the blockchain records.

C. Blockchain for ITS

As explained in Section II, vehicular communications contribute to better safety and efficiency in the ITS by facilitating the sharing of traffic-related information. However, safety often comes at the expense of poor security and privacy. Indeed, vehicular communications disclose rich details on road users and their mobility habits.

In this paper, we present an alternative approach based on blockchains and distributed cryptography that meets the three following requirements:

1) Vehicular communications are anonymous;
2) Vehicular communications are traceable;
3) No TTP is required during the setup of the infrastructure.

While we will explain that the two first requirements can be achieved with a carefully designed messaging system that builds upon distributed and threshold cryptography, the absence of the TTP implicitly means that anyone can be eligible to participate to the Traffic reporting service and that is justification enough for the use of a blockchain.

IV. Related work

There are several approaches to secure vehicular communications, among them some are based on the use of pseudonyms, public or even symmetric cryptography. In this section, we focus our analysis on group-signature based authentication schemes which can provide both anonymity and traceability. Indeed, theorized by Bellare *et al.* in [15], group signature schemes are a type of digital signature that allows members of a group to anonymously sign messages on behalf of the group. The signature does not reveal the identity of the signer, but it can be traced back to the group. There are two main central authorities in Bellare *et al.*'s group signatures: the Issuer and the Opener. The Issuer is responsible for issuing group membership certificates to authorized group members. The Opener, on the other hand, is a trusted party responsible for opening group signatures, *i.e.,* revealing the identity of the signer, when required by law enforcement or other authorized entities.

We identified three main works (selected for their recognition by experts on the topic, the presence of algorithms' description and performance analysis), listed in Table I, and analyze them in the following paragraphs.

In [16], Zhang et *al.* propose a decentralized group-authentication protocol based on group signatures and signcryption [17]. The underlying idea is to cope with certificate distribution and revocation challenges, avoidance of computation and communication bottlenecks, and reduction of reliance on tamper-proof devices. The decentralization comes from considering that each RSU maintains and manages an on-the-fly group of vehicles evolving in its range. The Opener authority is played by an external TTP and is called whenever a message seems fraudulent. The scheme is designed to apply the signature to an ITS message. It defines the safety message as a concatenation of a group ID, the payload (i.e. the actual ITS message as, for instance, a DENM), a timestamp and the signature. The total length of the new safety message structure is 474 bytes (including a payload of 100 bytes and a signature of 368 bytes). The signature scheme employed is defined in [18]. Among other parameters, the simulation presented shows that the scheme achieves a density-constant message delay that grows linearly with the time to batch verify the signatures.

In [19], Zhu et *al.* follow the same idea. They leverage the advantages of a group signature scheme and consider the RSUs as group managers. It facilitates the distribution of the secret keys and reduces the communication overhead. In addition, they use Hash-based Message Authentication Code (HMAC) to avoid the time-consuming step of verifying the revoked certificates and propose a cooperative message authentication mechanism to reduce the number of messages a vehicle must verify. Once again, the signature scheme is applied to the safety payload of CAM only. The structure of the messages broadcast by the vehicles for vehicle-to-vehicle positioning consists of a group ID, message ID, timestamp, location, signature and HMAC. The signature is 56-byte-long, and the size of the final message is 72 bytes.

In [20], Shao et *al.* also work in the decentralized group model that considers an ITS as separate groups, each one controlled by an RSU. In this configuration, they too develop a group signature-based authentication scheme for ITSs. However, the novelty lies in the threshold authentication of messages. Instead of verifying all the messages, the vehicles may equally accept messages that have been checked by a threshold number of peers. They adopt the same technique as the two previous works and apply the signature scheme to the payload. Therefore, the broadcast message consists of a message identifier (shorten as ID), a payload (100 bytes), a timestamp, a Time To Live (TTL), a group ID, and a signature of 826 bytes. The size of the messages is 935 bytes.

Similarly to the listed references, we focused on using a

group signature-based anonymous-yet-traceable authentication scheme to build BEAT-Traffic, a new Traffic reporting service that is privacy-preserving, accountable, and censorship-resistant. However, instead of augmenting an ITS message (e.g., CAM or DENM) with a group signature for authentication purposes, we propose to redefine the DENM structure to embed privacy security by design. In addition, our proposition goes further in terms of decentralization of the authority nodes (which favors the protection of nodes' anonymity). We use blockchains to support a peer-to-peer infrastructure for authority distribution, while ensuring transparency of the power distribution and the acquired authority usage (improving accountability).

V. Preliminaries

The use of two types of messages, CAMs and DENMs, in ITS communications for road safety applications has been discussed in Section II. While CAMs have received considerable attention in terms of security and privacy preservation, DENM security and privacy issues have been largely ignored or considered out of scope. This is a critical gap that needs to be addressed.

A. Problem statement

DENMs are the messages that enable traffic hazard warnings. Unlike CAMs, used for the vehicle-to-vehicle positioning, DENMs are sent to alert the network about specific hazardous events, e.g., a car accident. The construction of a DENM is triggered by an ITS-station upon detection of a road hazard or abnormal traffic conditions. The DENM is transferred to other relevant (e.g., in the specified geographical area) ITS-stations through the DEN basic service. This transmission is performed via V2V or V2I communications. Therefore, the broadcast of DENMs can breach users' identity and their location privacy either directly (e.g., presence of the `StationID` field) or indirectly (e.g., by analysis of the location traces). Growing efforts towards improving the safety of vehicular networks are focusing on securing the wireless communications and data transferred from vehicle to infrastructure nodes to communicate safety-critical information.

To contribute to the growing effort in securing vehicular communications, we propose the design of a traffic reporting mechanism that protects the anonymity of smart vehicles. However, regulations require the ITS to remain auditable, making it necessary to ensure that nodes are accountable for their actions.

Our contributions are as follows:

- We propose a message structure called `newDEN` that protects the vehicle's identity. We build on related work on group-signature based authentication schemes and construct a message in which we replace the `StationID` field by a group signature.
- However, group signature schemes rely on centralized authorities. Therefore, in addition to the modification of the messages, we describe a blockchain-based framework that enables the distributed, transparent bootstrapping of authorities. We discuss how the Enrollment Authority (EA) can be distributed over a set of RSUs and how the Auditor Authority (AA) can also be spread over another set of RSUs. We explain how this blockchain-based framework is a valid implementation of the "hierarchical VANET" as mentioned in [8].
- We show some expected performance results and compare our messaging system to existing work on CAMs.
- Finally, we give arguments of security supporting our claim that with the new message strucutre and the blockchain-based bootstrapping framework the ITS becomes a safer, more secure, censorship-resistant, and privacy-preserving reporting environment.

B. Nodes

The vehicular network architecture is composed of different types of actors, all sharing information to enhance the safety and security of the past, future and ongoing events in the VANET. Our network is made of three main components defined as follows:

- The Vehicle nodes (VNs) simplified vehicles. The vehicles are the users of the network. They witness road events and produce hazard warning messages, under the form of DENMs, to be broadcast to their peers for safety reasons. The vehicles are mobile. As such, we may assume that they have limited communication, computational and storage resources.
- The Infrastructure nodes (INs) also called RSUs. The RSUs are similar to vehicles in that they participate in hazarding warnings, and the difference is that they are static nodes. Therefore, we can assume that their resources are more important than the vehicles' and that additional backup mechanisms are implemented to increase their availability and make their logs resilient to data loss and component failures.
- The Administration nodes (ANs). Lastly, the Administration nodes perform the deployment of the blockchain before runtime and ensure the auditing process. It is the authority entitled to query the network regarding one specific event and request that sensitive data be released for further investigations.

C. `newDEN` Messages

The frame of a DENM, as standardized by ETSI in [2], is divided into 16 blocks of different sizes to result in a at least 40-byte-long message. The header container is 8-byte-long and contains the protocol version. It also contains a message ID associated to each DENM, and a timestamp. The management container is 14-byte-long. It specifies the identifier of the ITS station that broadcast the DENM, and a sequence number, unique to the event being reported. The field 'data version' indicates an update of the situation (e.g., 255 is for cancellation of the event). The 'expiry time' sets a timestamp after which the event is obsolete. The 'frequency' value defines the transmission frequency of the DENM, and

the 'reliability' represents the probability for the event information to be true. Lastly, the boolean 'isNegation' confirms or not the existence of the event. In the Decentralized Situation container, we find three bytes related to the situation itself. More specifically, the 'CauseCode' identifies the event direct cause according to a predetermined table of referenced values; the 'SubCauseCode' provides additional information; and the 'severity' value evaluates the seriousness of the event. Finally, the Decentralized Situation Location container provides geographical information about the event, including its latitude, its longitude and altitude. It also precises the accuracy of the position in the field 'accuracy' and can provide more details.

As mentioned in the previous section, the ITS messages already contain the necessary information of location, timestamp, and event unique identifiers. In addition, the payload contains identifying information in the `StationID` field. We argue that applying an anonymous authentication scheme on top the current structure of DENMs will not have the desired effect to protect the anonymity of the users. Instead, we suggest to modify the structure of the DENM itself by replacing the `StationID` field by a group signature issued by the reporting ITS station. A modified version of the DENM structure is therefore proposed in Figure 1.

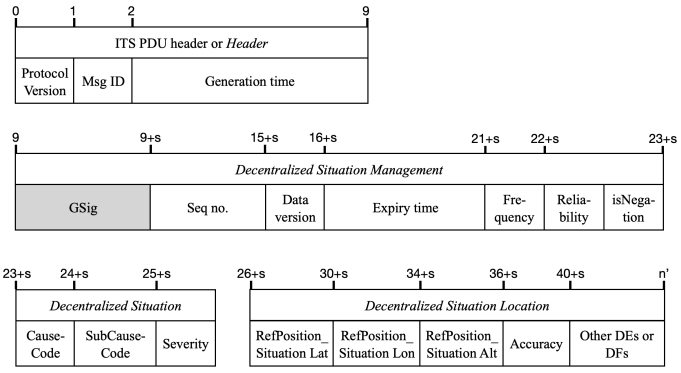

Fig. 1. Detailed newDEN

D. Security requirements

From the traditional security requirements applicable to anonymous authentication schemes in ITSs and the desired properties mentioned in Sub-section III-C, we have drawn the following security definitions for the proposed BEAT-Traffic reporting service based on the `newDEN` message construction.

a) Privacy-preservation.: Let $\mathcal{M}$ be $(m_1, ..., m_k)$ be a list of k broadcast `newDEN` messages such that exactly 2 of them have been sent by the same node. The *privacy-preservation* property requires that no Probabilistic Polynomial Time (PPT) adversary $\mathcal{A}$, with the knowledge that the same user broadcast exactly two messages, can guess which messages with non- negligible (in λ the security parameter) advantage.

b) Valid `newDEN` message.: A `newDEN` message is said to be *valid* if and only if all the fields inherited from the initial DENM satisfy the original requirements **AND** the $GSig$ value is correct.

c) Accountability.: Let m_0 be a broadcast `newDEN` message. The *accountability* property requires that no PPT adversary $\mathcal{A}$ can generate a valid m_0 which does not link to its identity with non negligible (in λ the security parameter) advantage.

d) Service Censorship-resistance.: Let $P_1, ..., P_N$ be $N \geq 3$ nodes constituting the network that proposes a service S, and let $\mathcal{A}$ be an adversary that can compromise t nodes in the system (without loss of generality, we consider that the corrupted parties are $P_{N-t}, ..., P_N$). The *censorship-resistance* property guarantees that there exists $r < N - t$ such that $P_1, ..., P_r$ can still provide S.

VI. Our approach

In the following section, we introduce a layered overview of the ITS and integrate our blockchain-based architecture for the support of a traffic reporting mechanism that complies with the security requirements listed in Sub-section V-D.

A. Data collection

a) Smart contracts.: In our system, the Infrastructure nodes (RSUs) and Vehicles nodes maintain together a shared and synchronized database that is distributed across the vehicular network, namely a blockchain, which supports smart contract programming. There are five contracts in our solution:

- the EA contract (Enrollment Authority): any RSU that wants to become a blockchain node and subsequently be called to participate as a sub-authority for new vehicle/RSU nodes. As such, it may play the role of an sub-auditor (*i.e.* participate in revealing the identity of a faulty/maliciously behaving peer) and/or a sub-enroller node (*i.e.* participate to the enrollment process of a new node).
- the AA contract (Auditor Authority): this contract is used to create a distributed auditor authority. Behind this role, the contract enables the generation of the distributed Opening authority which is involved when reports have been issued and someone has to be revealed.
- the Registration contract: is used for vehicle nodes to join the service and benefit from the security properties it brings; they register themselves towards a EA node.
- the Reporting contract: it is the contract by which Vehicle nodes can issue and log the transactions associated with the broadcast of `newDEN` messages.
- Finally, the Auditing contract: which tracks all audit requests and subsequently releases the requested information.

We will show in the following section how these contracts are used to broadcast information by describing a simple scenario.

B. A layered overview

There are three phases in the workflow execution. The first phase relates to the secure bootstrapping of the distributed authorities. The second phase presents the use of the infrastructure with the `newDEN` messaging protocol and the

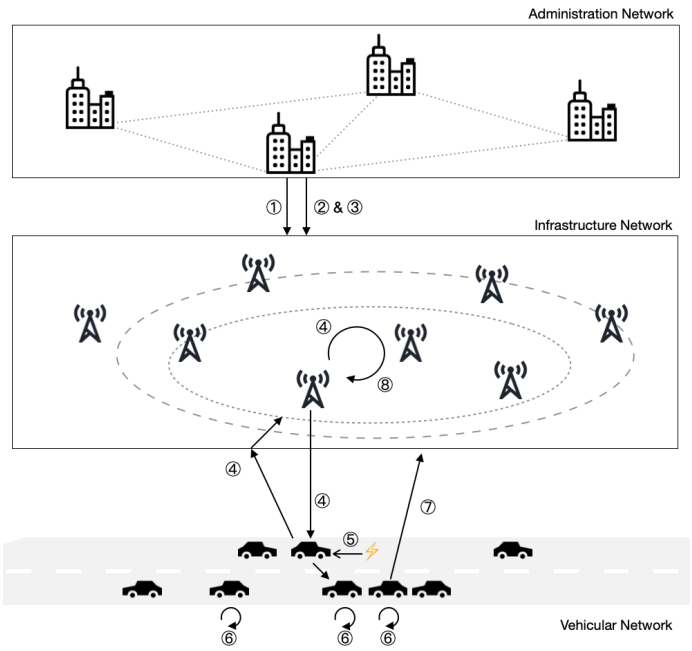

Fig. 2. A top-down description of the proposed framework and workflow

construction of the blockchain-based Traffic Reporting system. The third one relates to the auditing actions.

Figure 2 illustrates a top-down description of the proposed framework. Each step, from ① through ⑧ , is detailed in the following paragraphs. The description discusses the secure distributed bootstrapping of the Infrastructure and the life of the network in providing the Traffic reporting service.

The setup of the infrastructure consists in the following steps: the registration of the RSUs in the blockchain network ① , the establishment of the Opening/Auditing authority ② and the Issuing/Enrollment authority ③. After this bootstrapping, the vehicles can registrer as group members ④ so that they can protect their anonymity in further communications. Then, they can use the system to anonymously report road hazardous events. This reporting protocol consists in: the generation, signing and broadcast of the `newDEN` messages ⑤ ; the reception the `newDEN` messages and verification of their validity ⑥. The usage of the Traffic Reporting service also defines the reporting of malicious events ⑧ and the distributed auditing of the associated signatures ⑦.

C. A scenario

In this section, we present the nominal workflow for the use of our BEAT-Traffic, Blockchain-Enabled Anonymous yet Traceable Traffic reporting service. Figure 2 illustrates the following explanation.

a) Phase 1 - Setting up the authorities: The initialization of our framework starts with the bootstrapping of the distributed authorities in the system. This is not a time-sensitive operation.

① **Bootstrap.** The protocol starts with a TTP identifying the RSUs that are authorized to participate to the construction of the ITS distributed authorities, namely the Enrollment and the Auditing authorities. This third party is of no importance and only considered for simplicity of speech. In the end, it might be replaced by any authorized user. Since we base our solution on blockchains, the selection of RSUs can be done on their reputation, the amount of stakes they own, etc. We consider that since RSUs are static entities, they can act as sub-authorities for the vehicles nodes. During the bootstrap, the TTP deploys the five aforementioned constracts (Subsection VI-A) and declares trusted N RSUs.

② **Enrollment Authority (EA) Setup.** The EA is in charge of registering new vehicle nodes that want to benefit from the proposed anonymous architecture. As such, they form a group of users, based on the pseudonym that was registred for them and that they will use when communicating. These users can issue signatures on behalf of the group, but cannot be directly identified as the signer. At a cryptographic level, the EA plays the role of the Issuer in group signature schemes [15]. In our case, the Issuer is a distributed entity. We achieve this property by leveraging a blockchain-based distributed key generation protocol [21], [22]. Each of the N selected RSUs engage in the protocol which outputs a public/private keypair where the public part is the EA public key denoted ipk (which stands for Issuer Public Key), and a set of (private) EA secret keys $isk_1, ..., isk_N$ s.t. the secret key isk corresponding to ipk is never reconstructed. Instead, it is obtained by combining the $isk_i{}_{i=1}^{N}$ ($isk = \sum_{i=1}^{N}$). At the end of the protocol, an event is broadcast which contains the list of RSU enrollers and the resulting enrolling public key ipk.

③ **Auditing Authority (AA) Setup.** Similarly to the previous step, the RSUs are also asked to engage in a second blockchain-based distributed key generation protocol in order to define the AA. The AA does not know who is in the group formed by the EA. Its role is to protect the pseudonym of the registered users. At a cryptographic level, the public key of the AA is used to make the group signatures, issued by one user, unlinkable. In the context of group signature, the AA plays the role of the Opener, the one that reveals the pseudonym. Then it gives this information to the Issuer for them to identify the user (e.g., via their canonical identifiers). At the end of this second execution of the protocol (which can be performed in parallel of the previous one), an event is broadcast which contains the list of RSU auditors and the fingerprint (the hash value) of the resulting auditing public key opk.

b) Phase 2 - Application: Now that the distributed authorities are setup, accessible and auditable via the blockchain records, the vehicle nodes can register and use the proposed Anonymous yet Traceable Traffic Reporting service which runs on top of the blockchain-based networking infrastructure.

④ **Vehicles' registration.** In previous registration processes, a vehicle V_i would interact with a single TTP to get its credentials certified. Now, the V_i can engage with any of the identified enrollers and its registration process is tracked via the Registration contract. At a cryptographic level, the vehicle uses a join/issue joint protocols to give its personal parameters to the nearest RSU. In parallel, it issues

a transaction via the Registration contract which logs and broadcasts a fingerprint of the same parameters. This double transmission has two advantages: firstly, V_i personal identifiers are transmitted privately to the EA via the contacted RSU and can only be accessed if all the enrollers collaborate; secondly, the publication and broadcast of a blockchain transaction logs the registration attempt and helps detecting malicious/faulty enrollers (if the delay of registration is too long), and modification attacks (whether in between the vehicle and the RSU, or between the contacted RSU and other enrollers). The enrollers collaborate to decrypt the registration request and further processing. Then, one of them is randomly selected to certify V_i's temporary credentials, and sends the user its certificate and the AA's parameters. In parallel, the enroller logs its actions in the blockchain. Upon reception, thanks to the blockchain records, the user can check the validity of the transmitted data.

⑤ & ⑥ **Reporting Road Hazard events.** Once the registration phase is completed, the registered vehicles can use the `newDEN` messages. Indeed, steps ① to ③ are only about setting up distributed authorities for the group signature scheme. Instead of relying on one Opener and one Issuer, the combination of the blockchain and the distributed key generation protocol enabled us to build secure and transparent EA and AA. Thus, the $GSig$ signatures used in the `newDEN` messages can be verified the same way as the underlying group signature scheme.

c) Phase 3 - Exposing fake news and malicious nodes ⑦ & ⑧: In addition to enabling the anonymous-yet-traceable traffic reporting, the distributed and transparent nature of blockchains can be leverage to identify fake news and malicious entities.

When a fake message is suspected, any node can issue an audit request via the Auditing contract. It sends the suspected message, its identity to the Auditing contract. An event is emitted for further processing. This triggers calls to the EA and AA contracts which can jointly de-anonymize the signer.

Conclusion: We cannot log all the communication inside the blockchain for several reasons including the scalability (cost to store all this information)and security(private keys). In this work, we use the blockchain as a distributed platform for integrity checks: on data via traditional integrity checks with hashes, and entities by logging the activities of each enroller and vehicles. This is feasible due to the transparent, public and distributed nature of blockchains. With use distributed cryptographic tools such as group signature schemes as an overlay of anonymity and traceability. Here again, the blockchain enable us to monitor the "legitimacy" of selected authority nodes and thus bootstrap a distributed system without relying on any trusted party (which is only mentioned to select entities).

VII. Arguments of security

In this section, we present the security arguments that show how the proposed BEAT-Traffic service complies with the security requirements described in Sub-section V-D.

a) Privacy-preservation: When considering the `newDEN` messages, the anonymity of the reporting vehicle nodes boils down to the anonymity of the $GSig$ field. Thus, the privacy-preservation property is guaranteed by the use of a secure group signature scheme as described by [15].

b) Valid `newDEN` message: Similarly, proving the validity of a `newDEN` message returns to proving that the $GSig$ field is correct which is again guaranteed by the use of a secure group signature scheme.

c) Accountability: Let us consider that a PPT adversary $\mathcal{A}$ can generate a valid `newDEN` m_0 which does not link to its identity. As such, the adversary is able to produce a $GSig$ value that breaches the traceability property of group signatures. This is not possible since we are considering the use of a secure group signature scheme.

d) Service Censorship-resistance: Let us consider a PPT adversary $\mathcal{A}$ that corrupted t enroller nodes in the system (without loss of generality, we consider that the corrupted enroller nodes are $P_{N-t}, ..., P_N$). We assume that all enroller nodes have the same decisional power in the EA. As long as $t < 1/2 \times N$, there exists a majority of uncorrupted enroller nodes. As such, the blockchain's inherent properties guarantees that there exists $r < N - t$ enroller nodes such that $P_1, ..., P_r$ can still register vehicle nodes.

The same reasoning can be applied to the auditor nodes. Thus, the use of blockchain guarantees the service censorship-resistance and ensures that EA and AA still operate under Sybil attacks when the Sybil nodes are in inferior number.

VIII. Comparison with other works

Through theoretical analysis, we obtain a comparison Table I between the three schemes analyzed and our scheme. From a theoretical point of view, our scheme provides the same security services as those of the best popular references but at the expense of lower trust assumptions. Indeed, we do not consider a trusted infrastructure nor do we rely on a trusted tracing authority. Instead, we acknowledged that RSUs can be corrupted and assumed that at least a threshold number of them $t < N/2$, where N is the number of selected RSUs in the system, is dishonest. In addition, we opted for total distribution of the powerful authorities namely the Enrollment Authority and the Auditing Authority as well. While references [16] and [19] focus on the CAMs, we target the DENMs which are bigger in size and contain the personal identifiers of their origins.

TABLE I
SECURITY SERVICES AND TRUST ASSUMPTIONS - A COMPARATIVE TABLE WITH THE REFERENCED SCHEMES *(MA: Message Authentication, CA: Conditional Anonymity, TA: Trusted Authority, TI: Trusted Infrastructure, $|m|$: size of the safety message in bytes, $|\sigma|$: size of the signature in bytes)*

Ref	MA	CA	TA	TI	Type	$\lvert m \rvert$	$\lvert \sigma \rvert$
[16]	●	●	One	Yes	CAM	474	368
[19]	●	●	One	Yes	CAM	72	56
[20]	●	●	One	Yes	unknown	935	826
Our	●	●	> 1	Threshold t	DENM	200	160 [KLAP20]

We demonstrated in this paper that our proposition theoretically improves on the referenced schemes. Yet, we need to evaluate the impact of changing the structure of the

newDEN messages and determine which group signature fits best in our model. There were several candidates. Considering the performance and security aspects of group signature schemes, we think that KLAP20 [23] is quite interesting: smallest signature size, fastest signing, verifying and batch verifying processes. In addition, it provides the opening soundness by which the auditing process can always find the user as the owner of a valid signature. Yet, additional work on the implementation and evaluation of the proposition must be done to validate this hypothesis about the viability of a KLAP20-based Traffic Reporting system.

IX. Conclusion

In this paper, we have presented BEAT-Traffic, a solution to improve the sharing of sensitive data over ITS using blockchains and distributed cryptography. We have demonstrated how our proposed solution can be applied to the reporting of Road Hazard Warnings, creating a blockchain-based data collection service that ensures the dissemination and security of reported messages. Our results demonstrate the potential of blockchain-based solutions for addressing the challenges of secure and efficient information sharing in ITS. We believe that our work will contribute to the development of secure and privacy-preserving ITS systems, and encourage further exploration of blockchain-based solutions in the field of intelligent transportation.

However, there are some challenges to tackle in implementing our proposed blockchain-based solution for secure and efficient information sharing in ITS. These challenges include issues related to scalability, interoperability, and regulatory compliance. While our approach has shown promising theoretical results in ensuring privacy preservation and censorship resistance, further research is needed to address these challenges and ensure the practical feasibility of our solution. In particular, the next steps in this research involve conducting simulations to validate the proposed solution's efficacy and further testing it with real-world data to ensure its applicability in practical settings. These measures will help improve the system's accuracy and reliability. Moreover, we plan on exploring several scalability mechanisms, such as sharding, off-chain solutions like sidechains, and consensus algorithms with improved efficiency like the proof-of-stake.

In addition, the adoption of blockchain technology in the transportation industry requires collaboration and standardization across different stakeholders, including government regulators, car manufacturers, and transportation service providers. Despite these challenges, we believe that the potential benefits of blockchain-based solutions in ITS, such as improved road safety and efficiency, make it an exciting and promising area for future research and development.

Acknowledgement

References

[1] "ETSI TS 102 637-2 V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," standard, European Telecommunications Standards Institute, Mar. 2011.

[2] "ETSI TS 102 637-3 V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," standard, European Telecommunications Standards Institute, Sept. 2010.

[3] C. Miller, "Lessons learned from hacking a car," *IEEE Design & Test*, vol. 36, no. 6, pp. 7–9, 2019.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, p. 21260, 2008.

[5] V. Kumar, S. Mishra, N. Chand, *et al.*, "Applications of vanets: present & future," *Communications and Network*, vol. 5, no. 01, p. 12, 2013.

[6] "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.

[7] "ETSI TR 102 638 V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," standard, European Telecommunications Standards Institute, June 2009.

[8] "ETSI TS 102 940 V2.1.1 - Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2," standard, European Telecommunications Standards Institute, July 2021.

[9] M. M. Queiroz, R. Telles, and S. H. Bonilla, "Blockchain and supply chain management integration: a systematic review of the literature," *Supply chain management: An international journal*, vol. 25, no. 2, pp. 241–254, 2020.

[10] M. Alves, J. V. D'Aiguebonne, T. Gateau, and J. Lacan, "Blockchain-enabled redundant fractionated spacecraft system," in *2022 IEEE Aerospace Conference (AERO)*, pp. 1–13, IEEE, 2022.

[11] M. D. Clementi, N. Larrieu, E. Lochin, M. A. Kaafar, and H. Asghar, "When air traffic management meets blockchain technology: a blockchain-based concept for securing the sharing of flight data," in *2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, pp. 1–10, Ieee, 2019.

[12] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," in *Healthcare*, vol. 7, p. 56, MDPI, 2019.

[13] M. T. de Oliveira, L. H. Reis, D. S. Medeiros, R. C. Carrano, S. D. Olabarriaga, and D. M. Mattos, "Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications," *Computer Networks*, vol. 179, p. 107367, 2020.

[14] H. Wang, H. Qin, M. Zhao, X. Wei, H. Shen, and W. Susilo, "Blockchain-based fair payment smart contract for public cloud storage auditing," *Information Sciences*, vol. 519, pp. 348–362, 2020.

[15] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," in *Topics in Cryptology–CT-RSA 2005, San Francisco, CA, USA*, pp. 136–153, Springer, 2005.

[16] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2009.

[17] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)$\ll$ cost (signature)+ cost (encryption)," in *Annual international cryptology conference*, pp. 165–179, Springer, 1997.

[18] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical short signature batch verification," in *Cryptographers' Track at the RSA Conference*, pp. 309–324, Springer, 2009.

[19] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy-preserving authentication based on group signature for vanets," in *2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 4609–4614, IEEE, 2013.

[20] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for vanets," *IEEE Transactions on vehicular technology*, vol. 65, no. 3, pp. 1711–1720, 2015.

[21] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," in *Advances in Cryptology—EUROCRYPT'99, Prague, Czech Republic*, pp. 295–310, Springer, 1999.

[22] P. Schindler, A. Judmayer, N. Stifter, and E. Weippl, "Ethdkg: Distributed key generation with ethereum smart contracts," *Cryptology ePrint Archive*, 2019.

[23] H. Kim, Y. Lee, M. Abdalla, and J. H. Park, "Practical dynamic group signature with efficient concurrent joins and batch verifications," *Journal of information security and applications*, vol. 63, p. 103003, 2021.