Blockchain-based Data Integrity Verification for Autonomous Vehicle Telemetry

By Dr. Marc Hansenne

Professor of Geomatics Engineering, Université Laval, Canada

1. Introduction

The idea of applying blockchain-based approaches in data exchange applications like this has already been shown to be feasible. Results presented in these papers show that blockchain technologies have great potential to be a security and privacy-preserving environment for IoT data. One of the main advantages of a blockchain compared to a centralized server is its ability to verify the correctness, authenticity, and integrity of provided data without the need to trust any intermediary. This exactly fits autonomous driving, which poses strict challenges to data protection requirements regarding data integrity and provenance. This study focuses on dealing with the problem above by introducing a way how to ensure data integrity and provenance in the context of autonomous vehicle telemetry by deploying DLT-based data integrity verification methods [1].

Blockchain technology offers novel solutions for a variety of challenges in the Internet of Things (IoT) and vehicular networks. These technologies can be used for data sharing applications, trust-based systems, security solutions, autonomous vehicle operations, etc. Several previous studies demonstrated the applicability of blockchain technologies (including smart contracts, consortium blockchains, etc.) within vehicular ad-hoc networks. Autonomous vehicles' value-creation depends on access to trustworthy data which includes process, telemetry observations, and various context information that is being automatically collected by infrastructure components like sensors and hardware required for autonomous driving. The introduction of autonomous vehicles into our environment hence requires new requirements for data management systems which ensure trustworthy data collection, processing, exchange and storage. Additionally, autonomous vehicles and all related systems must be aware of privacy considerations. Trustworthy and privacy-preserving data exchange

approaches with autonomy-relevant information in general and autonomous vehicle telemetry in particular are currently not sufficiently addressed [2].

1.1. Background and Motivation

Ontology is a platform for building various decentralized data applications which leverages blockchain technology; it can be applied in a number of industries: insurance, medical, and financial, among others. Obstruction, the future application of Ontology in autonomous vehicles, has the potential for integrating data from all adjacent IoT nodes on one platform. This data will act as an imperative element for autonomous vehicles in road traffic and control [3]. Blockchain technology has revealed its potential benefits in the automotive, aviation, and naval fields and achieved the good results in the fields of connected and autonomous vehicles (CAV), vehicle networks, vehicle marketing systems and as backbone protection architecture for unmanned aerial vehicles (UAVs). The goal of these projects are to strengthen vehicle network projects at high confidentiality, penetration testing, data sharing, and end-to-end authentication and accountability. Furthermore, some projects mentioned above enable a secured data sharing platform among several or unlimited devices. However, every device must submit data in an undivided data pool on a cumulative server, which may be hacked by malicious users with the help of distributed denial of service (DDoS) attacks, assuming that alarms/warnings are illustrative.

Blockchain technology, which has revolutionized the economy via its decentralized and tamper-proof data log, promises potential upgrades to some security and privacy concerns in sectors ranging from connected vehicles and Internet of Things to healthcare and retail [4]. Blockchain-based networks ensure tamper resistance, data correctness, and security. Despite being an attractive solution, plugging into the blockchain ecosystem introduces a new set of challenges such as scalability and interoperability, latency, and energy consumption. Autonomous vehicles, which leverage a broad spectrum of IoT ecosystems, would perhaps intensify these challenges.

1.2. Research Objectives

[5] In summary, autonomous vehicles generate and consume a large amount of data, from both in-vehicle and external sensors, and also as outputs from the autonomous vehicle control algorithms. However, this data is currently used for real-time vehicle and traffic management

or post-exploration for research purposes only. To enhance autonomous vehicles' normal and complex situational awareness performance, all these data types should be utilised, integrated into a unified spatial and temporal structured environment, and made publicly available for providing feedback to retrain the digital twinning model. The research aims to build an autonomous vehicle data-driven (AVDD) framework using blockchain-based service cooperation for providing more advanced decision-making services for both autonomous and non-autonomous vehicles.[6] Some of the unique features of blockchain like its immutability and distributed structure make it an ideal candidate for maintaining the integrity of such datasets. At present, leading manufacturers like IBM, Google and Apple, along with many auto-mobility researchers, are extensively researching the capabilities of blockchain. This system is beneficial to solve the data challenges faced by autonomous vehicles, where a centralised database becomes a single point of failure, an open system undermines client privacy, and a federated learning system may not be completely trustworthy. In conclusion, a system that is a blend of these aforementioned evolution strategies would be the most effective for facilitating large-scale coordinated vehicular data acquisition and consumption.

1.3. Scope and Limitations

[7] The research at hand pays particular attention to blockchain-based strategies for connected and autonomous vehicle communication, as they promise improvements in trust and security aspects. To date, numerous blockchain technologies have been successfully adopted in various applications, reaping the benefits of the mature and proven blockchain structure. Examples include traffic participant identification, vehicle service management, and establishing smart contracts. Blockchain enables tamper-resistant data history management in modern, data-rich services (like the automotive industry) and, thus, it promotes trust in these services. This work expands upon previous research by utilising these capabilities and the corresponding implementations, while examining parts of the message stream between connected vehicles and a common transport service provider (TSP).[8] The implemented blockchain system is then used to store and manage data from conducted communication, specifically maintaining the data integrity and seamless verification of all transmitted real-time data. To achieve this goal, messages exchanged between vehicles, as well as data collected from various sources (like edge devices or IoT sensors) are transmitted using a modified connected and autonomous vehicle (CAV) environment and recorded on the blockchain structure. Once a message or other interest arrives at the transport service provider

or another node considered to be trusted, the blockchain structure is used to verify the order of newly incoming data messages by looking into previous records and the chronological order of blocks and transactions, alike. Given the use of blockchain technology, the data recorded from specific vehicles at a specific time not only cannot be the subject of any malicious actions (like deletion, tampering, etc.) after the fact (post facto), but all users may call upon this stored history and validate the real-time data.

2. Autonomous Vehicles and Telemetry

Certain characteristics of telemetry architecture, including execution of data flow from sensor(s), non-volatile data collection(s), data processing and decision-making adoption support autonomous vehicle applications. In most current architectures, the data from each sensor and module are processed and analysed to decide accordingly, as part of functionality, integration and cross-correlation in core modules such as vehicle localization, navigation, driver intention, sensor fusion, path planning, and motion control. An example in Action Module making SCB decision is shown in. The IC2 interface between sensors and CH3 Controller to receive the readings and transmit to host module, i.e., Linux Core Module (LCM) is referred to backbone operation in AV. The parameters obtained from sensors are stored and retrieved using the logger module located in the LinuxCore. Therefore, the traditional telemetry system in the autonomous navigation car monitoring infrastructure is a complex island plus cloud architecture. It required the ease of proactive actions and real-time accessibility assurance [1].

A key area of vehicle telematics is the Autonomous Vehicle (AV) segment, which is expected to grow at a much faster rate as the level of autonomy in conventional vehicles increases in the near future [9]. It is well-known that vehicles operating in autonomous mode do not receive human intervention and need multi-modular technologies to make decisions and act accordingly. Telemetry, therefore, plays a significant role in AVs. However, the storage and accessibility of telemetry data, are typical issues that blockchain can address [8].

2.1. Overview of Autonomous Vehicles

In this literature we propose a Decentralized Ecosystem of Autonomous Vehicles—VERITAS dialect, internalizing a hybrid Blockchain based PoW-PoA consensus model. This will be the main scenario with MANET networks containing moving entities and NOignet clusters.

While performing decentralization, we will deeply minimize the burden for involved primary Dynamic Vehicle Telemetry vendors. AV telemetry data must be 100% authentic, accurate, precise and anonymous with high level of Privacy Security to protect AV, Driver, and Public Safety, as per Article 18, Article 6(1f) of GDPR, 2012, Preliminary. Only unmodified & finally authenticated data from AVs can produce the "the best of the best"- for at-the-moment situation awareness and data integrity feature for automatic reactions within critical milliseconds in real time scenario in AV. The official data from Vendors must have the even longer retention time if required by Legal or if caught in Supervisory Activities during their existence track. Other novelties we will deploy, are: Global Network of Hub-Cores to coordinate Fast hybrid BlockChain for MAP vendors, Indexers and Dynamic Vendors. This global network of indexers will capture and donate AV data for free for securing the best Map and Extended OSM. The DIMS will be a part of an Information Provenance feature. Each event type of the Meta, concerning the DIMs in the BlockChain, is a successive level of the Event Logging with all the needed information, for use by all stakeholders [10].

The increasing use of autonomous vehicles (AVs) in smart transportation has made driverless systems the new trend. This chapter gives an overview of smart transportation and focuses on the autonomous vehicle network and related technologies, specifically with respect to the impact of transmission data management on the collection and verification of autonomous vehicle telemetry. If we can trust the data from AVs and roads, we can provide much more accurate and reliable transportation, with the potential to save many lives by the prevention of road traffic injuries or fatalities. However, the current framework of transportation has a fundamental problem in that we can hardly find information on the origin and the real ownership of the incoming data. This directly causes us to heavily rely on only one source of proprietary data from big AV companies, which can actually even be faked or manipulated [11].

2.2. Telemetry in Autonomous Vehicles

One solution for dealing with such issues is to use blockchain as a solution. AV telemetry can be transformed into a shared ledger that leverages blockchain, where manufacturers can then use the data on the ledger for product improvement. Additionally, all smart contracts are developed on the basis of different blockchain platforms like Hyperledger, i.e., Ethereum or

Proof of Work (PoW) [12]. Finally, a basic architecture of AV telemetry using blockchain has been conceptualized to provide the practice of the proposed approach.

Blockchain technology has been introduced to various industries, such as the distributed energy trading market [13], supply chain market, and IoV market with the proliferation of autonomous vehicles (AVs) [14]. In the future, AVs are expected to drive without human intervention and become intelligent ―goal-seeking‖ system by taking advantage of artificial intelligence. Communication and interaction with the physical environment via various sensors and other connected AVs, known as vehicle-to-everything (V2X) communication. The majority of V2X communication is operated based on cloud servers. As a result, access control, data integrity, authentication, and privacy of the shared data may be a future security issue.

3. Blockchain Technology

On the other hand, if the gradual continuous operation of the miner node data and density information is recorded on the blockchain, the central control strategy can be used to calculate the risk dropping greatly because of the voting mode. Notably, under the scenario of smart transportation, it is difficult to use smart contracts to model the subtle connection between the participants. This means that with different vehicle manufacturers, different control networks and even the accelerator pedal will be implemented differently and need to be re-established as different contracts. Secondly, the current empirical car networks operate under typical IP-based network mode, and the balance between security, expandability and computational efficiency still needs to be considered carefully in the future. The best design solution helps to solve the problem of easily changing dynamic IP addresses with DID identifier technology, which is not yet widely used in the world [5].

Blockchain technology is used to ensure secure and trusted transactions between participants without centralized trust third party. In contrast to traditional centralized authentication mechanisms, a process called mining is introduced for obtaining and verifying blocks. Mining transaction blocks are to verify the legitimacy of a block whose data carries sufficient computational rankings. When a block is found to terminate, the transactions contained in the Miner will receive legal and effective authorization, and the receiver instantly knows its block has been packaged. Compared with traditional centralized networks, the deployment of blockchain can be a good fit with the decentralization of the structure. For instance, in the Internet of Things (IoT) network designed for remote monitoring of intelligent monitoring

driver health, the recorded data format is generally different from vehicle to vehicle, even if the same telematics adapter is used [10].

3.1. Fundamentals of Blockchain

Blockchain technology can be used for enhancing coherence between entities involved in the VANET. In VANET, we can make use of secure and reliable V2V communication, which can also be done in blockchain communication by ensuring end-to-end security. This communication of other vehicles' safety related information such as camphor and break application, speed of the automobile tires and so on increases the network delay, load and decreases communication reliability. By introducing blockchain communication, these data can be exchanged in a secure and reliable manner between vehicles with confidentiality also along with the cooperative traffic light control [12]. The surveyed papers also show that a number of frameworks and models has been adopted by researchers for test bed setup like omnet++ framework with the veins and sumo module for VANET test bed set-up, likewise internet of vehicle and social internet of vehicle have been employed with the federal learning and blockchain that is one of the best known Internet of things deployment and has become an integral part in the new generation of the internet in the IOT based VANET.

Blockchain technology can address issues in the transport industry such as, for example, the alteration of driving and traffic information by providing secure, transparent, and traceable data between moving vehicles in the vehicular ad-hoc network (VANET) [15]. Due to the tamper-resistant grade, the information which has been sent by a vehicle will remain unchanged during the entire communication broadcast event. This technology will ensure the security of the data and increase the speed of data processing simultaneously. By adopting the blockchain technology, other vehicles can obtain transmission and reception information easily. Blockchain can be used further in the transport industry in three main areas: security, decentralization, and reduced data-file size. The 5G-BLS tool integrates blockchain with select algorithms to mindful of efficient resource and energy usage in the network applicable to this transportation and communication use case. The results show the potential applicability of the 5G-BLS framework in the telecommunications and transportation sectors.

3.2. Key Features for Data Integrity Verification

Efficient metrics and techniques for evaluating suppliers intending to convey capabilities and contributions on a continuous basis should be proposed in the partnership strategies. Furthermore, in some incentives, stakeholders are awarded based on sustained performance or achieving specific predetermined targets. If an IE report is classified as a genuine member of target TE, then an approved certificate will be issued. However, for first-time holders of IE report, the information about telation is missing, which means that the IE report perhaps could belong to the TE labeled by AEs. Moving forward, the proposed E-gHas-IIR training process considers complex scenarios of data preprocessing. The majority of masking (8/64) and filter over writing (11/64) jobs were significantly affected by adding various noise perturbations on the MNIST data samples.

Comprehensive research on the challenges arising from asynchronous and multi-attribute features between the ART and BDI calls [16] is still in its infancy, especially for data integrity verification. This method was introduced by S. Wang (2019) for BDI-ART communication with synchronous attributes. In such a way, the supply of ART must either be diminished to BD or extended to the full size of BDI. Moreover, the competition between foreground and background data brought a lot of errors to mapping BDI to the ART. In such an uncomplicated cooperation, preparing five different hasse-dilations to acquire all needed attribute sets caused redundant attribute set generation. Additionally, a bilattice suffers from the problems faced in both of its association bilattices.

4. Integration of Blockchain in Telemetry Systems

After the overview given in Section 2, in this section we will synthesise investigations where blockchain technology has been implemented in telemetry solutions for AVs and other advanced road users to monitor the authenticity of data during a cooperative event. The following five sections will provide a full investigation of automotive technological aspects in AV design. Therefore, these sections must be interconnected and their reliance must be presented for coherent results [10].

Junaid et al. (2020) introduce a blockchain framework for securing connected and autonomous vehicles (CAVs) through the use of secure decentralized identifiers, parties that offer different services, and perform transactions that are then resolute in a blockchain-based ledger. They also provide specifics of the creation, transmission, and registration of the data in the blockchain through the Ethereum and Hyperledger Fabric platform. On the other hand,

authors in Fatima et al. (2020) propose VINCy, a tool with a community exploring automated vehicle integrity using an Ethereum blockchain. They include external data structures and oracle systems in smart contracts for ensuring data integrity in the blockchain and at runtime for cryptographic purposes. The SHA-256, RIPEMD-160, ECC signature scheme, and an honest chain derived are used to verify data consistency in VINCy. And, two-layer blockchain security mechanisms ensure the trustworthiness of data collection and information exchange.

Several approaches have been proposed for integrating blockchain in autonomous vehicles (AVs). Furthermore, blockchain technology can be integrated with a vehicle to ensure maintenance, safety, and quality control in the automotive industry. In conclusion, blockchain technology, while not yet fully mature enough to be easily implemented into AVs, is likely the most practical solution for maintaining data integrity with limited latency in the future of vehicular networks (Bornschein et al., 2018).

4.1. Challenges and Solutions

Working of the autonomous vehicle depends on the data coming from all sources and being integrated by the on-board ECU. To attain high quality of the control decisions, an autonomous vehicle critically relies on physical parameters such as vehicle speed, ambient temperature, acceleration, GPS location, and motion sensors readings. This information is utmost crucial for manual and automated vehicle diagnosis but can be largely manipulated as it is rec- orded on-board before showing to a remote server. As a result of this, results based on these parameters can be manipulated for denial of a claim, can lead to extensive vehicle damage, and can be a cost significant setup for factual and operational data in judiciary. Hence, it is inevitable to ensure the integrity and credibility assurance of the on-board ecological, operational, and infotainment telemetry.

In this subsection, we discuss various challenges w.r.t anonymous and real-time verification of autonomous vehicle telemetry and their solutions [ref: 44913a0a-a000-4d12-857c-62b623743918,ref: d3af00e5-a5c5-4572-83fa-bde636991191,ref: 9e83d226-f25e-4fde-837c-dbeddfb03c36]. The presence of anonymized crypto- identity of autonomous vehicles and non-persistent connectivity that makes the offline verification of data integrity and credibility of a remote data-source a challenging problem to address. Contrary to traditional online verification, in which connected verifiers can externally verify received data, we need to perform a similar verification process in an offline manner embracing the properties of an

automated vehicle context (vehicular ad-hoc network). Hence, the proposed approach should be lightweight, and work in non-persistent communication and semi-trusted networ- king. Moreover, the reasoning of credibility and integrity of the telemetry need to be computationally easy and efficient in order to work in continuous interactive contexts.

5. Case Studies and Applications

When combined with several other complementing technologies such as the Internet of Things, it can create a trustable integrated ecosystem for the future last-mile delivery systems utilizing Unmanned Aerial Vehicles and autonomous ground vehicles which, in case of COVID-like disaster situations, could prove to be an asset in functioning discontinuous supply chains. IoT can host the data sensors from the vehicles of the last-mile ecosystem system and once the interaction of such data with blockchain is secured a reliable and trustable environment is known resulting in blockchain-enabled intelligent contract storage. In such systems, if the data flow is secured with blockchain technology for only authorized stakeholders, it could result in a demand-driven and autonomously functioning logistic network with decentralized transactions making use of data readily available in the ecosystem. Such technology could be helpful in structuring a trustable decentralized environment that could be used to provide real-time data-driven solutions adhering to the demand of the current partial stakes in real-time. Also, this technology is especially useful while individual and personalized route optimization problems are involved.

Blockchain has several benefits in assuring the trustworthiness of a vehicle's telemetry data by means of formulating a transparent and decentralized environment for both intransigent and transient stakeholders in a vehicular ecosystem. Technology companies like IBM, and consortia like the Mobility Open Blockchain Initiative have signaled the importance of blockchain in creating an open platform to facilitate mobility services including autonomous vehicles. In fact, 82.5% of the global automotive executives agreed that blockchain has the potential to disrupt the auto industry by providing greater transparency in multiple functional areas of the car ecosystem. Blockchain is the perfect technology to establish the provenance of the data that is spatially and temporally available in the ecosystem originating from the multitude of vehicles and connected objects in the ecosystem. This includes data such as geographical location, acceleration, and deceleration of the vehicle, air quality data, and speed and temperature data.

5.1. Real-world Implementations

Until this step in adoption of DLTs and Blockchain in V2X communication systems and other applications [17], using completely public Blockchain systems with open participation would not only strengthen proof-of-trust and proofof-authorship (1) privacy properties, but it would waste too much energy, slow down the Globalpoint Ledger system, and introduce unnecessary risks (e.g. block re-organizations and confidentiality leakages via shared linkability attacks). (2) Our proposed model needs a trustworthy PKI to work and pre-existing certificate authorities mostly should not be trusted. One-thread-based cryptographic credentials as improvements to DSRC certificates current mechanisms — which we learned to be barely secure — were proposed long ago but have not worked so far. This is why it is important that standards like the ETSI EN 302 663 (3) CC and AS version 1.5.4 — that we have been closely following since its inception — should be immediately updated to leverage decentralized ledgers, offer a transport layer security (TLS) backed by its proposed decentralized BCP (++), Digital Logbook, V2X short-term device credentials (@, ++), and a desired privacy-preserving CBCC solution.

[4] Leveraging Blockchain-enhanced trusted and tamper-proof data exchange and validation is only the very first step that should make Autonomous Vehicles as well as Advanced Driver-assistance Systems more reliable and thus mature. This technology will enable receiving the same accurate and trustworthy telemetry data in real-world scenarios such as precise geographic location and time turtle data, as well as proving vehicle-to-everything (V2X) interactions and verifying take-over readiness warnings. Our scheme, however, can be instantiated in many other protocols and standards. After designing a gateway-friendly mechanism for integrations, future works should be focusing on broadening compatibility to many other blockchain platforms like Ethereum or Hyperledger tint, leveraging on-chain data-stores like Bitcoin's OP_RETURN field to further decrease transactions fees and to incorporate upgradable and generic smart contracts principles. This last step would be even more important to comply with, as V2X communication particles must comply with their respective standards. A tariff data-centric variant of our approach would be especially interesting as such central vehicle data stores as Ethereum without temporary data garbage collection capabilities are deemed unsuitable for data-heavy sensor data streams in general and real-time communication in particular [2].

6. Security and Privacy Considerations

Since it is a trust-based system, the implementation of Blockchain in IoV comes with several implications, like increased complexity for privacy and security matters. Each node in the blockchain network can see all blocks, since the ledger is public, but each block can be publicly transparent or partially encrypted. Public blockchain protocols solve the issue of double spend, but they expose the entire information. Each block without the first one is transitive observable, and a spying adversary can easily corrupt the content. In case of partially encrypted data in different fields of the block, post-quantum asymmetric algorithms can be applied with references stored in a beacon pool that could be any reference to a global hash value from a known block in the blockchain. The initial RSA Algorithm Application applies a SHA-3 hashing function over the private channel message and ECC over the encrypted symmetric AES-GCM key to compress the size of the encryption [10].

Blockchain technology is a decentralised and trust-based approach towards transmitting, protecting and sharing data. It can be beneficial for the future Internet of Vehicles (IoV) and Autonomous Vehicle Transportation, creating trust in telematic data and ensuring microtransactions for accessing it or for providing trusted and certified requests [17]. Telematic data about vehicle state updates, like sensors, actuators or trajectories, contain information that is enforceable and proactive in maintaining the integrity, provenance and consistency of various services like insurance, service and maintenance, smart cities and public and private transport. Blockchain can be applied in different contexts: from data provenance and integrity in Vehicle-to-Everything (V2X) communications, to data processing and collaborative learning in centralized or federated learning in decentralized environments [4].

6.1. Threats and Vulnerabilities

The pure proof of work (PoW) blockchains suffer from the 51% attacks. PoS is another consensus algorithm used in public blockchains that utilizes the proportion of cryptocurrency owned by a validator as a measure to decide who gets to create a new block. Thus, a vulnerability might exist with PoS employing the largest coin holder attacks. In the Delegated Proof of Stake (DPoS) protocol, nodes have delegated authorities to make decisions. This would hugely impact the distributive characteristic of blockchain. There is no option to compromise or delegate in PoW like mechanisms; proof of burn (PoB) and proof of capacity

(PoC) are two such algorithms. If the vehicle means to delegate the task, they could represent the possible solutions as far as a three-layer consensus model is concerned.

It is critical that future research and deployment clearly addresses these threats and vulnerabilities to ensure timely and widespread acceptance of blockchain applications by AV and users. These issues should prompt researchers to build blockchain architectures based on real operational requirements while ensuring high throughput, low latency, high security, and low costs [18]. GRT is one of the potential candidates acting as a transaction validator and distributor [19]. The main threat associated with an unreliable GRT is an inconsistency in transaction message propagation. During gossip messaging, the potential damage cannot strictly be monitored at the time of delivery, accelerating the occurrence of existential fraud. In addition, gossip communication may only reach part of the peers, leading to a portion of nodes lacking transaction data. This unexpected heavy network burden would impact reliability and performance [20].

6.2. Privacy-enhancing Techniques

To measure the privacy preserving on raw data, the following system could be utilized for evaluating the privacy-optimized. We consider the raw data as x and the noisy data as $x* = x+\eta$. Where, η means the noise with a parameter Δ is drawn from the Laplacian distribution, and $\eta \sim$ Laplacian $(0, \Delta)$. Here, y is the noisy response data. Thus, the linear equation measure for the ratio of jitter Δ vs. private data x can be accessed as $\eta = |F(x) - F(x*)| \|F(x)\|$ where F is the linear transform, L1 norm is measured as L1-norm$(||F(x)||) = \sum|| F(x)|$ as a vector norm. It can be seen that Δ is zero when y = F(x) that means the noise is not added for private data and the privacy measurement should be unity. For more specific measures of privacy, when all the parameters are designed, the simple open source tool, ePGD tool can be used to evaluate the privacy optimal.

To guarantee privacy protection, differential privacy has been applied to integrate noise into data instead of using cryptographic techniques [17]. Differential privacy could balance the tradeoff between privacy and data accuracy well, and thus is especially suitable for some applications to maintain the privacy as much as possible when guaranteeing the sufficient accuracy requirement of data. In this subsection, a brief case of noise addition is utilized to illustrate a possible scheme of protecting privacy for data-related process. In such a scenario, the raw data, or additional private data, is added by noise. The private data is used in

constructing each block during the blockchain constructing, and thus it could keep all the nodes' preference and requirement achieving all successful blocks but do not disclose the exact origins of data.

7. Performance Evaluation

A secure and device-to-device communication (V2V) network is created among the over-the-road (OTR) vehicles, and among OTR vehicle to the first, second and third emergency vehicle especially driving with the different speed (DS) point of view. The blockchain technology is also used among all the vehicles involved in a group of vehicles sharing the road at every point of time. The traffic on the roads rolls in clusters of vehicles waiting and moving with a possible speed of DS in a binary pointing DS direction across the roads and the tracks. The blockchain provides incredible speed and privacy at V2V communication level. It ensures privacy for first responders and provides a lot of information about the condition of the road at every point of time [21].

Blockchain-based Data Integrity Verification for Autonomous Vehicle Telemetry and Control The Blockchain technology is used in the transportation field to create secure and trusted information exchanging scenarios among the users without any security concerns. The blockchain technology is used in the vehicle acceleration and comfortable passenger ride, to create a safe and quick divorce of Algorithmic solutions of how to practically correct the data at the correct time on a blockchain aware vehicle operation, and hence immense safety. It achieves the solution by the secure data sharing applications for vehicles in ad-hoc or cooperative network scenarios using the blockchain technology [2].

7.1. Metrics and Evaluation Techniques

The evaluation of blockchain-based data-integrity verification techniques can be categorized into two broad categories: (i) quantitative evaluation and (ii) qualitative evaluation. However, metrics proposed in the literature [10]. They reveal three categories of metrics: (i) general, (ii) blockchain-based, and (iii) system-based. Even though different techniques have been proposed, they share some core foundations. We present the next section discussing these metrics and evaluation techniques in the paper.

A number of metrics and techniques have been proposed in the literature to measure the performance of blockchain-based DBIV systems [22]. The metrics have been identified and

categorized into different categories. We then explore the possible techniques that can be used to evaluate the performance. We present their categorization based on the metrics they are using for evaluation.

8. Future Directions and Emerging Trends

In the same paper, the various applications that potentially relate to VANET big data could also be examined. Hence, this proposal by the authors refer to the need for research in VANET big data security. It would suitably fulfill the need of the hour to provide a safe and secure environment for the big data emanating from a VANET. The authors of [11] conduct their future work using a consensus algorithm known as the Clique algorithm in the near future. This is a proof-of-authority consensus algorithm where, instead of allowing all validators to validate new blocks in a blockchain system as in the case of a proof- of-work or a proof-of-stake blockchain, only predefined validators or validators with authorisation are allowed to participate. *Another author suggests working on blockchain enabled trust in safety-critical systems. blockchain has proven to be a beneficial technology in the case of data integrity verification schemes in a V2V and V2X information sharing environment through the core concepts of immutable, distributed and decentralized databases with encryption and smart contracts implemented to enforce the predefined conditions between involved participants.

According to the previously mentioned work of various scholars, we deduce that the research on blockchain and vehicles only started approximately seven years ago. It is clear that the research is emerging in the area, where there is huge potential and a large number of open challenges across numerous research fields. The authors of [2] provide future research directions. Initially, they suggest other systems than VANETs in the context of blockchain. Naturally, we are particularly interested in this future work, where one will focus on VANETs through blockchain. The same authors cite 41 references and also conclude at the end that no particular paper or study addressed security threats to blockchain verification schemes for VANET big data.

8.1. Potential Innovations

Automotive giants are embracing the digitization trends. They are heavily investing in driverless cars because of the automated car-sharing economy, which is around the corner. Autonomous vehicle (AV)-derived data is a lucrative market for data scientists, but there are

many system-specific challenges that need to be addressed before AV data can be safely shared among car manufacturers, charging systems, and other entities. AV data include motion, speed, location, planned route, health, and environment-related data, with which the vehicle is diagnosed. As data infrastructure changes to accommodate self-driven cars need to dynamically and autonomously adjust to their surrounding environment, vehicle data needs to be exchanged in high-frequency updates [11].

Blockchain is a decentralized open and distributed ledger that securely stores digital transactions. Blockchain technology provides secure means of communication, archive-shared ability, and data integrity. There are several use-cases for blockchain in IoT and smart systems; some of them are: (a) information and communication security, as distributed ledgers can be used to prevent unauthorized access of data, (b) health care, as patient data can be stored in a distributed ledger to assure authenticity, (c) supply chain, as the distributed ledger maintains the ledger immutable, so all the information related to the product life cycle (sourcing, production, packaging, storage, and shipping) can be stored in the ledger permanently for data integrity [23].

9. Conclusion and Key Findings

Yet, while the blockchain can be trusted, it is nonetheless necessary to develop a mechanism that can elucidate the fault detection mechanism in data. The scheme can release in a blockchain solution which can enable vehicles on a large scale to verify data they receive from a blockchain-based data integrity verification system for vehicle telemetry datasets namely BDIV [2]. Here, blockchain transaction data, stationary artefacts (for instance Roadside units), and the vehicle-generated dataset are combined and stored in a block. With consent from the participants, the relevant block time-series data that have taken part in a consensus round are stored on the blockchain. In particular, in the Euler tour, which connects the fixed artefacts in sequential order, there are different options for logging vehicles to ensure necessary and sufficient vehicle coverage, which is scalable.

Blockchain technology provides trustworthy and secure data records. In an era where malicious attacks and vulnerabilities in connected and autonomous vehicles cannot be overlooked, it is apparent that a large, decentralized network is needed for a secure and trustworthy data exchange. To establish a secure and decentralized solution for data exchange with a large number of participants, an earlier study proposed a blockchain framework for

securing connected and autonomous vehicles, named B-AVEN [3]. B-AVEN's permissionless blockchain ensures data integrity and security. The vehicle-generated telemetry data is stored on a blockchain, which guarantees data authenticity and origin. Moreover, B-AVEN is equipped with smart contracts which allow legal and financial agreements to be transparent, automated and unbreakable.

Reference:

1. Tatineni, Sumanth. "Exploring the Challenges and Prospects in Data Science and Information Professions." *International Journal of Management (IJM)* 12.2 (2021): 1009-1014.

2. Vemori, Vamsi. "Human-in-the-Loop Moral Decision-Making Frameworks for Situationally Aware Multi-Modal Autonomous Vehicle Networks: An Accessibility-Focused Approach." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 54-87.

3. Shaik, Mahammad, Srinivasan Venkataramanan, and Ashok Kumar Reddy Sadhu. "Fortifying the Expanding Internet of Things Landscape: A Zero Trust Network Architecture Approach for Enhanced Security and Mitigating Resource Constraints." *Journal of Science & Technology* 1.1 (2020): 170-192.

4. Tatineni, Sumanth. "Climate Change Modeling and Analysis: Leveraging Big Data for Environmental Sustainability." *International Journal of Computer Engineering and Technology* 11.1 (2020).

5. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.