TrustDrive: Blockchain-Powered Driving Evidence Generation System

Carles Anglés-Tafalla,
Jordi Castellà-Roca y Alexandre Viejo
Universitat Rovira i Virgili,
Dept. d'Eng Inf i Mat, CYBERCAT,
{jordi.castella, carles.angles,
alexandre.viejo}@urv.cat

Josep M. Gastó
Fundació URV,
CYBERCAT,
43007 Tarragona, Spain,
jmgasto@cristech.org

***Resumen*—The increasing digitalization of vehicles enables new opportunities for generating trustworthy digital evidence in traffic, regulatory, and insurance contexts. However, current vehicular evidence collection mechanisms, such as police reports or dashcam recordings, lack strong guarantees of authenticity, integrity, and privacy compliance, limiting their legal value and increasing litigation and enforcement costs.**

This paper presents TrustDrive, a blockchain-powered vehicular evidence generation system designed to autonomously collect, process, and register tamper-proof driving-related incidents. The solution integrates vehicle-side sensing, cryptographic mechanisms, and a blockchain-based integrity layer to provide legal-admissible, GDPR-compliant digital evidence. Currently at TRL 3, TrustDrive has achieved an analytical and experimental proof-of-concept of its core components, including a modular vehicle-side prototype and a blockchain-based privacy-preserving integrity layer.

Beyond its technical architecture, this work emphasizes the transfer pathway from academic research to market-oriented innovation. We describe stakeholder engagement activities, intellectual property strategy development, and the roadmap toward TRL 6 validation through pilot deployment in restricted vehicular zones. The paper illustrates how structured collaboration, regulatory alignment, and strategic valorization can enable the progressive transfer of blockchain-based security solutions into real-world smart mobility ecosystems.

***Index Terms*—Blockchain, Vehicular Forensics, Vehicular Crowdsourcing, Technology Transfer, Smart Mobility**

Type of contribution: *Technology Transfer Article*

I. Introduction

The increasing digitalization of the automotive sector is transforming vehicles into highly connected systems equipped with advanced sensing, communication, and processing capabilities. Modern vehicles integrate cameras, GNSS positioning (GPS/Galileo), telemetry systems, and Vehicle-to-Everything (V2X) communication modules, enabling real-time interaction with their environment [1]. While these technologies were initially designed to enhance driving safety and automation, they have also opened new opportunities for generating digital vehicular evidence in traffic, regulatory, and insurance contexts.

Currently, traffic incidents, vehicular regulatory violations, and insurance claims are typically supported by police reports, eyewitness testimonies, telemetry logs or dashcam recordings. However, these sources often suffer from subjectivity, incomplete contextual information, or vulnerability to manipulation [2]. As a result, in legal and insurance scenarios, the lack of guarantees of authenticity and integrity reduces the evidentiary value of such data, frequently leading to prolonged litigation processes, higher costs, and reduced trust among the involved parties.

TrustDrive addresses this gap by proposing a blockchain-powered vehicular evidence generation system capable of collecting, processing, and securely registering tamper-proof driving-related incidents. By integrating vehicle-side sensing technologies with cryptographic mechanisms and a blockchain-based integrity layer, TrustDrive aims to provide forensic-grade, GDPR-compliant digital evidence suitable for vehicular regulatory enforcement, insurance claim resolution, and legal dispute management.

Unlike conventional dashcam-based solutions, TrustDrive is designed as a forensic-grade evidence generation system rather than a simple recording device. The system digitally signs and encrypts relevant incident data, and registers cryptographic proofs on a blockchain network to guarantee integrity, traceability, and non-repudiation.

In addition, a privacy-aware backend infrastructure enables controlled access to anonymized or full versions of the evidence, depending on users' authorization and regulatory requirements. This approach addresses both the need for trust in evidential data and the strict regulatory requirements imposed on personal data processing.

This paper presents the transfer-oriented development of TrustDrive, describing its technological foundation, stakeholder engagement process, intellectual property strategy, and roadmap towards real-world deployment. Rather than only focusing on the technical design, we emphasize the knowledge transfer pathway from academic research in cryptography and blockchain systems to an applied solution aligned with industrial and regulatory needs. The work illustrates how blockchain-based security architectures research can evolve into a market-oriented innovation addressing concrete societal and economic challenges in smart mobility ecosystems.

II. Prior Research Results and Technological Foundation

The scientific foundation of TrustDrive is grounded in previous research conducted over the last decade in vehicular sensing, digital forensics, and blockchain-based control systems for regulated mobility environments. Originally designed to assist drivers, vehicle-installed sensors and cameras

evolved into sophisticated data acquisition platforms. Modern vehicle platforms, such as Android Automotive OS (AAOS) and Android Auto, have accelerated this transformation by enabling vehicles to interact not only with drivers but also with their surrounding environment through real-time sensing, connectivity, and data exchange capabilities. This evolution created a technological foundation for moving from passive recording towards structured and verifiable vehicle digital evidence generation.

Several studies, including [3], [4], [5], [6], explore the use of dash cameras to collect evidence by surveilling their surroundings to report road incidents, traffic violations or tracking specific vehicles. In the context of sustainable mobility enforcement, the work of [7] proposes a collaborative surveillance approach where vehicles equipped with Automatic Number Plate Recognition (ANPR) cameras use Vehicle-to-Vehicle (V2V) communication to monitor and report to authorities unauthorized vehicles entering restricted zones. Similarly, [8] introduces a distributed system combining ANPR and V2V communication to detect toll evasion attempts on barrier-free highways.

Nevertheless, these approaches rely on posterior validation by authorities or collective witness reports, lacking an immutable and tamper-proof data layer that guarantees admissibility in legal and regulatory contexts.

To address this gap, several works have explored tamper-proof data generation mechanisms in vehicular forensics. The approach in [9] embeds watermarking information—such as timestamp and device metadata—into accident-related ANPR-images to verify data authenticity. Likewise, [10] proposes an incentive-driven system where vehicles and roadside units collaboratively capture and transmit incident images to the cloud for forensic analysis.

Further key precursors of TrustDrive are our prior works on blockchain-based mechanisms for regulating vehicular access to restricted mobility areas, particularly in the context of Congestion Charge (*CC*) and Low Emission Zones (*LEZs*) [11], [12]. In these proposals, smart contracts were employed to ensure transparency, traceability, and integrity in vehicular authorization processes. This research demonstrated that blockchain infrastructures can provide immutable auditability while preserving user privacy through advanced cryptographic techniques. The results of these works validated the feasibility of generating digital vehicular evidence with distributed ledger technologies in regulatory contexts.

Building on these academic foundations, TrustDrive extends the vehicular access control model towards a generalized legal-admissible evidence generation system. While earlier research focused on validating access permissions in restricted zones, TrustDrive broadens the scope to any driving-related incident, including regulatory violations, incident reconstruction, and compliance monitoring.

The technological architecture of TrustDrive integrates four core components:

- A vehicle-side *On-Board Unit (OBU) prototype* capable of collecting telemetry, positioning, and video inputs. A dedicated AAOS-based application is envisioned to provide the graphical user interface and interaction layer. This application interfaces with Evidence Generation Module of the proposal to locally generate tamper-proof digital evidence.
- An *Evidence Generation Module* that structures incident data, applies advanced cryptographic mechanisms, and generates the necessary components to transform raw sensor data into legally admissible, tamper-proof digital evidence.
- A *Backend Infrastructure* incorporating privacy-preserving access control and anonymization mechanisms, enabling controlled disclosure of evidence in compliance with GDPR requirements.
- A *Blockchain layer* that registers cryptographic components and anonymized data of generated evidence. By anchoring cryptographic elements and integrity proofs on a distributed ledger, this layer ensures immutability, traceability, and non-repudiation.

From a maturity point of view, the project has reached Technology Readiness Level (TRL) 3 [13]. An experimental proof-of-concept has been developed, validating the feasibility of secure evidence generation and blockchain-based integrity anchoring under controlled laboratory conditions. Key components have been independently tested, including cryptographic primitives and smart contract registration on test networks. However, full system integration and real-world pilot validation remain part of the planned roadmap.

Importantly, the technological architecture has been designed with transferability in mind. Rather than relying on proprietary manufacturer-integrated OBUs, the current prototype is implemented on a modular single-board computer. This design choice enables flexible integration across vehicular platforms and facilitates pilot experimentation without dependency on automotive Original Equipment Manufacturer (OEM) restrictions.

The maturity of the cryptographic primitives, the prior validation of blockchain-based regulatory mechanisms, and the existence of a functional proof-of-concept collectively provide a solid technological baseline for advancing toward higher TRLs and real-world pilot deployment.

III. Transfer Strategy and Industry Collaboration

The development of TrustDrive has been guided from its early stages by a transfer-oriented perspective, aiming to align scientific research outcomes with real industrial and regulatory needs. The transfer strategy of TrustDrive has been structured in four complementary operations: stakeholder engagement, intellectual property protection, business model validation, and progressive pilot deployment. The objective is to move from a research proof-of-concept (TRL 3) toward validation in relevant operational environments (TRL 6) through structured industrial collaboration.

III-A. Stakeholder Engagement and Use Case Definition

A structured stakeholder engagement process has been conducted to validate the practical applicability of the proposed system. Discussions have been conducted with APPlus+ IDIADA, AKKODIS, the Autoritat Portuària de Tarragona, and the Diputació de Tarragona to identify concrete use cases where tamper-proof vehicular evidence generation provides measurable value.

In particular, collaboration with automotive testing experts has contributed to assessing integration feasibility within vehicular environments. Engagement with regional public administrations and port authorities has helped define a realistic pilot scenario focused on enforcement in restricted vehicular areas, such as LEZs, CC and controlled port access environments. Additionally, discussions with mobility technology companies have facilitated alignment with ongoing European initiatives in connected vehicle ecosystems.

These interactions have resulted in three primary validated use cases: (i) regulatory enforcement in restricted traffic zones, (ii) insurance claim dispute resolution, and (iii) generation of trusted digital evidence for traffic incidents. Importantly, stakeholder feedback has been instrumental in refining system requirements, particularly regarding GDPR compliance and operational feasibility.

III-B. Intellectual Property and Commercialization Strategy

To ensure effective technology transfer, an initial intellectual property strategy has been defined (IPRL 3). This includes a preliminary patentability assessment and Freedom-to-Operate analysis to evaluate the protection potential of the tamper-proof evidence generation mechanism and its blockchain-based integrity anchoring process.

The commercialization approach considers multiple transfer options, including technology licensing to mobility solution providers, integration partnerships with automotive testing and certification entities, and potential creation of a spin-off focused on digital vehicular evidence services. This multi-path strategy reduces dependency on a single commercialization model and increases flexibility for future deployment scenarios.

Although the project was initially submitted to a regional knowledge valorization program and reached advanced evaluation stages, alternative funding mechanisms are currently being pursued to support pilot deployment and further TRL progression. This process has strengthened the project's IP positioning, clarified ownership structures, and consolidated its long-term transfer roadmap.

III-C. Business Model Validation and Funding Roadmap

From a business perspective, TrustDrive is currently positioned at BRL 3 and CRL 3. A preliminary Business Model Canvas has been defined, identifying key target customers such as public administrations responsible for traffic regulation enforcement, insurance companies seeking reliable claims validation mechanisms, fleet operators, and mobility infrastructure managers.

Initial stakeholder feedback has confirmed the economic relevance of reducing litigation costs, minimizing fraud risks, and lowering infrastructure investments required for regulatory enforcement. In particular, replacing or complementing fixed enforcement infrastructures with distributed, vehicle-generated evidence presents a potentially scalable and cost-efficient alternative.

The current roadmap prioritizes the development of a functional prototype suitable for controlled pilot testing, followed by validation in a relevant operational environment to reach TRL 6. Parallel to technical maturation, funding efforts are being directed toward public innovation programs, smart-mobility-focused grants, and strategic industrial partnerships.

IV. Current Results and Roadmap to Market Deployment

TrustDrive is currently positioned at TRL 3, with an analytical and experimental proof-of-concept of its core components already developed.

The main mechanisms for tamper-proof evidence generation (i.e. cryptographic methods, privacy-by-design protocols and blockchain-based integrity registry) have been implemented, tested, and validated under controlled laboratory conditions[12]. These experiments demonstrate the technical soundness of the proposed architecture, particularly regarding data immutability, traceability, and privacy-aware processing.

A modular vehicle-side prototype has been assembled using a single-board computer acting as a simulated OBU. This prototype enables the collection of telemetry and positioning data and supports the integration of camera-based inputs. In order to align the development path with current automotive industry trends, AAOS has been integrated into the simulated OBU environment as an experimental platform. This choice facilitates compatibility with emerging software-defined vehicle architectures and demonstrates the feasibility of future integration into manufacturer-native OBUs. Although not yet embedded in proprietary automotive platforms, this setup enables realistic experimentation and controlled validation without dependency on OEM-restricted environments.

On the server side, the backend infrastructure and blockchain layer architecture have been defined and partially implemented. Initial smart contract tests confirm the feasibility of registering and verifying cryptographic proofs of vehicular incidents on a blockchain test network, ensuring authenticity, immutability, and traceability of generated evidence. The integrity layer is currently implemented on an Ethereum-compatible test network, allowing smart-contract-based anchoring of cryptographic hashes.

The technological maturity achieved at this stage enabled the submission of the project to a regional knowledge valorization program. Although full funding was not secured in that call, the evaluation process contributed significantly to consolidating the technical roadmap and transfer strategy. In particular, reviewer feedback supported the refinement of the intellectual property protection approach, clarification of stakeholder alignment, and the definition of a pilot deployment plan.

The short-term roadmap focuses on advancing toward TRL 6 through three structured stages. First, a fully integrated functional prototype will be assembled, combining the vehicle-side module, user application interface, backend infrastructure, and blockchain layer (TRL 4). Second, controlled environment testing will be conducted to assess performance, operability, and regulatory compliance under simulated vehicular scenarios (TRL 5). Finally, pilot deployment in a stakeholder-defined relevant environment, such as restricted vehicular zones, will enable validation under real traffic conditions (TRL 6).

In parallel with technical maturation, efforts are being directed toward securing funding for pilot execution and strengthening industrial partnerships. The refinement of the

intellectual property strategy and the engagement of potential early adopters aim to reduce technological, regulatory, and market uncertainties before large-scale deployment.

This staged progression reflects a realistic and risk-aware transfer path. Rather than prematurely rush towards commercialization, the roadmap emphasizes the solution validation, its regulatory alignment, and stakeholder involvement for setting the prerequisites for a sustainable market entry.

V. Expected Impact and Conclusions

TrustDrive is positioned to generate an impact across regulatory, economic, and societal aspects within the smart mobility ecosystem.

From a regulatory perspective, the system provides a scalable mechanism for enforcing traffic and environmental regulations without relying exclusively on fixed infrastructure, particularly in restricted vehicular zones (e.g., CCs or LEZs) and controlled access infrastructures (e.g., ports or logistics hubs). By shifting from infrastructure surveillance approaches to in-vehicle evidence generation, the solution may reduce implementation and maintenance costs while increasing traceability and accountability. Furthermore, the generation of tamper-proof vehicular evidence enhances transparency and auditability in enforcement procedures, supporting public administrations in mobility governance.

Economically, TrustDrive addresses inefficiencies associated with insurance claim disputes, fraud detection, and litigation processes. By providing forensic-grade digital evidence with legal admissibility, the solution has the potential to reduce investigation times and administrative overhead. The distributed evidence-generation model may complement or partially replace costly enforcement infrastructures, improving cost-efficiency and scalability.

From a societal point of view, the availability of trustworthy vehicular evidence can increase confidence among drivers, authorities, insurers, and judicial actors. By reducing subjectivity and ambiguity in incident reconstruction, the system promotes fairness and transparency in mobility-related conflicts. Furthermore, the integration of a privacy-by-design paradigm ensures that tamper-proof requirements do not compromise data protection rights, aligning our solution with European regulatory standards.

Beyond its expected impact, the development of TrustDrive highlights several key conclusions regarding the knowledge transfer in *Security and Privacy-by-Design* mobility solutions.

First, access to proprietary automotive platforms remains a structural barrier for early-stage academic innovation. The implementation of a modular OBU prototype enabled technical validation without dependency on OEMs; however, long-term deployment will require strategic agreements with industrial partners or manufacturers.

Second, regulatory compliance, particularly regarding GDPR and evidentiary standards, must be integrated from the earliest design phases. In evidence-generation approaches, legal admissibility and privacy protection should be treated as critical as technical robustness.

Third, stakeholder engagement significantly shapes technological design. Early interactions with industry and public-sector actors helped to refine use cases, adapt architectural decisions, and align development priorities with operational realities.

Finally, the progression from research prototype to deployable mobility solution requires coordinated advancement on technical validation, intellectual property strategy, funding planning, and business model refinement. Transfer readiness cannot be achieved through technical excellence alone; it requires coordinated development across technological, legal, and commercial areas.

These observations reinforce the importance of integrating technical development, regulatory alignment, and market validation in parallel. TrustDrive illustrates how privacy-by-design-oriented research can progressively evolve into a transfer-oriented innovation through structured stakeholder collaboration, iterative validation, and strategic alignment with regulatory and market requirements.

Acknowledgments

This research is supported by the project "HERMES" funded by INCIBE and the European Union NextGenerationEU/PRTR; by projects SECURING/DATA (PID2021-125962OB-C32) and SAFE/DATA (PID2024-156914OB-C42) funded by MCIN/AEI/10.13039/501100011033/ FEDER, UE; and by the grant 2021SGR 00115 from the Government of Catalonia.

Referencias

[1] K. Strandberg and M. Eldefrawy, "Advances in automotive digital forensics: Recent trends and future directions," in *International Conference on Availability, Reliability and Security*. Springer, 2025, pp. 252–274.

[2] K. K. G. Buquerin, C. Corbett, and H.-J. Hof, "A generalized approach to automotive forensics," *Forensic Science International: Digital Investigation*, vol. 36, p. 301111, 2021.

[3] A. D. Sathe and V. D. Deshmukh, "Advance vehicle-road interaction and vehicle monitoring system using smart phone applications," in *2016 Online international conference on green engineering and technologies (IC-GET)*. IEEE, 2016, pp. 1–6.

[4] M. Jameela, H. Afzal, K. Khurshid, and A. W. Malik, "Crowdsourced system to report traffic violations," in *Proc. of the 4th Int. Conf. on Vehicle Technology and Intelligent Transport Systems (VEHITS-2018), Funchal, Madeira, Portugal*, vol. 1, 2018.

[5] H. Chen, B. Guo, Z. Yu, and Q. Han, "Crowdtracking: Real-time vehicle tracking through mobile crowdsensing," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7570–7583, 2019.

[6] Z. Jiang, H. Zhu, B. Zhou, C. Lu, M. Sun, X. Ma, X. Fan, C. Wang, and L. Chen, "Crowdpatrol: A mobile crowdsensing framework for traffic violation hotspot patrolling," *IEEE Transactions on Mobile Computing*, 2021.

[7] L.-W. Chen, Y.-C. Tseng, and K.-Z. Syue, "Surveillance on-the-road: Vehicular tracking and reporting by v2v communications," *Computer Networks*, vol. 67, pp. 154–163, 2014.

[8] S. Bouchelaghem and M. Omar, "Reliable and secure distributed smart road pricing system for smart cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1592–1603, 2018.

[9] Z. Ma, M. Jiang, and W. Huang, "Trusted forensics scheme based on digital watermark algorithm in intelligent vanet," *Neural Computing and Applications*, vol. 32, no. 6, pp. 1665–1678, 2020.

[10] R. Hussain, D. Kim, J. Son, J. Lee, C. A. Kerrache, A. Benslimane, and H. Oh, "Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2441–2448, 2018.

[11] C. Anglés-Tafalla, A. Viejo, J. Castellà-Roca, M. Mut-Puigserver, and M. M. Payeras-Capellà, "Security and privacy in a blockchain-powered access control system for low emission zones," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 580–595, 2023.

[12] C. Anglés-Tafalla, A. Viejo, R. Trujillo-Rasua, and J. Castellà-Roca, "From panoptic to secure and privacy-preserving lateral surveillance in vehicle restricted areas," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[13] E. I. Delivered, "The trl scale as a research & innovation policy tool, earto recommendations," *Earto Impact Delivered*, 2014.