Blockchain-Enabled Trust Framework for Vehicle-to-Everything (V2X) Systems

Ana Kovacevic
Software Engineering and E-Business Department,
Faculty of Organizational Sciences, University of Belgrade
Research and Development Department,
Zentrix Lab
Belgrade, Serbia
ana.kovacevic@zentrixlab.com

Nenad Gligoric
Blockchain Development Department,
Zentrix Lab
Belgrade, Serbia
nenad.gligoric@zentrixlab.io

I. Research problem

Modern vehicles are becoming increasingly connected and autonomous, communicating with other vehicles, infrastructure, and cloud services in what is known as Vehicle-to-Everything (V2X) communications. Although vehicle connectivity offers numerous advantages, such as real-time traffic information [1], over-the-air (OTA) updates [2], and cooperative safety features, it simultaneously introduces additional communication channels that require access control, protection of data from driver assistance and autonomous systems, and the preservation of data integrity [3]. This expansion increases the potential attack surface and exposes critical systems to cybersecurity threats, as demonstrated in recent high-profile incidents [4,5].

A core challenge in V2X security is trust management: vehicles must be able to trust that messages, for example, safety warnings, traffic signals, or software updates, are authentic and untampered. Traditionally, the automotive industry has relied on Public Key Infrastructure (PKI) and certificate authorities to authenticate devices and messages [6]. Standards like IEEE 1609.2 [7], ETSI ITS [8] use digital certificates for V2V and V2I messages, and OEMs use code-signing certificates for updates. However, centralized PKI systems have inherent weaknesses – a single point of failure at the Certificate Authority (CA) can compromise the whole system, as demonstrated in [9, 10]. While effective in structured environments, PKI-based systems suffer from inherent centralization, scalability bottlenecks, and revocation inefficiencies, particularly in highly dynamic vehicular networks [11]. V2X networks involve potentially millions of entities (vehicles, roadside units, etc.) that join and leave networks frequently. Managing and distributing cryptographic certificates at this scale, including revocation of compromised certificates, is complex and can be slow. Moreover, many in-vehicle networks (e.g., CAN bus) lack built-in security; if an attacker penetrates the vehicle's external communication interfaces, they can move laterally due to weak internal authentication. This highlights that securing V2X is not only about encrypting messages, but also about ensuring only legitimate, trusted entities can influence a vehicle's operation.

The central research problem is: How can we enhance the security and trust of V2X communications in a decentralized manner, eliminating single points of failure and mitigating cyber-attacks on connected vehicles? We focus on vehicular identity and message authentication as the foundation of trust. The research addresses the gap between the increasing connectivity of vehicles and the inadequacy of current centralized security mechanisms. By doing so, it aims to prevent malicious actors from impersonating vehicles or tampering with critical data exchanges, thereby improving overall vehicle safety in intelligent transportation systems.

II. Outline of objectives

To tackle the above problem, the research sets the following objectives:

1) *Develop a Decentralized Identity Framework for V2X:* Design a system where each vehicle and infrastructure component is equipped with a decentralized digital identity using Decentralized Identities (DIDs) and Verifiable Credentials (VCs). The framework will leverage a distributed ledger to manage credential issuance, verification, and revocation, thus eliminating single points of failure associated with traditional PKI. Trust relationships between participants will be established and logged on-chain, supporting privacy-preserving authentication and secure data exchange across administrative domains.

2) *Map and Demonstrate Critical Use Cases:* To demonstrate the practical relevance of the proposed decentralized security framework, the research will focus on mapping and evaluating V2X use cases that are well-suited for blockchain integration. These include scenarios where trust, data integrity, and auditability are more critical than

ultra-low latency. Examples include OTA firmware updates, where update metadata can be anchored on a distributed ledger to ensure authenticity and detect tampering; electric vehicle (EV) charging [12] and vehicle-to-grid (V2G) interactions [13] where blockchain can enable decentralized identity verification and secure transaction logging; and cross-border vehicle identity verification, which benefits from a unified trust infrastructure that transcends administrative boundaries. Additionally, the system can support misbehavior reporting and event logging for post-incident forensics and trust scoring. For selected use cases, prototype implementations or simulations will be developed to illustrate how decentralized identifiers and distributed ledgers enhance security, transparency, and trust management compared to conventional centralized approaches.

4) *Evaluate Security and Performance:* Analyze security using threat modeling to confirm that it addresses known threats and introduces no new vulnerabilities. Evaluate performance metrics such as communication latency, throughput, and scalability to ensure that the solution meets the real-time constraints of V2X. The aim is to show that decentralization and security enhancements do not unduly degrade network performance.

III. State of the Art

Connected vehicle security is a well-established yet continuously evolving research area. While connectivity enables cooperative awareness, OTA updates, and autonomous driving capabilities, it simultaneously introduces critical security and privacy challenges across both inter-vehicle (V2V) and intra-vehicle (IVN) networks [14]. Attacks such as spoofing, Sybil, message replay, and false data injection can lead to serious consequences, including road accidents, service disruption, or systemic failure. Common use cases like emergency vehicle alerts, traffic signal coordination, and EV charging authentication require robust identity verification and data integrity mechanisms to prevent unauthorized manipulation. PKI has traditionally provided authentication and message integrity via digital certificates issued by Certificate Authorities (CAs). However, PKI systems introduce several limitations in the V2X context: they are centralized, often inflexible, and pose a single point of failure. High communication overhead, latency in certificate revocation, and limited scalability under dynamic V2X conditions further complicate their applicability. Moreover, cross-border trust interoperability remains challenging due to inconsistent certificate trust models.

Distributed Ledger Technologies (DLTs) are increasingly explored as promising alternatives to centralized trust infrastructures in V2X systems. DLT systems offer immutability, distributed consensus, and decentralized credential verification, capabilities well suited to supporting resilient identity management and logging services in vehicular networks. Rather than replacing all networking protocols, blockchain is typically positioned between the network and application layers, where it enables services such as secure timestamping, credential revocation tracking, and trust management [15].

Several studies have proposed blockchain-based solutions to overcome the trust and identity challenges in V2X. For example, Lim et al. [16] use DIDs and VCs on Hyperledger Indy to eliminate dependency on centralized CAs. Oham et al. propose B-FERL, a permissioned blockchain framework that authenticates messages and monitors Electronic Control Units (ECUs) via a challenge–response mechanism [17]. Similarly, Noh et al. [18] develop a blockchain-based one-time authentication scheme leveraging publicly verifiable secret sharing to resist insider attacks. In prior work, the authors proposed a blockchain-based OTA firmware update verification system using DIDs [19], demonstrating how distributed ledgers can enhance trust and software integrity in the update process. Further, a decentralized identity management framework for V2X was introduced, leveraging DIDs, VCs, and Zero-Knowledge Proofs (ZKPs) to improve resistance to impersonation and tampering attacks [20].

These studies underline the growing interest in decentralizing identity and trust in V2X ecosystems. However, most existing approaches address isolated use cases or lack comprehensive performance evaluations. This research seeks to bridge that gap by proposing and validating an integrated, scalable framework for decentralized identity and trust management tailored to the unique demands of V2X communication.

IV. Methodology

To address the research problem, we apply a design science research methodology, iteratively designing, prototyping, and evaluating a blockchain-based security framework for V2X. The methodology encompasses the following stages:

- Use Case Mapping and Requirements: We begin by identifying representative V2X scenarios (e.g., OTA firmware updates, EV charging, vehicle-to-grid (V2G) interactions, and cross-border vehicle identity verification) and conducting threat modeling to define their security requirements.
- Architecture Design: We propose a two-layer architecture that combines identity management and distributed ledger functionalities. The Identity Management Layer utilizes DIDs and VCs to enable decentralized authentication among vehicles, OEMs, and infrastructure actors. Credential schemas will be defined and resolved via a

distributed ledger, eliminating the need for centralized authorities. The DLT layer provides a tamper-evident registry that records OTA update metadata (hashes), credential status and revocation events, and other security-relevant logs; interactions with this layer are designed to be asynchronous and kept off the safety-critical path. Platform selection will be guided by scalability, latency, and interoperability considerations.

- Prototype Implementation: Prototypes will be developed for each use case. In the OTA scenario, an OEM publishes update metadata on-chain, and vehicles verify authenticity via ledger lookups and VC validation. For EV charging identity-based access and logging will be simulated, ensuring each participant can verify counterparties through their issued credentials. In the V2X messaging context, simulated vehicular environments will be used to evaluate DID-based identity resolution and message signature verification.
- Security and Privacy Analysis: The security of the proposed framework will be evaluated using the STRIDE threat modeling methodology [21]. This analysis will guide the identification of potential attack vectors and the validation of corresponding mitigation strategies embedded within the architecture.
- Performance Evaluation: performance evaluation will be assessed by measuring latency, throughput, and scalability across key operations such as credential verification and ledger interactions. Special attention will be given to evaluating whether the added trust layer can meet real-time requirements for selected V2X scenarios.
- Ethics and Compliance: Privacy-by-design will be enforced, using hashed or anonymized data and optionally ZKPs to meet regulatory and ethical standards.

V. Expected outcome

The expected outcomes of this research are both scientific contributions and practical advancements for automotive cybersecurity:

1. *A Novel Security Framework:* The primary outcome will be a decentralized security framework for V2X that leverages DLT and SSI. The framework will define how vehicles and infrastructure can establish trust without a central authority, relying on tamper-proof ledger records for critical events. Its design will be thoroughly documented, covering data flows, cryptographic protocols, and smart contract logic on the ledger, providing a clear blueprint for further research or real-world application.
2. *Enhanced Security and Resilience:* We expect the proposed solution to significantly improve the security posture of connected vehicles. By removing reliance on a single CA, the system becomes resilient to single-point failures or insider attacks on a central authority. Any attempt by an attacker to issue fraudulent credentials or messages would require breaching a majority of the consensus nodes, which is markedly more difficult than compromising one server. Threat analyses and simulation results will show that common attack scenarios are mitigated. For example, spoofed vehicles or roadside units will be rejected due to missing or invalid blockchain-backed credentials, thwarting impersonation attempts. False or altered messages will similarly be identified by signature or hash mismatches. We also incorporate a mechanism for rapid revocation of trust, if a vehicle is reported as compromised or a software version is found vulnerable, the corresponding DID or credential can be flagged on the ledger (analogous to a certificate revocation list but globally visible and instantly effective). This ensures that other participants can refuse communication with compromised entities in real-time, containing security breaches more effectively than current systems.
3. *Performance Feasibility Demonstrated:* As part of this research, we will assess whether a decentralized trust layer based on DLT, combined with the use of DIDs and VCs, can meet the performance requirements of V2X environments. The evaluation will focus on key operations such as identity verification, credential status checks via the ledger, and logging of security-relevant events. We will analyze the latency introduced by these processes and determine whether the additional processing time is acceptable for different use cases. If results indicate minimal delays, this would suggest potential applicability even in time-sensitive scenarios such as safety messaging; however, this will be confirmed through empirical testing.
4. *Use Case Implementations:* The solution will deliver working implementations (at least in a lab or simulation environment) for the selected use cases. For example, a demo of a secure OTA update process will be produced, showing how a compromised update is detected and rejected by a vehicle. Another demo may show two vehicles exchanging safety messages and a malicious third vehicle attempting to inject a false message; with our system, the honest vehicles will ignore the malicious one due to lack of a valid decentralized

identity proof. These demonstrations will help assess the system’s effectiveness in mitigating specific threats such as false data injection or unauthorized access. The goal is to better understand under which conditions blockchain-based trust mechanisms can enhance the security posture of connected vehicles, rather than to presume universal applicability.

On the practical side, we foresee this work informing industry best practices. Car manufacturers and suppliers could adopt elements of our framework (for instance, using DLT to distribute and verify software updates, as a complement to their existing update servers). Transportation agencies might consider DLT-based credentialing for smart infrastructure devices (traffic signals, charging stations) to ensure only trusted devices interact with vehicles. The research will highlight any challenges in integration, such as how to manage the onboarding of millions of vehicles onto a ledger, or how to handle key management for vehicles in a user-friendly way, and propose solutions, thus serving as a guide for future deployments. Overall, the expected outcome is a step toward a more secure and trustworthy ecosystem for connected and autonomous vehicles, reducing the risk of cyber-attacks that could undermine public confidence or cause harm.

VI. Discussion

In the early phase of this research, a comprehensive literature review and problem analysis were conducted, identifying OTA updates and V2X message integrity as critical challenges. This initial work resulted in two published studies that laid the foundation for the current dissertation. The first proposed a decentralized identity framework for securing V2X communications [20], introducing SSI and ZKPs to authenticate vehicles without reliance on central authorities. The second extended this concept by designing a blockchain-based OTA firmware update verification mechanism [19], validated through STRIDE threat modeling and experimental evaluation, showing that the system effectively mitigates malicious firmware injection while maintaining low latency. Together, these studies demonstrated the feasibility of leveraging DLT and SSI principles in vehicular networks. Building upon these findings, the research has evolved toward a broader and more integrated system architecture. Current efforts focus on extending decentralized identity and trust management across multiple V2X use cases, such as secure EV charging, cross-border vehicle authentication, and misbehavior reporting. During this stage, different infrastructure configurations are being evaluated, including trade-offs between permissioned and consortium blockchains, as well as performance-security balances in credential issuance, verification, and revocation. A key contribution of this research lies in the integration of decentralized identity management (DIDs, VCs, and ZKPs) with blockchain-backed credential tracking into a unified trust framework for V2X systems. Unlike previous studies that addressed isolated problems [16–18], the proposed approach encompasses identity management, message authentication, and update verification as a cohesive system. In doing so, it overcomes the limitations of traditional PKI schemes, introduces decentralized revocation and distributed trust logging, and provides scalability across domains. This integrative perspective represents the novel contribution of the research and sets it apart from prior frameworks.

VII. Conclusion

This paper consolidates prior component-level results into an integrated, blockchain-enabled trust framework for V2X security. The approach synthesizes DIDs, VCs optional ZKPs, and a distributed-ledger plane for credential status, revocation, and security-relevant logging into a single architectural blueprint. Building on published evidence for key building blocks, the framework addresses centralization bottlenecks and supports privacy-preserving authentication and trustworthy update verification without imposing synchronous ledger dependencies on time-critical operations. The originality of the work lies in presenting a comprehensive architecture that spans identity bootstrapping, message authentication, and OTA verification within one framework; in making revocation and misbehavior handling decentralized and auditable across administrative domains; and in explicitly decoupling ledger interactions from the real-time safety path via asynchronous verification. This contribution advances beyond prior V2X trust frameworks and sets a clear foundation for the implementation and measurement campaigns planned in the next stage of the research.

VIII. Future work

The next stage of the research will focus on systematic evaluation, architectural refinement, and extension to additional V2X use cases. A primary near-term objective is to assess the performance of the proposed framework in a simulated environment, with emphasis on optimizing trust-establishment workflows, credential resolution, caching and refresh policies for credential status, and ledger interaction patterns to ensure scalability, modularity, and robustness under realistic conditions. Interoperability with existing standards will be examined through bridging strategies between certificate-centric and DID/VC-centric models, while privacy will be evaluated with selective-disclosure techniques to minimize PII exposure. The research is progressing according to the planned doctoral timeline. The literature review and initial concept validation have been completed. The current year is focused on implementation planning and generating intermediate results through prototyping of non–safety critical components (issuance/verification services, decentralized revocation registry, misbehavior/event logging). By the end of the second year, a functional prototype and initial evaluation results are expected to be finalized. The third year will be dedicated to refining the system, conducting comprehensive measurement campaigns (latency, throughput, revocation propagation, and scalability), and completing the dissertation. The final write-up and defense are anticipated by mid-next year, assuming the remaining work continues as planned.

References

[1] S. Kim, M. E. Lewis, and C. C. White, "Optimal vehicle routing with real-time traffic information," *IEEE Transactions on Intelligent Transportation Systems*, vol. 6, no. 2, pp. 178–188, Jun. 2005.

[2] J. Bauwens, P. Ruckebusch, S. Giannoulis, I. Moerman, and E. De Poorter, "Over-the-air software updates in the internet of things: An overview of key principles," *IEEE Communications Magazine*, vol. 58, no. 2, pp. 35–41, Feb. 2020.

[3] C. V. Kifor and A. Popescu, "Automotive cybersecurity: A survey on frameworks, standards, and testing and monitoring technologies," *Sensors*, vol. 24, no. 18, Sep. 2024. [Online]. Available: https://doi.org/10.3390/s24186139

[4] S. Curry, "Web hackers vs. the auto industry: Critical vulnerabilities found in automotive systems, affecting over 15 million vehicles," [Online]. Available: https://samcurry.net/web-hackers-vs-the-auto-industry. Accessed: july. 7, 2025.

[5] C. Miller, "Lessons learned from hacking a car," *IEEE Design & Test*, vol. 36, pp. 7–9, 2019.

[6] H. Rathore, A. Samant, M. Jadliwala, and A. Mohamed, "TangleCV: Decentralized technique for secure message sharing in connected vehicles," in *Proc. ACM Workshop on Automotive Cybersecurity*, Richardson, TX, USA, Mar. 27, 2019, pp. 45–48.]

[7] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages, IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), Mar. 2016. [Online]. Available: https://standards.ieee.org/ieee/1609.2/10258/

[8] ETSI, “Intelligent Transport Systems (ITS); Layer 1 and Layer 2 radio interface; DEN/ITS-00445,” Sophia Antipolis, France, 2023. [Online]. Available: https://www.etsi.org/standards-search. [Accessed: Jun. 29, 2025].

[9] Cybersecurity and Infrastructure Security Agency (CISA), “Lenovo Superfish Adware Vulnerable to HTTPS Spoofing,” Feb. 20, 2015. [Online]. Available: https://www.cisa.gov/news-events/alerts/2015/02/20/lenovo-superfish-adware-vulnerable-https-spoofing [Accessed: Jul. 2, 2025].

[10] H. Hoogstraaten, “Black Tulip: Report of the Investigation into the DigiNotar Certificate Authority Breach,” 2012. [Online]. Available: https://www.researchgate.net/publication/269333601_Black_Tulip_Report_of_the_investigation_into_the_DigiNotar_Certificate_Authority_breach?channel=doi&linkId=5486fcf80cf268d28f06fa61&showFulltext=true [Accessed: Jul. 2, 2025].

[11] Z. Ying, K. Wang, J. Xiong, and M. Ma, “A literature review on V2X communications security: Foundation, solutions, status, and future,” *IET Communications*, vol. 18, no. 20, pp. 1683–1715, 2024. [Online]. Available: https://doi.org/10.1049/cmu2.12778

[12] K. Khan et al., "Blockchain-based applications and energy effective electric vehicle charging – A systematic literature review, challenges, comparative analysis and opportunities," Computers and Electrical Engineering, vol. 112, p. 108959, 2023, doi: 10.1016/j.compeleceng.2023.108959.

[13] S. S. Ravi and M. Aziz, "Utilization of electric vehicles for vehicle-to-grid services: Progress and perspectives," Energies, vol. 15, no. 2, p. 589, 2022, doi: 10.3390/en15020589.

[14] B. Chah, A. Lombard, A. Bkakria, R. Yaich, A. Abbas-Turki, and S. Galland, "Privacy threat analysis for connected and autonomous vehicles," Procedia Computer Science, vol. 210, pp. 36–44, 2022, doi: 10.1016/j.procs.2022.10.117.

[15] J. Meijers, P. Michalopoulos, S. Motepalli, G. Zhang, S. Zhang, A. Veneris, and H. A. Jacobsen, "Blockchain for V2X: Applications and architectures," IEEE Open Journal of Vehicular Technology, vol. 3, pp. 193–209, 2022, doi: 10.1109/OJVT.2022.3172709.

[16] J. Lim, H. Oh, K. Sim, S. Kim, and K. H. Kim, "A V2X access authorization mechanism based on decentralized ID (DID) and verifiable credentials (VC)," in Proc. 2023 Int. Conf. on Information Networking (ICOIN), Bangkok, Thailand, Jan. 2023, pp. 801–805, doi: 10.1109/ICOIN56524.2023.10051355.

[17] C. Oham, R. Michelin, S. S. Kanhere, R. Jurdak, and S. Jha, "B-FERL: Blockchain-Based Framework for Securing Smart Vehicles," arXiv preprint arXiv:2003.03737, 2020. [Online]. Available: https://arxiv.org/abs/2003.03737.

[18] J. Noh, Y. Kwon, J. Son, and S. Cho, "Blockchain-Based One-Time Authentication for Secure V2X Communication Against Insiders and Authority Compromise Attacks," IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1–1, Jan. 2022, doi: 10.1109/JIOT.2022.3224465.

[19] A. Kovacevic and N. Gligoric, "Enhancing Security of Automotive OTA Firmware Updates via Decentralized Identifiers and Distributed Ledger Technology," Electronics, vol. 13, no. 23, p. 4640, Nov. 2024, doi: 10.3390/electronics13234640.

[20] A. Kovačević, N. Gligorić, and S. Jokić, "Decentralized Identities for Enhanced Security in Vehicle-to-Everything (V2X)," in Proc. 32nd Telecommunications Forum (TELFOR), Belgrade, Serbia, Nov. 2024, doi: 10.1109/TELFOR63250.2024.10819049.

[21] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modelling for cyber-physical systems," in Proc. 2017 IEEE PES Innovative Smart Grid Technologies Conf. Europe (ISGT-Europe), Turin, Italy, 26–29 Sep. 2017, pp. 1–6, doi: 10.1109/ISGTEurope.2017.8260113