Theme Article: Digital Trust: Trust Management in Cyberspace

A Review on the Application of Distributed Ledgers in the Evolution of Road Transport

Gianmarco Baldini, José L. Hernández-Ramos, Gary Steri, Ricardo Neisse, and Igor Nai Fovino
European Commission, Joint Research Centre

***Abstract*—In recent years, distributed ledger technologies (DLTs) and blockchain have become disruptive technologies to support distributed and trusted sharing ecosystems in various domains. Among the potential scenarios that can leverage their benefits, cooperative intelligent transport systems (C-ITS) and autonomous vehicles (AV) represent a key trend of the next digital era to build a safer society. However, different aspects such as performance and practical issues, as well as conformance with current standards and legislation, may hinder the adoption of DLT in such scenarios. This article analyses the potential applications that could leverage DLTs features and the challenges to be overcome in the coming years to foster the adoption of DLTs in C-ITS and AV. Through this analysis, we additionally provide a set of potential research directions and ways forward to exploit the advantages of DLTs in C-ITS and AV in terms of decentralized trust and transparency.**

Road transportation is on the verge of an evolutionary step toward a scenario where vehicles will be increasingly connected and automated. Such evolution will be based on enablers like wireless connectivity technologies to support the mobility of vehicles, artificial intelligence (AI) to support automated decisions in the vehicles, various type of sensors, which provide data to the automation cognitive engine,

Digital Object Identifier 10.1109/MIC.2020.3023295
Date of publication 14 September 2020; date of current version 20 November 2020.

Published by the IEEE Computer Society

smart grid connection to electric vehicles, and so on. As defined in the recent EU communication COM (2016)/766—A European strategy on cooperative intelligent transport systems, a milestone toward cooperative, connected, and automated mobility (CCAM), this wave of new technological advancements will probably generate disruptive business models and impact our quality of life.

The concept of cooperative vehicles is that vehicles will interact directly with each other and with the road infrastructure base stations using dedicated short-range communication (DSRC) or other communication means. This level of cooperation will significantly improve road safety, traffic efficiency, and comfort of driving by helping the driver to make the right decisions and adapt to the traffic situation. Another key aspect is the increased level of automation toward the idea of fully autonomous vehicles where the driver is not involved any longer in the driving of the vehicle (note that lower degrees of automation are already present in the market). Finally, the increasing electrification of vehicles is another factor to be taken in consideration. Electric vehicles may require exchange of information with the smart grid or with other infrastructures to improve traffic efficiency.

In this context, interactions and information exchange require the establishment of a trusted ecosystem among different stakeholders, such as regulatory bodies, vehicle manufacturers, road authorities, and service providers. Such ecosystem must ensure that CCAM-related information is shared through a transparent and distributed platform, with immutability and acountability properties. We claim that such needs may be satisfied by the application of distributed ledger technologies (DLTs), which can act as a distributed mediator among stakeholders to provide mutual and distributed trust for CCAM services. While most of current CCAM deployments are based on the use of a public key infrastructure (PKI), the integration of DLTs could foster the creation of a trusted data sharing ecosystem, which can be used to improve existing CCAM applications, and to design other innovative use cases. Indeed, in recent years, the application of blockchain (as the main example of DLTs) has attracted an increasing interest from the research community.[1] In particular, the creation of a transparent ledger to share vehicles and road infrastructure information is already considered for misbehavior detection, revocation, vehicle forensics, or advanced insurance services. Other complementary applications have been also proposed to improve supply chain processes or to track software versions of vehicles components. These potential applications will gain increasing importance with the advent of autonomous vehicles.

Based on these aspects, this work identifies key applications that can be enhanced with distributed ledger and blockchain technologies (the term DLT/blockchain is used in the rest of this article), and propose additional use cases based on our experience in the scope of different EU initiatives related to CCAM scenarios. While other recent research efforts have been proposed in this direction (e.g.,[1,2]), we provide a comprehensive analysis based on technical and legal aspects to be considered for the integration of DLT/blockchain in such scenarios. Furthermore, we identify potential challenges, which may lead to research opportunities. Our analysis is intended to serve as a reference for a secure and trusted development of new CCAM services based on DLT/blockchain.

The structure of this article is the following. Section II provides a brief overview of the basic concepts of DLT/blockchain. Section III identifies the key applications in connected cooperative and autonomous vehicles that can be benefited by DLT/blockchain technologies, including the main advantages of such integration. Section IV discusses the research challenges and potential ways forward to enable the use of DLT/blockchain in this context by considering the applications previously analyzed. Finally, Section V concludes this article.

DISTRIBUTED LEDGER AND BLOCKCHAIN CONCEPTS

When defining DLT/blockchain technologies, it is useful to resort to the basic concept of *ledger*, i.e., a list of transaction records which are meant to be final. From this, we can easily define a distributed ledger as a ledger shared by a set

of nodes that synchronize the list of transactions through a given *consensus mechanism*, which is the way of agreement among nodes about the validity of transactions, thus, supporting the consistency of the ledger itself. The consensus mechanism can be based on proofs of work, stake, authority, on byzantine fault tolerance, and many others.

The immutability of transaction records deriving from the concept of ledger is both achieved, thanks to the consensus mechanism and the way transactions are stored. In the case of a blockchain (that is indeed a type of distributed ledger), blocks of transactions are added in an append-only mode and chained using cryptographic links that make unfeasible any modification of the chain by single or small groups of participants (tamper resistance). However, not all the distributed ledgers rely on a blockchain when meant as the data structure just described above. For example, IOTA uses as data structure, the so-called *tangle*, a direct acyclic graph (DAG) whose vertices represent the transactions.

DLTs and blockckhains can be classified in different ways regarding the authorization model. One classification is between *public* and *private* systems: a public system accessible for use by any user and a private one only by a limited group of users. Another classification is between *permissioned* and *permissionless* systems. The first ones require authorization to perform specific activities (e.g., submit a transaction), while the second ones do not. In addition, authentication and authorization mechanisms can also be different. Some platforms like Hyperledger Fabric have their own certification authority assigning certificates to specific users and nodes, while other simply rely on anonymous key pairs, thus, requiring additional components to enforce specific access and permission rules.

The characteristics described above make DLT/blockchain particularly appealing for what concerns their decentralization, transparency, and more in general, an enhanced level of data integrity, which is particularly useful in interactions among multiple parties that do not necessarily trust each other. C-ITS use cases represent a field of application where these properties are particularly needed, since several (mobile) entities, which may not know and trust each other, have to exchange information to implement C-ITS scenarios where integrity of data and applications are crucial to support safety and security. To this regard, another important feature of some distributed ledger platforms, the *smart contract*, represents a fundamental building block for offering a high level of trust in an C-ITS scenario. The smart contract is executed by the nodes in the DLT, it benefits from all the properties described above, and it can be used to implement specific C-ITS rules like transport regulations.

ANALYSIS OF THE USE OF DTL/ BLOCKCHAIN IN CONNECTED, COOPERATIVE, AND AUTONOMOUS VEHICLES APPLICATIONS

This section summarizes the potential applications of DLT/blockchain in the automotive sector based on the analysis of existing literature and authors' expertise on this area.

Insurance and Liability

In recent years, *vehicle insurance* was modernized by more sophisticated approaches, such as the Use-Based Insurance (UBI), which determines insurance premiums using detailed driving patterns. The history of the vehicle is essential because insurance models are often based on it. Additionally, insurance companies may use such data to determine the liability of each participant in the event of an accident. Unlike centralized databases (e.g., owned by the insurance company), the use of DLT/blockchain enables the creation of a more robust and trusted data repository. In this direction, Bader *et al.*[3] use blockchain to record encrypted driving data and smart contracts that calculate insurance premiums. Additionally, Demir *et al.*[4] propose a registration system for insurance companies by using different types of transactions and smart contracts.

Tracking Driver Score

The use of DLT/blockchain can also be considered to track a driver's compliance with road safety regulations. Indeed, most of the countries have adopted the use of driving licenses based

on penalty point or demerit point systems, so that the corresponding road safety authority can cancel the license of a driver after several infractions. In this case, tracking the driver's record is also important because penalties are often based on past activities of the driver. Additionally, insurance companies can also adapt their policies based on the penalties of each driver. In this way, both insurance companies and road safety authorities can benefit from the use of DLT/blockchain to adapt their services or revoke a driver's license. Despite the benefits provided by DLT/blockchain, currently there is a gap of research proposals to realize this scenario.

Vehicle Forensics and Event Data Recording

Traditional forensics in the automotive sector uses physical evidence (e.g., photographs) collected from roadside areas where the accident took place. However, there is a growing interest by the research community for using the data generated by the vehicle through the event data recorder (EDR). Because the integrity of such data is essential (e.g., so that it can be used for legal purposes), the use of DLT/blockchain is convenient. In this direction, Cebe *et al.*[5] propose a lightweight permissioned blockchain implementation, which is combined with a PKI approach to create a comprehensive solution for vehicular forensics. Furthermore, Guo *et al.*[6] adopt a *proof of event* approach (instead the typical proof-of-work) to create a blockchain-based forensics system, in which accident events are added in a new block. Also based on a proof of event mechanism, Yang *et al.*[7] use a blockchain to store incident events, which are notified through roadside units.

Misbehavior Detection and Revocation

Misbehavior detection is essential to complement existing PKI deployments, since even legitimate and authorized vehicles could become misbehaving entities, which need to be revoked. In this context, the use of DLT/blockchain could be used to store the vehicle's history for the misbehavior detection, and consensus mechanisms could also be useful when there are ambiguities on the evaluation of a misbehavior across different road regions or countries. For example, Baldini *et al.*[8] use blockchain to collect the misbehavior reports and implement revocation using zones as an extension to ITS PKIs. In[9] the authors designed a message and revocation accountability system based on blockchain as an alternative to ITS PKI. In addition, Lasla *et al.*[10] address revocation aspects through blockchain in which roadside units use a consensus protocol to decide about admission/revocation of vehicles.

Supply Chain and Proactive Maintenance of the Vehicle Components

The application of DLT/blockchain to supply chains is one of the most cited applications in the literature, and the automotive sector is a specific use case. Integrity of supply chains will become more important with CCAM because the performance and quality of vehicles components is crucial to support automated driving functions. DLT/blockchain can be used to register the complete traceability and auditability of each component during the manufacturing process even if they are manufactured in companies from different countries. These aspects were highlighted by Lu *et al.*,[11] which proposed a permissioned blockchain to prevent counterfeiting in automotive supply chains. Furthermore, DLT/blockchain could also be used for *proactive maintenance* of the vehicle's components by tracking their state throughout the vehicle lifecycle. Beyond manufacturers, other parties can be involved in the maintenance of the vehicle (e.g., workshops) as it was investigated in the paper by Fraga-Lamas and Fernández-Caramés,[2] which uses blockchain to register the payments associated to maintenance tasks.

Software/Firmware Updates

The evolution of transport is related to the evolution of software components, which improve vehicles safety and comfort conditions. These software modules will be updated throughout the vehicle lifecycle by using over-the-air (OTA) techniques. In this context, the application of DLT/blockchain could ensure the integrity of software updates, and the traceability of different software versions. Furthermore, an autonomous vehicle can use many software modules by different vendors requiring a

multiparty interaction where the DLT/blockchain technology can be leveraged. In this direction, Dorri *et al.*[1] designed a software update system by integrating an overlay network and a cloud-based solution to store the vehicles software packages. Based on a similar approach, a proof-of-concept implementation is described by Steger *et al.*,[12] which compared the solution's performances with a PKI architecture. Furthermore, Baza *et al.*[13] proposed a blockchain system composed by vehicle manufacturers to distribute software updates, and a reward system for vehicles distributing such updates that is integrated with attribute-based encryption, so that only authorized vehicles access the update.

Car Sharing Services

This application is already present today in which drivers can rent a vehicle for a certain period of time. For this scenario, service providers and users need to share different information, such as vehicle location, drivers payment data, or the keys required to unlock the vehicle. Therefore, the use of DLT/blockchain enables the interconnection of such entities through a decentralized approach, in which authorization, accountability, and users' payments are decentralized.[1] In addition to existing car sharing services, different research efforts have been proposed to improve such services with DLT/blockchain technology. For example, Valaštín *et al.*[14] designed a car sharing application by using Ethereum implementation and smart contracts based on the solidity programming language. Furthermore, the authors in[15] also proposed Ethereum blockchain to address the booking and payment functionality of car sharing services.

Electric Vehicles and Smart Charging Stations

The increasing number of electric vehicles is fostering the development of strategies to efficiently manage the charging procedures. In this context, the use of DLT/blockchain could be used to manage the payments and contracts involving electricity companies, manufacturers, electric vehicles, and users. In addition to commercial applications, other research proposals have been recently proposed. For example, Liu *et al.*[16] use blockchain to register vehicles information and energy data through a distributed consensus, in which data and energy amounts are applied for proof determination. Furthermore, Huang *et al.*[17] designed a blockchain system to manage the registration, scheduling, authentication, and charging phases to enhance security between electric vehicles and charging stations.

Improving Existing PKI-Based Trust Models

The use of DLT/blockchain has also been considered to improve different security and privacy aspects in the automotive sector. Indeed, the use of PKI services can benefit of DLT/blockchain technologies to improve authentication, key management, or trust and reputation models. For authentication aspects, Wang *et al.*[18] combines PKI with a consensus mechanism to authenticate vehicles joining a group of cars. For trust and reputation models, Yang *et al.*[19] uses a Bayesian inference model to give a score to vehicles based on the received messages. In this case, the blockchain is maintained by the roadside units. Moreover, key management aspects are addressed by Lei *et al.*,[20] which uses blockchain to build a distributed approach, in which the transaction period is dynamically changed with respect to different traffic levels.

Regulated Applications for Commercial Vehicles

Many regulated applications can be implemented using DLT/blockchain, especially when records of activity or state of the vehicle (e.g., how much weight is carried) must be collected and stored in a secure way. Regulations, which are valid across different jurisdictions, can benefit from the application of the distributed nature of DLT/blockchain because data will be provided by each jurisdiction (which can act as a blockchain node). For example, blockchain can be used to record the weight of the commercial vehicles collected by weighing-in-motion (WIM) stations across Europe, to monitor the driving time of commercial drivers in the tachograph application, or support the fuel emissions regulation.

Traffic Management

The management of traffic in a certain road or city can benefit from the application of blockchain

regarding the collection and secure recording of traffic information. The distributed structure of traffic management systems across different jurisdictions can take advantage of the distributed nature of the blockchain, and traffic forecast systems can exploit the historical data, which can be preserved in the "blocks."

Cybersecurity Certification

An additional possible application is related to the creation of a platform to share the cybersecurity information of vehicles' components. In the EU, the new regulation "Cybersecurity Act" was adopted in March 2019 to foster the creation of a cybersecurity certification framework for any ICT product, service, or process. In this context, the use of blockchain would help to track the security level provided by vehicles' components, and other elements of the road infrastructure, including information regarding certification authorities, manufacturers, or vulnerabilities associated to such components.

CHALLENGES AND POTENTIAL RESEARCH OPPORTUNITIES

This section identifies and describes potential issues with the deployment of DLT/blockchain in the transport domain, which may lead to research opportunities. Furthermore, we analyze the impact of such challenges regarding the applications previously analyzed. This analysis is described in Table 1.

Scalability: One of the most widely recognized issues related to the application of blockchain is the computational effort required by cryptographic operations and consensus mechanisms. This issue can prevent the use of blockchain in use cases that require data sharing and processing in real-time (e.g., traffic management). To deal with this problem, most of the mentioned approaches consider special and powerful nodes (instead of roadside units or vehicles) to be part of the blockchain. For example, Dorri *et al.*[1] propose the concept of Lightweight and Scalable Blockchain (LSB), which is based on an overlay network made up of groups of nodes or clusters, where only one node (the Cluster Head) is part of the blockchain. Other proposals also make use of intermediate entities to participate in the blockchain in order to reach a tradeoff between decentralization and practicality. Furthermore, these approaches must be tailored to the specific features of the transport domain with millions of vehicles and specific functional architectures already defined in standards.

Interoperability: Another important aspect is related to interoperability both at the level of applications and security. Interoperability challenges may arise between different implementations of DLT/blockchain solutions and with existing or planned security infrastructures (e.g., PKIs). For example, each nation could maintain a different blockchain implementation based on its regulations, or a certain region could have several blockchains that need to be interconnected. In this context, the use of interledger approaches should be further analyzed in the coming years to ensure the deployment of secure and interoperable blockchains in the road transportation sector.

Privacy: Many of the applications described in the previous section (e.g., insurance services, tracking the driver's score) require large amounts of information about drivers' historical activities. Due to the immutability feature of blockchain, this can represent an issue to ensure users privacy, as well as legal implications regarding the compliance with existing regulations, such as the general data protection regulation (GDPR). Indeed, the enforcement of the rights to rectification or erasure could be not possible when using blockchain if the information is directly stored on the ledger. Therefore, complementary access control and encryption approaches may be required to provide a tradeoff between transparency and privacy.

Compatibility with existing operational processes and governance aspects. Due to safety reasons, the automotive sector is characterized by well-defined governance bodies, which manage road infrastructures through specific operational processes. These processes include vehicle registration, type approval, and applications of road regulations with a clear definition of roles. For example, only authorized entities are allowed to enforce regulations with authentication and authorization mechanisms in place to ensure that (e.g., with the use of PKI). In this context, DLT/blockchain technologies must be

Table 1. List of Blockchain Applications in Cooperative and Automated Vehicles and Related Challenges.

Application	Analysis of main challenges	Related References
Insurance and liability	Scalability can be a significant challenge because of the large number of vehicles enrolled in an insurance company, but interoperability and compatibility challenges can be limited because the company controls its own customer base. The data collected and used to monitor driver behaviour can generate privacy risks.	Scalability is mentioned as an open issue in[3,4] but solutions are not presented. For privacy concerns, advanced cryptographic techniques, such as zero-knowledge proofs, are mentioned.
Tracking driver score	A large number of drivers could represent a scalability issue but only limited information (e.g., noncompliance records) must be stored. These records should be only accessed by law enforcement authorities to mitigate privacy risks. Interoperability ad compatibility aspects could be also impacted due to the need of integrating different DLT/ blockchains (e.g., for each region)	-
Vehicle forensics and Event Data Recording	Scalability is a significant challenge because the amount of data related to events and accident recordings could be quite extensive. DLT/blockchain frameworks for event data recording are being developed, but they will need to be integrated through an interoperable design. The access to events and vehicle forensics data poses significant privacy threats.	Scalability and communication overhead is identified as a research challenge in[5–7] but solutions are not provided. Privacy is only addressed by[5] with classical pseudonym certificates.
Misbehaviour detection and revocation	The amount of information required for this application could represent a scalability concern. The access to misbehaviour detection information could also generate privacy risks. Interoperability among different DLT/blockchains is required, and compatibility is paramount to make the integration of DLT/blockchain compatible with existing operational processes for misbehavior detection and revocation.	Scalability is mentioned as a research challenge in[8–10] and[8,9] propose mitigation solutions. However, approaches to improve integration with existing operation processes are not discussed.
Supply chain and proactive maintenance	Supply chains can be quite extensive due to the amount of data and transactions to be considered and scalability can be a significant challenge. Existing supply chain infrastructures must be made interoperable when DLT/blockchain technologies are applied, which can be a complex task to implement taking into account manufacturers from different countries.	Interoperability among blockchains is cited as future development in[2,11] and potential solutions for privacy concerns are presented in[11].
Software and Firmware Updates	Scalability is a significant challenge because support for software/firmware updates could include millions of vehicles and different software versions. Software update frameworks have yet to be developed, which can facilitate the integration of DLT/blockchain, but interoperability aspects could be required to consider different software providers	Scalability is recognized as a problem in[1], and preliminary performance studies are presented in[12,13] where the proposed solutions are shown to be efficient, even if further studies are needed.
Car sharing services	While the market for car sharing services may be limited, the number of potential car sharing transactions can be huge, and existing applications are usually not interoperable. Personal data is also processed in these applications and privacy risks may arise.	A preliminary performance evaluation is proposed in[14] but neither[14] or[15] have investigated interoperability and privacy issues.
Electric Vehicles and smart charging stations	The number of electric vehicles and transactions can be huge, which poses scalability issues. The integration and governance of DLT/blockchain can also be difficult to implement by considering the requirements of transport and energy sectors.	Performance considerations are presented in[16] and a preliminary evaluation is proposed in[17] but governance aspects must be investigated further.

Table 1. (*Continued*)

Application	Analysis of main challenges	Related References
Improving existing PKI-based trust models	The evolution of existing PKI trust models and backward compatibility may be slightly complex but privacy and governance aspects are usually taken care by the existing PKIs. Scalability may be a challenge for the management of cryptographic material (e.g., certificates), but it depends on the size of the PKI and its customer base.	Performance evaluations to support scalability are presented in[18–20] but an analysis of the integration with existing or proposed PKIs in CCAM is still needed.
Regulated applications in commercial vehicles	Compatibility, and governance can be significant challenges in the application of DLT/blockchain because of existing technical and regulatory frameworks. Scalability issues depend on the particular application.	-
Traffic management	Scalability is the most significant challenge due to the large number of vehicles and data to be processed. Interoperability, backward compatibility and governance are also significant challenges due to the fragmentation of the domain. Furthermore, privacy issues could also arise because of the possibility to track the vehicle and its driver.	-
Cybersecurity certification	Scalability is a major challenge because all the vehicles and their internal components could be impacted. The integration of several DLT/blockchain implementations could be required for each country and manufacturer, and compatibility aspects are paramount as existing type approval frameworks need to be considered, when they include cybersecurity aspects.	-

Note: Applications apply to any vehicle type apart from 'regulated applications in commercial vehicles" which is only for commercial vehicles. The DLT/blockchain model is permissioned for all applications apart from the car sharing services, which can also be permissionless.

adapted to such processes, which may require significant operational research. Indeed, it is crucial to guarantee that the integration of DLT/blockchain will not negatively impact the already deployed operational processes and organizational structure.

A future roadmap for the deployment of DLT/blockchain in C-ITS and AV (i.e., CCAM) would require the resolution of the challenges presented above. Even if the studies identified in this article have proposed interesting solutions to mitigate scalability challenges (see Table 1), there is still a lack of comprehensive evaluations in real-world scenarios. To ensure higher user's privacy and the respect of GDPR constraints, advanced cryptographic architectures could be deployed, but they still need to be tailored to avoid performance issues. Interoperability and compatibility with existing deployments would require significant effort by government and industry parties. In this context, several initiatives, such as the cross-border corridors in the EU, could foster the deployment of tested and validated approaches to be considered in real-world scenarios. Indeed, the deployment of such solutions will be key to leverage the potential of DLT/blockchain for the establishment of a trusted ecosystem for CCAM.

CONCLUSION

This article has provided a review on the potential use of DLT/blockchain technologies for cooperative and automated vehicles, which is supported by the findings from research literature. Novel potential applications are also identified. The article describes the possible benefits of DLT/blockchain, but it also identifies key challenges, which must be overcome by future research activities. Based on our analysis, we believe that the realization of a DLT-enabled automotive sector still needs to face technical and legal challenges, including deployment aspects addressing scalability and interoperability requirements. Toward this end, the involvement of vehicles manufacturers, road authorities, and end users is crucial to address the needs of a trusted and privacy-aware sharing ecosystem for the next generation of cooperative and autonomous vehicles.

ACKNOWLEDGMENTS

This work was in part supported by the European Commission through the H2020-780139 SerIoT project.

REFERENCES

1. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.
2. P. Fraga-Lamas, and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17 578–17 598, 2019.
3. L. Bader, J. C. Bürger, R. Matzutt, and K. Wehrle, "Smart contract-based car insurance policies," in *Proc. IEEE Globecom Workshops*, 2018, pp. 1–7.
4. M. Demir, O. Turetken, and A. Ferworn, "Blockchain based transparent vehicle insurance management," in *Proc. 6th Int. Conf. Softw. Defined Syst.*, 2019, pp. 213–220.
5. M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.
6. H. Guo, E. Meamari, and C.-C. Shen, "Blockchain-inspired event recording system for autonomous vehicles," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw.*, 2018, pp. 218–222.
7. Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for vanets," *IEEE Access*, vol. 7, pp. 30 868–30 877, 2019.
8. G. Baldini, J. L. Hernández-Ramos, G. Steri, and S. N. Matheu, "Zone keys trust management in vehicular networks based on blockchain," in *Proc. Global IoT Summit*, 2019, pp. 1–6.
9. R. W. van der Heijden, F. Engelmann, D. Mödinger, F. Schönig, and F. Kargl, "Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication," in *Proc. 1st Workshop Scalable Resilient Infrastructures Distributed Ledgers*, 2017, pp. 1–5.
10. N. Lasla, M. Younis, W. Znaidi, and D. B. Arbia, "Efficient distributed admission and revocation using blockchain for cooperative its," in *Proc. 9th IFIP Int. Conf. New Technologies, Mobility Secur.*, 2018, pp. 1–5.
11. D. Lu *et al.*, "Reducing automotive counterfeiting using blockchain: Benefits and challenges," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures*, 2019, pp. 39–48.
12. M. Steger, A. Dorri, S. S. Kanhere, K. Römer, R. Jurdak, and M. Karner, "Secure wireless automotive software updates using blockchains: A proof of concept," in *Advanced Microsystems for Automotive Applications 2017*. Berlin, Germany: Springer, 2018, pp. 137–149.
13. M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2019, pp. 1–7.
14. V. Valaštín, K. Koštál, R. Bencel, and I. Kotuliak, "Blockchain based car-sharing platform," in *Proc. Int. Symp. ELMAR*, 2019, pp. 5–8.
15. M. Akash, I. Symeonidis, M. A Mustafa, B. Preneel, and R. Zhang, "Sc2share: Smart contract for secure car sharing," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy.*, 2019, pp. 163–171.
16. H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.
17. X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13 565–13 574, 2018.
18. X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45 061–45 072, 2019.
19. Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2018.
20. A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

Gianmarco Baldini has been a Scientific Project Manager with the Joint Research Centre (JRC), the European Commission, Ispra, Italy since 2007. He received the Laurea degree in electronic engineering and the Ph.D. degree from the University of Rome, Rome, Italy, in 1993 and 2019, respectively. Contact him at gianmarco.baldini@ec.europa.eu.

José L. Hernández-Ramos is currently a Scientific Project Officer with the Joint Research Centre, the European Commission, Ispra, Italy. He received the Ph.D. degree in computer science from the University of Murcia, Murcia, Spain. He is the corresponding author of this article. Contact him at jose-luis.hernandez-ramos@ec.europa.eu.

Gary Steri is currently a Researcher with the Joint Research Centre, the European Commission, Ispra, Italy. He received the Ph.D. degree in computer science from the University of Cagliari, Sardinia, Italy, in 2011. Contact him at gary.steri@ec.europa.eu.

Ricardo Neisse is currently a Scientific Project Officer with the Joint Research Centre, the European Commission, Ispra, Italy. He received the Ph.D. degree in computer science from the University of Twente, Enschede, Netherlands, in 2009. Contact him at ricardo.neisse@ec.europa.eu.

Igor Nai Fovino is currently a Scientific Project Manager with the Joint Research Centre, Ispra, Italy. He was a Contractual Researcher with the University of Milano. He received the Ph.D. degree in computer security from the Università degli Studi di Milano, Italy. Contact him at igor.nai-fovino@ec.europa.eu.