IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ADVANCED SOFTWARE AND DATA ENGINEERING FOR SECURE SOCIETIES

Received January 6, 2019, accepted January 21, 2019, date of publication January 25, 2019, date of current version February 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2895302

A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry

PAULA FRAGA-LAMAS, (Member, IEEE), AND TIAGO M. FERNÁNDEZ-CARAMÉS, (Senior Member, IEEE)

Department of Computer Engineering, Faculty of Computer Science, Campus de Elviña, Universidade da Coruña, 15071 A Coruña, Spain

Corresponding authors: Paula Fraga-Lamas (paula.fraga@udc.es) and Tiago M. Fernández-Caramés (tiago.fernandez@udc.es)

This work was supported in part by the Xunta de Galicia under Grant ED431C 2016-045 and Grant ED431G/01, in part by the Agencia Estatal de Investigación of Spain under Grant TEC2016-75067-C4-1-R, and by ERDF Funds under Grant AEI/FEDER, EU. The work of P. Fraga-Lamas was supported in part by BBVA and in part by the BritishSpanish Society.

ABSTRACT In the last century, the automotive industry has arguably transformed society, being one of the most complex, sophisticated, and technologically advanced industries, with innovations ranging from the hybrid, electric, and self-driving smart cars to the development of IoT-connected cars. Due to its complexity, it requires the involvement of many Industry 4.0 technologies, like robotics, advanced manufacturing systems, cyber-physical systems, or augmented reality. One of the latest technologies that can benefit the automotive industry is blockchain, which can enhance its data security, privacy, anonymity, traceability, accountability, integrity, robustness, transparency, trustworthiness, and authentication, as well as provide long-term sustainability and a higher operational efficiency to the whole industry. This review analyzes the great potential of applying blockchain technologies to the automotive industry emphasizing its cybersecurity features. Thus, the applicability of blockchain is evaluated after examining the state-of-the-art and devising the main stakeholders' current challenges. Furthermore, the article describes the most relevant use cases, since the broad adoption of blockchain unlocks a wide area of short- and medium-term promising automotive applications that can create new business models and even disrupt the car-sharing economy as we know it. Finally, after strengths, weaknesses, opportunities, and threats analysis, some recommendations are enumerated with the aim of guiding researchers and companies in future cyber-resilient automotive industry developments.

INDEX TERMS Blockchain, distributed ledger technology (DLT), Industry 4.0, IIoT, cyber-physical system, cryptography, cybersecurity, tamper-proof data, privacy, traceability.

I. INTRODUCTION

The automotive industry is one of the most technologically advanced industries with innovations ranging from hybrid, electric and self-driving smart cars to the Industrial Internet of Things (IIoT) integration in the form of IoT-connected cars. Under the Industry 4.0. paradigm [1], which represents the next stage in the digitalization of the sector, the automotive industry is facing operational inefficiencies and security issues that lead to cyber-attacks, unnecessary casualties, incidents, losses, costs and inflated prices for parts and services. Such issues are currently passed on to the different and heterogeneous stakeholders (i.e., individual and corporate car owners, service users, logistic businesses' clients or end customers) involved in the vehicle lifecycle. Industry 4.0 harnesses the advances from multiple fields, which allow for the massive deployment of sensors, the application of big data techniques, the improvements in connectivity and computational power, the emergence of new machine learning approaches, the development of new computing paradigms (e.g., cloud, fog, mist and edge computing), novel human-machine interfaces [2]–[4], IIoT enhancements [5] or the use of robotics and 3-D/4-D printing. The increasing capabilities offered by complex heterogeneous connected and autonomous networked systems enable a wide range of features and services, but they come with the threat of malicious attacks or additional risks that make cybersecurity even

more challenging. In scenarios where the controlled systems are vehicles or vehicle-related systems, public safety is at stake, therefore strong cybersecurity becomes an essential requirement.

According to a Frost & Sullivan forecast regarding near-future investments [6], automotive IIoT spend is bound to increase from $ 12.3 bn in 2015 to $ 36.7 bn in 2025 at a Compound Annual Growth Rate (CAGR) of 11.5 %. In addition, the digital retailing in automotive IoT spending will increase at a CAGR of 29.1% from 2015 to 2025 and data driven business models will grow to a CAGR of 35% from $ 524.4 mn in 2015 to $10.5 bn in 2025. Automotive ICT spending is expected to increase from $ 37.9 bn in 2015 to $ 168.7 bn in 2025 with a CAGR of 16.1% due to new digitization initiatives that will include pilot software projects that will involve automotive Original Equipment Manufacturers (OEMs) and Tier 1s. Furthermore, OEMs digital transformation strategy roadmap is to currently develop digital services and move to a Car as a Service (CaaS) business model in the 2020s to then develop a Mobility as a Service (MaaS) model to eventually position the vehicle as an element of the future connected living solutions by 2030s.

In this context, blockchain technologies represent nowadays a move in the evolution of the Internet, enabling the migration from the 'Internet of Information' to the 'Internet of Value' and the creation of a true peer-to-peer sharing economy [7], [8]. According to a World Economic Forum survey report, 10 % of the worldwide Gross Domestic Product (GDP) will be stored on a blockchain by 2027 [9]. Considering also the prospects of the automotive ecosystem, blockchain technology can offer a seamless decentralized platform where information about insurance, proof of ownership, patents, repairs, maintenance and tangible/intangible assets can be securely recorded, tracked and managed. The ensured integrity of ledgers is one of the main aspects when dealing with transactions between the participants of the automotive industry. Their accuracy and immutability is essential for enforcing real-life contractual relations, avoiding poor practices and efficiently managing the supply chain. Furthermore, the ability to access verified data in real-time opens up a realm of opportunities and business models such as the automation of processes through Internet of Things (IoT) [10]–[14] and smart contracts, advances in predictive maintenance and forensics, smart charging services for electric vehicles, peer-to-peer lending, leasing and financing, or the introduction of novel models of collaborative mobility or MaaS.

Although a detailed description on the inner workings of blockchain technology is out of the scope of this paper, the interested reader can find detailed information in recent general reviews [15]–[23]. Specifically, a comprehensive overview on blockchain that emphasizes its application to IoT is provided in [24]. There is not much research work focused on the use of blockchain to enable cybersecurity. For instance, Dai *et al.* [25] reviewed the main security issues that blockchain can tackle. Other works focused on specific security aspects. An example is presented in [26], where a cloud-based access control model is proposed. Other authors [27] focused on user identity management for cloud-based blockchain applications. Regarding the utilization of blockchain for specific applications, in [28] it is used to guarantee security and scalability in smart grid communications. Similarly, a Cyber-Physical System (CPS) [29] that makes use of a payment system based on reputation is presented in [30]. An interesting work is presented in [31], where a framework for fighting cyber-attacks when multiple organizations participate in information sharing is proposed. In the article, some game-based cyber-attacks are formally analyzed and validated through simulations. Finally, Ortega *et al.* [32], the authors review the use of blockchain and Content-Centric Networking (CCN) to ensure the security requirements for trusted 5G vehicular networks.

In contrast to the references previously cited, this work presents a holistic approach to blockchain for the automotive industry that includes both the basics for designing blockchain-based cyber-resilient applications and a detailed analysis on how to deploy and optimize blockchain technologies for the automotive industry. In addition, this paper is aimed at providing a global vision on how blockchain can transform the automotive sector radically and thus tackle part of its current challenges. The specifics of the blockchain implementation and other technical details of each use case are out of the scope of this article.

The rest of this paper is organized as follows. Section II reviews the most relevant security aspects involved in a blockchain-based development. Section III overviews the main issues and inefficiencies of the automotive industry and details a methodology for determining whether blockchain can help to tackle such issues. Section IV identifies scenarios where the automotive industry could leverage blockchain capabilities to enhance security, to reduce costs and to increase operation efficiency. Section V analyzes optimization strategies for designing blockchain-based automotive applications and studies their main challenges. Finally, Section VI is devoted to conclusions.

II. BLOCKCHAIN BASICS FOR CYBERSECURITY

A blockchain is a distributed ledger based on a chain of linked blocks that enables sharing information among peers and that provides a solution for the double-spending problem [33]–[35].

Blockchain can provide multiple security benefits, which are detailed in the next subsections and are summarized in Figure 1, including the ones required by a cyber-resilient application: decentralization, cryptographic security, transparency and immutability.

A. TAMPER-PROOF DATA

Any industry with different stakeholders needs a unique consistent data structure to read, update and take decisions [36]. Once a transaction is created in the blockchain, a new timestamp is recorded so that further modifications after such a timestamp will not be allowed. Traditional timestamping

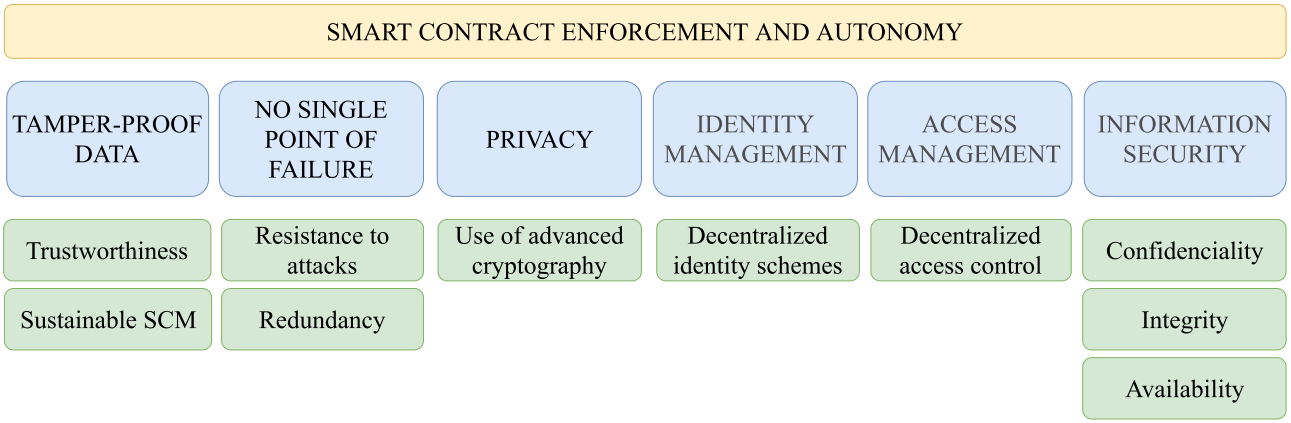

FIGURE 1. Blockchain key capabilities for cybersecurity.

mechanisms rely on a trusted server that signs and timestamps the transactions with its own private key. Nevertheless, there is a risk: a malicious server might sign past transactions. Timestamping may be distributed, but then it can be prone to Sybil attacks [37], which blockchains like Bitcoin [38] prevent by linking blocks and using a Proof-of-Work (PoW) consensus mechanism. Another authors propose a decentralized timestamping service utilizing a similar concept of the long-term signature scheme standardized by ETSI [39] or a method to construct a secure and trusted timestamping authority [40].

B. NO SINGLE POINT OF FAILURE

Blockchain performs data recording and storing using synchronous communication among the nodes through open-source sharing protocols. Open-source code has the advantage of being less prone to be altered by malicious parties, since it is monitored continuously by multiple contributors. However, like any other form of software, it can contain bugs and vulnerabilities.

Unlike traditional centralized databases, which store data in centralized clouds or server farms, a full blockchain node (a node of the blockchain that validates transactions) has a complete copy of the whole blockchain. This mechanism may derive into redundancy to some extent in specific scenarios, but the network becomes fault-tolerant and more reliable. In contrast, in cloud-centered architectures the cloud may become a single point of failure [41], since it can be unavailable due to multiple reasons (e.g., Denial of Service (DoS) attacks, maintenance tasks, software problems), and, therefore, the entire system may stop working. Moreover, only one single rogue node is required to alter the network performance through DoS attacks [42], eavesdropping or modifying the collected data [43]–[45]. To avoid the previously mentioned problems, a blockchain distributes its computing power among multiple nodes and, when a threat from a node is detected, the system is able to block its updates.

C. PRIVACY

Blockchain uses public-key cryptography for providing security and privacy. Nowadays, there are two main public-key cipher suites for Transport Layer Security (TLS) [46], [47]: Rivest-Shamir-Adleman (RSA) based cipher suites [48] that also make use of RSA as the key exchange algorithm [49], [50]; and Elliptic Curve Diffie-Hellman Exchange (ECDHE), which is based on Elliptic Curve Cryptography (ECC) and performs exchanges through Ephemeral Diffie-Hellman [51]. Previous papers have already demonstrated that, in general, ECC is faster [52]–[55] and more energy efficient [56]–[62] than RSA. Nonetheless, in 2015 the National Security Agency (NSA) discouraged the use of Suite B, a set of cryptographic algorithms that made use of RSA and ECC. Apparently, the reason for such a statement was the fast evolution of quantum computing. In addition, National Institute of Standards and Technology (NIST) announced its plan to move forward to post-quantum schemes [63]. Recent developments in that way are described in [64]–[66] and in [67], where a cryptocurrency scheme based on Post-Quantum Blockchain (PQB) is defined.

It is also important to note that every user of a blockchain is identified by a public key or its hash. Although, to protect privacy, public keys are independent from the identity of a user, it is possible to determine certain identities by analyzing the performed transactions [68], [69], although such an analysis can be made more difficult by using multichains [70] or mixing protocols [71]–[73]. In addition, zero-knowledge proofs can be used for authentication, which enable proving that someone owns certain information without revealing it [74]–[77].

With respect to hash functions, they are essential for a blockchain, since they are needed for signing transactions. Therefore, hash functions should be fast and secure in terms of collision avoidance [78], [79]. Examples of such hash functions are SHA-256d, SHA-256 and Scrypt, which are already being used by multiple cryptocurrencies [80]–[85].

Finally, it is also worth noting that privacy has been recently considered as essential in different recent initiatives [86]–[88], which have suggested the use of techniques like ring signatures [89] or homomorphic encryption [90]–[93].

D. IDENTITY MANAGEMENT

It is defined by the ISO/IEC [94] as the processes and policies involved in managing the life cycle and value, type and optional metadata of attributes in identities for a particular domain. Therefore, the identity provider controls the authorization of the different entities. Several approaches can be considered:

- Centralized schemes: the owner is a single entity that controls the system. It must be noted that their scope and utilization usually transcends this central organization (e.g., governments issue national identity cards valid for numerous entities).
- Federated schemes: the information, initially established in one security domain, can be utilized to access another domain (e.g., single sign-on schemes).
- User-centric schemes: the identity is owned and controlled by the single end-user (e.g., network anonymization).

For instance, decentralized identity schemes have emerged recently. Current strengths and challenges of applying DLT to identity management together with the evaluation of three proposals (i.e., uPort, ShoCard, and Sovrin) are analyzed in [95]. An example of implementation is illustrated in [96], where a permissioned blockchain with distributed identity management is used to increase security protection by rotating asymmetric keys.

An experimental cybersecurity cloud testbed with blockchain-based user identity management is described in [27]. The article includes experimental results of a penetration test in an Hyperledger application. Other authors [97] presented a cloud identity management solution to ease the creation of secure Infrastructure as a Service (IaaS) cloud federations. Other works focused on specific authentication schemes such as the proposed Horcrux protocol [98] that allows the end-users of self-sovereign identity to have the control of accessing their identities through a biometric authentication, or a cryptographic membership authentication scheme to support blockchain-based identity management [99].

E. ACCESS MANAGEMENT

It represents the policies, processes and tools to identify, control and manage the authorized access to a system or application. For example, a system to control access and permissions through a blockchain is proposed in [100].

F. INFORMATION SECURITY

Three main properties of the exchanged information should be preserved in order to consider it secure:

- Confidentiality. Unauthorized accesses should not be allowed to critical information. Therefore, the privacy of data transactions should be protected. This is a problem in centralized storage systems, which are really common in finance or industry, since such an infrastructure can suffer attacks or internal leaks [101], [102]. To prevent such issues, blockchain decentralizes storage. Thus, if a node becomes compromised, the rest of the system should operate normally.

  To preserve the confidentiality of a user, his/her private key has to be protected, because such a key is what is needed together with the user's public key in order to impersonate him/her. Key management systems like the one proposed in [103] can help to avoid key tampering.

  Moreover, blockchain technology can also prevent IP spoofing and forgery attacks [41]. Furthermore, blockchain can help certificate authorities and support initiatives like Google's Certificate Transparency [104] in order to prevent fake certificates [105].
- Integrity. It prevents data modifications from unauthorized users. Moreover, it allows for recovering information modified by authorized users in case certain damage occurs.

  Blockchains are conceived for storing data so that, once stored, it is very difficult to modify them. However, in very exceptional cases information can be altered by using hard forks, which originate a divergence from the previous version of the blockchain.

  In the case of collecting information from third-parties (e.g., in financial or industrial processes), data integrity is essential, especially when such parties are not trusted beforehand. To solve this problem, some authors proposed a cloud-based framework for IoT devices that preserves information integrity with the help of a blockchain [106].
- Availability. It is the possibility of accessing the system data when needed. A blockchain guarantees the availability by distributing data among peers. However, in some scenarios, availability can be compromised through attacks. The most feared is the 51-percent attack (also called majority attack), where a single miner (i.e., a transaction validator) can control the whole blockchain and perform transactions at wish. In this case, although data are available, the availability for performing transactions can be blocked by the attacker. Obviously, data integrity is also affected by this attack.

G. SMART CONTRACT ENFORCEMENT AND AUTONOMY

Effectively, a smart contract takes the terms of a traditional contract, encoding it up in the form of a business process and sharing it around the business network. Smart contracts are verified and signed when they are distributed across the business network. A smart contract is actually a piece of decentralized code that is stored on the blockchain and that runs autonomously when certain conditions are fulfilled. Therefore, there is no concept of reneging on a smart contract.

A smart contract can be regarded as an executable program that follows certain legal terms to manage physical or digital elements. Although smart contracts avoid issues related to human ambiguity, they do not depend on a state for their enforcement. Therefore, they are a mechanism to preserve performance on the deals of the parties involved.

In terms of legality, two different types of smart contracts can be distinguished: strong and weak. In contrast to weak smart contracts, strong smart contracts usually involve high revocation and modification costs. In addition, in the case of strong smart contracts, traditional law enforcers will be helpless after they are executed, since they cannot be stopped once initiated (either by involved parties or by a judge).

A smart contract can also be updated, so they need methods to add modifications that may be required legally. For instance, an online public database or Application Programming Interface (API) may be used to access the latest legal terms of the contract. Another method would consist in asking the involved parties to update the source code by themselves, what avoids depending on third-parties to perform such a task. To prevent one of the parties to modify a contract unilaterally, its terms may be defined as unmodifiable.

Although smart contracts are stored on the blockchain, they received data from external services called oracles that collect information from different sources. For instance, an oracle can monitor the status of an item in order to determine if it has arrived and write such a status on the blockchain. Then, the change on the status of the item could be detected by the smart contract, which can trigger the payment related to the purchase of the item.

There are different types of oracles depending on the collected data and on how they interact with their sources:

- Software oracles handle online information. Examples of such an information could be the temperature of a stored product or the prices of purchased parts. The data originate mainly from web sources, like company websites. The software oracle extracts the needed information and pushes it into the smart contract.
- Hardware oracles are designed to obtain data directly from the physical world. For example, Radio Frequency Identification (RFID) sensors in the supply chain industry. The biggest challenge for these hardware oracles is to report readings without sacrificing data security.
- Inbound oracles insert information from the external world into the blockchain (e.g., an automatic buy if some asset hits a certain price).
- Outbound oracles enable smart contracts to transmit data to the external world (e.g., a smart lock in the physical world which receives a payment on its blockchain address and unlocks automatically).
- Consensus based oracles imply the combination of different oracles to determine the outcome of an event. Prediction markets like Augur [107] and Gnosis [108] rely heavily on a rating system for oracles to confirm future outcomes and to avoid market manipulation.

In practice, oracles are responsible for the correct execution of a smart contract, since the insertion of incorrect information may derive into an action that may not be reverted easily (e.g., certain money transfers). Due to this problem, several companies presented oracles that verify the collected data [109]. Recently, some blockchain-based applications have become more complex and involve the use of the concepts of smart contract, oracles and Decentralized Autonomous Organization (DAO). A DAO is a distributed application implemented to make it possible for multiple parties, humans or machines, to interact with each other [110]. The interaction between the members is arbitrated by a blockchain application that is controlled exclusively by a set of immutable and incorruptible rules embedded in its source code. A DAO can provide services or resources to third-parties, or even hire people to perform specific tasks. Hence, individuals can transact with a DAO in order to access its service or get paid for their contributions. DAOs are fully autonomous, as they do not rely on any central server and, therefore, they cannot be shut down randomly by any single party (unless their code was specifically designed for it).

Ethereum provides a programming language for distributed applications, but it is far from sufficient for complex DAOs [111]. Further research will be needed to explore new approaches to building DAOs with the appropriate standardization and interoperability [112].

In addition, it is still necessary to develop legal regulations to enforce smart contracts and resolve disputes properly. Only a few researchers have studied the problem of binding real-world contracts with smart contracts [113], as well as the issues that happen when the outcome diverges from the one demanded by the law [114]. Furthermore, the main security vulnerabilities of Ethereum smart contracts have already been analyzed in the literature [115], but there are still numerous issues to be further studied.

III. EVALUATION OF THE NEED OF BLOCKCHAIN IN THE AUTOMOTIVE INDUSTRY

This section provides a comprehensive identification and classification of the current stakeholders of the automotive industry. Next, we introduce specific challenges of each stakeholder that can be faced by the use of blockchain. These challenges are then grouped into key management areas of interest. Finally, we present a flow diagram that can be used as a general guidance for deciding when it is appropriate to make use of blockchain and deciding its specific type.

In the automotive industry, wealth is created through transactions and contracts in business networks that generate a flow of goods and services. The underlying markets could include open markets such as a car auction, or a private market such as a supply chain financing. In every case, assets are transferred across the business network between the different stakeholders. There are mainly two different types of assets: tangible assets (e.g., a car) and intangible assets. Intangible assets can be subdivided into financial

TABLE 1. Main blockchain categories based on its main function.

Category	Explanation	Use cases
Static registry	Distributed database for storing reference data	• Proof of ownership • Traceability • Patents
Identity	Distributed database with identity related information	• Identity fraud • Identity records
Smart contracts	Trigger automated and self-executing actions when predefined conditions are met	• Insurance-claim payout • Cash-equity trading
Dynamic registry	Distributed database that is updated with asset transactions	• Supply chain • Fractional investing
Payment infrastructure	Dynamic distributed database that is updated with payment transactions	• Cross-border payments • Peer-to-peer payments • Insurance claims
Several categories	Use cases composed by several of the previous groups Standalone cases not fitting in any of the previous categories	• Initial Coin Offering (ICO) • Blockchain as a Service (BaaS)

assets (e.g., instruments such as bonds); intellectual (e.g., a piece of intellectual property like a patent) or digital assets.

As it can be seen in Table 1, blockchain use cases can be structured into several categories across its two fundamental functions in the automotive industry: record keeping (static registry, identity and smart contracts) and transactions (dynamic registry or payments infrastructure).

After reviewing the current state of the automotive industry, it was decided to target stakeholders who are impacted by or can influence the outcome of a blockchain deployment. This includes customers, shareholders, internal and external stakeholders. Figure 2 represents the main analyzed stakeholders.

Moreover, after examining carefully their current role, the automotive business network and the strategic agenda of a number of platforms, projects and research programs [116]–[126], a list was compiled on the specific challenges of each stakeholder related to trust, transaction costs or other areas where blockchain can be applicable to face inefficiencies. The most important detected challenges are summarized in Table 2.

Furthermore, after analyzing the collected data, it can be concluded that most of the stakeholders face similar challenges and a joint strategy will be needed to maximize the impact of blockchain applications. As it can be seen in Table 3, challenge concerns can be grouped into three specific management areas: data, operations and finance:

1) Data management. A shared set of reference data between all the stakeholders is needed. Today, all

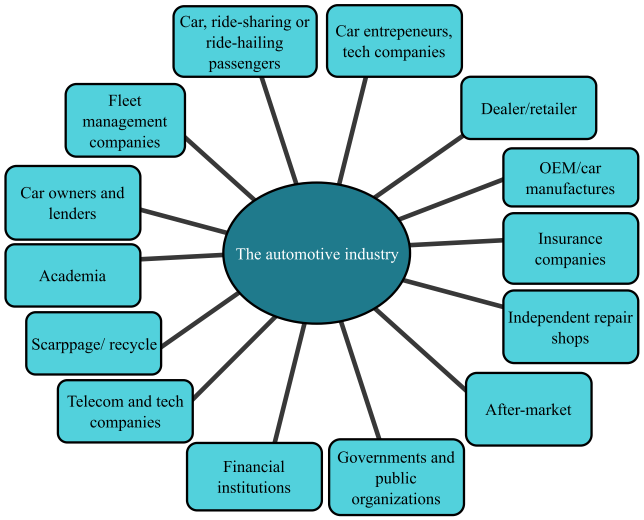

FIGURE 2. Main stakeholders in the automotive industry.

the different stakeholders of the business network keep their own copy of the reference data and update it according to some procedure, maybe by e-mail or paper, when information changes. There is a need for a distributed record system that has to be used and shared across the business network. In this way, all the participants in the business network can have their own copy of the distributed ledger. Examples of these data could be a job card, an employment record or the tracking codes of a spare part.

By putting all the information in a distributed ledger, it can actually be controlled who can change the data and who can actually get access to the data once they have been changed, thus making the whole process much more reliable.

Considering that the automotive industry spreads across different industries, countries and different regulatory boundaries, a shared set of data can be a very efficient way of managing reference data. The benefits imply reducing errors, improving real-time access to critical data and supporting natural workflows around creation, modification and deletion of the data elements.

Likewise, auditing (e.g., regulatory compliance) is a complex process, considering the fact that data and transactions are spread throughout many locations and are owned by many stakeholders. The fact that transactions are endorsed or validated by selected members of the business network has the effect of increasing the net trust within the business network. Furthermore, the fact that each member of the business network knows that they are sharing a common business process with the rest of the network also boosts trust.

When introducing a blockchain, privacy services control who can see what across the business network (appropriate confidentiality between subsets of participants) and are also used to maintain this property of

TABLE 2. Current specific challenges of the automotive industry that can be confronted using blockchain technologies.

Stakeholder	Specific challenges
Car owners and lenders / buyers and sellers of pre-owned cars [127]–[129]	1) Lack of transparency regarding the car's history 2) Unpredictable car maintenance and repair costs 3) Lack of trust in the outcome of maintenance and repair jobs 4) Absence of informed buying options 5) Absence of car insurance options 6) Lack of trust in autonomous vehicles and IoT-connected vehicles 7) High-level transactional experience to consumers whilst reducing the costs incurred by them
Fleet management companies / Car leasing or sharing (car-sharing, ride-sharing or ride-hailing) companies [120], [130]	1) Lack of transparency regarding the car's history 2) Unpredictable car maintenance and repair costs 3) Lack of trust in the outcome of maintenance and repair jobs 4) Lack of interoperability with business partners 5) High operational costs, low margin 6) High costs in the car-sharing, ride-sharing and ride-hailing economy 7) Lack of trust in autonomous vehicles and IoT-connected vehicles
Car-sharing, ride-sharing or ride-hailing passengers [131], [132]	1) More affordable car rides 2) Better maintained cars 3) Lack of trust in autonomous vehicles and IoT-connected vehicles 4) Lack of a common mobility provider platform 5) Lack of instant payment
Car entrepreneurs [122], [130]	1) Expensive rates for car leasing and rental 2) Lower car-sharing, ride-sharing or ride-hailing partnership fees 3) Difficulties to set up business, unfair competition 4) Lack of trust in autonomous vehicles and IoT-connected vehicles 5) Lack of information sharing
Car dealers and retailers [122], [133], [134]	1) Updated car ownership records 2) Updated repair and maintenance records 3) Updated purchase records 4) Lack of trust in autonomous vehicles and IoT-connected vehicles 5) Lack of information sharing
OEM / Car manufacturers and suppliers [118], [122], [134]–[137]	1) Huge warranty claim costs 2) Enforcement of recommended maintenance and repair prices on the dealers 3) Customer complaints due to car dealers' violation of recommended maintenance prices set by car manufacturers 4) Lack of control of the car maintenance performed by authorized dealers 5) Weak customer loyalty 6) Cyber-attacks, system failure risks and enhanced security in autonomous vehicles and IoT-connected vehicles 7) Control of the logistics 8) Lack of information sharing
Insurance companies [138]–[140]	1) Inflexible and non-customized policy pricing 2) 5-10% of all claims worldwide are fraudulent [143] 3) Costly and inefficient claim management 4) Inaccurate customer policy pricing 5) Lack of oversight over the quality and pricing for a collision repair
Independent repair shops [129], [134]	1) Underutilized capacity 2) Customer retention 3) Low margins 4) Lack of brand confidence
After-market (producers, distributors and retailers of spare parts, garages) [134]	1) Inefficient stock management 2) Market for counterfeit spare parts 3) Lack of transparency in warranty monitoring and enforcement 4) Low margins 5) Lack of brand confidence

TABLE 2. *(Continued.)* **Current specific challenges of the automotive industry that can be confronted using blockchain technologies.**

Stakeholder	Specific challenges
Governments and public organizations [120], [124]	1) Updated state registries (e.g., vehicle maintenance records, ownership rights, vehicle taxes, history of traffic fines) 2) Lack of trust in autonomous vehicles and IoT-connected vehicles 3) Compliance with the current legislation, particularly in terms of driver liability [117] or data protection 4) Enhanced interconnectivity with provision of open-source traffic and infrastructure data through a data cloud and willingness to shift to digital radio and universal network coverage. 5) Greater use of anonymisation and pseudonymisation in data collection and processing and provision of comprehensive information to vehicle owners and drivers about what data is collected and by whom. 6) Notifications of road conditions and traffic congestion in real-time 7) Trusted data for accident investigation and mitigating actions
Financial institutions [116]	1) Updated car ownership records and insurance, maintenance and lien records on cars 2) Non availability of single reference point on all transactions
Telecommunication and tech companies, content and service providers [120], [141]	1) Guarantee stable and secured Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication to ensure efficient and safe vehicle coordination and cooperation 2) Lack of trusted connectivity among vehicles and between vehicles and infrastructure [117]
Scrappage/recycle and environmental groups [123]	1) Control of greenhouse gas emissions 2) Full traceability of components 3) Long-term sustainability
Academia [121]	1) Guarantee vehicle safety, security and autonomy 2) More efficient driving, development of optimized Human-Machine Interface (HMI) 3) Handle traffic management of highly and fully automated vehicles under mixed traffic conditions

immutability across the blockchain, so the blockchain becomes tamper-proof. In a permissioned blockchain, it can be controlled who can see what parts (i.e., parts that are relevant to the stakeholders and their way of doing business) of the ledger. This creates a verifiable audit trail of everything owned/traded across the business network from the time it was created and put onto the blockchain. Such transactions cannot be altered, inserted or erased thanks to consensus, provenance and immutability, and the business logic actually embedded into the blockchain in the form of a smart contract.

2) Operations management is probably the most common cross-industry inefficiency considering the low implementation degree of the instruments of supply chain risk management [144]. SSCM [145] includes the complete traceability of the key assets, (i.e., a record when a car part is assembled or disassembled or is in the shipping process). Traditionally, traceability in the supply chain has been managed by using technologies like RFID [146]–[149], but blockchain technology, goes one step forward, enabling a new era of end-to-end transparency in the global supply chain system where stakeholders are able to share information rapidly and with confidence across a strong trusted network. Furthermore, the use of smart contracts provides a lower cost of transaction with a trusted contract monitored without the intervention of third parties. For instance, all the manufacturing data of where each part/asset of a subsystem has been in its journey from the manufacturer all the way through its integration into a car can be recorded. Note that this network can evolve with the shared set of referenced data to a more integrated and interlinked network of the different stakeholders.

Supply chain information can also include smart manufacturing processes (e.g., the individual computer-aided machine programming module that was used to create the part or other considerations), if they are relevant. Therefore, it ensures the traceability of an asset throughout its lifecycle. The advantages of this traceability are clear. Trust increases because it is possible to know who has owned each asset or where it has been, and hence, the whole supply chain becomes much more efficient.

It must be noted that if something goes wrong with a batch of cars or spare parts (i.e., a maintenance task or an insurance claim) diagnosing the incident or finding which subsystems or parts were actually involved can be easily solved, thus avoiding to perform a whole cross-fleet analysis or recall in the case of failure.

As a result, including blockchain into a transaction processing system will derive in the following operational benefits:

TABLE 3. Confronting today stakeholders' challenges.

Management area	Stakeholders' challenges	Solutions	Benefits
Data	1) Competitors and collaborators in a business network 2) Each business partner keeps their own database and forwards requests to a central authority for data collection and distribution 3) The owner of each information subset can be one or several organizations 4) Access to all the transactions over a specific reporting period is needed 5) Sensitive information must be continuously sent to the insurance companies 6) Some stakeholders (e.g., end-user) lack control over the exchanged data	1) Shared set of referenced data 2) Each business partner maintains its own system (e.g., specific codification) within the blockchain network 3) There is a single view of the complete dataset in the business network 4) Privacy ensures only authorized user access	1) Consolidated, immutable and consistent dataset with reduced probability of errors 2) Near real-time access to data 3) Interlinked network where code updates and transactions between stakeholders are naturally supported 4) Private sensitive data is shared on demand
Operations	1) The provenance of each asset is hard to track 2) Traceability information: manufacturer, production date or batch data	1) Sustainable Supply Chain Management (SSCM) 2) Complete provenance and traceability details of each critical asset 3) Data are accessible by each stakeholder (e.g., manufacturers, suppliers, car owners, insurance companies, government regulators)	1) No single authority is the guarantor of provenance therefore, trust increases 2) More efficient ledger utilization 3) Individual and specific rather than cross-fleet information
Finance	1) Financial data is dispersed throughout many systems with different characteristics and geographical locations 2) Letter of credits of a wider range of clients 3) Time and cost constraints	1) Common ledger for letters of credit 2) Counterparties have the same validated record of transaction 3) Transaction records collected from diverse financial sources 4) A financial audit trail created with tamper-proof data	1) Increased speed of execution 2) Reduced cost 3) Reduced uncertainty and risks (e.g., fluctuations in currency exchange rates) 4) Added-value applications (e.g., incremental claim payments) 5) An auditor is able to trace the accounting information from the blockchain to the source document (e.g., an invoice, a receipt, a form, a voucher) and view the complete process of a given transaction

- Transactions can be transformed to something that can take a number of days to almost real time.
- Overheads and cost intermediaries that do not provide added-value can actually be taken out, making more efficient the whole business network. The distributed ledger and privacy services are used to manage the elements of the blockchain, therefore reducing the risk within the business network of tampering, fraud, or cyber-attacks. Furthermore, a net improvement of trust within the business network can be achieved because everyone uses the same way to keep their ledgers updated and their business processes flowing.

3) Financial management. In the automotive industry, these services involve letters of credit, financing, leasing, and cross-border import and export systems. Letters of credit are fundamental to the way that buying and selling occurs across borders. Numerous different individual documents are exchanged and signed by the banks and the different counterparties that represent the buyer and the seller in the business network.

Furthermore, automotive financing includes some verification steps (e.g., review of documents, scoring the risk or loan approval) that smart contracts can ease, therefore enabling to automatically negotiate payment on a car lease without a middleman.
Financial and logistics operations can be coupled with IoT devices. For example, when a pallet of goods actually crosses through an RFID reader into a warehouse. The seller could draw down a certain percentage of the letter of credit because through this RFID event, it can be ensured automatically that the goods actually made it part of the way to the end customer as well as the condition of the goods (e.g., if the assets were delivered in the agreed conditions of humidity, tilt or other parameters). These automated processes reduce the time of execution to almost real time. Therefore, they vastly reduce costs and risk for both the seller, the buyer and the correspondent banks who are involved in the process. This process could be applied to a number of other financing, and cross-border import and export systems.

Beyond the hype of Distributed Ledger Technology (DLT) technologies, it must be noted that in a trustful scenario

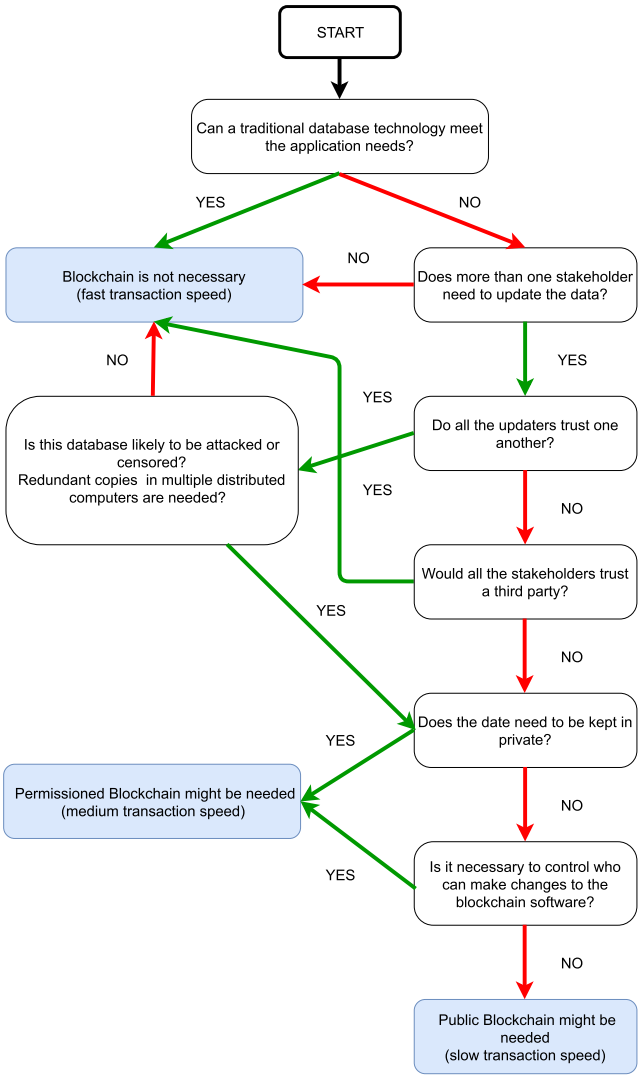

FIGURE 3. Flow diagram to determine the need of blockchain technologies in a specific application.

or when stakeholders can trade directly, traditional databases or ledgers based on Directed Acyclic Graphs (DAG) [150] may be a better solution for daily operations. Certain industrial processes are inherently better suited for blockchain solutions. For example, financial services and governments core functions are clearly aligned with blockchain capabilities [151]. Specifically, Figure 3 shows a simplified flow diagram that can be used as a general guidance for deciding when it is appropriate to make use of blockchain technologies and to determine the type needed in a particular application. Further details on the specifics of the different types of blockchain can be found in [24].

IV. ADVANCED BLOCKCHAIN-BASED COMPELLING APPLICATIONS

This section reviews the most relevant blockchain applications for automotive environments (Figure 4).

- **Extended global vehicle ledger**
  A ledger that securely stores, updates, traces and shares data (e.g., car's maintenance, ownership history) in real time. Manufacturers can partner with a blockchain service provider to create a unique ledger among the network of OEMs to address logistics monitoring and control (e.g., issues related with spare parts quality and authenticity). The ledger can gather information about cars' history from different sources and even charge users to access the data [152]. The platform could be extended to receive payment for the rendered services (e.g., repairing a vehicle, or purchasing/selling vehicle data from/to a third party).

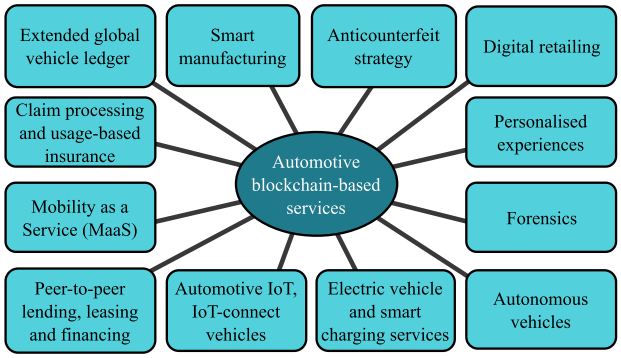

FIGURE 4. Automotive blockchain-based services.

- **Smart manufacturing**
  The inclusion of blockchain in software-based manufacturing can increase productivity and quality control, reducing the costs for tracking in inspections (e.g., it simplifies version management), warranty, inventory management [153], [154], ownership issues, maintenance or recycling tasks.

  A blockchain can also be used in a digital twin [120], [155], which represents digitally a physical asset in order to monitor its current state and to recreate its past and future [156]. In the automotive industry, assets (e.g., vehicles, tools, parts) may send data and notify events to its digital twin during their lifecycle. Thus, blockchain can be used to store securely all the mentioned information.

  An example of implementation was presented in July 2017 by Groupe Renault [157], which released a prototype created with Microsoft and VISEO to connect each car maintenance book to the vehicle's digital twin. These data are tamper-proof, fully traceable and visible to authorized parties such as the vehicle owner.
- **Anti-counterfeiting**
  Blockchain and IoT can provide an effective way to avoid fraud. On the one hand, counterparties can update the status of the items from the source to the point of sale, or even in some cases the whole lifecycle. On the other hand, sensors can be added to assets (e.g., to each part pallet shipped from the Original Equipment Supplier (OES)) to track their real-time location and status (e.g., that the shipment complies with the Estimated Time of Arrival (ETA)). It must be noted that this

strategy will imply an extensive level of cooperation among automotive stakeholders and software developers.

Regarding odometer fraud, a solution that uses an in-car connector can be proposed to send vehicle mileage data to its digital logbook on a regular basis. If tampering is suspected, the displayed mileage can be compared with the recorded via an app. Furthermore, a car owner can log its mileage on a blockchain and receive a certificate of accuracy that could be used for guaranteeing selling conditions. For example, Bosch and TÜV Rheinland (a German certification authority) are collaborating to prevent the widespread practice of odometer fraud through a digital logbook solution [158].

- **Digital retailing and customer personalized experience**
  Loyalty and reward programs can serve as customer incentives. In this use case a blockchain and smart contract-based solution can record customer purchases and issue loyalty points that can be used as a currency within the stakeholder loyalty network. The points are visualized and updated (e.g., redeemed as a discount) instantly for the whole network.
- **Claim processing and usage-based insurance**
  Claims, particularly with complex insurance instruments, involve multiple parties. Nowadays, in the event of an accident, the liability is largely attributed to the driver, but autonomous vehicles need the consideration of other entities in the automotive ecosystem such as auto manufacturers, software providers, service technicians or vehicle owners. For instance, the insurance cost for a driver may be reduced by granting insurance companies access to driving data to demonstrate safe driving habits. In addition, certain collected information like braking patterns and speed may be used to avoid frauds.

  The system would work as follows. First, the insurance company would create a public and a private key for every car, as well as a personal account stored in a cloud. The personal account is required by the company to know the actual identity of the policyholder. The public key would be stored into a secure database. The public and private keys would be used by the vehicle for every subsequent transaction with the insurance company. Thus, the vehicle stores in the cloud information on driving patterns that would be used by the insurance company to provide services. Certain critical information (e.g., vehicle location) could be stored in a blockchain in the in-vehicle storage. In case of an accident, the vehicle might fill a claim automatically by sending the information to the insurance company.
  The vehicle owner may discontinue its contract with the insurance company or sell its vehicle. In such cases, the insurance company would remove the account from the cloud storage, so the vehicle would not receive further services.
- **MaaS**
  Emerging technologies have created a new 'As-a-Service' business model in which initiatives such as Car Next Door [159] are growing fast. A blockchain-based platform would enable the interconnection of IoT-connected vehicles, autonomous vehicles, car-sharing, ride-sharing or ride-hailing providers and end-users to create a solution that records and executes agreements and monetary transactions to allow vehicle owners to monetize trips. Data (e.g., cost per mile, keys to unlock the car, insurance details, payment/billing details, information about vehicle owners, drivers and passengers) would be exchanged in a secure, reliable and seamless manner. The connections between the involved parties would be secured in order to protect their privacy (e.g., there would be no link between the actual user's identity and his/her route) and any unauthorized accesses to the vehicle (i.e., only authorized users would be able to locate, to unlock and to use a specific car). Furthermore, the platform could process all the payments upon completion of the trip and update the user's record with a history of the trip performed.

  It is worth mentioning as an example an initiative of the Toyota Research Institute [160], which is exploring together with the MIT Media Lab the development of a new mobility blockchain-based ecosystem fostering the use of open-source software tools.
- **Peer-to-peer lending, leasing and financing**
  Peer-to-peer models offer a business model that connects the involved entities and performs Know Your Customer (KYC) checks prior to leasing a vehicle, stores the leasing contract and automates the payment. Blockchain platforms will leverage secure communications and eliminate data risks. The extracted data can be used for analytics and for monitoring consumer behavior (KYC) in car leasing or rental. A couple of initiatives have studied the mentioned scenarios. For instance, in 2015 Visa and Docusign implemented a blockchain for a car leasing pilot service [161]. Similarly, Daimler AG and Landesbank Baden-Württemberg (LBBW) [162] made use of blockchain to perform financial transactions in a pilot project for monitoring capital market transactions and financial processes.
- **Connected services**
  Vehicle owners can purchase infotainment or added-value services (e.g., parking, tolls) in a seamless manner based on pre-defined contracts that are stored and executed on the blockchain. For example, Carewallet [163] is a platform that allows for a full end-to-end integration of mobility services, vehicles and infrastructure.

  Another application would be the introduction of blockchain for conventional wireless remote software updates. Nowadays, this is a centralized and non-scalable process with a partial participation of the supply chain (i.e., it does not include all the way from a service provider to a service center). Furthermore, there

are potential privacy issues, since a direct link between the vehicle and the OEM can compromise the driver's privacy (e.g., its behavior or location) and only an OEM can verify communications or the history of update downloads. The use of a blockchain would imply an end-to-end distributed data exchange that involves service providers, OEMs, vehicles, service centers or assembly lines, and it will guarantee the user's privacy and the updated history, as well as the public verification of the authenticity of the software.

- **Automotive IoT and IoT-connected vehicles**
  Vehicles are becoming interconnected Cyber-Physical systems (CPSs) [164]. These CPSs have special-purpose sensors, control units (Electronic Control Unit (ECU) and On-Board Unit (OBU)) and wireless adapters to monitor their operations and communicate with their surroundings (e.g., Road Side Unit (RSU)) [165]). The penetration of the IoT paradigm in vehicles enables the collection of a huge amount of data. For instance, most vehicles manufactured in the last decade have On-Board diagnostics (OBD) ports, which are used for retrieving vehicle diagnostics. Another major development is the deployment of an Event Data Recorder (EDR) to store incident data based on triggering events (e.g., drastic speed reduction). Sensors and devices connected over a defined mobile network will enable the collection of data like driving events (e.g., mileage, speed), safety events (e.g., spare part replacement warning), maintenance events (e.g., annual service) and will be able to send these data to a ledger shared among the stakeholders (including the owner).

  IoT applications help to monitor and control devices remotely and create new insights from real-time data. IoT, together with blockchain, can help to track, process and exchange transactions among connected devices. An example of intelligent communication between vehicles is proposed in [166]. Other authors [167] presented a lightweight scalable blockchain solution to face the challenges of traditional security and privacy methods in IoT-connected cars: centralization, lack of privacy or safety threats.
- **Electric Vehicle and smart charging services**
  Electric vehicle industry is growing in parallel with the demand for charging infrastructure. The connection of electric vehicles to the owner's smart home [168] and/or smart devices could lead to advanced services. For instance, the charging procedure might be customized according to the user personal habits (e.g., through the personal calendar). Such data could be used to guarantee that the vehicle is fully charged when needed. Furthermore, it also enables to choose the cheapest or more convenient charging cycle (e.g., avoiding peak load times).

  A blockchain-based solution can be proposed for distributed accounting, for managing contracts or for automating billing and payments. Two scenarios could be considered: when the car owner charges the vehicle at a charging station owned by a third party or when the car owner discharges the electricity from the electric vehicle to the grid to support the stabilization of the energy network. The location and behavior of the user (e.g., using a specific charger on a specific day) could be tracked, but such a location information can remain private.

  In the literature, there are some examples of implementations. For instance, a decentralized security model based on the lightning network and smart contracts is proposed in [169]. It involves registration, scheduling, authentication and charging phases. The proposed security model can be easily integrated with current scheduling mechanisms to enhance the security of trading between electric vehicles and charging piles. Another interesting example is described in [170], where a privacy-preserving selection of charging stations is presented.
- **Autonomous or self-driving vehicles**
  Since most of the car crashes are the result of human errors, a computer would be an ideal driver, as it can use complicated algorithms to determine appropriate driving measures. Autonomous vehicles are equipped with advanced IoT capabilities, navigation devices and computer vision technology to drive autonomously with limited or no human intervention. Leveraging blockchain as an underlying communication mechanism will guarantee trust and dependability on these systems. Furthermore, since cybersecurity is currently a main concern for autonomous and IoT-connected vehicles, the main threats and attacks to automated vehicles have been identified in [171]. For instance, another authors are focused on introducing peer-to-peer usage models. For example, Hasan *et al.* [172] propose a blockchain-based platform that can provide autonomous vehicles with share ride services.
- **Forensics**
  Forensics is becoming an important feature in a vehicle design and operational lifecycle. Interested stakeholders include insurance companies and law enforcement who are interested in crime solving (e.g., vehicle location information can be useful in a burglary or homicide) or crash incident investigations. In recent years, forensics has been further used by insurance providers and by companies giving vehicles to their employees for business-related activities.

  IoT-connected and autonomous vehicles gather a huge amount of information that can be significant for manufacturers, service providers, drivers or insurance companies in case of an incident or accident. This capability to collect data within and around the vehicles can make a significant impact on the forensics field. The topics has to be further studied, but an example of permissioned blockchain forensic framework can be found in [139].

TABLE 4. SWOT analysis for blockchain in the automotive industry.

	Positive	*Negative*
	Strengths	**Weaknesses**
Internal	1) Operational efficiency 2) Cyber resiliency 3) No need for intermediaries that do not provide added-value 4) Fast and simple transfers with low fees 5) Automated transactions by means of smart contracts, IoT enabler 6) Reduction in human errors 7) Accountability, verified, timestamped, and immutable auditable data 8) No data loss neither modified nor falsified data 9) Security and modern cryptography 10) Non-repudiation 11) Transparency 12) Global accessibility 13) Trusted big data analytics platform 14) Decentralization 15) Traceability, asset provenance 16) Dynamic and fluid value exchange 17) Accountability, proof of ownership and rights	1) Immature, early stage of development 2) Scalability issues 3) High energy consumption 4) Low performance 5) Lack of interoperability 6) Privacy issues (in some scenarios) 7) Criminal activity, malicious attacks 8) Dependent on input information from external oracles 9) Poor user experience, customer unfamiliarity 10) In case of users' credentials loss (e.g., a wallet), no intermediary can be contacted 11) In specific use cases, subject to cryptocurrency volatility 12) Limitation of smart contract code programming model 13) Wallet and key management 14) High-skilled human resources (scarce and costly) 15) Complexity (blockchain concepts are difficult to be mastered) 16) Lack of trust in new technology suppliers 17) Core business use cases or processes may not be suitable for the use of blockchain 18) Poor corporate governance
	Opportunities	**Threats**
External	1) Industrial competitiveness (e.g., reduced transaction costs, enhanced cybersecurity, full IoT automation) 2) Market diversification (e.g., supporting car sharing) 3) New business-model enabler 4) Rebalancing information symmetry between stakeholders 5) Fraud reduction 6) Reduced systemic risk 7) Network effect 8) A huge amount of heterogeneous data pushed into the blockchain by different actors for data analysis (big data applications) 9) Open-source code 10) Ease in cross-border trade 11) Reduction of verification procedures 12) Digital twin enabler 13) Circular economy enabler	1) Perception of insecurity or unreliability 2) Technological vulnerabilities 3) Divergent blockchains, ledger competition 4) Low adoption from important stakeholders 5) Unfavorable government policies, legal jurisdiction barriers 6) Institutional adoption barriers 7) Medium or long-term investment 8) Not adequate for external customers, readiness for adoption

V. BLOCKCHAIN IMPLEMENTATION AND DEPLOYMENT STRATEGY

A. SWOT ANALYSIS

After analyzing blockchain technologies in Section II, this subsection evaluates its applicability based on a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis that summarizes the main key issues that have to be considered when deploying blockchain technologies for the automotive industry.

1) STRENGTHS

As it can be observed in Table 4, blockchain brings numerous advantages. Its main strengths are operational efficiency and resiliency: by removing middlemen, transactions can be simplified and their cost can be lowered (e.g., banking fees).

Another strength is that smart contracts can be coded to perform autonomous transactions (e.g., decisions on business processes) based on data acquired by IoT devices or sent by different stakeholders. It must be noted that today, the data from the different stakeholders are stored in centralized databases, or even in paper, which implies costly and unreliable business processes. Moreover, these data are error prone and subject to hacking, unintentional errors or frauds as they go along the complex network of stakeholders. In contrast, the underlying technology behind blockchain (e.g., advanced cryptography) prevents the recorded data from being modified. Thus, records are irreversible and tamper-proof. Non-repudiation and immutability guarantee that there is a unique and historical version of the data that is agreed and shared among all the stakeholders (e.g., a shared set of referenced data).

Data transparency is guaranteed by providing global access to the blockchain. Since different stakeholders are able to upload information to the blockchain, it can become the

storage of an enormous amount of trusted information that might be used for big data analytics.

Moreover, the fact that a blockchain can be replicated on every full node provides redundancy and guarantees that the stored data will resist unexpected events and cyberattacks.

For instance, full traceability, asset provenance and quality control on how parts or cars are stored, inspected and transported, can enhance accountability and give proof of ownership for all the involved parties. Therefore, relevant stakeholders can verify or inspect such an information at any time or at a specific moment, thus creating dynamic and fluid value exchanges.

2) WEAKNESSES

The major blockchain weaknesses are related to the immature status of the technology (e.g., lack of scalability, high energy consumption, low performance, interoperability risks or privacy issues). In the case of IoT-connected cars or infrastructure, smart contracts will be automatically executed and in some cases they will depend on the injection of source information from external oracles. Therefore, it is presumable that this scenario will be indeed appealing for criminal activity or malicious attacks.

In addition, nowadays, usability is another challenge (e.g., no intermediaries can be contacted in case of users' credentials loss) and the customer is usually not familiarized with the technology.

An additional weakness is the cryptocurrencies volatility, which can represent a limitation to the short-term adoption of blockchain-based payments.

Regarding the available development tools, they are still in an early stage and the adoption of common standards is still ongoing. Besides, it must be noted that developing blockchain-based applications require high-level specific technical skills and human resources are scarce and costly.

Finally, it is worth remarking that, in some cases, blockchain may not be the most suitable technology for a business use case or process (as previously discussed in Section III) and it is key to succeed the adaptation of corporate governance models to decentralized exchanges of value.

3) OPPORTUNITIES

In relation to opportunities for the automotive industry, blockchain allows for gaining industrial competitiveness, for entering into new markets or for developing new types of business models thanks to the use of DAOs and low transactions fees. Blockchain also represents an opportunity to reduce the information asymmetry that today exists among the different stakeholders.

Moreover, in the automotive ecosystem, blockchain can definitely help to prevent fraud and to reduce the possibility of a systemic risk (e.g., the risk of collapse of an entire market caused by intermediaries and/or idiosyncratic events).

Specifically, due to the network effect, when a high number of stakeholders are involved, blockchain-based supply chains can be more efficient, since data can be shared nearly instantaneously among different heterogeneous actors. Nonetheless, the impact of such big data-enabled applications depends on the amount and quality of the collected information.

The use of open-source code is also essential in order to increase security and transparency. It is important to note that, although this kind of code is still susceptible to bugs and exploits, it is less prone to malicious modifications from third parties, since it can be monitored constantly by any stakeholder.

For instance, in shipping processes the transportation and logistics sector rely on a global chain of actors including shipping lines, freight forwarders, port and terminal operators, and customs authorities. All of them constantly need to exchange information about the origin of goods, tariff codes, status, classification data, import/export certificates, manifests and loading lists. Nowadays, some paperwork necessary to process cross-border shipping is done manually and operational information is transmitted over the phone, e-mail or fax. Such processes are prone to errors, tampering and delayed communication. If inserted into a blockchain, the trading with external stakeholders can be eased by offering integrity, transparency, security and paperless flows of data that can greatly decrease the time and costs associated with current intermediaries, as well as reduce the verification processes in order to ensure the overall conformity and delivery.

Blockchain can also enhance the capabilities of a digital twin, which enables digital representations of physical assets to reflect reality through simulations based on information collected from IoT devices. Examples of such improved features can be traceability of electric and electronic devices along their lifecycle, the guarantee of the provenance and authenticity of components, the registration of events from initial product design and approval processes through manufacturing, the verification of the delivery process to customers and the corresponding after sale events, the inventory management using blockchain to validate signatures and orders, or even the submission of offers from different suppliers directly to a blockchain.

Finally, blockchain can also bring new opportunities to the circular economy by ensuring traceability, by providing incentives to recycle and by enabling trust-based reputation systems.

4) THREATS

With respect to threats, they are related to several factors. First, technology can be still distrusted by the market, since it can consider it as insecure or unreliable, mainly due to software problems or cryptocurrency volatility.

Code vulnerabilities in blockchain or smart contracts are a threat to a sustainable adoption and can damage brand reputation. An infamous example is the DAO attack of 2016, which exploited a combination of previously reported security vulnerabilities with a cost of around $ 50 million worth of Ether and a devaluation of the DAO by a third [115].

As it was previously mentioned, in some cases information can be altered by using hard forks. Although this kind of forks can happen for technical reasons to fix vulnerabilities, they can also result from regulatory interventions (e.g., different jurisdictions that take varied approaches to blockchain management) or even as a result of a divergence on the ledger itself in order to provide different features.

Another threat if the fact that some stakeholders may think that the proposed system is too complicated, so the adoption rate on a worldwide basis could be low.

It must be noted that unfavorable government policies, legal regulations and institutional adoption barriers slow down and threaten the mainstream adoption of blockchain. Potential barriers may arise to the use of smart contracts. A new subset of law, denominated as Lex Cryptographia [142], that includes rules governed through self-executing smart contracts and DAOs, will have to re-evaluate the interaction between four regulatory forces: the threat of law enforcement, the manipulation of markets (financial incentives and disincentives), social pressure and the centralized intermediaries (i.e., internet service providers). For instance, the jurisdiction of smart contracts is still under debate [114].

With respect to Return On Investment (ROI) aspects, it must be indicated that applications based on blockchain technologies are considered as medium or long-term investments and as not adequate for being integrated into every existing process. In fact, most current solutions are still in the prototype stage, but it is likely that more mature applications will reach a broad market in the next years.

Moreover, if blockchain technology becomes a practice, it can have an impact on a company relationship with their customers. However, some customers may refuse to adopt it, as they might still consider personal interaction important. In addition, despite investing in human capital in order to improve customer service, market share may be lost, since companies may start to compete in terms of pricing.

B. FURTHER RECOMMENDATIONS

Despite the promising foreseen future of DLT, and specifically of blockchain technologies, the SWOT analysis of the previous Section revealed several challenges that may hinder their short-term development and deployment:

- Technical complexity: the scientific community is researching on scalability, privacy, security and post-quantum cryptography in order to face the main design limitations in transaction capacity, in validation protocols or in the design and implementation of smart contracts and DAOs. Moreover, it is necessary to introduce novel methods to foster decentralized approaches in business processes.
- Interoperability issues: the critical participants of the business network should be involved to guarantee the adoption of blockchain and its integration with third-party and legacy systems. To achieve full interoperability is necessary to adopt collaborative implementations and use international standards for trust and information protection (i.e., access control, authentication and authorization). For instance, Federated Identity Management (FIM) [173] is required to guarantee the authentication across multiple enterprises. At an international scale, such a FIM currently covers only a low Level of Assurance (LoA). The required LoA (from LoA 1 to LoA 4), as defined by the ISO/IEC 29115:2013 standard, is mainly based on the associated risks (probability of an event multiplied by its potential impact) derived from an authentication error and/or the misuse of credentials.
- Blockchain infrastructure: a comprehensive trust framework that can fulfill all the requirements for the use of blockchain must be created.
- Blockchain architecture: the design of the architecture should consider the company's decentralization requirements. In general, a private blockchain may be sufficient for the back-end. Private blockchains have been often undermined since the usage of a technology originally conceived to foster decentralization in a fully centralized way may be seen as a contradiction. Nevertheless, this type of blockchain is able to reduce the risk of data tampering and it can enable task automation.

  In the scenarios where multiple organizations need to access data, such as most of the applications of the automotive industry, a consortium or federated blockchain may be preferable. They restrict user access to the network and the actions performed by the participants. This kind of blockchain can be maintained by nodes that belong to organizations of the consortium, and it could be used as a shared ledger. For instance, a public blockchain can be used when managing automatic payments with existing cryptocurrencies, or when there is a need for provide trust between organizations using an unmodifiable ledger.
- Standardization [174]–[179] and testing: after a deep understanding of the actors, supply chains, products, markets, services, and Key Performance Indicators (KPIs) involved in an automotive specific use case, all the operational and technical requirements have to be analyzed and agreed. As a first stage, when the blockchain is created, it should be tested in the field with the agreed criteria to verify if it works as needed. As a second stage, different indicators should be evaluated in terms of privacy, security, energy efficiency, throughput, latency, privacy, cost efficiency, blockchain capacity or usability, among others. For instance, considering the hyped state of blockchain, developers may fake their blockchain performance to attract investors (e.g., Initial Coin Offerings (ICO)), driven by the expected profits.
- Regulatory and legal aspects: the lack of a clear regulatory environment (e.g., decentralized ownership, contingencies in smart contracts, international jurisdiction, cross-border trade) and democratic-by-design models of governance are concerns that hinder the potential impact

of blockchain. Companies in countries with supportive regulations will have a competitive advantage to develop innovative business models, that they will be willing to exploit legally. Furthermore, blockchain can enable value distribution models interoperable across organizations, improving the economic sustainability of both contributors and organizations.

- Organization, governance and culture: organizations' willingness and corporate governance will play an important role in the adoption of blockchain since coopetition (cooperative competition) and a collaborative mindset is required in order to engage all the stakeholders and adopt new ways for creating value.
  For instance, in the collective imaginary, Bitcoin is frequently associated with fraud and pyramid or Ponzi schemes and it has been often misused to refer to blockchain. Therefore, there are still cultural barriers and misinformation that must be confronted.
- Suitable training and advisors: mastering the blockchain concepts requires a highly technical background that is necessary to fully realize the potential of the technology. Advisory boards should be comprised of influential leaders and experts in the areas of blockchain, crypto-technologies, IoT, cyber security, insurance, financial technologies, venture capital and business development. For instance, the usability of blockchain-related applications is still not adequate for the average user. Therefore, further efforts should be carried out to avoid the excessive underlying complexity.
- Business strategies (investments, acquisitions and partnerships): there are huge prospects of investment and new players entering the market, over 1,700 digital startups are aiming to disrupt the automotive industry. Technology companies and specialized startups will support OEMs and Tier 1s on their digital transformation in two main platforms: Business to Business (B2B) and Business to Customer (B2C).

  Automotive companies will have to experiment with different blockchain projects in order to discover where the ROI/value resides or can be created (e.g., whether if there will be additional sources of revenues or profits, disruptive added-value services, cost savings, stronger brand image, cyber resilience, fraud reduction, improvements in customers' user experience). Nevertheless, in some scenarios the payoff may require that companies wait until blockchain solutions be more robust, scalable, interoperable or demand less custom development (i.e., long-term investment).

  Another challenge is the development of standards considering that several blockchain-based systems may have to coexist within the automotive industry; likely, there will be many private permissioned blockchains, due to the business competitiveness, and multiple public blockchains. Therefore, organizations will be compelled to guarantee the interoperability between blockchains. To tackle these challenges, consortiums are now beginning to emerge; for example, on May 2018, the global consortium Mobility Open Blockchain Initiative (MOBI) [180] was announced to examine the potential of blockchain and distributed ledger technologies to create a novel digital mobility ecosystem more efficient, greener, affordable, safer, and more widely accessible. The consortium hopes to bring together automakers, suppliers, startups, technology firms, blockchain companies, NGOs, academia and government agencies.
- Network effect: the degree of industry adoption will determine the benefits of blockchain technology in the automotive industry, as the volume of exchanged information will increase. When the adoption reaches a critical mass, it could evolve into an industry practice. However, at the beginning it may be difficult to obtain stakeholder commitment considering the different levels of digital readiness and the difficulty of integrating legacy processes with novel systems and practices. For instance, an initial requirement is the recognition of the gains of a blockchain-based collaboration.
- No one-size-fits-all solution: the adoption of blockchain unveils a broad area of short- and medium-term potential scenarios that could disrupt the automotive industry, as we know it today. Nevertheless, there is no one-size-fits-all technological solution for the automotive industry.

  From the business standpoint, it can be assumed that small ventures (e.g., start-ups) will be more disruptive and take more risk than established companies. In the short-term, the greatest impact will come from the technology-driven transformation of global supply chains, although ultimately many other aspects will be affected. Blockchain's strategic value in the automotive industry would be focused mainly in operational efficiencies and cost reduction. The costs in existing processes can be optimized by removing unnecessary intermediaries or diminishing the administrative workload of record keeping and transaction reconciliation (e.g., speeding up claim processing). The blockchain-based processes can capture lost revenues and create additional revenues (e.g., new business models) for service providers. In some scenarios, smart contracts could trigger actions (e.g., reimbursements) based on the data collected (e.g., from physical sensors) or ease identity verification. In the context of fraud prevention, the blockchain could act as a global shared ledger record, including for example, a person's previous history (e.g., previous claims, traffic violations).

VI. CONCLUSIONS

The transition to a data and value-driven world is fostered by the pace of the technological disruptions of an Internet-enabled global world, the challenges of future mobility, and an increasing business competition. In this ever more complex ecosystem, the use of blockchain can provide to the automotive industry a platform able to distribute

trusted and cyber-resilient information that defy current non-collaborative organizational structures. It must be noted that despite the hype reported by numerous organizations, it is necessary to perform an objective evaluation about how and whether to invest or not in blockchain from a business management and cybersecurity standpoint.

This article covered a broad suite of issues that arise from the advent of a disruptive technology like blockchain. In addition, we present a holistic approach to a blockchain-based advanced automotive industry with a review of the main scenarios and the optimization strategies for designing and deploying these applications. Furthermore, some recommendations were mentioned to guide future researchers and managers on some of the open issues that will have to be confronted before deploying the next generation of secure blockchain applications.

REFERENCES

[1] *Industrie 4.0 Project*. Accessed: Aug. 3, 2018. [Online]. Available: https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html

[2] Ó. Blanco-Novoa, T. M. Fernández-Caramés, P. Fraga-Lamas, and M. A. Vilar-Montesinos, "A practical evaluation of commercial industrial augmented reality systems in an Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 8201–8218, 2018.

[3] P. Fraga-Lamas, T. M. Fernández-Caramés, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, "A review on industrial augmented reality systems for the Industry 4.0 shipyard," *IEEE Access*, vol. 6, pp. 13358–13375, 2018.

[4] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. Vilar-Montesinos, "A fog computing and cloudlet based augmented reality system for the Industry 4.0 shipyard," *Sensors*, vol. 18, no. 6, p. 1798, 2018.

[5] P. Fraga-Lamas, T. M. Fernández-Caramés, and L. Castedo, "Towards the Internet of Smart Trains: A review on industrial IoT-connected railways," *Sensors*, vol. 17, no. 6, p. 1457, Jun. 2017.

[6] Frost & Sullivan. *Digital Transformation of the Automotive Industry Digitalization Spending to Grow Rapidly to $82.01 Billion in 2020*. Accessed: Aug. 3, 2018. [Online]. Available: https://store.frost.com/digital-transformation-of-the-automotive-industry.html

[7] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY, USA: Random House, 2016.

[8] T. M. Fernández-Caramés and P. Fraga-Lamas, "Design of a fog computing, blockchain and IoT-based continuous glucose monitoring system for crowdsourcing mHealth," in *Proc. 5th Int. Electron. Conf. Sensors Appl.*, Nov. 2018, pp. 1–6.

[9] World Economic Forum. (Sep. 2015). *Deep Shift Technology Tipping Points and Societal Impact. Survey Report*. Accessed: Jul. 2018. [Online]. Available: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[10] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, "Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications," *Sensors*, vol. 18, no. 1, p. 57, Dec. 2017.

[11] I. Froiz-Míguez, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes," in *Sensors*, vol. 18, no. 8, p. 2660, 2018.

[12] D. L. Hernández-Rojas, T. M. Fernández-Caramés, P. Fraga-Lamas, and C. J. Escudero, "A plug-and-play human-centered virtual TEDS architecture for the Web of Things," *Sensors*, vol. 18, no. 7, p. 2052, 2018.

[13] O. Blanco-Novoa, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A cost-effective IoT system for monitoring indoor radon gas concentration," *Sensors*, vol. 18, no. 7, p. 2198, 2018.

[14] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards the Internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e-textiles," *Electronics*, vol. 7, no. 12, p. 405, 2018.

[15] Z. Zheng, S. Xie, H. Dai, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[16] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.

[17] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE Int. Conf. Smart Technol.*, Ohrid, Macedonia, Jul. 2017, pp. 763–768.

[18] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in *Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON)*, Santa Clara, CA, USA, Jun. 2017, pp. 137–141.

[19] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov./Dec. 2016, pp. 1–6.

[20] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, 2016.

[21] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. Sebastopol, CA, USA: O'Reilly Media, Jan. 2015.

[22] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[23] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Secur. Commun. Netw.*, vol. 2018, Apr. 2018, Art. no. 9675050.

[24] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[25] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *Proc. 4th Int. Conf. Syst. Inform. (ICSAI)*, Hangzhou, China, Nov. 2017, pp. 975–979.

[26] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in *Proc. IEEE Conf. Russian Young Researchers Elect. Electron. Eng. (EIConRus)*, Moscow, Russia, Jan./Feb. 2018, pp. 1575–1578.

[27] C. DeCusatis, M. Zimmermann, and A. Sager, "Identity-based network security for commercial blockchain services," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2018, pp. 474–477.

[28] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Proc. Resilience Week (RWS)*, Wilmington, DE, USA, 2017, pp. 18–23.

[29] P. Fraga-Lamas, "Enabling technologies and cyber-physical systems for mission-critical scenarios," Ph.D. dissertation, Dept. Electrónica Sistemas, Univ. A Coruña, A Coruña, Spain, 2017.

[30] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.

[31] D. B. Rawat, L. Njilla, K. Kwiat, and C. Kamhoua, "iShare: Blockchain-based privacy-aware multi-agent information sharing games for cybersecurity," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Maui, HI, USA, 2018, pp. 425–431.

[32] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.

[33] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, San Jose, CA, USA, May 2015, pp. 180–184.

[34] P. Giungato, R. Rana, A. Tarabella, and C. Tricase, "Current trends in sustainability of bitcoins and related blockchain technology," *Sustainability*, vol. 9, no. 12, p. 2214, 2017.

[35] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proc. IEEE 13th Int. Conf. Peer-Peer Comput. (P2P)*, Trento, Italy, Sep. 2013, pp. 1–10.

[36] K. Kasemsap, "Mastering intelligent decision support systems in enterprise information management," in *Intelligent Systems: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global, pp. 2013–2034, 2018.

[37] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 523–538, 2013.
[38] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Aug. 3, 2018. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[39] M. Sato and S. Matsuo, "Long-term public blockchain: Resilience against compromise of underlying cryptography," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Vancouver, BC, Canada, Jul./Aug. 2017, pp. 1–8.
[40] A. Takura, S. Ono, and S. Naito, "A secure and trusted time stamping authority," in *Proc. Internet Workshop*, Osaka, Japan, Feb. 1999, pp. 88–93.
[41] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.
[42] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," in *Proc. Int. Conf. Comput., Commun. Signal Process. (ICCCSP)*, Chennai, India, Jan. 2017, pp. 1–4.
[43] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.
[44] X. Li, H. Wang, Y. Yu, and C. Qian, "An IoT data communication framework for authenticity and integrity," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Pittsburgh, PA, USA, Apr. 2017, pp. 159–170.
[45] T. Yu, X. Wang, and A. Shami, "Recursive principal component analysis-based data outlier detection and sensor data aggregation in IoT systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2207–2216, Dec. 2017.
[46] *NIST*. Accessed: Nov. 2018. [Online]. Available: https://www.nist.gov
[47] E. Rescorla. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*. Accessed: Dec. 2018. [Online]. Available: http://www.rfc-editor.org/info/rfc8446
[48] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[49] T. Kleinjung *et al.*, "Factorization of a 768-bit RSA modulus," in *Proc. 30th Annu. Conf. Adv. Cryptol.*, Santa Barbara, CA, USA, Aug. 2010, pp. 333–350.
[50] A. Pellegrini, V. Bertacco, and T. Austin, "Fault-based attack of RSA authentication," in *Proc. Design, Automat. Test Eur. Conf. Exhib.*, Dresden, Germany, Mar. 2010, pp. 855–860.
[51] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *Financial Cryptography and Data Security*, vol. 8437, N. Christin and R. Safavi-Naini, Eds. Berlin, Germany: Springer, 2014.
[52] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic curve lightweight cryptography: A survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018.
[53] M. Habib, T. Mehmood, F. Ullah, and M. Ibrahim, "Performance of WiMAX security algorithm (the comparative study of RSA encryption algorithm with ECC encryption algorithm)," in *Proc. Int. Conf. Comput. Technol. Develop.*, Kota Kinabalu, Malaysia, Nov. 2009, pp. 108–112.
[54] M. Savari, M. Montazerolzohour, and Y. E. Thiam, "Comparison of ECC and RSA algorithm in multipurpose smart card application," in *Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic*, Kuala Lumpur, Malaysia, Jun. 2012, pp. 49–53.
[55] M. Bafandehkar, S. M. Yasin, R. Mahmod, and Z. M. Hanapi, "Comparison of ECC and RSA algorithm in resource constrained devices," in *Proc. Int. Conf. IT Converg. Secur.*, Macao, China, Dec. 2013, pp. 1–3.
[56] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, Nov. 2018.
[57] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 577–601, 1st Quart., 2016.
[58] E. Noroozi, J. Kadivar, and S. H. Shafiee, "Energy analysis for wireless sensor networks," in *Proc. 2nd Int. Conf. Mech. Electron. Eng.*, Kyoto, Japan, Aug. 2010, pp. V2-382–V2-386.
[59] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors*, vol. 17, no. 9, p. 1978, 2017.
[60] P. R. de Oliveira, V. D. Feltrim, L. A. F. Martimiano, and G. B. M. Zanoni, "Energy consumption analysis of the cryptographic key generation process of RSA and ECC algorithms in embedded systems," *IEEE Latin Amer. Trans.*, vol. 12, no. 6, pp. 1141–1148, Sep. 2014.
[61] M. Suárez-Albela, P. Fraga-Lamas, L. Castedo, and T. M. Fernández-Caramés, "Clock frequency impact on the performance of high-security cryptographic cipher suites for energy-efficient resource-constrained IoT devices," *Sensors*, vol. 19, no. 1, p. 15, Jan. 2019.
[62] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," in *Proc. Int. Conf. Adv. Comput., Commun. Inform.*, Jaipur, India, Sep. 2016, pp. 1725–1729.
[63] NIST. *Report on Post-Quantum Cryptography, NISTIR 8105 DRAFT*. (Apr. 2016). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
[64] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.
[65] N. Koblitz and A. Menezes, "A riddle wrapped in an enigma," *IEEE Security Privacy*, vol. 14, no. 6, pp. 34–42, Nov./Dec. 2016.
[66] N. Koblitz and A. Menezes, "A riddle wrapped in an enigma," *IEEE Security Privacy*, vol. 14, no. 6, pp. 34–42, Nov. 2016.
[67] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.
[68] S. Meiklejohn *et al.*, "A fistful of bitcoins: Characterizing payments among men with no names," *Commun. ACM*, vol. 59, no. 4, pp. 86–93, Apr. 2016.
[69] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in *Proc. APWG eCrime Researchers Summit*, San Francisco, CA, USA, Sep. 2013, pp. 1–14.
[70] *Multichain White Paper*. Accessed: Aug. 3, 2018. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf
[71] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur.*, Christ Church, Barbados, Mar. 2014, pp. 486–504.
[72] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, San Juan, PR, USA, Jan. 2015, pp. 112–126.
[73] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.
[74] *Zerocoin*. Accessed: Aug. 3, 2018. [Online]. Available: http://zerocoin.org
[75] *Zerocash*. Accessed: Aug. 3, 2018. [Online]. Available: http://zerocash-project.org
[76] *Zcash*. Accessed: Aug. 3, 2018. [Online]. Available: https://z.cash
[77] M. Schukat and P. Flood, "Zero-knowledge proofs in M2M communication," in *Proc. 25th IET Irish Signals Syst. Conf. China-Ireland Int. Conf. Inf. Commun. Technol.*, Limerick, Ireland, Jun. 2014, pp. 269–273.
[78] E. Andreeva, B. Mennink, and B. Preneel, "Open problems in hash function security," *Des., Codes Cryptogr.*, vol. 77, nos. 2–3, pp. 611–631, Dec. 2015.
[79] M. Wang, M. Duan, and J. Zhu, "Research on the security criteria of hash functions in the blockchain," in *Proc. 2nd ACM Workshop Blockchains, Cryptocurrencies, Contracts (BCC)*, Incheon, South Korea, Jun. 2018, pp. 47–55.
[80] *Litecoin*. Accessed: Nov. 2018. [Online]. Available: https://litecoin.com
[81] *Namecoin*. Accessed: Nov. 2018. [Online]. Available: https://namecoin.org/
[82] *Emercoin*. Accessed: Nov. 2018. [Online]. Available: https://emercoin.com/es
[83] *Litecoin*. Accessed: Nov. 2018. [Online]. Available: https://litecoin.com
[84] *Gridcoin*. Accessed: Nov. 2018. [Online]. Available: https://gridcoin.us/
[85] *Dogecoin*. Accessed: Nov. 2018. [Online]. Available: https://dogecoin.com/
[86] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security Privacy*, vol. 16, no. 4, pp. 38–45, Jul./Aug. 2018.
[87] *Bytecoin*. Accessed: Aug. 3, 2018. [Online]. Available: https://bytecoin.org
[88] *Monero*. Accessed: Aug. 3, 2018. [Online]. Available: https://getmonero.org

[89] *CryptoNote*. Accessed: Aug. 3, 2018. [Online]. Available: https://cryptonote.org
[90] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doröz, and B. Sunar, "Practical homomorphic encryption: A survey," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Melbourne, VIC, Australia, Jun. 2014, pp. 2792–2795.
[91] H. Hayouni and M. Hamdi, "Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues," in *Proc. IEEE 13th Int. Conf. Netw., Sens., Control (ICNSC)*, Mexico City, Mexico, Apr. 2016, pp. 1–6.
[92] B. F. França. (Apr. 2015). *Homomorphic Mini-Blockchain Scheme*. Accessed: Aug. 3, 2018. [Online]. Available: http://cryptonite.info/files/HMBC.pdf
[93] D. Lukianov. (Dec. 2015). *Compact Confidential Transactions for Bitcoin*. Accessed: Aug. 3, 2018. [Online]. Available: http://voxelsoft.com/dev/cct.pdf
[94] *Information Technology—Security Techniques—A Framework for Identity Management—Part 1: Terminology and Concepts*, document ISO/IEC 24760-1:2011, ISO/IEC, 2011. Accessed: Nov. 7, 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-3:ed-1:v1:en
[95] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.
[96] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.
[97] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management," in *Proc. DASC/PiCom/DataCom/CyberSciTech*, Athens, Greece, 2018, pp. 724–729.
[98] A. Othman and J. Callahan, "The Horcrux protocol: A method for decentralized biometric-based self-sovereign identity," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Rio de Janeiro, Brazil, 2018, pp. 1–7.
[99] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," *IEEE Access*, vol. 6, pp. 28203–28212, 2018.
[100] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered IoT users," in *Proc. IEEE 1st Int. Conf. Internet-Things Design Implement. (IoTDI)*, Berlin, Germany, Apr. 2016, pp. 13–24.
[101] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," in *Proc. 18th Int. Conf. Adv. Commun. Technol. (ICACT)*, Pyeongchang, South Korea, Jan./Feb. 2016, pp. 117–123.
[102] A. O. F. Atya, Z. Qian, S. V. Krishnamurthy, T. La Porta, P. McDaniel, and L. Marvel, "Malicious co-residency on the cloud: Attacks and defense," in *Proc. IEEE Conf. Comput. Commun.*, Atlanta, GA, USA, May 2017, pp. 1–9.
[103] *CONIKS*. Accessed: Nov. 2018. [Online]. Available: https://coniks.cs.princeton.edu
[104] *Google's Certificate Transparency*. Accessed: Nov. 2018. [Online]. Available: https://www.certificate-transparency.org
[105] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, Apr. 2011.
[106] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services*, Honolulu, HI, USA, Jun. 2017, pp. 468–475.
[107] *Augur*. Accessed: Jul. 2018. [Online]. Available: https://www.augur.net/
[108] *Gnosis*. Accessed: Jul. 2018. [Online]. Available: https://gnosis.pm/
[109] *Oraclize*. Accessed: Jul. 2018. [Online]. Available: http://www.oraclize.it/
[110] V. Buterin *et al.*, "Ethereum white paper: A next-generation smart contract and decentralized application platform," White Paper, 2014.
[111] Q. DuPont, "Experiments in algorithmic governance: A history and ethnography of 'The DAO,' a failed Decentralized Autonomous Organization," in *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance*, M. Campbell-Verduyn, Ed. Evanston, IL, USA: Routledge, 2017.
[112] *ERC Project. P2P Models*. Accessed: Nov. 2018. [Online]. Available: https://p2pmodels.eu/
[113] N. Fabiano, "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard," in *Proc. Int. Conf. Internet Things Global Community (IoTGC)*, Funchal, Portugal, Jul. 2017, pp. 1–7.
[114] M. Raskin. (2017). *The Law and Legality of Smart Contracts (September 22, 2016). Georgetown Law Technology Review 304*. Accessed: Nov. 2018. [Online]. Available: https://ssrn.com/abstract=2959166 and http://dx.doi.org/10.2139/ssrn.2842258
[115] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts SoK," in *Proc. Int. Conf. Principles Secur. Trust*, Uppsala, Sweden, Apr. 2017, pp. 164–186.
[116] *Commercial White Paper, BTS-BPM. Blockchain and the Benefits It Brings to F&A Teams Across Industries*. Accessed: Dec. 2018. [Online]. Available: http://bps.techmahindra.com/pdf/White-Paper-Block-chain-and-its-usage-in-FA.PDF
[117] *Self-Piloted Cars: The Future of Road Transport?* Eur. Parliament's Committee Transport Tourism, Directorate-Gen. Internal Policies, Policy Dept. B: Structural Cohesion Policies, Transport Tourism, Res. TRAN Committee, Brussels, Belgium, Mar. 2016.
[118] *Competing for the Connected Customer—Perspectives on the Opportunities Created by Car Connectivity and Automation, Advanced Industries*, McKinsey Company, New York, NY, USA, Sep. 2015.
[119] *European Parliament Resolution of 3 October 2018 on Distributed Ledger Technologies and Blockchains: Building Trust With Disintermediation (2017/2772(RSP))*. Accessed: Dec. 2018. [Online]. Available: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN
[120] S. Nascimento, A. Pólvora, and J. Sousa-Lourenço, *Blockchain4EU: Blockchain for Industrial Transformations*, document EUR 29215 EN, Publications Office of the European Union, Luxembourg city, Luxembourg, 2018.
[121] European Road Transport Research Advisory Council (ERTRAC). (2018). *Strategic Research Agenda, Input to 9th EU Framework Programme*. Accessed: Dec. 2018. [Online]. Available: https://www.ertrac.org/uploads/documentsearch/id52/ERTRAC-Strategic-Research-Agenda-SRA-2018.pdf
[122] D. Stenholm, K. Stylidis, D. Bergsjö, and R. Söderberg, "Towards robust inter-organizational synergy: Perceived quality knowledge transfer in the automotive industry," in *Proc. 21st Int. Conf. Eng. Design*, vol. 6, Vancouver, BC, Canada, 2017, pp. 11–20.
[123] Y. Kayikci, "Sustainability impact of digitization in logistic," *Procedia Manuf.*, vol. 21, pp. 782–789, 2018.
[124] World Economic Forum in Collaboration With Accenture, "Digital transformation of industries: Automotive industry," World Economic Forum, Geneva, Switzerland, White Paper, Jan. 2016.
[125] *GlobalAutomakers*. Accessed: Dec. 2018. [Online]. Available: https://www.globalautomakers.org
[126] Ernst & Young, "Automotive retail 2030—Evolution of dealerships and potential new roles in retail," Ernst Young, London, U.K., White Paper, 2018.
[127] C. Murry and H. S. Schneider, "The economics of retail markets for new and used car," in *Handbook on the Economics of Retailing and Distribution*, vol. 343. Cheltenham, U.K.: Edward Elgar Publishing, 2016.
[128] *Robust Sense Project*. Accessed: Dec. 2018. [Online]. Available: https://robustsense.eu/project.html
[129] K. L. Brousmiche, T. Heno, C. Poulain, A. Dalmieres, and E. B. Hamida, "Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned," in *Proc. IEEE Int. Conf. New Technol., Mobility Secur.*, Feb. 2018, pp. 1–5.
[130] X. Luan, L. Cheng, Y. Zhou, and F. Tang, "Strategies of car-sharing promotion in real market," in *Proc. IEEE Int. Conf. Intell. Transp. Eng.*, Singapore, Sep. 2018, pp. 159–163.
[131] *OakenInnovation*. Accessed: Dec. 2018. [Online]. Available: https://www.oakeninnovations.com/
[132] *Cube Partners, P2P Car-Sharing*. Accessed: Dec. 2018. [Online]. Available: https://cubeint.io/
[133] Z. Han-Jiang and G. Fang, "The study of a dual-channel automotive supply chain based on Internet of Things," in *Proc. Int. Conf. Manage. Sci. Eng.*, Harbin, China, 2013, pp. 650–658.
[134] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, to be published. doi: 10.1109/TII.2018.2887101.
[135] *Volvo DriveMe*. Accessed: Dec. 2018. [Online]. Available: https://www.volvocars.com/intl/buy/explore/intellisafe/autonomous-driving/how-it-works
[136] *Tesla Autopilot*. Accessed: Dec. 2018. [Online]. Available: https://www.tesla.com/en_EU/autopilot

[137] N. Boysen, S. Emde, M. Hoeck, and M. Kauderer, "Part logistics in the automotive industry: Decision problems, literature review and research agenda," *Eur. J. Oper. Res.*, vol. 242, no. 1, pp. 107–120, 2015.

[138] F. Lamberti, V. Gatteschi, C. Demartini, M. Pelissier, A. Gomez, and V. Santamaria, "Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 72–81, Jul. 2018.

[139] 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.

[140] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?" *Future Internet*, vol. 10, no. 2, p. 20, Feb. 2018.

[141] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.

[142] A. Wright and P. De Filippi. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Accessed: Jul. 2018. [Online]. Available: https://ssrn.com/abstract=2580664

[143] *Global Automotive Warranty Survey Report*. Accessed: Nov. 2018. [Online]. Available: https://www.bearingpoint.com/files/AutoWarrantyReport_final_web.pdf

[144] J.-H. Thun and D. Hoenig, "An empirical analysis of supply chain risk management in the German automotive industry," *Int. J. Prod. Econ.*, vol. 131, no. 1, pp. 242–249, 2011.

[145] D. Mathivathanan, D. Kannan, and A. N. Haq, "Sustainable supply chain management practices in Indian automotive industry: A multi-stakeholder view," *Resour., Conservation Recycling*, vol. 128, pp. 284–305, Jan. 2018.

[146] P. Fraga-Lamas, T. M. Fernández-Caramés, D. Noceda-Davila, and M. Vilar-Montesinos, "RSS stabilization techniques for a real-time passive UHF RFID pipe monitoring system for smart shipyards," in *Proc. IEEE Int. Conf. RFID (IEEE RFID)*, Phoenix, AZ, USA, May 2017, pp. 161–166.

[147] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "A methodology for evaluating security in commercial RFID systems," in *Radio Frequency Identification*, 1st ed., P. C. Crepaldi and T. C. Pimenta, Eds. Rijeka, Croatia: InTech, 2016.

[148] P. Fraga-Lamas and T. M. Fernández-Caramés, "Reverse engineering the communications protocol of an RFID public transportation card," in *Proc. IEEE Int. Conf. RFID*, Phoenix, AZ, USA, May 2017, pp. 30–35.

[149] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and L. Castedo, "Reverse engineering and security evaluation of commercial tags for RFID-based IoT applications," *Sensors*, vol. 17, no. 1, p. 28, 2017.

[150] *IOTA*. Accessed: Aug. 3, 2018. [Online]. Available: https://www.iota.org

[151] A. Collomb and K. Sok, "Blockchain/distributed ledger technology (DLT): What impact on the financial sector?" *DigiWorld Econ. J.*, no. 103, pp. 93–111, 3rd Quart., 2016.

[152] *Carvertical*. Accessed: Jul. 2018. [Online]. Available: https://www.carvertical.com/

[153] T. M. Fernández-Caramés, O. Blanco-Novoa, M. Suárez-Albela, and P. Fraga-Lamas, "An UAV and blockchain-based system for Industry 4.0 inventory and traceability applications," in *Proc. 5th Int. Electron. Conf. Sens. Appl.*, Nov. 2018, p. 1.

[154] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on human-centered IoT-connected smart labels for the Industry 4.0," *IEEE Access*, vol. 6, pp. 25939–25957, 2018.

[155] D. Heber and M. Groll, "Towards a digital twin: How the blockchain can foster E/E-traceability in consideration of model-based systems engineering," in *Proc. 21st Int. Conf. Eng. Design, Product, Services Syst. Design*, Vancouver, BC, Canada, vol. 3, 2017, pp. 321–330.

[156] Q. Qi and F. Tao, "Digital twin and big data towards smart manufacturing and Industry 4.0: 360 degree comparison," *IEEE Access*, vol. 6, pp. 3585–3593, 2018.

[157] *Groupe Renault Teams With Microsoft and VISEO to Create the First-Ever Digital Car Maintenance Book Prototype*. Accessed: Aug. 3, 2018. [Online]. Available: https://bit.ly/2LXNUre

[158] *Blockchain: Bosch and TÜV Rheinland Present a Solution for Odometer Fraud*. Accessed: Aug. 3, 2018. [Online]. Available: https://bit.ly/2LMojCp

[159] *Car Next Door*. Accessed: Aug. 3, 2018. [Online]. Available: https://www.carnextdoor.com.au/

[160] *Toyota*. Accessed: Aug. 3, 2018. [Online]. Available: http://corporatenews.pressroom.toyota.com/releases/toyota+research+institute+explores+blockchain+technology.htm

[161] *Docusign*. Accessed: Aug. 3, 2018. [Online]. Available: https://www.docusign.com/products/blockchain

[162] *Daimler and LBBW Successfully Utilize Blockchain Technology for Launch of Corporate Schuldschein*. Accessed: Aug. 3, 2018. [Online]. Available: https://media.daimler.com/marsMediaSite/en/instance/ko/Daimler-and-LBBW-successfully-utilize-blockchain-technology-for-launch-of-corporate-Schuldschein.xhtml?oid=22744703

[163] *Car eWallet*. Accessed: Aug. 3, 2018. [Online]. Available: https://carewallet.zf.com/site/carewallet/en/car_ewallet.html

[164] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. A. Díaz-Bouza, "A fog computing based cyber-physical system for the automation of pipe-related tasks in the Industry 4.0 shipyard," *Sensors*, vol. 18, no. 6, p. 1961, 2018.

[165] *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)*, IEEE Standard 1609.12-2016 (Revision of IEEE Std 1609.12-2012). Accessed: Aug. 3, 2018. [Online]. Available: https://standards.ieee.org/findstds/standard/1609.12-2016.html

[166] M. Singh and S. Kim, "Introduce reward-based intelligent vehicles communication using blockchain," in *Proc. Int. SoC Design Conf. (ISOCC)*, Seoul, South Korea, 2017, pp. 15–16.

[167] 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.

[168] M. Suárez-Albela, P. Fraga-Lamas, T. M. Fernández-Caramés, A. Dapena, and M. González-López, "Home automation system based on intelligent transducer enablers," *Sensors*, vol. 16, no. 10, p. 1595, Sep. 2016.

[169] 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. 13565–13574, 2018.

[170] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Comput. Sci. Res. Develop.*, vol. 33, nos. 1–2, pp. 71–79, 2017.

[171] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[172] M. G. M. M. Hasan, A. Datta, M. A. Rahman, and H. Shahriar, "Chained of Things: A secure and dependable design of autonomous vehicle services," in *Proc. 42nd IEEE Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Tokyo, Japan, Jul. 2018, pp. 498–503.

[173] E. Birrell and F. B. Schneider, "Federated identity management systems: A privacy-based characterization," *IEEE Security Privacy*, vol. 11, no. 5, pp. 36–48, Sep./Oct. 2013.

[174] *International Telecommunications Union (ITU) Focus Group on Application of Distributed Ledger Technology (FG DLT)*. Accessed: Dec. 2018. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[175] *International Standards Organisation (ISO) Technical Committee 307 on Blockchain and Distributed Ledger Technologies*. Accessed: Dec. 2018. [Online]. Available: https://www.iso.org/committee/6266604.html

[176] *European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) Focus Group on Blockchain and Distributed Ledger Technologies (DLT)*. Accessed: Dec. 2018. [Online]. Available: https://www.cencenelec.eu/standards/Sectors/ICT/BlockchainLedgerTechnologies/Pages/default.aspx

[177] CENELEC, "Recommendations for successful adoption in europe of emerging technical standards on distributed ledger/blockchain technologies," CEN-CENELEC Focus Group Blockchain Distrib. Ledger Technol., Torino, Italy, White Paper 001, Sep. 2018.

[178] *Blockchain in Transport Alliance (BiTA)*. Accessed: Dec. 2018. [Online]. Available: https://bita.studio/

[179] *IEEE Blockchain*. Accessed: Dec. 2018. [Online]. Available: https://Blockchain.ieee.org/
[180] *MOBI*. Accessed: Aug. 3, 2018. [Online]. Available: https://www.dlt.mobi/

PAULA FRAGA-LAMAS (M'17) received the M.Sc. degree in computer science from the Universidade da Coruña (UDC), in 2009, and the joint M.Sc. and Ph.D. degrees in mobile network information and communication technologies from five Spanish universities: the University of the Basque Country, the University of Cantabria, the University of Zaragoza, the University of Oviedo, and UDC, in 2011 and 2017, respectively. She holds an MBA and master's studies in business innovation management (JMC of European Industrial Economy), sustainability (CSR), and social innovation (INDITEX-UDC Chair). Since 2009, she has been with the Group of Electronic Technology and Communications, Department of Computer Engineering, UDC. She has been participating in more than 20 research projects funded by the regional and national government and research and development contracts with private companies. She has co-authored more than 50 peer-reviewed indexed journals, international conferences, and book chapters. Her current research interests include wireless communications in mission-critical scenarios, Industry 4.0, the Internet of Things, augmented reality, blockchain, RFID, and cyber-physical systems.

TIAGO M. FERNÁNDEZ-CARAMÉS (S'08–M'12–SM'15) received the M.Sc. and Ph.D. degrees in computer science from the Universidade da Coruña, Spain, in 2005 and 2011, respectively, where he has been a Researcher and a Professor with the Group of Electronic Technology and Communications, Department of Computer Engineering, since 2005. His current research interests include the IIoT/IoT systems, RFID, wireless sensor networks, Industry 4.0, blockchain, and augmented reality.