Journal of Cybersecurity and Privacy

MDPI

Review

Using Blockchain for Data Collection in the Automotive Industry Sector: A Literature Review

Abdulghafour Mohammad *, Sergio Vargas and Pavel Čermák

The Department of Informatics, University West, 461 32 Trollhattan, Sweden; sergio.vargas@student.hv.se (S.V.); pavel.cermak@student.hv.se (P.Č.)

* Correspondence: abdulghafour.mohammad@hv.se

Abstract: Today's cars can share data with other cars, automakers, and service providers. Shared data can help improve the driving experience, the performance of the car, and the traffic situations. Among all data-collection techniques, blockchain technology offers an immutable and secure solution to support data collection in the automotive industry. Despite its advantages, collecting auto data with blockchain still faces several challenges. Thus, the purpose of this study was to conduct a review of published articles that have addressed the challenges of adopting blockchain for data collection in the automotive industry. This paper allowed us to answer the predefined research question: "What are the challenges of using blockchain for data collection in the automotive industry as presented in the published literature?" The review included articles published from 2017 to January 2022, and from the screened records, 13 articles were analyzed in full-text form. The founded challenges were categorized into seven categories: connectivity, privacy, security attacks, scalability, performance, costs, and monetizing. This review will help researchers, car manufacturers, and third-party suppliers to assess the applicability of the blockchain for data collection.

Keywords: blockchain; automotive industry; data collection; security attacks; cost; efficiency; connectivity; latency; monetizing

Citation: Mohammad, A.; Vargas, S.; Čermák, P. Using Blockchain for Data Collection in the Automotive Industry Sector: A Literature Review. *J. Cybersecur. Priv.* **2022**, *2*, 257–275. https://doi.org/10.3390/jcp2020014

Academic Editor: Danda B. Rawat

Received: 2 March 2022
Accepted: 11 April 2022
Published: 13 April 2022

1. Introduction

The collection of vehicle data is a promising technology. In recent years, car manufacturers have benefited from Internet connections, cameras, and sensors integrated into the current cars to gather valuable information about cars. In addition, the number of vehicles connected to the Internet will increase over time; according to Statista, this number will be more than 400 million cars by 2025, compared with 237 million in 2021 [1]. As the number of connected cars grows rapidly, the amount of data collected will increase respectively. It is estimated that these data make connected vehicles safer, more fuel-efficient, more environmentally friendly, and better to navigate the roads and avoid traffic congestion [1]. In addition, these data are expected to enable better diagnosis of vehicles, maintenance, and other car services. Therefore, the technology that collects data has attracted great attention from academics and automotive companies to provide their customers with better services and options.

Despite all of these advantages, communication between automobiles is still insecure, and there are still several security gaps, such as privacy and reliability of data [2]. This is due to the inability of the traditional security methods used to collect and transfer data [3]. The collection of vehicle data also faces a number of serious ethical issues, such as where it is stored, how it is processed, and who is authorized to access it. In addition, we must take into account the sensitivity of the data collected; for example, the location might breach the customer's privacy [4].

A blockchain is a distributed database of all digital events and transactions implemented and shared among participating entities [5]. To avoid security vulnerabilities and

the technical and ethical limitations of traditional methods, blockchain, with its attractive functionality, offers solutions to various security problems [5–8]. In addition, it offers a secure option for the collection of automotive data [9–20]. These characteristics have been described by Reference [8], as follows:

- Decentralized: It does not require a centralized node to record, store or update data; instead, data can be recorded, stored, and updated in a distributed manner.
- Transparent: Data recording is transparent for each node, even when updating data, and this is why blockchain can be trusted.
- Open Source: People can use blockchain technologies to create any application, and records can be checked openly.
- Autonomy: All system nodes can securely transfer or update data, and no one can intercede.
- Immutable: Records will be kept indefinitely and can only be modified if 51% of the nodes are controlled simultaneously.
- Anonymity: The transport of data and even transactions can be anonymous, with only the addresses being know.

Although the use of blockchain for data collection is growing rapidly in academia and industry, several technical, ethical, and security challenges are reported [9–21]. Among all of these challenges are privacy [21], transaction latency, minimal throughput, difficult commit processes, and scalability [9]. To the best of the authors' knowledge, this is the first scholarly article to review the state-of-the-art blockchain adoption challenges for data collection in the automotive industry. Reference [2] carried out a review to analyze the ability of blockchain technologies to be used in the automotive industry. However, this review focused solely on a business administration and cybersecurity perspective by examining the challenges faced by key stakeholders in adopting blockchain. Furthermore, this review did not address the challenges of data collection in this sector. The review conducted in Reference [7] considered only solutions to address the privacy challenges that evolve from the network level in conventional blockchains. Although Reference [8] conducted a survey of the general challenges of blockchain adoption for governments and organizations, this survey was a general survey, and it did not examine the data-collection challenges in the automotive industry. Other researchers in this field have sought to consider blockchain solutions for the collection of data in the automotive sector. However, some of these solutions have not been implemented or tested in the real world [12,17,18,20], or are not yet usable [14] and even simply descriptive [13]. Furthermore, other solutions are vulnerable to cyber-attacks [11,16]. Even a solution that uses lightweight blockchain does not consider the security and scalability aspects [15], and the real-time application to solve Vehicle-to-Everything communication (V2X) does not take these features into account. [10]. However, the purpose of this review was to conduct a review of published articles that have addressed the challenges of adopting blockchain for data collection in the automotive industry. Thus, this review classified these challenges into seven categories, namely connectivity, privacy, security attacks, performance, costs, and monetizing. Therefore, the review aims to summarize these challenges to help researchers and car manufacturers assess the applicability of blockchain use to collect data in the automotive sector.

The rest of the paper is organized as follows. The Methods section describes the methodology used to search and filter articles. The Results section focuses on analyzing and presenting the findings obtained from the selected articles. In addition, we present the important findings, limitations, and future directions of research. Finally, the last section is the conclusion.

2. Methods

This study set out to answer the following research question:

"What are the challenges of using blockchain for data collection in the automotive industry as presented in the published literature?"

This research question was used to determine the content and structure of the review, to design strategies, to locate and select primary studies, to critically evaluate studies, and to analyze their results.

2.1. Search Method

A review of the literature concerning the adoption of blockchain technology to collect data from automobiles was conducted by using Springer, IEEE, MDPI, and Google Scholar. The following combinations of keywords were used to find relevant data ("data collection" AND blockchain AND vehicle AND privacy), ("driver data" AND blockchain AND automotive AND privacy), (blockchain AND cars), (blockchain AND automotive AND data collection), (blockchain AND driver data), and (automotive AND data AND blockchain). Relevant papers were also located by reviewing the references of previously found papers (backward search) and finding newer publications that contained the cited article (forward search).

2.2. Criteria

The articles were reviewed to meet four basic criteria: the study was written in English, published from 2017 to 2022, the article focused on blockchain, the study focused on automotive industry solutions, and the study used diverse data-collection methods. Studies that did not focus particularly on the blockchain were not focused on data collection (i.e., data from driver or vehicle) and did not focus on vehicles were all excluded.

2.3. Information Extraction

Information concerning challenge types, solutions, and study design characteristics was extracted from the articles. The information collected for each study concerned mainly blockchain solutions objectives, cases such as Vehicle-to-Vehicle or Vehicle-to-Human communication, privacy orientation, monetization of data collection, and security attacks. We have also taken note of the findings of the research and the conclusions drawn by the authors. To determine eligibility and extract answers to the research question, the three authors independently reviewed each of the relevant articles. Any differences between the three authors were resolved by discussion and agreement. This process was carried out by using the NVivo 12 analysis tool to facilitate the organization and analysis of unorganized data and to make better decisions. The characteristics of NVivo—in this case, the queries—serve for thematic analysis and the creation of notes, as well as the familiarity with the terms. The discrepancy between the codification of the three authors was minimal and resolved effectively. The articles and references were handled by using Mendeley software.

2.4. The Review Process

The selection process for the review was as follows: The first step was to search for databases on the topics to be addressed. The search terms mentioned above were used in these databases. Once the duplicates were deleted, the three authors of the article proceeded to a meticulous reading, and the definitive ones were selected according to the above criteria. To ensure up-to-date information, filtering by publication date was used, so articles published before 2017 were deleted, except for Google Scholar (where stricter filtering methods were chosen due to numerous results, exactly to show articles only from 2021 onward). To ensure the validity and reliability of the materials, a second filter rule was chosen, which requires the material to be an article or book. After applying all filters, results for each database were as follows: Springer 4553 articles, IEEE 36 articles, MDPI 17 articles, and Google Scholar 2286 articles. Relevant articles have also been discovered by reviewing references to previously identified articles (backward search) and finding newer works that incorporated the cited material (forward search). A total of 6843 records were screened for title and abstract, and 6789 were excluded. A total of 54 articles were evaluated for the full-text review, and 41 were excluded, because 22 articles did not focus on the automotive industry, 9 articles were not available in full text, and 8 did not mention

data collection. Thirteen articles were included as a valid source of data for this article. The number of articles that were located, evaluated, included, or excluded is shown in Figure 1.

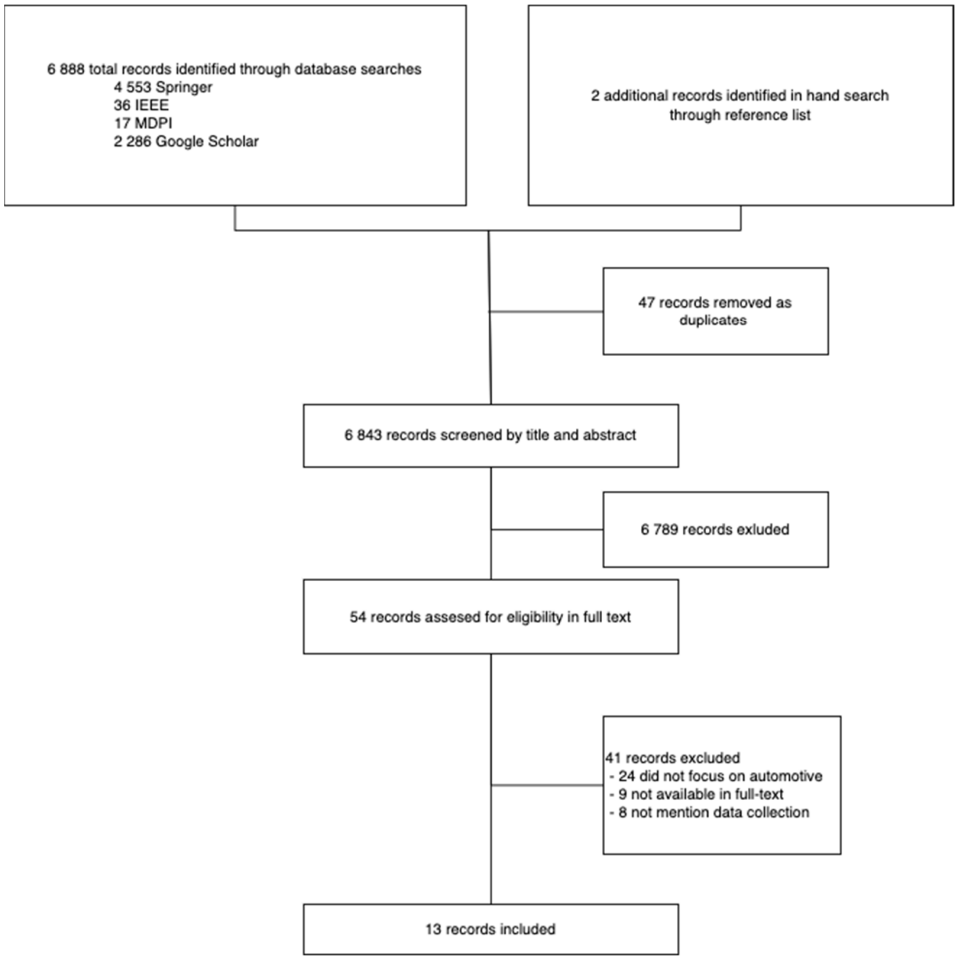

Figure 1. Diagram of the review process flow.

2.5. Characteristics of Research Studies

A total of 8 out of the 13 articles proposed blockchain solutions, such as a new model, framework, algorithm, or scheme (see Table 1). Five articles were literature reviews. A total of 12 of the 13 articles were published in 2019 and 2021, while only one was published in 2017 (see Figure 2).

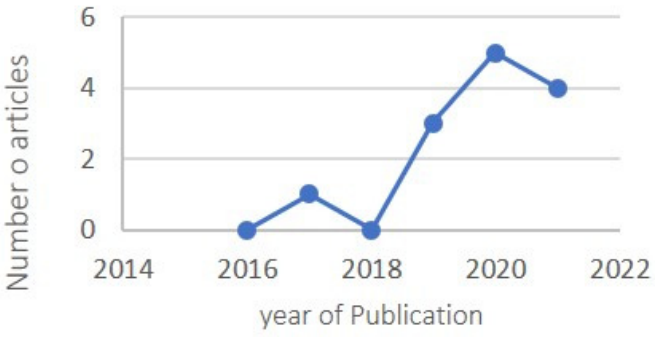

Figure 2. Publication year of included articles.

Table 1. List of relevant studies.

Ref	Year	Objective(s)	Techniques/Algorithms	Limitations
[8]	2021	Offer architecture for collecting traffic data with a focus on security and latency.	Deep Reinforcement Learning DRL algorithm empowered with Spatial Crowdsourcing System.	The offered solution has been tested only in a simulated environment and should move into a real test environment with real equipment.
[12]	2021	Introduce a framework for storing data from the Internet of Vehicles by using blockchain technology to follow the General Data Protection Regulation (GDPR).	Blockchain-based solution updated to fulfill the GDPR law.	The proposed architecture has not been tested either in reality or in simulation.
[15]	2021	Come up with a method of using a blockchain to solve the privacy problem and forgery of black-box image data.	Lightweight blockchain consensus algorithm	This blockchain lightweight solution is not facing the scalability and security topics, essential in the automotive industry.
[17]	2021	To resolve issues in terms of the secure and reliable sharing of sensory data in vehicular fog.	2-DNF cryptosystem with an identity-based signcryption scheme	The solution is not implemented and tested in the real environment.
[18]	2021	Offer a framework for Intelligent Transportation Systems (system for smart control of the traffic) by using blockchain technology.	The DRL-enabled algorithm is based on Blockchain.	The proposed system has been tested only in simulations, not in a real environment.
[9]	2020	Propose and implement proof-of-concept of architecture in which each car generates and sends reports, including the messages received from its neighbors, to the network infrastructure, which collects and stores the received reports through multiple blockchains based on geographical area.	The BIOFOCAL architecture is used to store and validate the CAMs that are exchanged between connected vehicles.	The article does not analyze the security in the architecture offered. Their solution is just based locally.
[10]	2020	To adapt blockchain technology for real-time application (RTA) to solve Vehicle-to-Everything (V2X) communications problems.	Ethereum Blockchain, proof of work (PoW).	The proposed blockchain system does not explain how it ensures the scalability of the solution.
[14]	2020	Present a blockchain-enabled AVSN framework to safeguard content delivery and investigate reputation models of CAVs and RSUs	Blockchain-based algorithm with PoR consensus protocol.	The solution depends on how to shard blockchain. Currently, all proposed algorithms and systems are under development, thus making the solution not usable at the current time.
[16]	2020	Develop a mechanism to offer personalize rental products and insurance products based on blockchain technology	PoS consensus with Bloom filter.	Security attacks are not considered in the paper; they were proposed as future work but not developed. There is no specific application to the automotive industry that is currently suggested.

Table 1. *Cont.*

Ref	Year	Objective(s)	Techniques/Algorithms	Limitations
[11]	2019	To propose a framework based on a permissioned blockchain that allows them to guarantee both driver data protection and evidential property of data.	Permissioned blockchain Ethereum, PoA (Metamask/Geth).	There is the risk of different cyberattacks, such as signal sniffing and possible malicious manipulation.
[19]	2020	Compare two possible solutions for car-sharing based on the Ethereum network.	Ethereum based blockchain, the Blockchain proof of concept (POC) with ZoKrates and Indy technologies.	One of the designed systems expects a connection to blockchain databases maintained by the government. Implementation of blockchain by the government is expected to take a long time.
[13]	2019	Describe privacy and security concerns about collecting drivers' data, but also showing their usability and a way that blockchain technology can assure the security of the data.	No solution, but as a future work, Reference [13] suggested a solution to offer various parties clear, safe, and trustworthy transactions of vehicle-collected data.	The article did not propose any specific platform, system, or solution.
[4]	2017	Proposal of blockchain architecture to protect the privacy of users and increase the security of vehicular ecosystems.	Changeable public keys technique in Lightweight Scalable Blockchain (LSB).	The blockchain solution does not offer a real implementation and does not go beyond possible use cases with specific actuation.

3. Results

At each level of the selection process, the number of studies identified, screened, and included or rejected is shown in Figure 1. The review includes a total of thirteen articles. Table 1 shows more detailed information on the research included in this review, as well as the objectives, methods, limitations, and challenges of each manuscript contained in the review.

The reviewed articles showed different challenges. These challenges should be considered when using blockchain for data collection in the automotive industry. We used the technology, organization, and environment (TOE) paradigm [22] to characterize the challenges. Researchers have utilized this approach extensively to analyze the adoption of information technology. The technological, organizational, and environmental aspects are all utilized in this framework to define technological advancement adoption decisions. The technological perspective defines the technological attributes that are related to the adopting organization, such as its security, scalability, performance, and cost-effectiveness. The organizational perspective implies the organizational attributes and assets of the organization, such as auditing, trust, and organizational readiness, that are important to the acceptance of technology. In the environmental setting, the environmental attributes in which the organization performs its essential services, such as monetizing, laws and regulations support, infrastructure support, and connectivity, are analyzed. This review focused on technological and environmental perspectives to categorize the challenges for adopting blockchain for collecting data in the automotive industry, as stated in the selected articles. Table 2 presents these categories and related articles that are included in each of these categories. Challenges related to technological characteristics obviously dominate the results from the articles. Security, performance, scalability, and cost-effectiveness are identified as the key technological challenges. It is interesting to note that security, the main force of blockchain technology, is still the main aspect questioned by many researchers. However, more details about these challenges are presented in the Results and Discussion sections.

Table 2. Categories of reviewed articles.

Aspects	Challenges	Description	Authors
Technological	Privacy	Protection of personal data and information collected from vehicle systems, such as location data and financial information.	[4,10–12,18]
	Security attacks	Security vulnerabilities in the vehicle's systems (hardware or software components) or any flaws in the connection.	[4,5,9–11,18,19]
	Scalability	The impact of blockchain use on data collection in the automotive industry from a scalability angle.	[4,9,10,16,18]
	Performance	The efficiency of the proposed solutions for data gathering.	[4,9,10,16,18–20]
	Cost	The transaction, services, and data-gathering costs.	[4,9–13,16,19]
Environmental	Connectivity	How a vehicle can be connected to its surroundings and communicate with them.	[9–11]
	Monetizing	The different alternatives to monetize data collection in the automotive industry thanks to blockchain technology.	[4,9–11,13,15,16,19]

3.1. Connectivity

Despite the benefits of blockchain, this technology suffers from significant drawbacks, such as transaction latency, minimal throughput, and difficult commit processes [9]. In addition, the time it takes to update a transaction onto a blockchain is the major source of worry [10]. This is due to the significant amount of processing required to commit

a transaction to the ledger for all agents [9]. To solve this issue, some of the solutions considered bulk report commits. That is, when a predetermined number of reports have been gathered, then a transaction is issued that causes numerous reports to be stored in the blockchain at the same time for the cost of a single commit [9]. Another approach is, instead of having a single blockchain layer in charge of communication over a broader territory, distinct blockchain levels inside smaller regions would make it easier for a limited number of cars by focusing on minimizing message size to increase transaction speed [10]. In Reference [10], receiving data from a blockchain once or hundreds of times had no significant impact on the execution time. However, storing data takes a long time, since the message must be mined before it can be added to the smart contract. In Reference [18], a large number of devices could connect simultaneously to the same base station to upload data when cluster heads uploaded messages to their nearest base stations.

Most of the proposed solutions have been tested and have shown significant improvement in blockchain technology, particularly with respect to the processing time. In Reference [4], the processing time associated with validating blocks decreased when using the Lightweight Scalable Blockchain (LSB) instead of the Bitcoin blockchain. In Reference [15], using a blockchain consensus algorithm instead of the PBFT (Practical Byzantine Fault Tolerance) algorithm reduced the time of uploading and downloading from 46 to 17 ms.

Another challenge to consider is that, as vehicles are fast-moving objects, there is not always a good connection with the receiver. In Reference [11], The researchers focused on the calculation of the 4G network in Italy. Even if the best case cannot be reached most of the time, we can certainly assume a bandwidth of 5.5 MB per second, which is sufficient for their solution, where the average message size is less than 5.5 MB [11]. In Reference [10], a hybrid system was proposed, either via Wi-Fi or via mobile Internet (3G/3G+/4G). Before transferring data to the server, the system in Reference [10] captured data locally. However, this method was shown to be an ineffective method of data collection when the connection is weak or unstable.

One of the connectivity challenges for the Internet of Vehicles (IoV) is latency, which is often faced in offering real-time cloud services to vehicular cloud subscribers, considering that all models targeted at improving the security and efficiency of the system require additional communication protocols [10]. In order to reduce latency, fog computing can be employed to provide real-time services to vehicular cloud subscribers [10]. To link them to vehicular clouds, the proposed method used single-hop mobile links (i.e., I2V TCP/IP-based) and Networked Fog Centers (NetFCs) at the network's edge. As a result, the vehicle service delivery time is reduced, and the overall efficiency is increased [10].

Other connectivity challenges in the IoV, especially in the Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications, are to guarantee high-speed, reliable connectivity, and accurate recording and collecting of data. However, in one of the 13 selected articles, Reference [10], the authors developed a blockchain-enabled Internet of Things (IoT) system by using a real-time application (RTA), adopting blockchain technology to overcome Vehicle-to-Everything (V2X) communication issues. The proposed solution created secure communication and built an entirely decentralized cloud computing platform. Furthermore, it improved connectivity by ensuring an easy data trade between different actors of intelligent transportation systems. However, the proposed approach might be built to include a reputational assessment mechanism for untrustworthy data sources [10].

As the blockchain is a perfect addition to vehicle communications, since it can increase interoperability, privacy, reliability, and scalability of the underlying infrastructure [23], in the context of resource management, blockchains can be used to perform spectrum sharing and store all spectrum usage and lease requests [23]. In addition, it can provide the necessary incentive for devices to share and exchange resources, as the current protocols do not include incentives to do so. The use of blockchain to collect vehicle data can offer rewards whenever devices share their power or data, thus allowing for a more cooperative and reliable network environment [23]. Furthermore, this reward approach can be used for

spectrum sharing, where a reward can be granted each time a user leases one spectrum to another, fostering spectrum efficiency and creating a more collaborative setting [23]. Moreover, by motivating cars to exchange power or information, blockchain can be utilized in the field of Vehicular-to-Anything (V2X) communication [23]. Furthermore, how to ensure secure communication between automobiles and public key infrastructures is a vital part of V2X communication (PKI). Blockchain can be employed as the infrastructure to enable private and secure communications to PKI, as well as communication between PKIs from various vendors [23].

Reference [23] dove deeper into the topic of blockchain-enabled resource sharing and spectrum management to overcome connectivity challenges. Based on this, Reference [23] argued that sixth-generation (6G) network-blockchain-enabled resource management, spectrum management, computing, and energy trading will be the key factors behind future application scenarios including autonomous vehicles and unmanned aerial vehicles (UAVs). In order to enable the blockchain resource and spectrum management, these resources are assumed to be in a pool of resources in which a spectrum is dynamically assigned, network slices are maintained, and infrastructure is virtualized [23]. On the basis of this proposed framework, blockchain can allow the sharing of resources between devices, such as computing power, energy, data, and spectrum lease.

3.2. Privacy

The role of privacy in collecting, storing, managing, and analyzing data from vehicle sensors is significant. In the European Union's regulatory discussion, privacy issues and regulation are a timely and pressing topic. The General Data Protection Regulation (GDPR) and all national laws that recognize, apply, or develop it have had a significant impact on both the provision of technological services and on the general attitude toward personal data [12]. Data, such as driving behavior, direction, trip data, fueling data, breaking and accelerating behavior, location, and so on, contain private information that can be used to identify the driver. Furthermore, because the data acquired from automobiles depend on the driver, data collected from a vehicle raise privacy problems. At the same time, because data collection can benefit various industries, the data acquired from vehicles are unavoidable, regardless of privacy concerns [13].

In the past, the only option to collect data was to rely solely on central authorities, putting individuals at risk, as the proper control of personal data did not belong to them [13]. However, the traditional security and data-protection methods used in smart cars were ineffective [13,24–27]. New methods were subsequently proposed; for example, current smart car architectures rely on centralized brokered communication models, in which all vehicles are identified, authenticated, authorized, and connected via central cloud servers. However, as many vehicles are coupled, it is unlikely that this model will be scaled. In addition, cloud servers will remain a bottleneck and a single point of failure that can cause the entire network to go down [4]. Most of the current secure communication architectures either ignore the privacy of users, for example, sending all car data without the owner's permission, or reveal noisy or summarized data to the requester [4]. Therefore, in some smart-car applications, the requester needs accurate vehicle data to provide individualized services [4].

Blockchain technology, with its attractive features, allows for the transparent management of personal data and allows for end-users and service providers to fully control the data obtained. This will attract more users to participate in data collection [4]. In addition, the usage of a blockchain and distributed ledgers transforms the way registry maintenance is performed by providing several benefits, including complete distribution and replication, fairness, reliability, openness, and responsibility-sharing [12]. Furthermore, blockchain is critical for tackling the privacy and security challenges on Internet-of-Vehicles networks (IoV) [10].

All the proposed data-collection solutions from the reviewed articles used hashing solutions for keeping the privacy and anonymity of data in the blockchain [4–20], where the

integrity and security of data stored on blockchain are dependent on cryptographic hashing. In Reference [10], security is ensured through encryption, whereas integrity is achieved by ensuring that signatures are updated when data are modified. Therefore, using asymmetric-key pairs to sign information made it not reputable and only available to stakeholders and authorities with a legitimate interest; for example, when authorized by judges, authorities may disclose it within the legal limits to share responsibilities, ensure and verify the inalterability of information, and reduce risks and protection costs without disclosing information [12]. Furthermore, anonymity and unlinkability can be accomplished by constantly changing pseudonyms (i.e., public keys) in different transactions to mask the genuine identities of drivers [14]. However, very few articles consider the GDPR Act. However, one of the critical issues for blockchain developers in ensuring full GDPR compliance is to comply with the right to rectification (Article 16) and the right to be forgotten (Article 17); this means that the users have the right to seek the rectification of their data and delete their data in certain circumstances. Even if the user does not request it, personal data must be erased when "the personal data are no longer necessary regarding the purposes for which they were acquired or otherwise processed" (Article 17) [12]. The solution for modification and data deletion was proposed by Reference [12]; data modification can be allowed by adding a block with updated information into blockchain, and similarly for data deletion by deleting the key, making encrypted blocks unreadable. However, this solution might cause privacy concerns—for instance, if the encryption is hacked—so even blocks with deleted private keys will become readable again. In Reference [20], the task assignment protocol was proposed that ensures the privacy of both sides, and the mechanism based on DRL was used to improve both privacy and performance. Since workers are analyzed and evaluated, according to the score, malicious workers will be discovered and will not be able to access private data.

3.3. Security Attacks

Vehicles and other automotive products are packed with sensors, computer systems, network entities, and other electromechanical devices. Examples of such systems are found in References [28–40]. This may constitute a security breach with respect to the data collection by these systems. One of these systems is the black box. Various possible attacks on the black box, which is placed by the insurance company in the vehicle, can be made, such as signal sniffing, encrypting the data before sending them. In addition, malicious attacks can be avoided by using the fingerprint as a hash code [11]. However, those attacks are not all the possible security attacks that can lead to low security in the vehicle systems. In Reference [11], the authors did not consider other types of attacks involving data collection in a black box, meaning that their solution is not optimal from a security perspective. In addition, the authors of Reference [15] used a lightweight blockchain in their investigation of the black box, without taking into account the possible attacks it may receive, except that the memory that can be attacked, making it a worse option for data collection from a cyber-security perspective. On the other hand, in the case of Reference [16], active attacks on the vehicle or driver on data integrity are considered, and the system is safe against chosen-ciphertext attacks, as well as against k-collision attack algorithm (KCAA). However, the system must be protected against collusion [17].

Some reviewed articles take the solution from a cyber-attack scenario. For example, Reference [4] laid the foundation in this context: if data are not collected securely, accidents may occur to drivers and passengers. Another example is the linking attack, which is avoided by blockchain data encryption. When the attacker wants to perform an attack on the cloud software, the vehicle collects the data and identifies another hash that quickly detects the infiltrator. In addition, the distribution of fake software updates is considered by requiring the primary key from the real provider [4]. However, one of the key attacks is the Distributed Denial of Service (DDoS) attack; based on a key pair in a key list, the attacker transactions would not generate correspondence in the key list. As a result, it would drop without affecting the target node [4]. Reference [18] also studied this attack;

the authors offered a broader view of data attacks, providing a comprehensive view on which the automotive industry can rely for its services. In addition, the solution of Reference [10] proposed a system for common attacks, such as Man-in-the-Middle (MITM) and DDoS, but without specifying the solution. However, the article has a full list of attacks and their requirements, such as injection, broken authentication, data exposure, using components with known vulnerabilities, or parameter attacks, among others [10]. This is a very comprehensive set that allows the automotive sector to spot a variety of threats. Cyber-attacks on connected cars are also a concern, as they can compromise physical security. The authors of Reference [13] were aware of this and described a blockchain approach based on security for data collection; it focused on the possibility of the driver, vehicle, driving, and traffic data being attacked by the previously mentioned attack methods. However, a specific applicable solution was recommended by the authors for future work.

The solution proposed by Reference [9] did not offer any vision of security beyond that settled by the blockchain itself. However, data-collection solutions must consider offering the users a valuable verification method to collect data between cars. An example is the carpooling service solution that was proposed by Reference [19]. It seems, however, that data-sharing security is poorly studied [14], and it is included often as a future direction of research. Regarding the Internet of Vehicles, the possible attacks are collusion and Sybil; the technical study in Reference [20] could support them and adapt them to the black-box usage, also in a complete view from Reference [12], where the possible corruption of data is analyzed with insurance. Additionally, active attacks can be made to vehicle sensors to violate data integrity with exhausting attacks trying different values [17]. It should be noted that the way to detect malicious vehicles or attackers is when data collected values are too high or too low, leading to incoherence in the blockchain [18].

3.4. Performance

This review showed that not all of the proposed solutions have been tested; however, the solutions that passed the test stage showed good performance results. In Reference [19], experiments were run on an Intel Core i7-4600U CPU 2.10 GHz machine with 8 GB RAM, Windows 10 (Enterprise Edition), with a focus on comparing two proposed solutions: Indy and ZoKrates. Both technologies require about the same amount of time to onboard. When compared to ZoKrates, Indy generates proofs and credentials 60 times quicker and verifies them five times faster. The most common operation in the system is proof verification. Because it is calculated off-chain in Indy, the performance benefit would be significant in (near) real-time applications. When equivalent use cases are explored, Indy-based systems are intrinsically more efficient and performant [19].

In Reference [9], experiments were run by using Docker containers hosted on a private university cloud running on Ubuntu 16.04. The first test focused on the performance of inserting and retrieving data traces within the blockchain. They examined a single organization (a mobile network provider) with two peers and one orderer. The latency for both insertion and query rose linearly with the quantity of data to insert/query, because the auxiliary database eliminated the need to scan the whole blockchain to get a specific item [9].

In Reference [17], experiments were conducted on a desktop with an Intel 3.4-GHz processor, 8-GB RAM, and a Windows 7 platform. The assessments were primarily concerned with the computational overhead imposed by cryptographic processes. They compared the suggested plan to the existing approach and demonstrated the computing overhead of the entire system as the number of cars increased from ten to forty. The suggested technique significantly lowered the computational cost involved [17].

To test the performance of the private Ethereum Blockchain, the authors in Reference [10] set up a server with Core i7-000 and 64-GB RAM. The result of the performance test showed that their solution receiving data from blockchain needed between 1 to 10 milliseconds; 10 milliseconds was needed when the server received a thousand requests. According to this result, there is no significant difference between receiving data from a

blockchain one or a hundred times. On the other hand, storing data in a blockchain requires more time. To process the data, the server takes less than 2 s when it is just one message, but for a 500-message-long list, the process time grows to up to 90 s. As a result of their performance testing, it is not recommended to store more than 25 messages at once [10].

An experiment to test the delay time for downloading and uploading video files into the blockchain using a consensus algorithm was performed by [15]. Three RaspberryPi 4 B((Broadcom BCM2711, Quad-core Cortex-A72) were used in the experiment. The result shows, that the proposed blockchain consensus algorithm for both upload and download took a delay time that did not affect performance, with a linear increase of the delay and the rise of the size did not have a significant effect on the delay.

On the other hand, the experiment in Reference [20] used a virtual machine for testing by Hyperledger Fabric1.2, running on a physical machine with Intel Core i5 CPU@3.2 GHZ, 16 GB RAM, and Windows 7 system. For virtual software, VMware Workstation 14 Pro with 4 GB virtual memory and two allocated processors with 40 GB of Ubuntu system were used. The first part of the experiment focused on performance results of single-chain, double-chain, and triple-chain, with a focus on CPU utilization ratio. The experiment showed that the throughput of the triple-chain structure is improved by 37–100% than the double-chain and single-chain [20]. The second experiment focused on the effects of worker credit on performance. The results show that a large amount of high credit workers are comparable to the SAT solution. However, in practical application, most of the workers do not have a high score, so the solution is more suitable for practical use. The last experiment focused on the comparison of fixed block size and different block sizes. Each scheme's throughput improves as the block size grows, but not always. Because latency restricts the maximum number of transactions in a block, even if block size grows and more transactions may be carried in a block, the throughput does not increase indefinitely [20]. According to the aforementioned findings, the suggested solution's throughput is optimal under various factors, demonstrating the efficacy of dynamically picking the relevant blockchain parameters, as this is more suitable for actual applications [20].

Reference [18] ran experiments on a Windows 10 64-bit operating system on a physical machine with an Intel Core i7-8700 processor, with 3.2 GHz frequency, NVIDIA GeForce GTX 1050, and 16 GB RAM, to test the performance of their proposed solution. The results showed that, due to the time limitation of transactions in the pool when Q (the number of transactions in the transaction pool) rises, the algorithm likes to choose more active miners to converge to an ideal performance improvement rate (PIR) and select more transactions to construct a block, while roadside units (RSUs) are fixed [18]. However, when Q is fixed, the number of active miners grows in lockstep with the number of RSUs, but the block size varies only a little. When Q grows, the blockchain latency increases for a certain number of RSUs, since more active miners and greater block sizes result in a larger delay. When Q is fixed, the blockchain latency grows as the number of RSUs increases, and the number of active miners increases the delay. The final result of the experiment is that the proposed solution may significantly cut the time spent queuing [18].

Reference [17] conducted experiments by using a computer with an Intel Core i7-8700 processor with 3.2 GHz frequency, 8 GB RAM, and Windows 10 Enterprise operating system. The experiment compared the efficiency of the proposed scheme (solution using Bloom filter) with the one that does not use Bloom filter. In the classic system, the computing cost was proportional to the increase in both speed and time-slot length. The result of the experiment showed that the proposed algorithm that uses the Bloom filter is, in some cases, almost 10 times faster than the traditional scheme.

3.5. Scalability

The blockchain has many challenges to face, and scalability is considered the greatest. Vehicle sales have grown substantially from 2005 to 2020 [21], as well as the technology inside them. Using blockchain for data collection in the automotive industry has various implications from a scalability angle. In the Vehicle-to-Everything (V2X) communication

with the limited computer and networking resources of the vehicle, efficiency is desired, so network scalability is important [10], but in practical analyses and tests, the data-gathering load increases the execution time and the power usage exponentially. Therefore, it is not a viable option for data collection, due to its inadequate scalability; thus, the message-receiving function should be improved. Reference [9] investigated scalability thanks to the separate ledgers, but the increase in the amount of data collected creates problems. In the simulation, a linear GPU and CPU usage was observed that did not seriously affect scalability, and the time was raised by 11%. In addition, in Reference [9] complete comprehensive statistics were provided that facilitate understanding of the situations and open doors for future improvement.

In recent efforts, network innovations have been used to improve the scalability of blockchain. However, these technologies are still in the early stages of development, and the question of how to construct lightweight and scalable blockchain networks remains a major concern [14]. The offered idea is to fragment data and collect them in parallel. In addition, other solutions are using the lightweight blockchain approach that has a scalability orientation; for example, Reference [15] considered the Lightweight Consensus Algorithm for Scalable IoT Business Blockchain to reduce the delay time. The Lightweight Scalable Blockchain from Reference [4] manages the blockchain dynamically, so as not to overload it with accumulated data; Reference [4] serves also as a basis for the previously mentioned articles on the lightweight blockchain.

Reference [11] recommended including the scalability in the black-box solution studies to satisfy the need for automotive companies to gather data with a vision for their use in large networks and systems. Although Reference [17] mentioned performance tests regarding scalable transactions, this study was not further developed. However, it is recommended to develop scalability in transactions from a data-collection angle. Unfortunately, the rest of the articles, References [12,17–20], did not consider the scalability in their solutions, thus putting their solutions at a disadvantage compared to other solutions.

3.6. Cost

The transaction costs should not be ignored when blockchain technology is used in the automotive data-collection process and its services. This section explores the range of different costs taken into account in the selected articles. As indicated by Reference [11], the memory consumed by each action and type of data has been studied. However, this study did not refer to the cost of blockchain transactions to collect data. Based on the Ethereum network, the cost of creation and implementation was analyzed [10]. The Get Message function has no additional cost, because mining is not required when receiving messages from blocks, and the smart contract does not require any alterations. However, the cost arises when the information is processed, consuming 136 gas each byte; this gives a clear understanding of how much each transaction consumes (ETH in this case) [10].

Reference [9] considered when there are a lot of data to store, making the storage very costly, and the acquired data are stored simultaneously in a single commit, which incurs a transaction cost; however, this technique lowers the transaction cost. In addition, the use of a simulation in this study gave more validity and reputation. Moreover, the cost of centralized content administration for many dispersed connected automobiles may be too expensive, as the number of connected vehicles keeps increasing over the years [18]. It, therefore, used the different vehicles connected to the decentralized network to split the costs generated by the blockchain, reducing the signature from 320 bits to 160 bits in length. Reference [17] described the cost in bytes of the data-gathering step, but it did not address how it affects the blockchain.

Presently, Reference [13] is not considering costs from the service provider's perspective; this makes the cost of the service provider's vehicle data acquisition unknown. It is recommended that a cost study be carried out to give more visibility to the industry. Reference [4] was a groundwork which should be a starting point for many other researchers. Following Reference [17], a similar situation to Reference [11] was found, as the cost was

addressed, but not from the context of blockchain use. Reference [19] differentiated between the types of transactions but not their cost; with this information, it would be more complete. The same applies to Reference [12]. The rest of the authors did not consider cost in their manuscripts.

3.7. Monetizing

Thanks to digitalization, innovation, and new technologies, such as the blockchain, the automotive industry is growing rapidly. This section describes the different alternatives to monetize data collection in the vehicle industry, thanks to blockchain technology. As settled by [4] blockchain technology offers several advantages in automotive applications over conventional modes. Those applications are remote software updates where distributed data exchange offers scalability and privacy. Insurance to control the data and verify it supposes a groundwork for [11,15]. Electric vehicles benefit from the privacy of information and security of payments and car-sharing services the same benefits as above and distributed authorization. Considering [11] insurance firms and police departments may use the data collected by sensors to reconstruct accidents or events in general. The way of monetization in this manuscript surrounds insurance companies, by using a black box that collects data from the car to the insurance company. The suggested system can encrypt, pseudonymize, and secure drivers' data before transmitting it from the car to a remote server [11]. Consequently, this option is, therefore, a safe and innovative solution for the vehicle insurance market. Joined [15] where an answer to black-box limitation is made, and the purpose of identifying who is to blame for road accidents and how to avoid them with focus on the image. The merger of these two studies is a breakthrough for vehicle insurers. Moreover, Reference [17] offered a solution that focused on insurance. A proof-of-stake concept was used to verify the extracted data; this is a very innovative system that can be of great interest to insurers.

The Internet of Vehicles could efficiently tackle a variety of traffic and road safety issues, hence reducing fatal crashes. Reference [10] ensured data interchange between various participants in intelligent transportation networks. It could be used in several automotive sectors, such as vehicles and infrastructures, as well as communications between them; as future work, it can provide function as payment in tolls, charging, or parking. The data collected by the vehicles are used in a variety of ways throughout the enterprises [13]. These are solutions for insurance, vehicle management and maintenance, Original Equipment Manufacturers, urban planning, and road traffic. This article offers a variety of solutions based on the types of data collected, but it does not elaborate on them; thus, future work would enrich our understanding by exploring the uses in automation. In light of Reference [9], a blockchain architecture was proposed for vehicular applications in Vehicle-to-Vehicle communication that focuses on the messages between them; thanks to its proof of concept, it can be implemented by car manufacturing companies. Following Reference [18], there is no viewpoint in specific industry usage; thanks to the simulation, it can offer possibilities to car producers in regard to the safe sharing of data between cars, as in Reference [9]. As stated in Reference [20], the reinforcement blockchain system offers a real application to exchange data between cars to avoid accidents and improve driving regulations; this can be used by regulatory departments. The car-sharing service idea from Reference [4] is related to the BWM Group's car-sharing solution from Reference [19]; in the future, BWM could be implemented in the real world to take advantage of the competitors. In Reference [12], the framework proposed follows the GDPR laws for IoV [22–26] but does not show any specific application. It can be used to follow the law for car producers in gathering data from autonomous or connected vehicles. The study in Reference [16] does not have any reference to any use in industry, but in dealing with connected vehicles and infrastructures, it can have the same real-world applications as in Reference [9]. Moreover, the framework for Intelligent Transportation Systems can be used to not only collect data in traffic management systems but also in other industries and contexts [18], thus giving a broader vision from 5G in data collection, using the blockchain approach.

4. Discussion

The purpose of the current study was to conduct a review of published articles that describe the challenges of using blockchain technology for data collection in the automotive industry. Accordingly, this review investigated gaps in the proposed solutions for data collection. In addition, it offers practical suggestions to improve the data-collection process, taking into account the unique requirements and experiences of automotive industry stockholders. The following trends emerged: using mass messages to ensure good latency, changing public keys for driver anonymity, adapting security systems against security attacks, analyzing blockchain costs to know the feasibility of a solution, offering different uses in production and services for the automotive industry, and using segmental data collection to make the process more scalable and usable in a real context with large networks.

Connectivity is one of the most important challenges for data collection, because vehicles are fast objects and are not guaranteed to always be strongly connected to the Internet. This review showed that the selected articles proposed several solutions to this problem; these solutions combine the connection via the 3G/4G/5G mobile network and Wi-Fi with the possibility of short-time local data storing and guarantee quality and reliability of data sharing. However, future research could focus more on using public Wi-Fi networks or using connections from other cars as another possible solution for uploading data to the blockchain. Although it is proven that the use of bulk messages to shorten the time of loading and processing of data in the blockchain is an effective, secure solution and could be tested in a real-world example, only one article introduced a solution to ensure good connectivity and latency by this method.

This review showed that, although researchers have focused on solutions that preserve privacy in blockchain data collection, few have considered the GDPR; for example, only one article proposed a solution that allows the right to rectification and the right to be forgotten. However, the importance of compliance with all data-collection laws seems obvious, as vehicle data are collected worldwide. In addition, it is necessary to focus more on solutions that allow for data deletion when requested by the driver, especially as blockchain is built as an immutable solution.

Security attacks, which are the main challenge for data collection, should be studied in their entirety, as in Reference [10]. More specifically, researchers should classify attacks and carry out more tests and simulations for possible attacks (i.e., DDoS, MITM, collusion, and data exposure). This will improve integrity and provide a secure basis for the future expansion of data extraction. Moreover, if all types of attacks on large car networks are not avoided, conflicts and threats to traffic flow can be generated. In addition, insurance companies would also be affected and could allow fraud if the data were not verified biometrically. However, further work on possible anti-attack methods is needed.

This review revealed that nine of the thirteen proposed solutions have performed performance tests. The test results proved that blockchain technology could be used for data collection in the automotive industry. However, four articles [4,11–13] did not perform any tests or simulations to verify their solutions. Therefore, these solutions should be tested in simulations to ensure that they are usable. In addition, the other proposed solutions can be moved to the small-scale testing phase in the real world.

Scalability is a key factor in achieving sustainability in the automotive industry. In addition, potentially large vehicle networks must be scalable, as the number of connected vehicles increases. However, it still implies a limitation in the data-collection research area, because scalability has not been widely researched in the selected articles. Therefore, future research should consider scalability technologies, such as parallel data collection and segmentation, as in Reference [18], but combined with the concepts of a light blockchain, as in References [4,15], to minimize the consumption.

Since the intended purpose of this review was to assess the applicability of blockchain data collection, it is necessary to estimate the cost of blockchain solutions. Unfortunately, as shown in Figure 3, only four estimated the project's technological costs; Reference [10] analyzed a reasonable and affordable technical cost, but it was the only one that specified

the costs in monetary units. As scalability is one of the major challenges facing the automotive sector, researchers should consider the cost of blockchain technology to address this challenge.

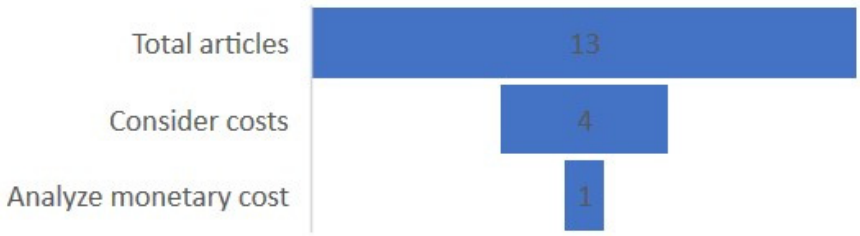

Figure 3. Funnel for cost analysis in articles.

The automotive industry offers a variety of services and products, and within this industry, there are various suppliers and manufacturers. The blockchain data-collection applications investigated by the authors can be classified as follows: solutions for insurance companies [16] and the proof-of-stake proposal [11,15] that the black box deceives with groundwork. In addition, Internet-of-Vehicles applications or traffic issues and communication between vehicles, with limitations on their actual application of data collection, are very new and difficult to apply quickly in the industry. The researchers are recommended to implement measures in applications that have short-term benefits for the automotive industry and to implement and monitor their consequences.

5. Challenges and Future Directions

The literature search was carried out through the use of the following databases: Springer, IEEE, MDPI, and Google Scholar. Although of these databases cover several areas and cover many individual databases, such as ScienceDirect, SCOPUS, and Web of Science, this decision may have influenced the number of relevant articles obtained. The use of other databases might have increased the number of articles analyzed and could have contributed to the improvement of the overall analysis. In addition, the research strategy was considered to limit the number of irrelevant articles (articles published many years ago, articles that are too general, or articles that do not focus on research goals). In addition, only articles in English were included. These options may have ruled out relevant articles, such as articles written in languages other than English.

These restrictions may have had a significant impact on the number of records obtained and may have had some effect on the retrieval of relevant papers. As a result, the small number of papers reviewed and the eligibility of varied studies constrained our study. They may also have influenced data extraction and analysis. However, these constraints had no significant impact on the discussion and conclusions.

This review allowed us to answer the predefined research question: "What are the challenges of using blockchain for data collection in the automotive industry as presented in the published literature?" Thus, this review focused on the challenges of using blockchain for data collection rather than delving deeply into the various mechanisms and solutions to address them, paving the way for further reviews to discuss and classify the latest techniques and mechanisms used to improve data collection through blockchains, such as blockchain-enabled resource sharing and management. In addition, future research focusing on the connection itself is needed, where cars can use a mobile network, Wi-Fi, and connections from other cars to reduce the time, where there is no connection at all. Moreover, further research should consider the following: scalability, given the increase in connected vehicles; the design of fully secure algorithms, so as to avoid fake data; and the costs of energy-intensive blockchain technology in its transitions.

As this review focused on technological and environmental perspectives to categorize the challenges of adopting a blockchain for data collection in the automotive industry, a

further review is needed to include organizational features, such as auditing, trust, and organizational readiness.

6. Conclusions

The role of blockchain in data collection is critical and has expanded in recent years. The key contribution of this review is to provide a clear picture that summarizes what has already been written about the challenges of using blockchain for data collection in the automotive industry. The review identified the most important and relevant studies in the field, providing details on the topics that have promoted more academic attention and detailing blockchain adoption challenges for data collection in the automotive industry sector. The methodology chosen to answer the research question was a literature review.

Our study question was as follows: "What are the challenges of using blockchain for data collection in the automotive industry, as presented in the published literature?" To address this question, we classified the challenges into the following seven areas: connectivity, privacy, security attacks, scalability, performance, cost, and monetization. This review showed that the cost of using blockchain in data collection has been partly considered in the design of most of the current solutions in the analyzed publications. In addition, nine out of thirteen articles conducted tests to verify the performance of the solutions, and all tests show that the proposed blockchain frameworks are a significant improvement over conventional solutions. In addition, this study showed that only one solution meets the requirements of the GDPR Act, such as the right to be forgotten and the right to update data. Therefore, future research should focus on how to use blockchain technology and fulfill the requirements declared in the GDPR. In the connectivity area, bulk messages appeared to be a big improvement in latency in blockchain technology. Thus, future research focusing on the connection itself is needed, where cars can use a mobile network, Wi-Fi, and connections from other cars to reduce the time, where there is no connection at all. Moreover, further research should consider the following: scalability, given the increase in connected vehicles; the design of fully secure algorithms, so as to avoid fake data; and the costs of energy-intensive blockchain technology in its transitions.

Author Contributions: Conceptualization, A.M., S.V. and P.Č.; methodology A.M., S.V. and P.Č.; validation, A.M., S.V. and P.Č.; formal analysis A.M., S.V. and P.Č.; investigation, A.M., S.V. and P.Č.; resources, A.M., S.V. and P.Č.; data curation, A.M., S.V. and P.Č.; writing—original draft preparation, A.M.; writing—review and editing, A.M.; visualization, A.M.; supervision, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Statista. Available online: https://www.statista.com (accessed on 17 February 2022).
2. Fraga-Lamas, P.; Fernández-Caramés, T.M. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access* **2019**, *7*, 17578–17598. [CrossRef]
3. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
4. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125. [CrossRef]
5. Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C. Current trends in sustainability of bitcoins and related blockchain technology. *Sustainability* **2017**, *9*, 2214. [CrossRef]
6. Decker, C.; Wattenhofer, R. Information propagation in the bitcoin network. In Proceedings of the IEEE P2P 2013 Proceedings, Trento, Italy, 9–11 September 2013; pp. 1–10.

7. Henry, R.; Herzberg, A.; Kate, A. Blockchain access privacy: Challenges and directions. *IEEE Secur. Priv.* **2018**, *16*, 38–45. [CrossRef]
8. Lin, I.C.; Liao, T.C. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659. [CrossRef]
9. Chiasserini, C.F.; Giaccone, P.; Malnati, G.; MacAgno, M.; Sviridov, G. Blockchain-based Mobility Verification of Connected Cars. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020. [CrossRef]
10. Jabbar, R.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, A.K. Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using Ethereum. *Sensors* **2020**, *20*, 3928. [CrossRef] [PubMed]
11. Morano, F.; Ferretti, C.; Leporati, A.; Napoletano, P.; Schettini, R. A blockchain technology for protection andprobative value preservation of vehicle driver data. In Proceedings of the 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), Ancona, Italy, 19–21 June 2019.
12. Campanile, L.; Iacono, M.; Marulli, F.; Mastroianni, M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Inf. Process. Manag.* **2021**, *58*, 102511. [CrossRef]
13. Sang-Oun, L.; Hyunseok, J.; Bosuk, H. Security Assured Vehicle Data Collection Platform by Blockchain: Service Provider's Perspective. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 17–20 February 2019; pp. 265–268. [CrossRef]
14. Wang, Y.; Su, Z.; Zhang, K.; Benslimane, A. Challenges and solutions in autonomous driving: A blockchain approach. *IEEE Netw.* **2020**, *34*, 218–226. [CrossRef]
15. Na, D.; Park, S. Lightweight blockchain to solve forgery and privacy issues of vehicle image data. In Proceedings of the 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), Tainan, Taiwan, 8–10 September 2021; pp. 37–40. [CrossRef]
16. Kong, Q.; Lu, R.; Yin, F.; Cui, S. Blockchain-Based Privacy-Preserving Driver Monitoring for MaaS in the Vehicular IoT. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3788–3799. [CrossRef]
17. Kong, Q.; Su, L.; Ma, M. Achieving Privacy-Preserving and Verifiable Data Sharing in Vehicular Fog with Blockchain. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4889–4898. [CrossRef]
18. Wang, S.; Sun, S.; Wang, X.; Ning, Z.; Rodrigues, J.J.P.C. Secure Crowdsensing in 5G Internet of Vehicles: When Deep Reinforcement Learning Meets Blockchain. *IEEE Consum. Electron. Mag.* **2021**, *10*, 72–81. [CrossRef]
19. Gudymenko, I.; Khalid, A.; Siddiqui, H.; Idrees, M.; Clauß, S.; Luckow, A.; Bolsinger, M.; Miehle, D. Privacy-Preserving Blockchain-Based Systems for Car Sharing Leveraging Zero-Knowledge Protocols. In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 3–6 August 2020; pp. 114–119. [CrossRef]
20. Lin, H.; Garg, S.; Hu, J.; Kaddoum, G.; Peng, M.; Hossain, M.S. Blockchain and Deep Reinforcement Learning Empowered Spatial Crowdsourcing in Software-Defined Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3755–3764. [CrossRef]
21. IEA. Global Car Sales by Key Markets, 2005–2020. Available online: https://www.iea.org/data-and-statistics/charts/global-car-sales-by-key-markets-2005-2020 (accessed on 6 January 2022).
22. Tornatzky, L.G.; Fleischer, M. *The Processes of Technological Innovation*; Lexington Books: Lanham, MD, USA, 1990.
23. Xu, H.; Klaine, P.V.; Onireti, O.; Cao, B.; Imran, M.; Zhang, L. Blockchain-enabled resource management and sharing for 6G communications. *Digit. Commun. Netw.* **2020**, *6*, 261–269. [CrossRef]
24. Koens, T.; Poll, E. What blockchain alter-native do you need? In *Data Privacy Management, Crypto-currencies and Blockchain Technology*; Springer: Cham, Switzerland, 2018; pp. 113–129.
25. de Sa, A.O.; da Costa Carmo, L.F.R.; Machado, R.C. Covert attacks in cyber-physical control systems. *IEEE Trans. Ind. Inform.* **2017**, *13*, 1641–1651.
26. Jolfaei, A.; Kant, K. Privacy and security of connected vehicles in intelligent transportation system. In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks–Supplemental Volume (DSN-S), Portland, OR, USA, 24–27 June 2019; pp. 9–10.
27. Haghighi, M.S.; Farivar, F.; Jolfaei, A.; Tadayon, M.H. Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack. *J. Supercomput.* **2020**, *76*, 3063–3085. [CrossRef]
28. Li, M.; Weng, J.; Yang, A.; Liu, J.; Lin, X. Toward blockchain-based fair and anonymous ad dissemination in vehicular networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11248–11259. [CrossRef]
29. Gruebler, A.; McDonald-Maier, K.D.; Alheeti, K.M.A. An intrusion detection system against black hole attacks on the communication network of self-driving cars. In Proceedings of the 2015 Sixth International Conference on Emerging Security Technologies (EST), Braunschweig, Germany, 3–5 September 2015; pp. 86–91.
30. Mitchell, R.; Chen, I.-R. Effect of intrusion detection and response on reliability of cyber physical systems. *IEEE Trans. Reliab.* **2013**, *62*, 199–210. [CrossRef]
31. Mitchell, R.; Chen, I.-R. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 16–30. [CrossRef]
32. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2012**, *100*, 210–224. [CrossRef]

33. Pathak, S.; Mani, A.; Sharma, M.; Chatterjee, A. Augmenting vehicular network with software defined Internet-of Vehicles paradigm. In Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 17–19 July 2019; pp. 1593–1598.
34. Gao, J.; Agyekum, K.O.B.O.; Sifah, E.B.; Acheampong, K.N.; Xia, Q.; Du, X.; Guizani, M.; Xia, H. A Blockchain-SDN-Enabled Internet of Vehicles environment for fog computing and 5G networks. *IEEE Internet Things J.* **2020**, *7*, 4278–4291. [CrossRef]
35. Kadhim, A.J.; Seno, S.A.H. Maximizing the utilization of fog computing in Internet of Vehicle using SDN. *IEEE Commun. Lett.* **2019**, *23*, 140–143. [CrossRef]
36. Garg, S.; Singh, A.; Aujla, G.S.; Kaur, S.; Batra, S.; Kumar, N. A probabilistic data structures-based anomaly detection scheme for software-defined Internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3557–3566. [CrossRef]
37. Alouache, L.; Maachaoui, M.; Aliouat, M.; Chelouah, R. Securing southbound interface of HSDN-GRA vehicular routing protocol using a distributed trust. In Proceedings of the 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 10–13 June 2019; pp. 90–97.
38. Li, M.; Zhu, L.; Lin, X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet Things J.* **2019**, *6*, 4573–4584. [CrossRef]
39. Gao, F.; Zhu, L.; Shen, M.; Sharif, K.; Wan, Z.; Ren, K. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Netw.* **2018**, *32*, 184–192. [CrossRef]
40. Mohammadali, A.; Haghighi, M.S.; Tadayon, M.H.; Mohammadi-Nodooshan, A. A novel identity-based key establishment method for advanced metering infrastructure in smart grid. *IEEE Trans. Smart Grid* **2018**, *9*, 2834–2842. [CrossRef]