applied sciences

MDPI

Review

Privacy-Preserving Solutions in Blockchain-Enabled Internet of Vehicles

Konstantinos Kaltakis [1], Panagiota Polyzi [1], George Drosatos [2] and Konstantinos Rantos [1,*]

[1] Department of Computer Science, International Hellenic University, 65404 Kavala, Greece; kokalna@cs.ihu.gr (K.K.); pkpolyz@cs.ihu.gr (P.P.)
[2] Athena Research Center, Institute for Language and Speech Processing, 67100 Xanthi, Greece; gdrosato@athenarc.gr
* Correspondence: krantos@cs.ihu.gr; Tel.: +30-2510-462611

Abstract: Blockchain, a promising technology that has matured and nowadays is widely used in many fields, such as supply chain management, smart grids, agriculture and logistics, has also been proposed for the Internet of Vehicles (IoV) ecosystem to enhance the protection of the data that roadside units and vehicles exchange. Blockchain technology can inherently guarantee the availability, integrity and immutability of data stored in IoV, yet it cannot protect privacy and data confidentiality on its own. As such, solutions that utilise this technology have to consider the adoption of privacy-preserving schemes to address users' privacy concerns. This paper provides a literature review of proposed solutions that provide different vehicular services using blockchain technology while preserving privacy. In this context, it analyses existing solutions' main characteristics and properties to provide a comprehensive and critical overview and identifies their contribution in the field. Moreover, it provides suggestions to researchers for future work in the field of privacy-preserving blockchain-enabled solutions for vehicular networks.

Keywords: Vehicular Ad-Hoc Networks (VANETs); Internet of Vehicles (IoV); blockchain technology; privacy preservation

check for updates

Citation: Kaltakis, K.; Polyzi, P.; Drosatos, G.; Rantos, K. Privacy-Preserving Solutions in Blockchain-Enabled Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 9792. https://doi.org/10.3390/app11219792

Academic Editor: Gianluca Lax

Received: 21 September 2021
Accepted: 15 October 2021
Published: 20 October 2021

1. Introduction

Internet of Vehicles (IoV) is a concept in the Internet of Things ecosystem representing intelligent transportation [1]. IoV is also a superset of Vehicular Ad-Hoc Networks (VANETs) and extends its scale and services [2]. VANET originates from Mobile Ad-Hoc Network (MANET) and is considered as a network in which different moving vehicles and other devices are connected with each other and exchange useful information to provide roadside services such as road safety, navigation and traffic control.

These exchanging messages include sensitive information such as vehicle identification, personal data (e.g., driver's identity and current location) and navigation information which participants may be unwilling to share [1]. In addition, the number of autonomous vehicles (self-driving cars) is anticipated to increase rapidly in the near future, so VANET will have to manage more information and user data. Moreover, attackers and malicious users may attempt to gain vehicle users' personal information in order to cause serious problems to the road network and drivers' safety. Therefore, it is highly important to ensure the privacy of participants and the security of the exchanged information and to prevent malicious attacks [1].

Furthermore, a key issue is to assure that the shared information will not be changed or leaked by third parties. Blockchain is a technology that can provide data protection due to the use of an immutable distributed ledger and the adoption of several cryptographic techniques, such as hash functions, Merkle trees and public-key cryptography, in a decentralised environment [1]. Thus, blockchain is used to deal with the problems mentioned above.

Although blockchain can provide a tamper-proof environment, it cannot ensure any aspects of privacy, so it needs to be combined with other technologies to achieve privacy preservation.

This paper examines proposed solutions for different sectors of IoV, which use blockchain technology, while also attempting to protect the privacy of involved parties. The protection concerns users' identity, vehicles' location and exchange data between vehicles and infrastructures.

The rest of this paper is organised as follows: Section 2 contains a brief introduction to the main topics discussed in this paper, i.e., IoV, blockchain and privacy in IoV. In Section 3, an overview of related works on blockchain-enabled privacy preserving solutions is provided. Section 4 describes the research methodology that has been followed in conducting this review and provides the research questions that this work addresses. Section 5 presents an analysis of this study's results and summarises key findings while, in Section 6, existing privacy-preserving blockchain-based solutions for IoV are presented in detail, grouped under seven major categories based on the services they provide. Finally, in Section 7, we provide a discussion on future research directions and open issues, while Section 8 concludes this review paper.

2. Background

In this section, the main concepts of Internet of Vehicles are described and analysed in order to provide a better understanding of the discussed issues. Firstly, there is a reference to the concept of IoV and its main components and services. Afterwards, the blockchain technology is described and also its main features which make use of blockchain in vehicular systems necessary. Lastly, there is a reference to the privacy issues related to vehicular systems.

2.1. IoV

IoV is a comprehensive platform which integrates IoT technologies and intelligent transportation systems [1]. It extends VANET's structure and applications. This platform can provide several services such as intelligent traffic control, driverless vehicles, safe driving, safe navigation, crash response, intelligent vehicle management, convenience services (remote door unlock, stolen vehicle recovery) and infotainment.

There are numerous participants in an IoV system such as vehicles, drivers and other passengers that act as users, sensors (like on traffic lights) and On-Board Units (OBUs) which are devices installed on vehicles to provide smart features, a Central Authority (CA) which is responsible for network access and maintenance, cloud servers for communications and storage and Roadside Units (RSUs) which are scattered across the road and provide communication between vehicles and infrastructures. These participants communicate with each other in many different ways (Vehicle-to-Vehicle (V2V), Vehicle-to-Road (V2R), Vehicle-to-Human (V2H), Vehicles-to-Infrastructure (V2I), Vehicle-to-Sensor (V2S)). Thus, a social network is created with intelligent objects, which receive traffic information by exchanging Safety Beacon Messages (SBM) [2,3]. IoV is an heterogeneous network as it involves several dissimilar participants and provided services. It faces various challenges due to its dynamic nature and real-time data requirements. Figure 1 shows the visual representation of an IoV system.

The typical architecture of IoV which consists of four layers is based on a centralised system as it relies on Trusted Central Authorities (CA) [4]:

- Environment sensing and control layer: In this phase, information is gathered by sensors which are stored within the vehicles. Those sensors detect SBMs, environmental and other vehicular information and also radio frequency identification perceive data such as satellite position, road environment, etc.
- Network access and transport layer: This layer is responsible for node management, data analysis and processing and communication between vehicles and other units in vehicular system.

- Coordinative computing layer: In this layer, management of the IoV system is accomplished. In addition, resource allocation and processing of data are also fulfilled in this layer.
- Application layer: The application layer is in charge of storing and analysing information and deciding about several risk situations. It represents several applications such as traffic safety, infotainment, etc. These provided services are divided into two categories: open and closed services. Open services consist of services such as real-time traffic service, while more specific services like control platform and traffic command are considered as close services [2,4].

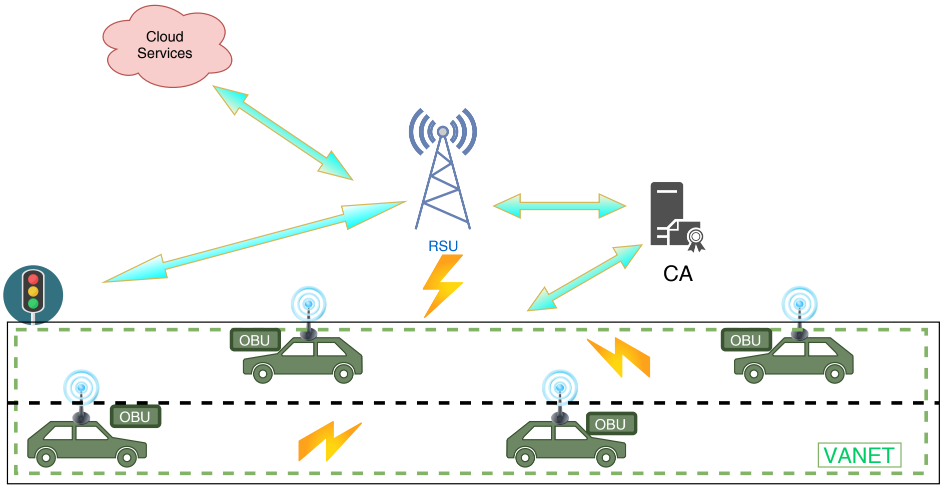


Figure 1. The IoV Ecosystem.

2.2. Blockchain

Blockchain is a shared and distributed ledger that can record transactions among untrusted peers [5]. This ledger is immutable and continually grows in a chronological order as new records, called blocks, are added holding the most recent transactions [6]. Each block contains, among others, transaction data, a timestamp and a hash of the previous block. The latter prevents alteration of data, as any attempt to modify data in a block would result in invalid hash values, unless all blocks' hashes are recalculated [7]. Blockchain is typically divided by the National Institute of Standards and Technology (NIST) [8] into two main types: *permissioned* (private), where participants need permission from authority to join the network and *permissionless* (public) where anyone can freely participate.

The benefits of using blockchain in IoV are numerous, because blockchain technology has the following main features:

- Immutability: Tampering or deletion of block's data is not feasible, as even a minor change in the block's data will alter its hash value and, as a result, the hash value of every subsequent block in the chain. Therefore, any modification to an old block's data would typically require replacing all following blocks.
- Distributed Ledger: Participating nodes can keep a copy of the ledger, which can facilitate trust establishment among them.
- Consensus Algorithm: Mechanism that is used to provide rules for verifying and validating blocks, as well as for ensuring that all participants agree with the current state of the chain.
- Smart Contract: A piece of code that executes automatically when certain conditions are met and the execution result must be agreed upon by all participants.

Considering all the above characteristics, blockchain technology can be used to solve security, trust establishment and distribution problems which may occur in vehicular networks.

2.3. Privacy in IoV

Privacy is the ability of a person or a group to preserve themselves and confidential information from unauthorised people [9]. There are numerous technologies and strategies [10] for preserving privacy. Pseudonyms, homomorphic encryption, k-anonymity via cloaking techniques and zero knowledge proofs, which are reviewed in this paper, are some of them. Especially for IoV, it is important to protect the privacy of involved users, as it is a dynamic heterogeneous system consisting of numerous participants which do not trust each other. Furthermore, as vehicular services expand, the exchangeable data grows too. Therefore, privacy by design [11] must be one of the key features of every vehicular technology. The privacy of participants in a IoV ecosystem can be divided into the following types:

- Identity privacy: It prevents real identity disclosure of a user, mainly protected by using pseudonyms during communication in a vehicular system [3].
- Location privacy: It protects user's location and can be generally protected by cloaking/clustering methods [3].
- Data privacy: It protects the disclosure of user personal data, such as vehicle's trajectory, speed and ad-hoc messages between vehicles. Data privacy can be achieved, for example, with homomorphic encryption or federated learning [12–14].

In addition, malicious users or attackers may attempt to cause problems to the system or to gain personal data of users. As participants do not trust each other and malicious users may occur, a fully anonymous network is not feasible. If a malicious user is detected, it should be removed from the network, considering that, these users have acquired a partial pseudonym and are subject to conditional privacy.

3. Related Work

In the past few years, several surveys have focused on privacy issues in different aspects of Internet of Vehicles. The authors of [15] examine existing applications aiming to solve and improve security and privacy issues of VANETs. The authors of [14] also discussed privacy and security issues in IoV against attacks. Paper [16] discussed the relationship between personal data, consent and privacy in vehicular systems and examined existing proposals aiming to solve security and privacy issues of exchanging data. In [17], the authors focused on privacy and security solutions for 5G vehicular networks. The authors of [18] presented the most common security attacks and discussed important security mechanisms aiming to prevent these attacks and protect the privacy of vehicular systems.

Some of the existing surveys have focused on authentication schemes in VANET. The authors of [19] conducted a survey on authentication methods proposed for VANET aiming to better preserve privacy. The authors of [20] analysed anonymous authentication mechanisms aiming to provide privacy protection and discussed several trust management models for VANET. Additionally, the authors of the survey [21] focused on authentication and privacy issues that can occur in VANET during message dissemination. For that reason, they conducted a comparative study of proposed schemes over the last ten years which aimed to address those issues. They analysed and compared these schemes and discussed open issues.

Location privacy and differential privacy have also concerned researchers in recent years. The survey [22] analysed proposed location privacy protection schemes for vehicular systems. The authors of [23] discussed location privacy and made a comprehensive review of existing trust models, aiming to protect privacy and security in vehicle cloud computing. In [24], the authors investigated and compared existing local differential privacy techniques and applications for privacy presentation in IoV.

A comprehensive survey on security with privacy aspects is presented in [25]. The survey does not focus on privacy but extends to various fields of IoV, including blockchain technology. VANET-based authentication schemes are compared in [26]. The authors categorise the schemes into cryptography, signature and verification, and some of the privacy-preservation aspects are discussed.

In contrast, only one survey investigated blockchain solutions in IoV. The authors of [27] focused on the use and integration of blockchain technology in the Internet of Vehicles. For that reason, they presented and compared existing blockchain solutions for Internet of Vehicles. They also provided an analysis of different requirements of blockchain-based applications in vehicular systems and a presentation of open challenges in this area.

Although there has been a lot of research on privacy issues in the field of IoV, IoV related systems that use blockchain technology have not been explored with respect to privacy. For that reason, in the present work, we investigate blockchain-based solutions which also aim at maintaining the privacy of the involved parties. In IoV, there are three main privacy concerns: the reveal of user identity, the location exposure and theft or disclosure of data.

4. Research Methodology

The methodology that is followed to define privacy-preserving blockchain solutions in IoV is divided into the following three steps:

1. Firstly, there is an extensive search in Scopus search engine (www.scopus.com, accessed on 25 May 2021) for papers relevant to blockchain based solutions in IoV. The purpose of this search is to find the most relevant papers to the search question: *"privacy-preserving blockchain-based solutions that have been proposed in IoV"*. Therefore, search terms such as "IoV", "VANET", "blockchain" and "privacy" are used to search in the titles, abstract and keywords of publications. The searched query is as follows:

```
TITLE-ABS-KEY ((VANET OR "smart vehicle" OR "vehicular network" OR
   "internet of vehicle" OR "IoV" OR "smart transport" OR "smart
mobility" OR "autonomous vehicle") AND (blockchain OR "distributed
            ledger") AND (privacy OR "personal data"))
```

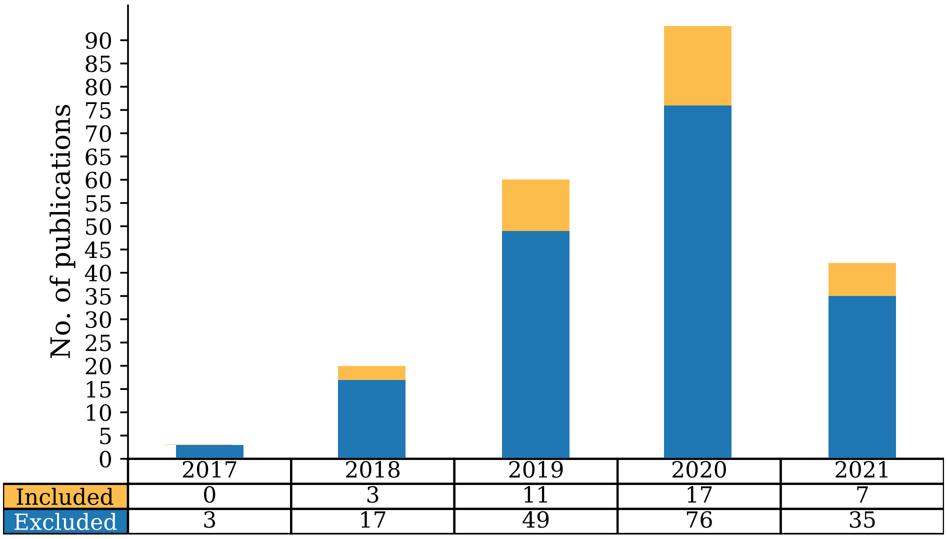
2. Subsequently, from those returned papers, the most relevant to our research are selected, including only papers which propose blockchain-based solutions aiming to ensure privacy in different aspects of IoV.
3. Finally, the included papers in our survey are divided into categories, according to the IoV service area that they focus on to provide a privacy-preserving blockchain-based solution. Thus, in Sections 5 and 6, the papers are grouped, analysed and presented using these categories.

Our scientific interests revolt around blockchain and privacy. Blockchain is a well-known technology for the immutability, availability and integrity of the stored data. As a promising technology, it does not have any built-in privacy mechanism. In this paper, we study literature to record what technologies can be combined to expand blockchain and add a privacy aspect. Particularly, the aim of this review paper is to explore existing applications or proposals regarding the use of blockchain technology in the field of IoV that simultaneously try to protect the privacy of involved parties. More specifically, in our analysis of this paper, we aim to answer, in total, the following seven research questions:

RQ1. Which IoV service areas utilise privacy-preserving blockchain-based solutions?
RQ2. What kind of privacy protection is provided in the existing solutions?
RQ3. What types of blockchain technology are used?
RQ4. Which blockchain frameworks do solutions utilise?
RQ5. What are the underlying privacy mechanisms that support blockchain-enabled IoV solutions?
RQ6. Do the proposed schemes provide a security analysis?
RQ7. What are their implementation maturity levels?

5. Analysis of Results

In this section, we present the analysis of papers that were included in our study following the methodology described in Section 4. Our search in Scopus on 25 May 2021 returned 217 papers of which 38 were selected as the most relevant to our research. Those are papers that use blockchain and at the same time try to ensure privacy in various areas of IoV. In Figure 2, we show the total number of papers that the query had returned as well as the number of papers that have been finally included and excluded in this study. The included papers are scattered between 2018 and 2021 showing a steady increase. More specifically, three papers were found in 2017, none of which correspond to our field of research, while for 2018, the search returned 17 papers, of which three were selected as the most relevant to our research questions. Moreover, in 2019 the query results were 49 papers and 11 were selected, while for the year 2020, 17 papers were selected as the most relevant. Finally, in 2021 the most relevant papers were only seven from a total of 35. Note that the small number of papers in 2021 compared to the previous years was due to the fact that the query was submitted in May, hence less than half of the year's papers were returned. As mentioned above, we chose only papers that used blockchain and tried to solve privacy issues on IoV.



	2017	2018	2019	2020	2021
Included	0	3	11	17	7
Excluded	3	17	49	76	35

Figure 2. Number of papers included and excluded in our review.

The IoV service areas that utilise privacy-preserving blockchain-based solutions (RQ1), as these have been identified in the analysed papers, are: *Authentication*, *Traffic Conditions*, *Data Exchange*, *Dynamic Navigation*, *Reputation Management*, *General Services* and *Advertising*. Based on this categorisation, a comparative analysis of those papers is presented in Table 1 answering our research questions in this paper and also an overview of this analysis is shown in Figure 3. In this table, many of the proposed schemes have been named by the authors. For those that are not referred to by any name, we chose to name them by the initial letter of the distinguished words found on the paper's title to facilitate distinguishability.

Table 1. Comparison of privacy-preserving blockchain-based solutions in the IoV.

Proposed Solution	Privacy Types (RQ2)	Blockchain Characteristic (RQ3 & RQ4)	Underlying Privacy Mechanisms (RQ5)	Security Analysis (RQ6)	Maturity Level (RQ7)
Authentication (Section 6.1):					
DAIA [28]	Identity	Permissioned	Dynamic Pseudonyms (using Tamper Proof Device), Hash	Informal	Simulation
BlockAPP [29]	Identity	Permissioned (Ethereum)	Pseudonyms	N/A	Experimental
VCS [30]	Identity	Permissioned (PoW)	Pseudonym Shuffling	N/A	Simulation (OMNeT++)
AMDS [31]	Identity	Permissionless, Permissioned	Pseudonyms (using Trusted Authority)	Informal	Experimental
TAAS [32]	Identity	Permissionless (PoW)	Pseudonyms (using Certificate Authority)	Informal	Simulation (GoLang)
PMF [33]	Identity, Location	Permissionless, Permissioned (with Public Read Access)	Temporal Pseudonyms, Ring Signature, One-Time Address (based on Hashes)	Informal	Proposal
VTMS [34]	Identity, Data	Permissioned (Two Layers)	Pseudonyms, Homomorphic Encryption	N/A	Simulation (PEPA)
VPPS [35]	Identity	Permissionless	Pseudonyms (using Public Keys)	Informal	Experimental
BCPKI [36]	Identity	Permissionless (Two Layers, PoW)	Pseudonyms (using Certificate Authority)	Informal	Proposal
SIMF [37]	Identity	Permissioned (Hyperledger Fabric, Solo)	Pseudonyms (using Authentication Parties)	N/A	Simulation (OMNet++, SUMO)
RSV [38]	Identity, Location	Permissioned	Pseudonyms (using Service Provider)	Informal	Experimental (OpenSSL)
ASCEV [39]	Identity, Location	Permissionless (Ethereum)	zkSNARKs, Pederson Commitment	Informal	Experimental (Zokrates, Ropsten)
FCB [40]	Identity	Permissioned (Multi-Level, Ethereum)	Cluster-based Medium Access Control, Pseudonyms (using Public Keys)	Informal	Proof of Concept (Truffle, Ganache, Metamask)
Traffic Conditions (Section 6.2):					
CreditCoint [41]	Identity	Permissioned (BFT)	Threshold Ring Signature, Combined-Public Keys (CPK)	Informal	Simulation (PolarSSL)
TCTBW [42]	Identity	Permissionless (Hybrid Consensus based on PoS and DAG)	Group Signatures	N/A	Experimental (IBM-Watson-IoT)
SCTSC [43]	Identity, Location, Data	Permissioned	Ciphertext Policy Attribute-Based Encryption (CP-ABE)	Informal	Experimental
CFTM [44]	Identity, Data	N/A	Certificateless Aggregate Signcryption (CLAS), Pseudonyms	Formal	Experimental
ZKRP [45]	Identity, Location, Data	Permissioned (Hyperledger Fabric)	Zero-Knowledge Range Proof (ZKRP)	Informal	Prototype
TMLP [46]	Identity, Location	Permissionless (Hyperledger Fabric, Thermal Reactor Consensus)	Anonymous Cloaking Regions, Pseudonyms	Informal	Experimental
TCAC [47]	Identity, Location	Permissioned	Trusted Cloaking Areas (providing k-Anonymity), Pseudonyms	Informal	Simulation (Python)
BELP [48]	Identity, Location	Permissioned (PBFT)	Pseudonyms, Random Encryption Period	N/A	Simulation (OPNET)
Data Exchange (Section 6.3):					
MSVSN [49]	Identity	Permissionless (Ethereum)	Pseudonyms (using Trusted Authority)	Informal	Experimental
PermiDag [50]	Data	Permissioned (DPoS-Based), Permissionless (Directed Acyclic Graph (DAG), PoW-Simplified)	Federated Learning	N/A	Experimental
CCCIoV [51]	Data	N/A	Content Broadcasting	N/A	Experimental
IoVChain [52]	Identity, Location, Data	Permissioned (Hyperledger Fabric, PBFT)	Homomorphic Encryption (Paillier), Zero-Knowledge Proof (Parameters Comparison)	N/A	Proof of Concept (Hyperledger Fabric)
Roac-B [13]	Data	Permissionless (per Cluster, Proof-of-Location)	Rainfall Optimisation Algorithm for Clustering	N/A	Simulation (NS-2, SUMO)
CPHAS [53]	Identity, Data	Permissioned	CLC-PKI Heterogeneous Aggregate Signcryption, Pseudonyms, Ciphertext Policy Attribute-Based Encryption (CP-ABE)	Informal	Simulation
BEIoV-EC [54]	Identity	Permissioned	Multiple One-Time Pseudonyms, Identity-based Aggregate Signature (IBAS)	Informal	Simulation (OMNeT++)
Dynamic Navigation (Section 6.4):					
HACIT [55]	Identity, Data	Permissioned (Hyperledger Fabric)	Pseudonyms (using Smart Contract Address), Encryption	N/A	Proposal
HACIT2 [56]	Identity	Permissioned (Hyperledger Fabric)	Zero-Knowledge Proof (Identity Mixer)	N/A	Proposal
SPIR [57]	Identity	Permissioned	Randomised RSA-Based Partially Blind Signature, Pseudonyms	Informal	Simulation (Matlab, PEPA)
Reputation Management (Section 6.5):					
BARS [58]	Identity	Permissionless (Three Layers, PoW)	Pseudonyms (using Public Keys)	Informal	Simulation (Python)
DRNA [1]	Data	Permissioned, Permissionless (DPoS-Based)	Access Control Policy	Informal	Simulation (Matlab)
TRVN [59]	Identity	Permissioned (PoA, Proof-of-Reputation, IPFS)	Pseudonyms	Informal	Simulation (Matlab)
General Services (Section 6.6):					
BMV [3]	Identity, Location	Permissioned (Ethereum, PoW)	Dynamic Threshold Encryption, k-Anonymity Unity (using Undirected Graphs)	Informal	Simulation (OPNET)
Ba-ITS [60]	Data	Permissioned (Three Layers, Ethereum)	Access Control, Data Encryption	N/A	Proof of Concept (Ethereum), Simulation (NS-3, SUMO)
BSSATV [61]	Identity	Permissioned (Hyperledger Fabric, PoA)	Blind Signature, Zero-Knowledge Proof (Identity Mixer)	Informal	Proof of Concept (Hyperledger Fabric), Simulation (Matlab)
Advertising (Section 6.7):					
ADVN [62]	Identity, Location	Permissioned (Parity Ethereum, PoA)	Zero-Knowledge Proof of Knowledge (ZKPoK)	Informal	Simulation (VANETsim)

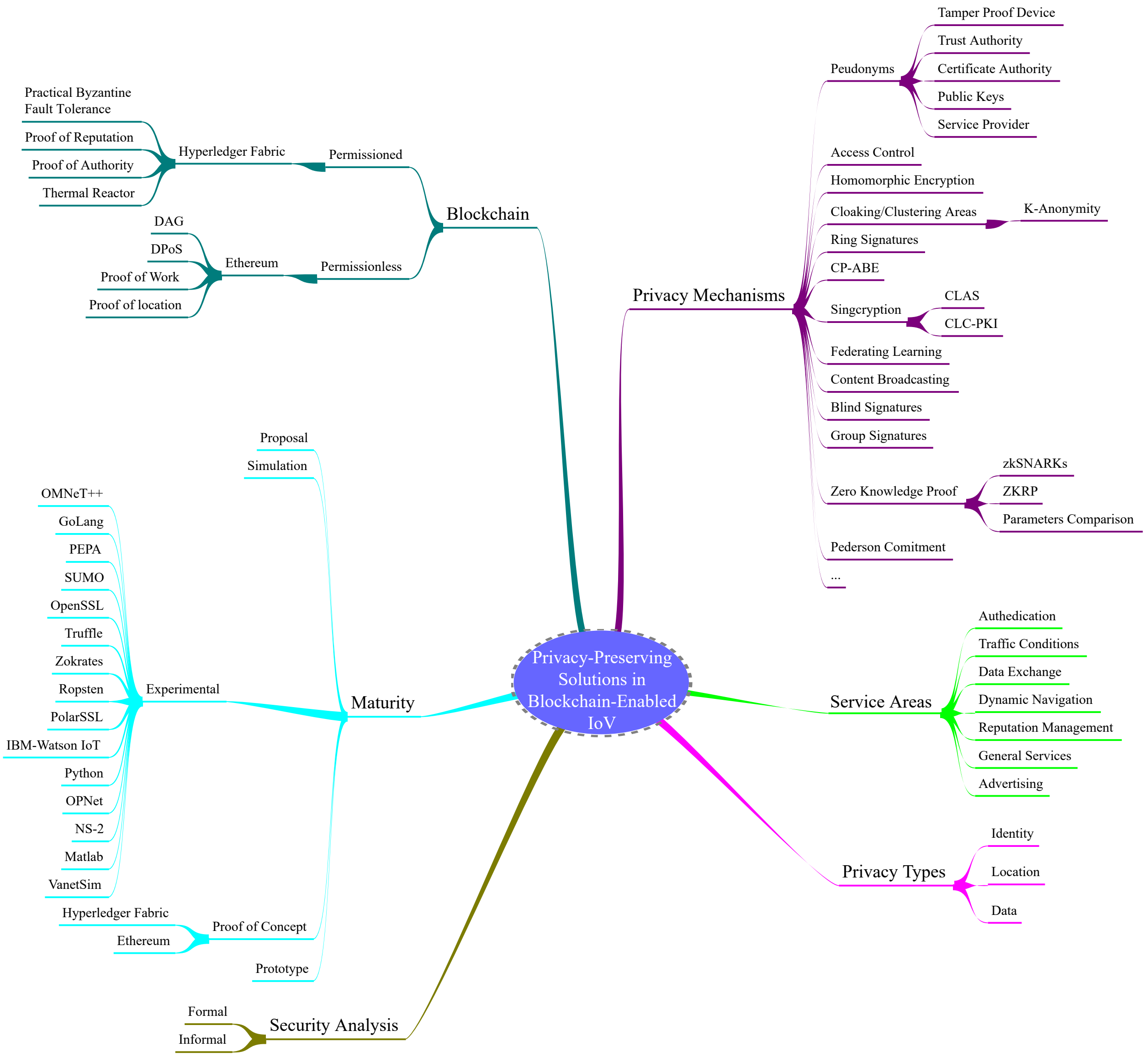


Figure 3. The classification scheme that emerged from the analysis of papers included in this review presented as a mind map.

The service areas (RQ1) covered by the proposed schemes are shown in Figure 4. Most of the schemes cover the authentication area (36.6%), with traffic conditions area to follow (19.5%). The data exchange is next (17.1%). Dynamic navigation (9.8%) and reputation management (7.3%) have some potential and finally general services (7.3%) and advertising (2.4%) complete the areas.

As for the privacy types (RQ2), most research papers (86.84%) included in our survey focus on the protection of vehicle identity, known as identity privacy, whereas location (28.95%) and data (31.58%) privacy are almost on the same level as shown in Figure 5. However, many papers simultaneously provide more than one privacy type, as shown in Figure 6, for example, 8 (21%) papers ensure identity and location privacy, 4 (11%) papers identity and data privacy and 3 (8%) papers provide all privacy types.

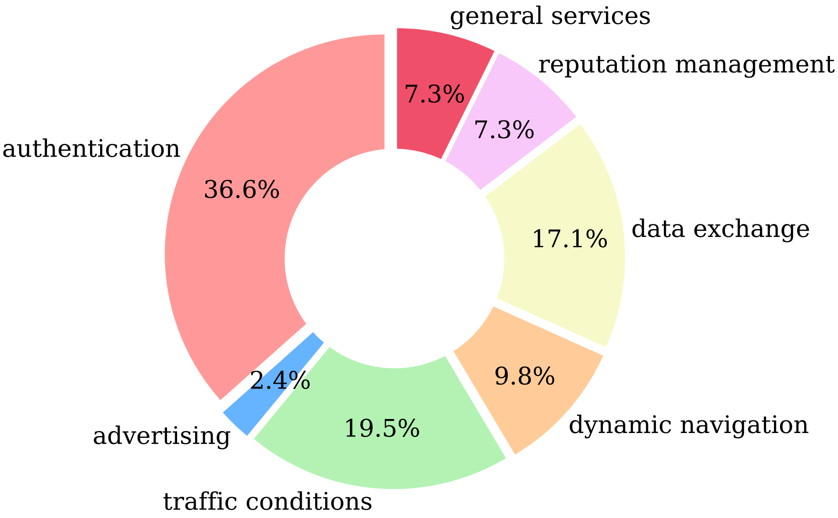


Figure 4. Service areas (RQ1) addressed in the papers included in our review.

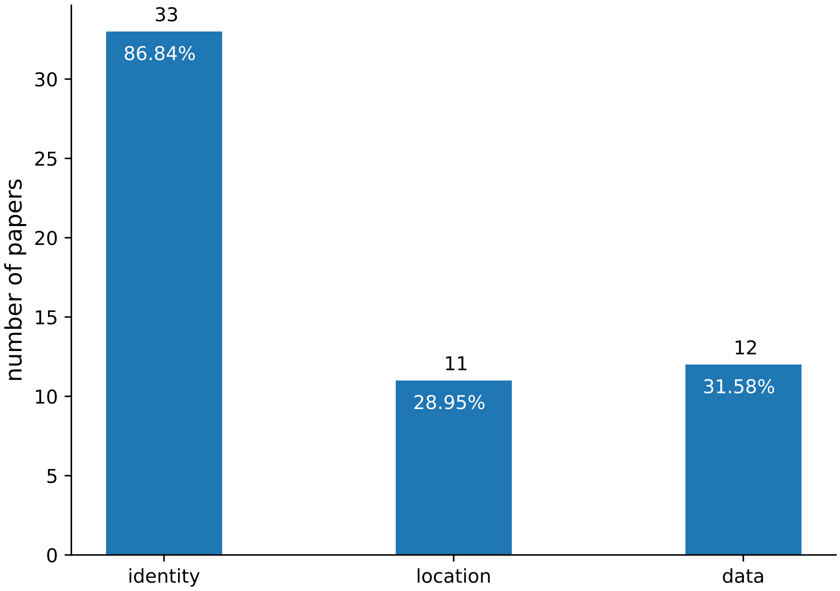


Figure 5. Privacy types (RQ2) presented in the papers included in our review.

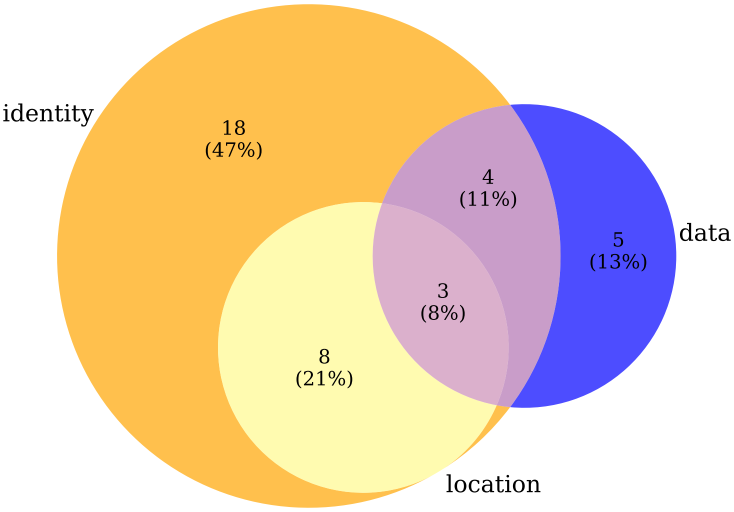


Figure 6. Privacy types (RQ2) overlapping using a Venn diagram.

Regarding the types of blockchain (RQ3) used per NIST definition [8], 24 (63.16%) of the proposed schemes utilise permissioned blockchain, 8 (21.05%) schemes use permissionless and 4 (10.53%) employ both permissioned and permissionless blockchains. Note that two (5.26%) papers do not specify the type of blockchain they used in their solutions, as shown in Figure 7.

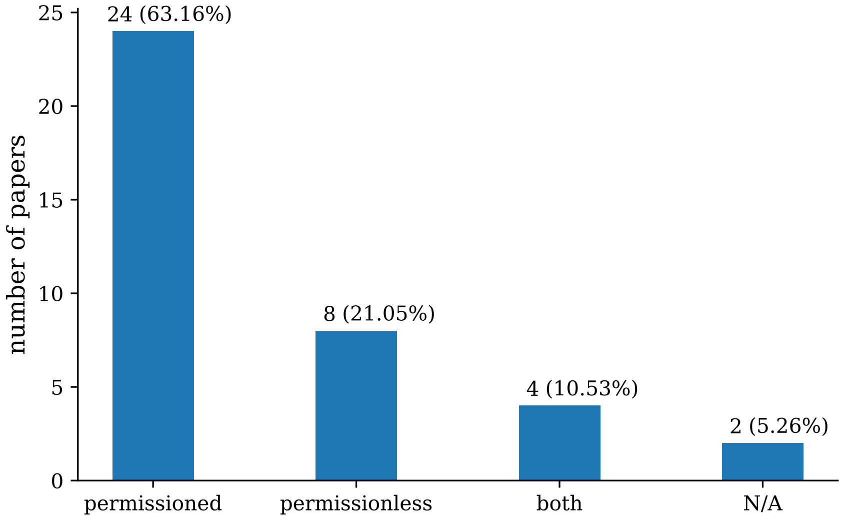


Figure 7. Blockchain types (RQ3) presented in the papers included in our review.

Although there are many blockchain frameworks (RQ4), Ethereum (15.79%) and Hyperledger Fabric (21.05%) are the ones mostly used by the proposed schemes, as shown in Figure 8, while the majority of the papers (63.16%) do not directly mention any framework.

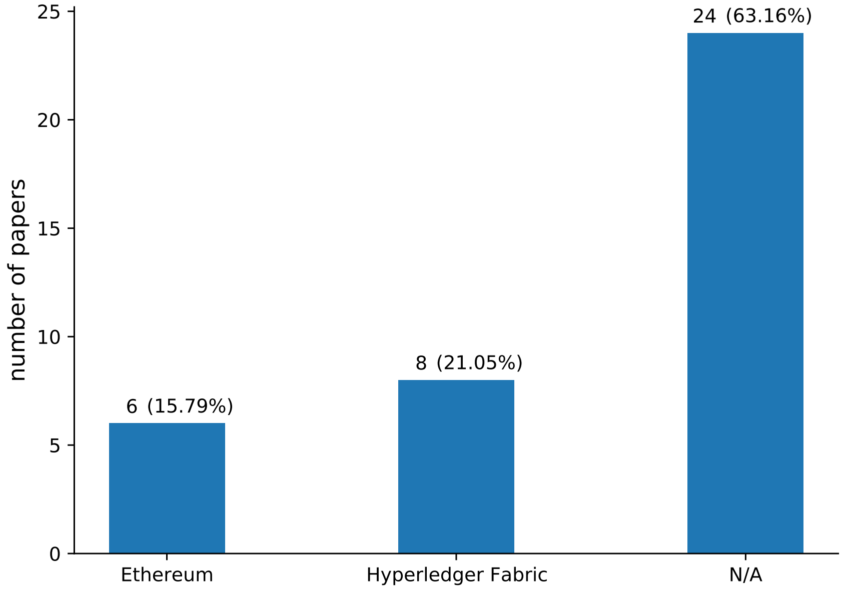


Figure 8. Blockchain frameworks (RQ4) presented in the papers included in our review.

Regarding the privacy mechanisms (RQ5), pseudonyms (52.63%) overwhelm the research papers as shown in Figure 9. Apart from pseudonyms, there are a lot more mechanisms to provide privacy preservation, the most significant ones being zero knowledge proof (15.79%), cloaking/clustering areas (7.89%), access control, homomorphic encryption, ring signatures and CP-ABE; signcryption and blind signatures shared the same percentage (5.26%). Likewise federating learning, content broadcasting and group signatures shared the same percentage (2.63%).

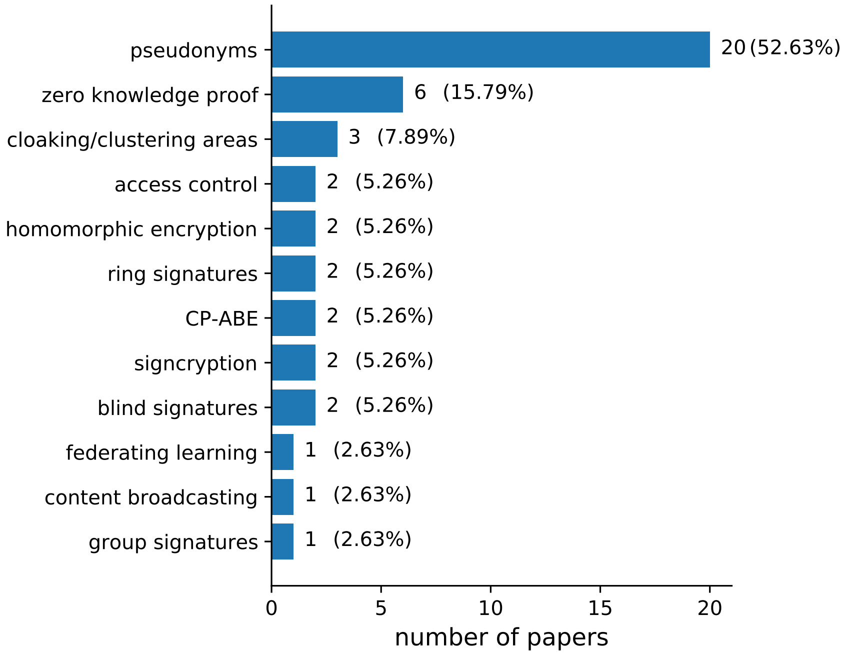


Figure 9. Privacy mechanisms (RQ5) addressed in the papers included in our review.

Regarding security analysis (RQ6), it is shown in Figure 10 that again most of the proposed solutions are informally analysed (63.16%), where only one solution (2.63%) provides a formal analysis. It is notable that 13 papers (34.21%) do not provide any security analysis.

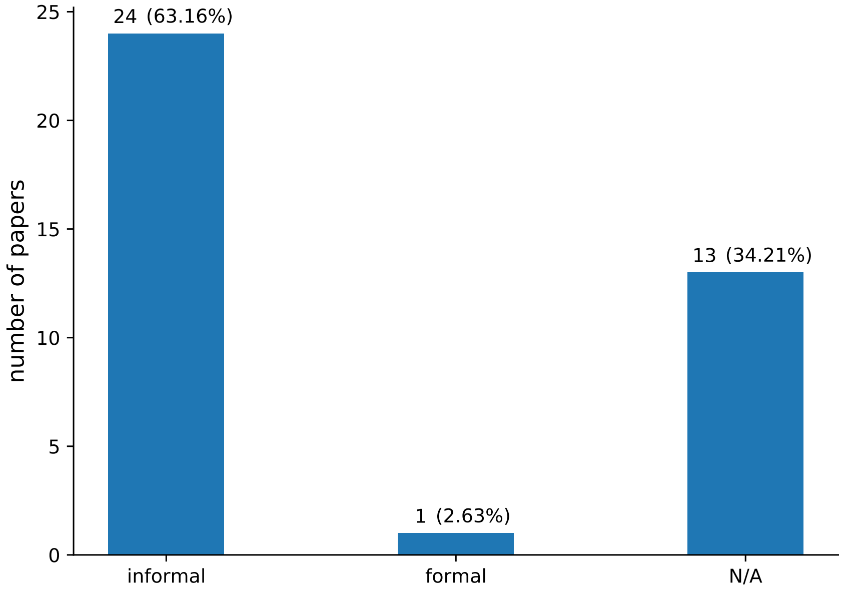


Figure 10. Security analysis (RQ6) provided in the papers included in our review.

Finally, regarding the maturity level (RQ7), most of the solutions have been tested only in simulation (47.37%) or in experimental environment (31.58%), as shown in Figure 11. It is notable that only 4 solutions (10.53%) are proposals, 4 (10.53%) are proof of concept and only 1 (2.63%) is prototype.

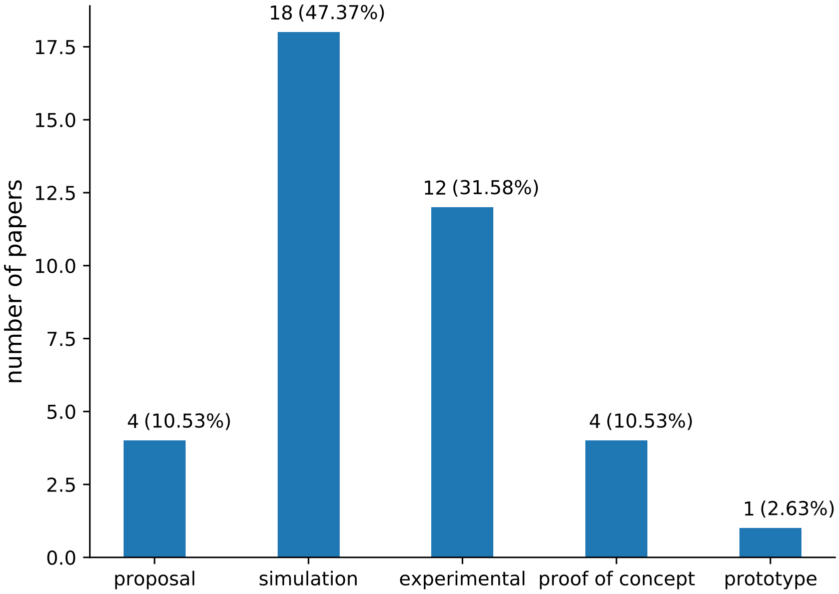


Figure 11. Maturity (RQ7) of the schemes presented in the papers included in our review.

6. Privacy-Preserving Blockchain-Based Solutions

In this section, solutions that have been proposed to preserve privacy by the usage of blockchain in different aspects of IoV are presented organised by their service area (RQ1).

6.1. Authentication

There have been several works published in the area of blockchain-based pseudonym management and authentication in vehicular networks and they are presented below.

Liu et al. [28] introduced DAIA, a system that can ensure identity authentication and privacy. DAIA is based on a permissioned blockchain and provides a dynamic pseudonym using a tamper proof device. The main participants in this system are a Certification Authority (CA), Roadside Units (RSUs) and vehicles. CA as master node manages the blockchain network and the new block generation and is responsible for the secure parameters' selection. Moreover, it acts as the primary node in the consortium, records all the information and publishes the public information of RSU and tracks malicious vehicles and keeps a list of them. It is assumed that it is a trusted entity and can backtrack the identity of a malicious vehicle. RSUs are spread across the road and can manage the vehicle in their range. They are wired connected with the CA and wireless with the vehicles. They can download the malicious vehicle list from CA and it is considered as semi-trusted. Vehicles are equipped with OBU and realistic TPD (Tamper-proof device). The OBU is responsible for the wireless communications and the TPD for the storage and management of the private parameters, pseudonyms and keys. Due to attacks the TDP must frequently change the key. The dynamic anonymous identity authentication consists of five phases: (1) Registration: CA sets the parameters, RSU and Vehicles are registered to the networks and their ids are published in the blockchain. (2) Anonymous identity generation: when a vehicle enters in RSU range the TPD creates the random pseudonym. (3) Communication: vehicle communicates with the RSU exchanging time stamped messages. (4) Tracking: when a RSU wants to trace a vehicle it sends a message to CA. Then, CA writes the vehicle in the malicious list. (5) Update system keys: when system keys expire it drops them and creates new ones.

The overall DAIA system is built up to be resistant to the following attacks: (i) Unlinkability: the true identity of the vehicle is stored to CA so an attacker cannot obtain the keys; an RSU does not carry any sensitive vehicle information. (ii) Non-repudiation: the vehicles cannot deny the message they send. (iii) Strong privacy protection: even if all the RSUs are compromised, the identities of the vehicles are stored with hash functions. (iv) Realistic TPD assumption: the TPD changes the keys frequently, so it is difficult to be compromised by side-channel attacks. (v) Man in the middle attack resistance: any attack of this type can be detected by the RSU. (vi) Efficiency analysis: the efficiency of the system is ensured by the ECDLP. Security analysis and simulation have shown that the proposed scheme is slower that others but achieves better security and strong privacy-preservation which make it suitable for practical VANET environments.

Sharma et al. [29] suggested a scheme for vehicle authentication and privacy preservation called BlockaAPP. Based on private blockchain technology, this system consists of four entities. The first entity is the vehicles. The second entity is a registration server, which is responsible for managing and validating vehicle's ID. The verification of the vehicles is carried out by the third entity, called Service Provider. Moreover, there are multiple service providers in order to supply different services to vehicles simultaneously. The last entity is the blockchain. A trusted authority gives access to the blockchain, where service providers can read and write, in contrary of the registration server which can only write to the blockchain. The trusted authority is the only one that has the ability to read the blocks and transaction timestamps in order to trace any malicious activities back to the real ID. The proposed system works in three phases. The first one is the registration phase. In this phase, to avoid identity spoofing and to preserve its privacy, every vehicle sends an encrypted message to the registration server and a trusted authority checks and exchanges their real ID with a pseudonym. This pseudo-id will be used for any future communications for one session. After a successful exchange, the registration server adds the necessary details of the transaction in a block and dumps all the other so that real ID cannot be retrieved. During the second phase which is called authentication phase, the vehicles send their pseudo ID and the requested services to the service providers. The service providers accept or decline the requests. Then, they add any valid or not request to the blockchain. The third and last phase is the authorisation phase. For every offered service, the service providers maintain a pair of private and public keys, in order to identify the service and the transactions. The vehicle sends a request message and its digital signature that is created using its private key. The service providers check the request message and add the transaction to the blockchain, whether it comes from a valid vehicle or not. For the exchange of keys, the proposed system has considered an asymmetric key cipher and the validity of the transaction is ensured using a consensus protocol. During registration phase, RSU, vehicles and cloud server act as intermediate access point to the registration server and to the service providers during authentication and authorisation phases. The authors built their system on a permissioned Ethereum platform and the smart contracts are implemented in Solidity language using the Remix development platform. The results demonstrate that by using the permissioned blockchain, privacy can be preserved.

Another pseudonym management system for IoV is VCS proposed by Bao et al. [30]. In this scheme, the authors use a four-layer type of nodes. The first three layers for the service providers consist of RSUs covering geographically all the roads, PMs (Private Manager) both with wireless communication devices, plus the RSU act as access point and Public key Infrastructure (PKI), containing Certificate Authority (CA), Anonymity Server (AS) and any other third party infrastructure, where all the pseudonym and cryptographic materials are created. The fourth layer called service user consists of the vehicles equipped with computerised device known as On-Board Unit (OBU). The PKI is isolated and generates all the cryptographic material to link the real identity to the pseudonym of the vehicle. The pseudonyms are not permanent, but they change after a period of time. Moreover, all these cryptographical materials must be kept in a secured facility to ensure the privacy and security requirements. The central managers can be accessed only for the initial registration of the vehicle and for revocation of a certificate, in case of malicious behaviour or identity compromise. In this proposed system, the PM are shuffling the pseudonyms and the PKI can keep track of the pseudonyms related to original identity, by keeping the transaction in a disturbed ledger, making the revocation of a certificate in the shortest possible time. The new revocation list will be broadcasted to the vehicle nodes. For the blockchain network to work properly, some assumptions are made: (1) Role of the miners: PM take the role of the service user and miner as they have powerful computation power to maintain the blockchain and do the block mining since there is not any reward, featuring in classic blockchain networks. (2) Approximate Mining Synchrony: to limit the deadline for each transaction collection interval, all the PMs start the mining at the same time, using a synchronised clock. (3) Consensus: the adapted consensus is Proof-of-Work, since it is the only one efficiently tested against security manners.

The function of the VCS is described below: (i) System initialisation: the cryptographic material is generated by the PKI and transmitted through highly secured connection to the vehicle and equipment manufacturers, who install it to the vehicles. (ii) Pseudonym Shuffle: the vehicle marks the pseudonym as used and when the expiration conditions are met, the vehicle can change it, only when it enters on an agreed place named mixed zone, where all vehicles are mixed in order to minimise the ability to be tracked. The expired pseudonyms are kept for a certain period in single package, and afterwards they are shuffled and disturbed back to the PMs for reuse. (iii) Certificate revocation: the proposed system has a malicious behaviour detector; PM collects all the activity and while communicating with the network, it broadcasts all the malicious reports. Even if a PM is compromised, the blockchain network is secured, as it needs 51% of them to work properly. The proposed system is built in permissioned blockchain and has been tested in simulation, using OMNET++ with dedicated simulation packages Veins and PREXT; the simulation results find the proposed system more effective than the traditional pseudonym solutions and more resilient to privacy and security attacks.

Guehguih et al. [31] presented an authentication and message dissemination scheme for vehicular systems which contains two different blockchains, a permissioned geographical blockchain and a permissionless blockchain. The permissioned blockchain is used for authentication of vehicles within the boundary of a country. In this blockchain a trusted authority (TA) is responsible for generating new blocks which represent pseudonyms of users in a chronological order. During the registration process, a secure channel is established between the vehicle and the TA, and then the vehicle sends to TA its real identity, obtained by Motor Vehicle's Division (MVD). Afterwards, TA cooperates with MVD to check the vehicles real identity and then produce a pseudonym for that vehicle. After the successful vehicle's authentication, TA appends a new transaction to blockchain. Vehicles can only read this blockchain to check the authenticity of other vehicles. In addition, special vehicles have the role of miners while other On-Board Units have only read rights, thus malicious behaviour is prevented. The public blockchain, named RSU-BC because it acts as an RSU, is used for event messages dissemination. RSUs are replaced by blockchain, in order to achieve decentralisation of the system and avoid a leakage of private information in case an RSU is attacked. In RSU-BC every entity can generate new blocks representing event messages. Vehicles can act either as miners in this blockchain or as light nodes which are only responsible for generating messages. After a new block is generated, all cars in the system update their blockchain and can be informed for information such as road conditions and safety. In the case of a vehicle travelling in another region, the miners of the new RSU-BC check its authenticity in authentication blockchain in order to participate in the message dissemination procedure.

By using geographical blockchain, consensus convergence time is reduced. In addition, because pseudonyms are stored in a blockchain, they cannot be modified by third parties. Moreover, because only trusted authority knows the association between pseudonyms and real identities and no other information is issued in transactions, privacy is prevented. During experiments' performance and security analysis, the proposed scheme was compared with previous models and proved that it requires the lowest computation and communication cost, according to the authors.

A privacy preserved framework in VANET is proposed by Zheng et al. [32]. The proposed system is based on blockchain and pseudonymity. The vehicle obtains its real identity from Motor Vehicle's Division and communicated with a trust Certificate Authority (CA) via a secure channel. CA verifies the real ID and issues a pseudonym (PID) with a pair of public and private ECC keys. Two hash functions are calculated by the CA. The H_0 is the vehicle pseudonym and public key and H_1 is the relationship between the vehicle's real identity and pseudonym. The H_0 function is stored in a Cloud server and the H_1 function is stored inside the vehicle's OBU and on the permissionless blockchain at the stage of authentication. As the authors mention, there are multiple cloud servers where the data are stored divided for decentralised reasons, and a Proof-of-Work consensus is used. When a Vehicle enters RSU range and sends its PID and public key, the RSU authenticates it calculating the H_0, querying the cloud server for trueness. The result is recorded on blockchain. To verify the secure communication, RSU sends a random integer encrypted with the vehicle's public key. Upon reception, the vehicle chooses another random integer and calculates the hash of both, sending it back. Finally, RSU verifies the hash function with vehicle's public key and packs it up as a transaction on the blockchain. When a Vehicle needs to announce a traffic condition, an accident for example, it is called event D. The event D can be a text, a photo or video. When an event D occurs, the vehicle utilises the random number previously exchanged with RSU; that way the RSU authenticates the event and packs it on the blockchain as a transaction and broadcasts it to the network. Simultaneously, the transaction details are divided on random cloud servers. If in any way, the RSU cannot validate the vehicles ID or event truthiness, it requests the true identity of the vehicle from the CA and broadcasts the malicious vehicle into the blockchain. The scheme has been simulated in GoLang to analyse and evaluate the security and performance.

Benarous et al. [33] focus on preserving a decentralised solution for the pseudonym management which ensures the privacy and security of involved participants. The supposed framework is a blockchain consisting of two blockchains: a certifying blockchain managed by registered vehicles and a revocation blockchain maintained by the Roadside Units (RSUs). Both blockchains are public and permissionless. Additionally, there is another one chain, the offline chain, which is permissioned and maintained and accessed only by the RSUs. The certifying blockchain is used by vehicles for saving the certified pseudonyms. RSUs have access to this blockchain only with read rights. In contrast, in revocation blockchain, RSUs have write access rights, while vehicles have only read rights. The offline chain is used to link the revoked the temporal pseudonyms with their users. The all framework is seen as one blockchain by the end user regardless of his role. The blockchain framework enables vehicles to generate, validate and handle their own pseudonyms without any authority's intervention. While registered, a vehicle creates a transaction that acts as a certificate for its pseudonym and appends it to the certifying blockchain, executing the Proof-of-Elapsed-Time consensus model to publish blocks. To eliminate central's authority usage, vehicles sign their transactions using ring signature. In revocation process, misbehaving nodes are detected by vehicles which inform RSUs. Then, RSUs revoke the pseudonyms of malicious nodes and after recomputing the one-time address to find their public key and all their unused pseudonyms, they append all malicious user's information (the revoked pseudonym, the public key and all unused pseudonyms) to the revocation blockchain which is then distributed to the network. RSUs execute round robin consensus model, in order to publish blocks. During the authentication phase, vehicles firstly check that the used pseudonym belongs to the certifying blockchain and not at revocation blockchain and afterwards they check the validity time and beacon's signature.

The users' identity privacy is protected, as blockchain prevents their identity and their car's identifier of being exposed. Furthermore, vehicles can check a pseudonym's or signature's validity, without being able to link it with the real singer, by using one-time addresses. In addition, blockchain does not record private keys, thus anonymity is ensured because identities are not exposed. Lastly, because all used pseudonyms are recorded in blockchain, malicious nodes cannot deny their committed actions. In addition, in case of misbehaving, all unused pseudonyms and their public key are revoked. Thus, the system is secure from attackers and malicious users. Lastly, through security analysis, by using attack tree method, the authors have shown that their model is more resistant to attacks than the conventional vehicular public key infrastructure (PKI).

Yao et al. [34] proposed a privacy preserving scheme with trust management. Their system considers responsible the Law Enforcement Agencies (LEA) to register a vehicle to network. The RSUs are responsible to distribute pseudonyms to the vehicles, as well as to maintain a two layer permissined blockchain. On the blockchain's consortium layer are stored the pseudonyms, to preserve privacy, and the messages of the vehicles. On the vehicular layer, the vehicle's authentication is stored, as well as the trust evaluation of the vehicles. The system has the ability to change a vehicle pseudonym if requested. To prevent any data tamper, trust calculation is secured by homomorphic encryption. A performance implementation has been employed using the Performance Evaluation Process Algebra (PEPA) model showing that homomorphic encryption and pseudonymity can protect the vehicles' privacy.

Su et al. [35] proposed a system based on permissioned blockchain for IoV with privacy protection. The system has three entities: LEA, RSU and Vehicles (users). The Law Enforcement Agency (LEA) is responsible for the registration of the vehicles. The owner of the vehicle must send the real information of the vehicle (like license plate number, name and type) and the LEA determines if it is legit to participate in the network in order to generate a username (pseudonym) and a pair of public-private keys and the validity period of the keys, as it must change on a regular basis to preserve the vehicle's privacy. RSUs are responsible for the communication between the vehicles and maintains the blockchain network, registering network's data. For that reason, RSUs should have powerful computation power and sufficient storage capabilities. Moreover, RSUs are responsible to detect distorted broadcasts and evaluate the vehicles, forming a reputation system. If any of the vehicles are flagged as malicious, its key is revoked and the process packed as a transaction registered into the ledger. Based on experiments, the location privacy is preserved by pseudonyms and by using encryption on the public keys.

Moussaoui et al. [36] proposed a scheme for VANET based on blockchain that uses PKI to preserve privacy called BCPKI. The scheme consists of Vehicles (users) and RSUs. The vehicle must register to the network via RSU. The vehicle requests to join the network and the RSU issues a pseudonym using PKI certificates and stores it to permissionless blockchain. Authors use pseudonyms as a primary privacy preserved technique for their proposed scheme.

A light-weight authentication scheme based on permissioned blockchain for VANET is proposed by George et al. [37]. The architecture includes Authentication Parties (AP) that are responsible for ledger maintenance and registration of the vehicles. The vehicles are the users and RSUs which have a read-only access to the ledger. Upon registration AP disturbs a set of public-private key set to the vehicles, as well as a pseudo ID, called PID, to preserve the vehicle's privacy. Moreover, AP is the only participant that can trigger transactions and write on the blockchain. Vehicles are equipped with OBU and can transmit Basic Safety Messages (BSM) to other vehicles or to the RSUs. The privacy, during the exchange, is preserved by the pseudo ID. The BSM have attached the private key of the sender that key can be used to authenticate the BSM without the intermediate use of RSU. The system is based on Hyperledger Fabric using a Solo ordering service and has been simulated on OMNET++ and SUMO, indicating that the system can reduce RSU computation power.

In [38], a blockchain-based decentralised reward solution is described. The suggested model is based on a permissioned blockchain which is distributed among multiple RSUs in a vehicular system. Every vehicle in the network is equipped with a tamper-resistant black box which uses smart cards to store credentials in order to ensure safety of transferred data. During registration phase, vehicle's black box (VBB) generates vehicle's keys and then shares the public key and vehicle's identifier to the service provider (SP). The connection between the SP and VBB is performed through a secure channel by using SSL and TLS protocols. Vehicles use pseudo-identities that are produced by their public key and random numbers, to communicate with RSUs and send data to them. Only SP knows the real identity of vehicles in order to reward them from sharing data. When vehicles travel in a vehicular system, their VBB send data to nearby RSUs which pack those data into blocks. Afterwards, the blocks are sent to the RSU with the smaller workload to upload them to the ledger. A copy of the blockchain is then stored in every RSU, and all copies are synchronised with each other, avoiding central vulnerabilities to attackers and location compromise. Because vehicles use pseudo-identities, RSUs cannot figure out which vehicle transmitted the shared data, but they can authenticate it.

Changing pseudonyms are used instead of a unique identifier, so they cannot be linked with their real identities. Furthermore, when a pseudonym is changed to a new one, network identifiers (IP, Mac addresses) change simultaneously to protect linking between those pseudonyms. Only service provider (SP) and no one else can trace the real identity of vehicles in order to reward them for sharing data. In addition, RSUs authenticate messages, without knowing or guessing which vehicle transmit them, but the signature verification of the proposed protocol ensures that only legal vehicles transmit data. Therefore, anonymity and privacy of transactions are ensured. Lastly, through experiments on open SSL and performance analysis, the authors support that anonymity is provided in authentication services.

Gabay et al. [39] proposed two different approaches for privacy preserving authentication of Electrical Vehicles (EVs) throughout charging process. Firstly, they implemented a framework which combines Ethereum blockchain technology with zero-knowledge proofs and more specific with Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARKs). In this model, EV Charging Service provider (EVSP) acts as the Trusted Third Party (TTP) which is responsible for user registration by producing a secret function and for generating, proving and verifying keys. Then, EVSP sends the function and proving key to the users and verifying key to smart contract of blockchain. The user (or prover) is the EV, which must solve the above function in order to generate a witness and then integrate this with proving key in order to generate a proof with a public timestamp, while the blockchain is in charge of verifying the prover's proof without knowing any details. A pseudonym address is used by EV to communicate with the blockchain smart contract, with the peculiarity to use a different pseudonym address whenever it desires to use charging service. Since the proof is verified and authentication is completed, a service token is created by the smart contract, which EV can use to plan its charging without having to confirm its identity. Then, this information is encrypted with EVSP's public key. EVSP uses encrypted information in order to schedule charging of an EV and a charging-token is returned to the EV which sends a cryptocurrency deposit as a warranty; this is the same for every EV to prevent fake charging schedules. During charging procedure, the charging station receives the EV's charging-token to confirm that it is the scheduled one.

Moreover, they improved their approach by using a Pederson Commitment rather than the token mechanism, in order to improve the efficiency and reduce the cost of provided services. The basic changes in this approach are that the EVs do not only receive from EVSPs the proving key and function that they have to solve but also the Pederson Commitment parameters. The function is also more difficult than the previous case in order to be more cryptographically secure. If the EV can open Pederson Commitment, it can schedule charging. With the given elements, EV creates its own commitment. Furthermore, the EV is aware of its preferred scheduled charging slot, as it is contained it the commitment, so it encrypts a message that EVSP can later decrypt to book the charging station. The EV verification during charging procedure is done through a comparison of EV's and EVSP's commitment. This comparison is accomplished by EVSP while the equality of those two commitments proves that the EV is the scheduled one. Like their first approach, EV use pseudonym addresses and a deposit in the form of cryptocurrency to pay for charging. Furthermore, in both approaches, a single smart contract is responsible for all EVs to improve the performance and efficiency of those models. Through security and privacy analysis, the authors have proved that their two approaches ensure that personal information of vehicles, like their ID or location, can be securely protected by using zkSNARKs, because EVSP can authenticate EVs without knowing any other information. Additionally, charging stations also cannot access any personal data, as they are only aware of the anonymous identities of EVs, and malicious users cannot match the Ids to their real users or obtain another information from the blockchain. Regarding the payment method, as it can by accomplished through cryptocurrency and blockchain, anonymous payment is permitted without using a credit card, thus protecting the privacy of users. Both proposed models were evaluated by using Zokrates, a toolbox for zkSNARKs on Ethereum, and results have shown that they are both feasible for real life, with the second approach prevailing first in time and money cost.

Akhter et al. [40] proposed VANET, a privacy-preserving system that uses multi-level blockchain-based on clustering. Their proposal consists of vehicles and Authentication Centres. Moreover, the system is based on 5G wireless networks so the use of RSU is not needed. The Authentication Centres are divided geographically; there are the locals (LAC) and a global (GAC) consists of all the LACs. The LACs keep a blockchain ledger with the registered vehicles in their region and the GAC maintains a blockchain ledger with all the registered vehicles. The system, to preserve the privacy of the vehicles, firstly needs to physically verify the vehicle by LAC and impute it with a private key. This private key is used as a pseudonym for information exchange on VANET. Moreover, the vehicles are divided into two categories, the General Vehicles (GVs) and Emergency Vehicles (EVs) such as ambulances. In order to preserve location privacy the vehicles moving at the same direction form a cluster. When an EV enters the cluster it can use the system to transmit an emergency signal and notify the other vehicles in order to provide it with safe passage. The network is based on Ethereum and simulation experiments that have been contacted on the Truffle suite, showing the proposed system is feasible.

6.2. Traffic Conditions

Another important service of VANET is the monitoring of traffic or road conditions in order to improve the performance of the road circulation and avoid accidents. The following papers suggest several systems which purpose is to upgrade road conditions while protecting privacy.

Li et al. [41] suggested CreditCoin, a system for announcement exchange in VANET. It develops a custom announcement protocol by the name “echo-announcement” and a permissioned blockchain network based on coin-exchange system for reliability and privacy. The key entities of CreditCoin are a Trusted authority (TA), which is responsible for managing the cryptography keys and user identity, the Trace manager (TM) to trace malicious users, users which are vehicles and On-Board Units (OBUs), Roadside Units (RSU), which are distributed alongside the roads and are responsible for the users inside their communication range and lastly, a cloud application server for non-cryptographic data exchange. The main idea of the system is that a user can broadcast in the network via the “echo-announcement” protocol, reliable information about the traffic and the receivers are able to take advantage of these information in order to make route changes. The blockchain network is based on coin-exchange logic for every valid announcement. Every user starts with a few coins in order to broadcast an announcement and a threshold ring signature of this announcement, for example a car accident, which nearby users must confirm and then RSU with official public vehicles take the role of the consensus server which creates the coins. Thus, there is not a need for a work-of-proof, instead a byzantine fault tolerance consensus algorithm is used and by taking advantage of combined-public keys (CPK) for reducing cryptographic time consumption, the transactions are fast. The confirmed announcement is signed by the nearby users and broadcasted in the whole network. As a result, the user is earning coins and reputation. A false announcement costs coins and for that reason, the network can be protected from malicious users. Moreover, to avoid attacks to user’s wallet, the coins and the reputation have time limitation for their use. If any misconduct was found, the trace authority Pseudonym Management sends the information to the cloud application to take actions. The proposed system had been tested thoroughly in PolarSSL simulation environment and the results have shown that privacy can be sufficiently preserved.

Bai et al. [42] suggested a blockchain-based warning scheme which aimed to solve traffic problems. This system is using a group signature-based authentication protocol in combination with blockchain technology, to guarantee privacy and security and parallel to ensure identity traceability. In contrast to traditional methods, where the status information of vehicles is acquired by the on-board diagnostics and the position data through the GPS sensors, the proposed system is using a smart terminal (for example a smartphone) to collect those data, through some adjustments and assumptions. Such assumptions are that a normal turn takes 5 s and a sharp turn takes 3 s. Furthermore, x and y axis of the terminal simulate the acceleration and angular velocity respectively. The irregular noise that may occur can be eliminated using a weighted moving average filter. The collected data is sent to the feature recognition module for driving behaviour identification. Detecting irregular driving can warn the driver early for possible accident. An edge node within the group is served to Group Managers which create a pair of public and private keys and broadcast the public and parameters to in range vehicles. The vehicle applies a blind signature and submits its authentication information back to the manager. Finally, the vehicle communicates with nearby vehicles through the edge node, having signed the status information through certificate and group public key. In case of an accident or a malicious behaviour, the manager can track back the vehicle through the public key in the group signature.

The edge nodes maintain the permissionless blockchain and also collect data from vehicles and put them into blocks. As a consensus protocol, the authors proposed a hybrid one based on PoS and DAG, as the popular Proof-of-Work consuming a lot of processing power. Because of the continuous change of the data that the road conditions impose and until the wide use of 5G, a Time Sensitive network is the best solution at present as the authors mentioned. Security tests have been made by collecting real life data, by using iPhone 7 as smart terminal and computer with Ubuntu OS for the data processing. The data had been collected by taxis and family cars, and then the evens were edited by hand. The authentication protocol and blockchain have been tested in simulation on IBM-Watson platform, which proved than they can be used for quickly obtaining warnings and in parallel protecting a user's privacy.

Cheng et al. [43] proposed a semi-decentralised scheme called SCTSC for privacy preservation in identity, location and data. The scheme uses a permissioned attribute-based blockchain to control traffic lights. In this scheme, in order to reduce traffic, signals of traffic lights are controlled by vehicles. Vehicles are divided into groups according to their dynamic attributes such as their location or direction. In these groups, every vehicle votes for the time of signal change and their agreement along with other related messages are encrypted and then recorded to blockchain. The procedure to reach an agreement is divided into four phases: (1) The *setup phase*, where public parameters are generated using ciphertext policy attribute-based encryption (CP-ABE) and also verification of users' identity is done. (2) The *drafting phase*, where a proposer chooses a voting group according to vehicles' attributes and poses a suggestion for signal control. A fixed number of voters is needed to reach an agreement. The threshold value is decided and stays unchangeable in next phases. (3) The *reply phase* where a number of voters reply in order to reach an agreement. The voters verify signatures and send their replies to a recorder who appends those as records into blockchain. (4) The *decision phase*, the proposer collects all replies, decrypts their ciphertext and after checking the pseudonyms and signatures or double entries, if the number of voters is the expected, he sends the decision record to the recorder; otherwise, he continues collecting votes. Consequently, the recorder, which does not know the real identities of proposers and voters, records the agreement to blockchain by performing a cooperation consensus algorithm.

In SCTSC, vehicles communicate with each other through blockchain and not directly. Other groups or traffic signal controllers can receive this final agreement without breach of users' privacy. This is achieved due to the anonymity of users who use pseudonyms during communication process. Authentication centre is responsible for verifying users' actual identities and distributing keys and pseudonyms but cannot decline any user. Trace manager is responsible for detecting malicious users by querying their pseudonyms in authentication centre. In addition, intermediate messages and other contents cannot be read by third parties outside those groups, thus privacy is also preserved inside the groups. Through extensive experiments and security analysis, the authors proved that SCTSC is feasible and effective.

Wang et al. [44] suggested a framework, called CFTM, which describes the monitoring of road conditions by using cloud-fog computing for location and data privacy. In this scheme, vehicles signcrypt messages by using certificateless aggregation singcryption (CLAS) technology and then send them to RSUs which act as fog servers and also verify if the vehicle user is legal or malicious. Single verification is performed in the case of one sent message and aggregation of signatures parts of multiple ciphertexts in the case of multiple messages. Afterwards, the aggregated signature is sent to a cloud server for verification and then transmitted in ciphertext format to the blockchain. A root authority decrypts and verifies the ciphertext on the blockchain in order to respond in situations of emergency.

In CFTM, The privacy and anonymity of vehicles are ensured as they are using pseudonyms during communication procedure. Only the traceability authority, which is responsible for generating pseudonyms for vehicles, knows their real identity. Thus, the identity of vehicles is protected. In addition, while communicating, signcryption is used, so the transferred data is in a ciphertext format and cannot be decrypted by fog server, nor cloud server or malicious users. Furthermore, the cloud server carries on the ciphertext equivalent test process and sends the ciphertext, which exceeds the threshold to the blockchain. The ciphertext cannot be modified or deleted after being added to the blockchain; therefore, road condition information and sensitive information of users remain immutable and are secured from malicious behaviours. Moreover, as traceability authority can trace the real vehicles' identity, it is easy to find malicious users. Formal security analysis of the proposed model and extensive comparisons with other existing models have shown that it satisfies the security requirements and works efficiently.

Wanxin Li et al. [45] addressed the problem of traversing between different blockchain networks, preserving the privacy of the vehicles. To achieve the above, they propose a gateway system with non-interactive zero knowledge range proof scheme (ZKRP). When a vehicle wants to leave a network and enter another's territory, it encrypts its information with the proposed ZKRP and broadcasts the request to the nearby gateway. Upon request receipt, the gateway validates the request and the vehicle connects to the new permissioned blockchain network based on Hyperledger Fabric, with the ability to start sharing data. The authors have built and tested a prototype, which shows data integrity and vehicle privacy can be maintained while switching networks.

Bohan Li et al. [46] proposed a location cloaking system in VANET based on a dual-layer permissionless blockchain. Their system consists of vehicles which are the users, RAs, which are responsible to register, update or revoke the vehicle's certification and store the certifications on blockchain layer named CerBC. The certificate acts as a pseudonym for the vehicles. RSUs are responsible to manage vehicle's requests and form the clocking region with k-anonymity algorithm. Moreover, they are responsible to forward the requests to LSP. In addition, they maintain the requests of another layer blockchain named ReqBC. The LSPs are responsible to process the query requests using the query algorithm and return the queries to RSUs. LSPs do not interact directly with the users and users do not interact directly with each other. The system uses a trust reputation system based on vehicle's Querying reasonability, from space and from frequency, plus, rationally and authenticity of location information. In summary, the privacy preserved with no direct communication between entities, certifications which act as pseudonyms and cloaking location with clustering $k - 1$ vehicles. Experiments were made in Hyperledger Fabric using PBFT consensus protocol and ECC for the cryptographic algorithm. The results show that the system can preserve privacy.

Feng et al. [47] proposed an identity and location privacy scheme called Trusted Cloaking Area Construction (TCAC). Using k-anonymity [63], a well-known privacy technique and a trusted third-party entity, called anonymiser, can expand the precise location area of one vehicle to a circle location, with addition of $k-1$ vehicles as cooperative vehicles, concealing the actual location of the vehicle. The designed architecture is composed by three layers. The first layer is the permissioned blockchain architecture where a set of anonymisers take the place of the miners and maintain a blockchain consortium. On the second layer, between blockchain and Vehicles, are deployed the RSUs, to serve as intermediate nodes, to help collect data and for trusting evaluation. Finally, in the third layer, we found the users (vehicles) where they can broadcast or receive location relative information, within a small area. To achieve the data immutability and trust, only anonymiser can propose a block. The anonymiser sends his proposal to anonymiser president, who is being elected by timestamp voting and who is in charge of validating a block. If the president validated a block, then he added it to the chain, based on the timestamp, and broadcasted it to the network. The difference between the traditional blocks is that the TCAC block header includes more information, such as the ID of the anonymiser that proposed the block, the signature of Merkle tree root added by anonymiser, the ID of a vehicle that sends request based on its current location, the ID of cooperative vehicles set, the number of the location information, marked as true, false or rejected, of the particular vehicle and the block ID with the most recent change in location information status. Moreover, the authors to avoid chain load have created a redundant block deletion strategy, where blocks, based on the number of the recorded data, are considered to be deleted.

In TCAC, when a vehicle inserts the anonymiser's area, it gets a pseudonym and when a vehicle broadcasts location related data, the anonymiser choose $k-1$ more nearby vehicles, based on the vehicle's reputation, to perform the location cloak and preserve the privacy of the broadcaster. If the anonymiser finds that the broadcast is made outside of his area, it flags the transmission as false and lowers the vehicle's reputation; in contrast, when the transmission is legit it increases the reputation of the vehicle. Additionally, if a region is populated by one anonymiser, it can be easy for an attacker to find the vehicle's location; for that reason more than two anonymisers must overlap each other's region in order to form a region-cross cloaking area. Finally, the authors have contacted a python simulation between their scheme and a traditional cloaking area construction system and their proposal performed better in detection of dishonest vehicles and false alarms.

Chaudhary and Singh [48] proposed a location and identity privacy scheme for VANET called BELP. The proposed system consists of a Registered Authority (RA), the users (vehicles) and RSUs. When a vehicle enters an RSU territory, it sends a join request to the nearest RA and RSU. RA is responsible to determine if the vehicle is eligible to join the network, using smart contract pre-made rules. If the vehicle is qualified by the rules, RA index the vehicle with a pseudonym. All the data will be registered into the federated blockchain by all RAs. Vehicles that participate in the network can exchange information using their pseudonyms. To preserve the location privacy and to avoid traceability, at any time a vehicle can change its pseudonym using random encryption period. When a pseudonym change occurs, it is mandatory that the vehicles are not less that two and the vehicle should change its speed and direction. Simulation in OPNET indicates that the proposed system preserves the identity and location privacy efficiently.

6.3. Data Exchange

There have been several research works which aimed to provide efficient data exchange, while ensuring privacy between users and between users and infrastructure in IoV, and they are presented below.

Shi et al. [49] proposed a scheme that focused in multimedia data sharing and threat management in vehicular system using blockchain. In this model, the participants involved are electric vehicles (EV) and their users, Roadside Units (RSUs), Trust Authority (TA) and a permisionless blockchain based on Ethereum. At the time of system initialisation, the Trust Authority identifies the entities involved and distributes their keys. The registration takes place as described: Vehicles' users or RSUs send their personal identities to the TA which generates a unique identity for each of them by performing a pseudo-random function and also a key pair by using a key generation algorithm. Furthermore, a hash chain is generated for each participant in order to be used in multimedia sharing authentication phase. Afterwards, the association relationship between each participant's (users and RSUs) identity and his public key is published to blockchain by the TA which also saves the connection between the users and their vehicles locally. Afterwards, TA stays offline, thus it does not have any influence to the decentralisation of blockchain. RSUs are considered as the full nodes which record on the blockchain registration and communication data among the vehicular system. Each entity that wants to share data firstly connects with the nearest RSU through his hash chain and afterwards calculates the hash value of the multimedia data, records the timestamp and signs those data which are then sent to the RSU. The RSU is responsible for verifying those data and updating the blockchain with the new transactions. Finally, a connection between the RSU and the receiver of the data is established, in order to send the shared data to him.

During multimedia data sharing, users use pseudonyms to communicate with each other. The association between each entity's pseudonym (ID) and its personal data is known only by TA. The real identity of the participants and their sharing information is hidden through cryptographical primitives, so attackers cannot gain personal information and communication data. Furthermore, because every entity must be registered by the TA, unauthorised users who do not own keys and pseudonyms cannot communicate with others. In addition, malicious users trying to share illegal data are tracked and punished by TA. Therefore, the anonymous environment prevents the privacy of involved users, helps tracing malicious behaviour and also ensures the integrity and reliability of shared data. The blockchain adopted to test system's performance is Ethereum and according to the evaluation results the integrity of data is efficiently ensured while also protecting the privacy of the users involved.

A cognitive engine can be added to improve the intelligence of traditional IoV. In addition, technologies like artificial intelligence and cloud/edge computing can be used to create an intelligent vehicular system. Therefore, Cognitive Internet of Vehicles (CIoV) have been developed to upgrade intelligence, security and safety of vehicular system by mining significant information from the network and from the environment [51,64]. Experiments have been conducted on Ethereum chain to evaluate the system's performance and prove that the proposed scheme achieves privacy protection.

Lu et al. [50] proposed a scenario of using a hybrid blockchain architecture named PermiDAG, which is based on federated learning, in order to ensure data transmission in IoV. In the asynchronous learning proposed, the aggregation slot is divided into local and global aggregations. Vehicles run the local Directed Acyclic Graph (DAG) for local training and shared update models in federated learning while RSUs maintain the main permissioned blockchain for global aggregation. DAG is updated asynchronously by vehicles and is periodically synchronised to the main blockchain. Two types of transactions are recorded to the main blockchain: data sharing between vehicles and the summary of transactions in DAG. In order to ensure the quality and integrity of shared information, verification is carried out in two stages, firstly by vehicles involved in local DAG and afterwards by RSUs in the main blockchain. Deep Reinforcement Learning (DRL) and Deep Deterministic Policy Gradient (DDPG) algorithms are used to select vehicles with most resources, which act as verifiers in blockchain network. The consensus algorithm used in blockchain is Delegated-Proof-of-Stake (DPoS). Blockchain and federated learning are used to protect the vehicles' privacy and to utilise the limited resources. Through evaluation of the model's performance and comparison with other two baseline methods, the authors have proved that the proposed model is accurate and efficient.

Qian et al. [51] proposed a privacy-aware content caching architecture in CIoV based on blockchain technology. This model is separated into three layers: the first one is the vehicles, which have several sensors to collect data and upload them to the cloud. The second layer is the RSUs, which cover different geographical areas and provide data to nearby vehicles. The third layer is remote-cloud-based providers and cognitive engines which can perceive and analyse vehicles' needs so that content is provided according to vehicles' needs. Deep learning and machine learning algorithms are used to improve the procedures of analysing and perceiving the vehicles' needs. The vehicles and RSUs willing to provide contents cache the contents and then broadcast them along with the specific download time according to the needs of other vehicles. Surrounding vehicles download those contents that match to their needs via V2V or V2R communication. Thus, vehicles do not submit their content requirements when they need information, but they download the content most suitable to their needs. Therefore, no personal information is uploaded and thus the privacy of vehicles is protected. Vehicles can serve as a content provider or content receiver and can also change their role at any time. As content receivers they must pay a fee to receive contents. Experimental results have shown that the proposed scheme has high cache rate and robustness but the type of blockchain is not mentioned.

Vehicles' privacy is protected, because they do not need to submit requests with their own privacy information and content requirements to RSUs when willing to receive data. In addition, because vehicles and RSUs do not trust each other, blockchain technology is used in order to protect the security and privacy of involved vehicles. Completed contents sharing are recorded as transactions by RSU and cognitive engine. RSU generates the new block which records the latest content transactions and then broadcasts those transactions to other RSUs which confirm the transactions ensuring their safety and immutability. The main characteristics of this architecture are more intelligent content requirement analysis and secure and flexible content access in shorter response time.

Zhaofeg et al. [52] proposed a data sharing scheme in IoV driven by blockchain technology called IoVChain. The system consists of two entities: the RSUs and the vehicles. The RSUs maintain a consortium blockchain and can host public or private data exchanged between the vehicles. Public data can be the weather or road conditions and private data could be vehicle's speed or location. The vehicles can register to the network by the RSUs, invoking a smart contract and checking the vehicles key card that holds its real information, acting as a pseudo ID. IoVChain is based on permissioned Hyperledger Fabric and take advantage of Fabric's technology called channels. Only members of a channel can read and write on the channel's ledger. Users can join multiple channels. Simulating the system points out that zero knowledge protocol and homomorphic encryption combined with Fabric's channels can preserve user's privacy.

Joshi et al. [13] proposed a data transmission system for VANET called ROAC-B, with all data registered on a permissionless blockchain and the vehicles forming clusters. The proposal is using clustering to protect the privacy of the vehicle's data transmission. The cluster is formed using the rainfall optimisation algorithm (ROA) and based on various characteristics such as the vehicle's speed and position. The proposed scheme has been simulated in NS-2 and SUMO proving that the ROAC-B technique is better that others.

Liu et al. [53] proposed CPHAS, a heterogeneous aggregate signcryption between Certificateless Cryptosystem (CLC) and Public Key Infrastructure (PKI), and based on that, a protocol for traffic data sharing that uses cloud storage. During system initialisation, Transportation Management Centre (TMC) generates real identity RID and password PWD of each vehicle and store RID and PWD in vehicle's On-Board Unit (OBU). A tamper-resistant device is responsible for checking if a vehicle's RID and PWD are valid in order to generate a pseudonym for that with limited validity time. Afterwards, the vehicle validates its pseudonym and calculates its public and private keys. Likewise, RSUs generate their public and private keys which are sent to TMC for validation. A vehicle can upload data, only after a cloud server confirm its validity. After the verification, a signcryption ciphertext is created by the vehicle and then is sent to the nearest RSU which collects all ciphertexts, verifies their validity and transmit them to the cloud server, which saves those data in the database, in case of a valid signature. Then, the storage address of data is encrypted by the cloud server and is sent to the vehicle through the RSU. Furthermore, a metadata index created by the vehicle is sent to the nearest RSU which accumulates all messages in a set and transmits it into the network, where a block is generated and added to the permissionless blockchain. During data sharing, if the requester belongs to the access control list of the vehicle, he sends a request to the blockchain and then, the data storage address is encrypted and returned by the smart contract. Afterwards, this address is sent to the cloud server which returns the ciphertext, if all the required conditions are met, to the requester who can decrypt it. Meanwhile, a block representing the data sharing process is generated and added to the blockchain. On the other hand, if the requester does not belong to vehicle's access control list, he must pay an amount of money as reward to the vehicle. After a period of time, if the identity of the applicant is recorded in the list, the money is transferred to the owner's account; otherwise, it is returned to the original account. If the vehicle is willing to share data for a long period of time, the ciphertext is updated by cloud server and a new smart contract is applied. After receiving traffic data, the money is transferred to the appropriate vehicle's account. Whether a vehicle no longer wishes to share information, a transaction is written in blockchain and vehicle can redeem its money. Two lists of malicious vehicles are maintained by RSUs: a warning list holding information for illegal vehicles and revocation list for vehicles that have violated the law several times which are excluded from any transaction. The authors claim that vehicle's privacy is protected because pseudonyms are used in all procedures of data sharing and communication with blockchain, thus the true identity of vehicles is kept hidden from third parties. Simulation confirmed that their proposed protocol can reduce time and computational consumption by simulating it in Linux.

BEIoV-EC, proposed by Mei et al. [54], is a blockchain enabled IoV system divided into three layers and it consists of four entities. A Trust Authority (TA) is responsible to register Vehicles (users) with a unique VIN code. This code is the vehicle's one-time multiple pseudonym to protect its real identity, allowing it to participate in the network and enjoy its benefits. Moreover, to boost privacy, nearby vehicles will form a cluster and a cluster leader will be selected dynamically by smart contract and identity-based aggregate signature. The cluster leader will take the role of proxy between the cluster and the RSUs scattered across the road. Similar, to vehicle clusters, RSUs will form their cluster named Edge Services Cluster (ESC) where the permissioned blockchains are deployed; these clusters are providing computing power and temporary storage capabilities to vehicles. The ESCs are manageable by TA via a cloud server in the cloud layer. In the vehicular layer, vehicles will exchange information between them and the RSUs; all transmissions will be stored in RSU blockchain in the edge layer. Finally, TA will keep a reputation system of the vehicles and has the ability to track the real identity of malicious vehicles. Based on simulation experiments, the authors simulate their proposal on OMNet++ and prove that it meets security requirements and is a feasible solution in IoV.

6.4. Dynamic Navigation

The following research works aim to provide dynamic navigation services in IoV and also to ensure the privacy of participants.

Decoster et al. [55] presented HACIT, a system for traffic avoidance and dynamic navigation in VANET, which also can securely store data from vehicles and traffic. The proposed system uses permissioned Hyperledger Fabric as the blockchain technology and takes advantage of the chaincode (Hyperledger Fabric's smart contract) used as pseudonym in combination with blockchain cryptomaterial, to preserve user's and data privacy. HACIT is using a well-known technology to achieve all of the above. Firstly, a Raspberry Pi 3 model B is installed in each vehicle. The bipolar antennas of Raspberry Pi enable ad-hoc network capabilities and vehicles can communicate with each other or can be connected to the Internet. Raspberry Pi uses the GRCBox framework for the wireless communications.

Every vehicle calculates the shortest path of a weighted graph, using the Dijkstra algorithm and stores it in a database alongside with other useful data such as the average speed, the road ID and timestamp. The concept is that, when a vehicle joins a network, it transmits the database to any other node. The information that is stored in the database can help other vehicles to determine traffic and reroute course to avoid a dense one. All the above data for security and privacy are stored in a blockchain network which uses asymmetric encryption. Especially, HACIT is using the Hyperledger Fabric framework as blockchain technology, taking advantage of the unique techniques, such as chaincode (smart contract), and no use of Proof-of-Work, which make the transactions fast and secure. Vehicles are using two Wi-Fi interfaces for network and internet communication. They store a weight graph which represents the roads and calculates the shortest path by using the Dijkstra algorithm. The graph is also used for rerouting process. All data are stored in local database and transmitted to all nodes when the vehicle connects to the network. To avoid network overload during dense traffic the system uses the 1-hop broadcasting scheme. Authors did not provide any evaluation methods and supported their privacy preserving methods in python simulation.

HACIT2 [56] is an improved version of HACIT [55]. It keeps the same basic infrastructure with some differences. As its predecessor, it uses a Raspberry Pi for the communication and the Hyperledger Fabric as the blockchain technology to maintain the privacy. The basic difference from the prototype is the distinction of the traffic congestion detector client and dynamic navigation rerouting server. The first module is in charge of detecting traffic jam and logs the speed changes to the distributed ledger. The second module listens to the ledger changers and takes advantage of the information to recalculate the route based on the given data. The vehicle needs an android device and app in order to run and maintain the Hyperledger Fabric network. Moreover, a connection to the internet is a prerequisite. Through the app, the nodes exchange traffic messages and every vehicle reroutes based on shared information. The authors did not refer to any evaluation method but they supported their privacy-preserving aspect to Hyperledger Fabric's Zero Knowledge technology.

Mapping plays a significant role in many vehicular services such as location, navigation and transportation. Digital maps designed for that purpose are mainly based on satellite images and do not represent latest map information. In contrast, vehicle maps must be continually updated so that they effectively represent the traffic situation and navigation on vehicular networks which are constantly changing. Lai et al. [57] proposed a scheme, called SPIR, which was designed to solve this problem. The authors tried to figure out a secure and privacy-preserving solution for real-time maps updates by using permissioned blockchain. The proposed scheme achieves payment control for map service platform (MPS) and also assures completion quality for vehicle users so that benefits of MPS can be maximised. The main entities of SPIR are the certification authority (CA), the pseudonym CA (PCA), the map service platform (MPS), the trace manager (TM) and vehicle users. In this suggested model, when MSP is interested in information relevant to road conditions, it publishes the type of needed data. Then, vehicle users bid to provide the required data that fulfils MPS's requirements. Afterwards, the MSP defines a winner according to its budget and vehicle user's quotation and this winner provides the exchange data with a reward. Blockchain technology is used to support the payment system so that it is safe and secure.

In SPIR, the privacy of vehicle users is protected, as pseudonyms are used to provide anonymity and to protect the identity of users while communicating with MSP. CAs verify users' identities and sign pseudonyms submitted by them, while not knowing the content of signed pseudonyms due to adoption of the randomised RSA-based partially blind signature technique. In addition, PCA is not aware of the real identity of vehicle users but verifies the validity of the signature of their pseudonyms. Furthermore, TM which does not participate in the processes of signature publication and verification, can trace malicious users, find the real identity from their pseudonyms and inform CA which sustain a credit account for each user to record his real identity and credit value. The use of blockchain prevents malicious behaviours, as it assists in subtracting credits from malicious vehicles and informing CA via blockchain for recent changes. In their next attempt to register, CA after checking their account refuses their registration, and thus, the system is safe. Moreover, fake pseudonyms and certificates, not related to any vehicle user's identity, cannot tamper with the real users' identity if CA is attacked. Lastly, vehicle users can change their pseudonyms whenever they want, without making it easy for others to predict the next pseudonym change. Results of theoretical analysis and simulations in Matlab and PEPA have shown that SPIR guarantees the security and reliability of data in real-time map updates without leaking of private information and also that vehicles and MSPs will effectively receive fair rewards or budgets.

6.5. Vehicle Reputation Services

The following research works aim to provide trust and reputation in vehicular networks and at the same time to maintain privacy.

The Blockchain-based anonymous reputation system (BARS) [58], as the name implies, is a proposed message broadcast system for VANET. The main entities of the system are the vehicles which basically are the users, the Law Enforcement Authority (LEA), which is in charge of the vehicle registration, the behaviour and evaluation of the scores and the RSU, which are responsible for message transmission and for blockchain records too. There are three prerequisites for BARS to work efficiently. Firstly, the cryptographic material must be secure as public keys act as a pseudonym. Secondly, LEA can securely keep the dataset. Thirdly, the authority and RSU have all the appropriate computer power and there is no possibility of half of the users being compromised. BARS consists of three permissionless blockchains, blockchain for messages (MesBC) where the messages are stored, blockchain for certificate (CerBC) where all the certificates are stored and blockchain for revoked public keys (RevBC) where all the revoked public keys are stored, and it acts and as Proof-of-Absence too. The basic idea of BARS is that every vehicle/user can transmit three types of messages: (1) when it loses control, (2) when it alerts nearby vehicles before changing its driving status and (3) when poor road conditions are detected. When a message is broadcasted, LEA is responsible to evaluate the message. If the message is authentic the reputation score of the user transmitted increases and when a false message is detected, the reputation score of the user decreases. The messages have weights, thus more important messages give more reputation score and in contrary messages with very negative effect decrease reputation score. Finally, an informal security analysis is provided and the proposed system was tested in a Python environment to evaluate its performance.

Ma et al. [1] proposed a privacy-preserving reputation-based blockchain system in VANETs. This solution uses two-layer blockchain, permissioned intrachain and permissionless interchain. Intrachain is installed inside the vehicle including sensors, actuators, smartphones, etc. This private blockchain network, due to the sensitive data that it includes, must use cryptographic algorithms for the communications. For that reason, the central manager of the vehicle will store the data into the blockchain according to vehicle owner. Interchain is a public ledger that includes the vehicle and the RSU for their communication between each other and between infrastructure. Every vehicle can request or provide data to the ledger in order to prevent accidents or to inform for traffic jams. Additionally, it adopts a hierarchical structure in order to provide flexible control and to optimise resource consumption. The network consists of RSUs, where the blockchain is stored. They act as full nodes and they are responsible for block generation and reputation consensus. Moreover, they monitor the traffic conditions and supervise the vehicles. The vehicles are basically the users, which are responsible to interact with RSUs and other vehicles, exchanging messages relative to road conditions. Based on these messages they gain or lose reputation. Sensors and actuators gather all the necessary information for the vehicles. Lastly, Cloud server also participates in the network, whose main purpose is to backup the blockchain data.

To ensure the stability and availability of the system, a novel consensus protocol is proposed based on Delegated-Proof-of-Stake (DPoS), for better management of the reputation and the avoidance of malicious vehicles. Finally, the evaluation of the system proves the security of the framework. Evaluation has been made by observing malicious nodes in three scenarios. The observations of results of no reputation system, random rating reputation system and the proposed system using Matlab simulation show that the proposed system can guarantee the accuracy, security and privacy preservation of the framework.

Malik et al. [59] proposed a reputation system that uses permissioned blockchain technology. It consists of three phases: (1) Registration of the vehicle: uses Proof-of-Authority consensus algorithm to add the vehicle into the blockchain with pseudonym. (2) Reputation evaluation: where the reputed nodes verify the vehicle's messages and store a local copy of them. (3) Reputation update and query: the reputation algorithm is used to choose the nearest most reputed nodes in order to validate the requested vehicle. The entities that participate in the network are motor vehicle division (MVD), Law enforcement authority (LEA), light IPFS vehicles (LIV), Reputable IPFS vehicles (RIV) and edge nodes (RSU). MVD is a vehicle with valid Electronic license plate number (ELP), while Law enforcement authority provides the blockchain platform and the reputation management and runs the smart contracts to ensure traceability and avoid malicious nodes. Light IPFS vehicles are regular vehicles with the difference that they do not have accessibility to the ledger but they can query other nodes. Reputable IPFS vehicles have verified and proven functionality through honest message delivery and gain reputation as being trusted across the network. RSUs act as miners as they have the computation power, they mine and they validate transactions.

The data structure of the network consists of: (i) Registration smart contract: it is triggered in order to add validated and authorised users to the registration and authentication ledger. That includes adding new users or update old entries. The transactions are verified by the MVD and LEA. (ii) Reputation smart contract: LIVs can run these contracts to put their reputation scores in their respective IPFS objects. (iii) The Repuchain: a private ledger for vehicle management, running Proof-of-Authority and Proof-of-Reputations consensus algorithms. (iv) Off-chain event information storage: it stores details of informing and emergency event information about the vehicles. (v) Reputation review storage: it stores the reviews of vehicles in order to use them as evaluation of the final rating. (vi) RepuWallet: it represents the users' wallet, where the public/private key, reputation scores and reward points are stored.

Running the network, there are two assumptions. Firstly, The LEA and MVD are trusted parties and RSUs are the demarcation point for different networks. Secondly, RIVs are vehicles with high reputation score, so the can ensure the trust and transparency among the other vehicles. In the Repuchain, there are two types of messages that are broadcasted, (1) regular messages, such as a bad driving behaviour, and (2) emergency messages, such as messages that warn other vehicles for a possible accident. The messages are collected by the nearby vehicles and transmitted over the network for evaluation. The evaluation criteria are the vehicle's location details retrieved from RSU and querying nearby vehicles for reputation and if similar message has been transmitted. As the evaluation is successful, reputation points are gained and stored in user's wallet. Security evaluation, made by theoretical proofs and testing on four vehicles, for over 90 h, using Matlab simulation have shown that the reputation increased for trust entities and decreased reputation for entities broadcasting fake messages, but it does not enhance privacy in any aspect.

6.6. General Services

Here are two general solutions that promise to provide privacy protection in blockchain-enabled IoV.

Hui Li et al. [3] proposed a general decentralised architecture for VANET aiming to protect identity and location privacy. The system is starting with the initialisation of the blockchain network, where the edge nodes, which are the nodes that run the smart contracts and participate in the consensus, are equal and enjoy the same rights and obligations. Then, the registration process occurs where a Certification Authority server, through smart contracts, validates a vehicle into the blockchain network. If the validation fails, the details are recorded in a block and broadcasted to the network, so that all participants are warned.

To protect the identity and the location of vehicles during message broadcasting, the proposed system adopts the k-anonymity unity. When a vehicle is ready to transmit a message, with the help of an RSU it forms a group with the nearby vehicles, then selects other $k-1$ sub-identities including his own and all the messages are uploaded together, so the server of the core network cannot identify the location and the identity of the vehicle. Every message is considered as a transaction and recorded in the blockchain network. After the transmission of the message, the agent broadcasts the block to all nodes and using practical byzantine fault tolerance as consensus algorithm, the transactions are validated. The validated blocks are stored on every node. To be protected against any thread, this system uses undirected graph generation algorithm for privacy protection of the vehicles, a way of dynamic threshold encryption to protect the vehicular identity and the k-anonymity unity to protect location privacy. The security evaluation performed in simulation environment using OPNET and Ethereum. As a result of the evaluation, the proposed system seems to be faster than the commodity blockchain solutions and the location privacy greatly improved.

Yuhong Li et al. [60] proposed an intelligent transportation system, called Ba-ITS, based on permissioned Blockchain technology that aims to provide different vehicular services. The proposed structure consists of three layers called ITS network infrastructure layer, cloud computing and service provisioning layer and blockchain overlay layer. Aiming to concentrate only in data of a certain area, three layers of private hierarchical blockchains are used, called vehicle-chain (V-chain), RSU-chain (R-chain) and gateway-chain.

Vehicle-chain consists of vehicles and RSUs in order to upload or obtain data and services. RSU-chain consists of RSUs and the gateway in which they are connected and its purpose is to synchronise data from different vehicle-chains. The gateway-chain aims to ensure data exchange among different gateways and has the highest priority in the network as it maintains all data. The main components of gateway-chain are a gateway, server nodes and a router. Some nodes participate in several chains in order to synchronise data between them. When exchanging data, vehicles collect data using sensors and upload them to the system in order to inform other vehicles for road conditions, and as a reward they gain some points which they can use in the future to request data or services. In services such as route planning, in contrast with traditional navigation services where location information of vehicles are collected and stored, in this proposed model, root is performed by a smart contract. Therefore, private information of users are protected. In addition, data exchanges involve only blockchain address of vehicles, thus no personal data is provided. Moreover, smart contract and transactions support data exchanging and other services, ensuring that privacy is better protected. Furthermore, the privacy is implemented by using private chains with access control and by encrypting the data stored in V-chain. The authors implemented their model using Ethereum Blockchain. They also used Ganache to generate participants' accounts, Truffle to develop the application which connects drivers with blockchain, Solidity to implement the smart contracts and JSON-RPC API and Web3 library to interact with blockchain. OSM and SUMO have also been used to simulate data transmission and route planning in the proposed system. From the simulation results, the authors ensure the feasibility of the proposed model claiming that the estimated response time is satisfying and that the most time is spent to add data to the ledger.

Wang et al. [61] proposed an IoV block-streaming service awareness and trusted verification scheme in 6G. As wireless technology advances and offers high bandwidth and low latency with the forthcoming 6G [65], it opens up opportunities for more services to be available in IoV, such as short videos and online games. Despite this, there are devices that have limited storage capability. To this end, the authors proposed a scheme where the offered services are divided into microservices (or blocks) [66] and only the requested block will be streamed to users, thus saving storage space and bandwidth, as it does not require downloading the entire service. The proposed scheme is divided into three layers: the central cloud layer, the edge layer and the terminal layer. In the central cloud layer, there are high-performance, super storage-capable servers that are responsible for large-scale computing and mass data storage. In the edge layer, there are roadside units and base stations that are scattered in various locations. At this layer the blockchain is deployed and is the interface between the cloud servers and the users, where the users form the terminal layer. The proposed scheme is based on Hyperledger Fabric with Proof-of-Authority (PoA) consensus. Each edge server has to submit a registration request for authorisation in order to join the network. To protect the privacy of the participants, the proposed scheme uses a suite of encryption protocols in Hyperledger Fabric, called Identity Mixer, which provides anonymity and unlinkability using zero-knowledge proofs. Additionally, the divided service function blocks as well as the service call graphs are stored in the blockchain by the service provider. All interaction between edge servers and users is recorded in the blockchain utilising its non-tampering and traceability characteristics. Users do not reveal their identity by requesting a service from providers applying the technique of blind signatures. After the request, the edger server verifies the rationality of the microservice using the blockchain network. Moreover, users can verify that the requested microservice is legitimate by comparing the service hash with the hash stored in the blockchain. In addition, to improve the cache hit rate, the proposed scheme uses an edge cache replacement mechanism (ECRM). The proposed scheme is theoretically analysed using an informal security analysis and tested in Hyperledger Fabric; the data traffic performance has been simulated in Matlab.

6.7. Advertising

The evolution of vehicular system contributed to the development of various relevant services such as entertainment, advertising and online shopping. Advertisement dissemination in VANETs is a service which is considered very popular for the effective promotion of products and is discussed in the following privacy-preserving solution.

Ming Li et al. [62] proposed a blockchain-based advertisement dissemination framework. In this proposed scheme, a register authority is responsible for users' identification with a single certification and key generation, while vehicles' private key is generated by two parts, one part by their-selves and another by RSUs. After their registration, advertisers promote their ads to one or more RSUs which fulfil their requirements and provide rewards depending on the number of vehicles receiving the ad. When a vehicle receives an advertisement, it returns a response with a signature to the sender or forward it to nearby vehicles with economic motivation. A smart contract is used to ensure the fairness and honesty of the advertisement dissemination and to ensure the predefined reward. Vehicles generate anonymous credentials with zero-knowledge proof of knowledge techniques to prove the validity of the dissemination without revealing any private information. Receivers of ads send a transaction to the permissioned blockchain, proving that they have broadcast the advertisement in order to receive the predefined reward by the smart contract. For that purpose, a secure wallet is used by users to manage coins which act as rewards and also to connect to blockchain. RSUs sustain the blockchain and verify the validation of blocks. In addition, RSUs communicate with vehicles and broadcast advertisements.

The privacy of advertisers is not considered as they want to communicate their products and services. In contrast, vehicles' privacy is protected, as they use anonymous credentials signed by blinded signature based on zero-knowledge proof of knowledge (ZKPoK) which protect them from malicious users who might want to learn their real identity. Even RSUs and Register authority cannot identify their real identity. In addition, vehicles can change their blockchain address whenever they want, so their position and direction cannot be traced by the information stored in the blockchain by different ads. The authors used VANETsim platform, Parity permissioned Ethereum blockchain and the programming languages Java and Solidity to simulate their scheme. In addition, Proof-of-Authority (PoA) consensus protocol was adopted. The experimental results and security analysis have shown that this model can work properly and efficiently.

7. Discussion and Open Issues

By studying the above papers, it is observed that most of the proposed schemes in IoV use permissioned blockchain frameworks instead of permissionless (Figure 7). In these authorised environments, data tampering and partial pseudonymity seem to be more important, because it is easier to detect malicious users due to some kind of authority presence, than in a complete permissionless system. Additionally, it is important to highlight that two proposed schemes [1,60] are using access control to enrol their users, providing even more control of participants in the blockchain network.

With regards to privacy mechanisms, various techniques have been used to protect the involved users and the aggregated data. More specifically, the purpose of the above techniques was to protect either location privacy, identity privacy of involved parties and data exchange. In most papers, it seems that identity privacy is achieved mainly through the use of pseudonyms during communication (e.g., [37,38]), cloaking/clustering areas for location privacy (e.g., [40,47]) and homomorphic encryption to ensure data privacy [34,52]. However, in some papers, some other more advanced techniques, such as zero knowledge proofs (e.g., [39,45]), ring signatures [33,41], blind signatures [57,61], and group signatures [42] are also used to ensure privacy. It is significant here to point out some unique techniques proposed to preserve privacy, such as federating learning [50].

However, as a whole, none of these proposed solutions has been tested in real conditions and their privacy preserving aspect remains in theory (e.g., [33,36]) or in simulation (e.g., [13,48]), and only four of them are in a proof of concept stage [40,52,60,61].

Given the above, technologies that are used in IoV, can only run in limited hardware and must have the minimum energy consumption, while the proposed consensus protocols, the energy efficiency and performance must be tested thoroughly and in scale. Moreover, blockchain is a technology that can surely protect from data alteration but cannot guarantee privacy preservation. An equally important issue is how all these technologies can be integrated to an existing infrastructure and estimate the cost of integration, as many of the proposed schemes do not address any hardware or software requirements. Based on these characteristics, limitations and requirements of the Privacy-Enhancing Technologies (PETs) need to be optimised.

8. Conclusions

Internet of Vehicles (IoV), with its unique characteristics, is an emerging technology and a promising research area. Moreover, blockchain is a well-known technology with applications in IoV; however, it does not have any built-in privacy mechanisms that are very important to the vehicle ecosystem. In this review paper, we looked at the literature on technologies that have tried to solve several privacy issues using blockchain in IoV. For that reason, we classified, compared and presented the schemes that have been used to provide privacy and we categorised the areas in which these approaches and techniques can be used.

The provided classification and the discussion on the identified solutions demonstrate that well-established privacy-preserving techniques should be, and are already being, considered in blockchain-enabled IoV ecosystem to address privacy concerns. Pseudonymisation is the most prominent privacy enhancing technology used in IoV, especially for providing authentication services with permissioned and permissionless infrastructures. Although, the majority of the proposed solutions focus on identity privacy, with only a small subset considering location privacy; they span a variety of services in IoV, clearly demonstrating that blockchains can be efficiently combined with privacy enhancing technologies, to provide privacy-preserving services in IoV, such as authentication, traffic conditions, data exchange, dynamic navigation and reputation management. Finally, as it has already been demonstrated, the majority of the proposed solutions only provide an informal security analysis, which can be considered as a weakness for the soundness of the solutions.

Author Contributions: Conceptualisation, G.D. and K.R.; methodology, G.D. and K.R.; validation, K.K., G.D. and K.R.; formal analysis, K.K. and G.D.; investigation, K.K., P.P., G.D. and K.R.; data curation, G.D.; writing—original draft preparation, K.K. and P.P.; writing—review and editing, G.D. and K.R.; visualisation, K.K.; supervision, G.D. and K.R. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by the MPhil program "Advanced Technologies in Informatics and Computers", hosted by the Department of Computer Science, International Hellenic University, Kavala, Greece.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the MPhil program "Advanced Technologies in Informatics and Computers", Department of Computer Science, International Hellenic University, for facilitating this research study.

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

References

1. Ma, X.; Ge, C.; Liu, Z. Blockchain-Enabled Privacy-Preserving Internet of Vehicles: Decentralized and Reputation-Based Network Architecture. In Proceedings of the International Conference on Network and System Security, Sapporo, Japan, 15–18 December 2019; Volume 11928, pp. 336–351.[CrossRef]
2. Sadiku, M.; Tembely, M.; Musa, S. Internet of Vehicles: An Introduction. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2018**, *8*, 11. [CrossRef]
3. Li, H.; Pei, L.; Liao, D.; Sun, G.; Xu, D. Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET. *Peer- Netw. Appl.* **2019**, *12*, 1178–1193. [CrossRef]
4. Sharma, S.; Kaushik, B. A survey on internet of vehicles: Applications, security issues & solutions. *Veh. Commun.* **2019**, *20*, 100182. [CrossRef]
5. Gaur, N.; Desrosiers, L.; Ramakrishna, V.; Novotny, P.; Baset, S.A.; O'Dowd, A. *Hands-On Blockchain With Hyperledger*, 1st ed.; Packt: Birmingham, UK, 2018.
6. Swan, M. *Blockchain Blueprint For A New Economy*, 1st ed.; O'Reilly: Newton, MA, USA, 2015.
7. Singhal, B.; Dhameja, G.; Panda, P.S. *Beginning Blockchain*, 1st ed.; Apress: New York, NY, USA, 2018.
8. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *Blockchain Technology Overview*; Technical Report NIST IR 8202; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018. [CrossRef]
9. Kalaiarasy, C.; Sreenath, N.; Amuthan, A. Location Privacy Preservation in VANET using Mix Zones—A survey. In Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2019; pp. 1–5.
10. Christen, M.; Gordijn, B.; Loi, M. (Eds.) The Ethics of Cybersecurity. In *The International Library of Ethics, Law and Technology*; Springer International Publishing: Cham, Switzerland, 2020; Volume 21. [CrossRef]
11. Danezis, G.; Domingo-Ferrer, J.; Hansen, M.; Hoepman, J.H.; Metayer, D.L.; Tirtea, R.; Schiffner, S. *Privacy and Data Protection by Design—From Policy to Engineering*; European Union Agency for Network and Information Security (ENISA): Athens, Greece, 2014. [CrossRef]
12. Hu, P.; Wang, Y.; Gong, B.; Wang, Y.; Li, Y.; Zhao, R.; Li, H.; Li, B. A secure and lightweight privacy-preserving data aggregation scheme for internet of vehicles. *Peer-Netw. Appl.* **2020**, *13*, 1002–1013. [CrossRef]
13. Joshi, G.P.; Perumal, E.; Shankar, K.; Tariq, U.; Ahmad, T.; Ibrahim, A. Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. *Electronics* **2020**, *9*, 1358. [CrossRef]
14. Garg, T.; Kagalwalla, N.; Churi, P.; Pawar, A.; Deshmukh, S. A survey on security and privacy issues in IoV. *Int. J. Electr. Comput. Eng. (IJECE)* **2020**, *10*, 5409. [CrossRef]
15. Luckshetty, A.; Dontal, S.; Tangade, S.; Manvi, S.S. A survey: Comparative study of applications, attacks, security and privacy in VANETs. In Proceedings of the 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 6–8 April 2016; pp. 1594–1598.
16. Akalu, R. Privacy, consent and vehicular ad hoc networks (VANETs). *Comput. Law Secur. Rev.* **2018**, *34*, 37–46. [CrossRef]
17. Sağlam, E.T.; Bahtiyar, Ş. A Survey: Security and Privacy in 5G Vehicular Networks. In Proceedings of the 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 108–112. [CrossRef]

18. Kaibalina, N.; Rizvi, A.E.M. Security and Privacy in VANETs. In Proceedings of the 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), Almaty, Kazakhstan, 17–19 October 2018; pp. 1–6.
19. Mathew, D.; Roy, H. A survey on different privacy-preserving authentication schemes in VANET. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *396*, 012033. [CrossRef]
20. Lu, Z.; Qu, G.; Liu, Z. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 760–776. [CrossRef]
21. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [CrossRef]
22. Talat, H.; Nomani, T.; Mohsin, M.; Sattar, S. A Survey on Location Privacy Techniques Deployed in Vehicular Networks. In Proceedings of the 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 8–12 January 2019; pp. 604–613.
23. Sheikh, M.S.; Liang, J.; Wang, W.; Guerrieri, A. Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 5129620. [CrossRef]
24. Zhao, P.; Zhang, G.; Wan, S.; Liu, G.; Umer, T. A survey of local differential privacy for securing internet of vehicles. *J. Supercomput.* **2020**, *76*, 8391–8412. [CrossRef]
25. Mikavica, B.; Kostić-Ljubisavljević, A. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey. *J. Supercomput.* **2021**, *77*, 9520. [CrossRef]
26. Azam, F.; Yadav, S.K.; Priyadarshi, N.; Padmanaban, S.; Bansal, R.C. A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network. *IEEE Access* **2021**, *9*, 31309–31321. [CrossRef]
27. Mendiboure, L.; Chalouf, M.; Krief, F. Survey on blockchain-based applications in internet of vehicles. *Comput. Electr. Eng.* **2020**, *84*, 106646. [CrossRef]
28. Liu, Y.N.; Lv, S.Z.; Xie, M.; Chen, Z.B.; Wang, P. Dynamic anonymous identity authentication (DAIA) scheme for VANET. *Int. J. Commun. Syst.* **2019**, *32*, 3892. [CrossRef]
29. Sharma, R.; Chakraborty, S. BlockAPP: Using Blockchain for Authentication and Privacy Preservation in IoV. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6. [CrossRef]
30. Bao, S.; Lei, A.; Cruickshank, H.; Sun, Z.; Asuquo, P.; Hathal, W. A Pseudonym Certificate Management Scheme Based on Blockchain for Internet of Vehicles. In Proceedings of the IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 5–8 August 2019; pp. 28–35. [CrossRef]
31. Guehguih, B.; Lu, H. Blockchain-Based Privacy-Preserving Authentication and Message Dissemination Scheme for VANET. In *ICSCC 2019, Proceedings of the 5th International Conference on Systems, Control and Communications, Wuhan, China, 21–23 December 2019*; ACM: New York, NY, USA, 2019; pp. 16–21. [CrossRef]
32. Zheng, D.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs. *IEEE Access* **2019**, *7*, 117716–117726. [CrossRef]
33. Benarous, L.; Kadri, B.; Bouridane, A. Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks. *Arab. J. Sci. Eng.* **2020**, 6033–6049. [CrossRef]
34. Yao, Y.; Chen, W.; Chen, X.; Ding, J.; Pan, S. A Blockchain-based Privacy Preserving Scheme for Vehicular Trust Management Systems. In Proceedings of the 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), Zhenjiang, China, 27–29 November 2020; pp. 1–5. [CrossRef]
35. Su, T.; Shao, S.; Guo, S.; Lei, M. Blockchain-Based Internet of Vehicles Privacy Protection System. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8870438. [CrossRef]
36. Moussaoui, D.; Kadri, B.; Feham, M.; Ammar Bensaber, B. A Distributed Blockchain Based PKI (BCPKI) architecture to enhance privacy in VANET. In Proceedings of the 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH), Boumerdes, Algeria, 9–10 February 2021; pp. 75–79. [CrossRef]
37. George, S.A.; Jaekel, A.; Saini, I. Secure Identity Management Framework for Vehicular Ad-hoc Network using Blockchain. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 1–6. [CrossRef]
38. Lee, J.; Lee, J.; Park, H. A Privacy Preserving Blockchain-based Reward Solution for Vehicular Networks. In Proceedings of the IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 4–6 January 2020; pp. 1–4. [CrossRef]
39. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5760–5772. [CrossRef]
40. Akhter, A.F.M.S.; Ahmed, M.; Shah, A.F.M.S.; Anwar, A.; Zengin, A. A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET. *Sustainability* **2021**, *13*, 400. [CrossRef]
41. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2204–2220. [CrossRef]
42. Bai, H.; Wu, C.; Yang, Y.; Xia, G.; Jiang, Y. A Blockchain-Based Traffic Conditions and Driving Behaviors Warning Scheme in the Internet of Vehicles. In Proceedings of the IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 16–19 October 2019; pp. 1160–1164. [CrossRef]

43. Cheng, L.; Liu, J.; Xu, G.; Zhang, Z.; Wang, H.; Dai, H.N.; Wu, Y.; Wang, W. SCTSC: A Semicentralized Traffic Signal Control Mode with Attribute-Based Blockchain in IoVs. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1373–1385. [CrossRef]
44. Wang, W.; Wu, L.; Qu, W.; Liu, Z.; Wang, H. Privacy-preserving cloud-fog–based traceable road condition monitoring in VANET. *Int. J. Netw. Manag.* **2020**, 2096. [CrossRef]
45. Li, W.; Guo, H.; Nejad, M.; Shen, C.C. Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. *IEEE Access* **2020**, *8*, 181733–181743. [CrossRef]
46. Li, B.; Liang, R.; Zhu, D.; Chen, W.; Lin, Q. Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3765–3775. [CrossRef]
47. Feng, J.; Wang, Y.; Wang, J.; Ren, F. Blockchain-Based Data Management and Edge-Assisted Trusted Cloaking Area Construction for Location Privacy Protection in Vehicular Networks. *IEEE Internet Things J.* **2021**, *8*, 2087–2101. [CrossRef]
48. Chaudhary, B.; Singh, K. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. *Peer-Peer Netw. Appl.* **2021**, 3198. [CrossRef]
49. Shi, K.; Zhu, L.; Zhang, C.; Xu, L.; Gao, F. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. *Multimed. Tools Appl.* **2020**, *79*, 8085–8105. [CrossRef]
50. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4298–4311. [CrossRef]
51. Qian, Y.; Jiang, Y.; Hu, L.; Hossain, M.; Alrashoud, M.; Al-Hammadi, M. Blockchain-based privacy-aware content caching in cognitive internet of vehicles. *IEEE Netw.* **2020**, *34*, 46–51. [CrossRef]
52. Zhaofeng, M.; Lingyun, W.; Weizhe, Z. Blockchain-Driven Trusted Data Sharing with Privacy-Protection in IoT Sensor Network. *IEEE Sens. J.* **2020**. [CrossRef]
53. Liu, J.; Zhang, G.; Sun, R.; Du, X.; Guizani, M. A Blockchain-based Conditional Privacy-Preserving Traffic Data Sharing in Cloud. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6. [CrossRef]
54. Mei, Q.; Xiong, H.; Zhao, Y.; Yeh, K.H. Toward Blockchain-Enabled IoV with Edge Computing: Efficient and Privacy-Preserving Vehicular Communication and Dynamic Updating. In Proceedings of the 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan, 30 January–2 February 2021; pp. 1–8. [CrossRef]
55. Decoster, K.; Billard, D. HACIT: A Privacy Preserving and Low Cost Solution for Dynamic Navigation and Forensics in VANET. In Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems—Volume 1: VEHITS, INSTICC, Funchal, Madeira, Portugal, 16–18 March 2018; SciTePress: Setubal, Portugal, 2018; pp. 454–461. [CrossRef]
56. Kevin, D.; David, B. HACIT2: A privacy preserving, region based and blockchain application for dynamic navigation and forensics in VANET. In Proceedings of the International Conference on Ad Hoc Networks, Cairns, QLD, Australia, 20–23 September 2018; Volume 258, pp. 225–236. [CrossRef]
57. Lai, C.; Zhang, M.; Cao, J.; Zheng, D. SPIR: A Secure and Privacy-Preserving Incentive Scheme for Reliable Real-Time Map Updates. *IEEE Internet Things J.* **2020**, *7*, 416–428. [CrossRef]
58. Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access* **2018**, *6*, 45655–45664. [CrossRef]
59. Malik, N.; Nanda, P.; He, X.; Liu, R. Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach. In Proceedings of the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 34–41. [CrossRef]
60. Li, Y.; Ouyang, K.; Li, N.; Rahmani, R.; Yang, H.; Pei, Y. A blockchain-assisted intelligent transportation system promoting data services with privacy protection. *Sensors* **2020**, *20*, 2483. [CrossRef]
61. Wang, Y.; Tian, Y.; Hei, X.; Zhu, L.; Ji, W. A Novel IoV Block-Streaming Service Awareness and Trusted Verification Scheme in 6G. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5197–5210. [CrossRef]
62. Li, M.; Weng, J.; Yang, A.; Liu, J.N.; Lin, X. Toward Blockchain-Based Fair and Anonymous Ad Dissemination in Vehicular Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11248–11259. [CrossRef]
63. Sweeney, L. k-Anonymity: A Model for Protecting Privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* **2002**, *10*, 557–570. [CrossRef]
64. Chen, M.; Tian, Y.; Fortino, G.; Zhang, J.; Humar, I. Cognitive Internet of Vehicles. *Comput. Commun.* **2018**, *120*, 58–70. [CrossRef]
65. Tariq, F.; Khandaker, M.R.A.; Wong, K.K.; Imran, M.A.; Bennis, M.; Debbah, M. A Speculative Study on 6G. *IEEE Wirel. Commun.* **2020**, *27*, 118–125. [CrossRef]
66. He, J.; Zhang, Y.; Lu, J.; Wu, M.; Huang, F. Block-Stream as a Service: A More Secure, Nimble, and Dynamically Balanced Cloud Service Model for Ambient Computing. *IEEE Netw.* **2018**, *32*, 126–132. [CrossRef]