WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain-Based Privacy-Preserving for Secure and Efficient Maas Ecosystem in the Context of IoV: A Survey

Timothy Murkomen

Masters in IT Security and Audit, *Email:* timothymurkomen@gmail.com

Department of Computer Science and Software Engineering – School of Informatics and Innovative Systems; Jaramogi Oginga Odinga University of Science and Technology (JOOUST); P.O Box 210-Bondo

ABSTRACT –

The rapid advancement of Mobility-as-a-Service (MaaS) within the transport sector has brought forth critical challenges in safeguarding privacy and ensuring data security for its participants. In response, blockchain technology has emerged as a promising solution, offering a decentralized and tamper-resistant infrastructure. This survey paper aims to present a comprehensive overview of the utilization of blockchain in the transport sector, with a specific focus on MaaS, and explores its potential role in preserving privacy and enhancing security. We delve into the privacy concerns related to data collection, sharing, and storage within MaaS systems, and examine how blockchain can address these issues through its unique characteristics of transparency, immutability, and cryptographic techniques. By conducting an extensive survey, we analyze the existing blockchain-based privacy-preserving mechanisms applied in the transport sector, shedding light on their efficacy, limitations, and potential applications. Through this survey, we aim to provide valuable insights to researchers, practitioners, and policymakers, highlighting the potential of blockchain-based privacy-preserving approaches in constructing secure and efficient MaaS ecosystems within the context of the Internet of Vehicles (IoV). The study emphasizes the significance of blockchain technology in safeguarding the privacy of participants' data and enhancing overall security, paving the way for the future of privacy-conscious and robust MaaS platforms in the dynamic transport sector.

Index Words: Blockchain, Blockchain-based, MaaS, Privacy, Mobility-as-a-Service, Transport-Sector, Security, IoV, Internet of Vehicles.

I. Introduction

In the transport sector, Mobility-as-a-service (MaaS) adoption has rapidly increased and it has revolutionized the entire transport ecosystem. It has changed the way people access and utilize transportation resources. These MaaS platforms provide integrated and most convenient solutions hence allowing people to plan, pay or book any transportation service. However, this widespread adoption has raised many concerns regarding the privacy and security of personal information that is confidential [1]. Some of this confidential information include for example the user identity number, the current location and any other information the user is unwilling to share [1]. Hence, it's very important to focus on security and privacy of user information to prevent any malicious attacks [1].

Blockchain technology has emerged as a promising solution to address this challenge especially within the context of Internet of Vehicles (IoV). IoV is a concept that expands on the idea of Vehicular Ad Hoc Networks (VANETs) [2]. In the IoV, vehicles are well equipped with sensors, devices to communicate and data processing capabilities that enable them to communicate and connect to the internet and exchange information within the ecosystem hence allows the vehicles to access real-time traffic updates, navigation services and or emergency notifications.

Blockchain inherent characteristics such as transparency, immutability, and decentralization [7] makes the best in ensuring privacy-preserving and secure MaaS platforms within the context of IoV. To solve the above problems, the technologies must comply with some legal regulations such as the General Data Protection Regulation (GDPR) [8], security threats [3], scalability [4], or privacy matters [5] – [6], which elaborates more about the confidentiality, anonymity and privacy of user's activities.

The paper examines proposed solutions and provide a comprehensive analysis of blockchain-based privacy-preserving solutions for secure and efficient MaaS ecosystems within the Internet of Vehicles (IoV) in the transport sector. The survey aims to offer valuable insights into the potential applications and benefits of blockchain technology in addressing privacy concerns while ensuring the integrity and efficiency of MaaS platforms.

To achieve this goal, we will start by presenting an overview of blockchain technology and its transformative impact on the transport sector, with a specific focus on MaaS systems. We will examine the fundamental characteristics of blockchain, such as decentralization and immutability, and explore their relevance to privacy preservation within the MaaS ecosystem from the context of IoV.

The survey will further analyze a range of privacy-preserving techniques and mechanisms enabled by blockchain technology within the MaaS ecosystem. These include cryptographic methods like homomorphic encryption, zero-knowledge proofs, and secure multi-party computation, which provide means for data confidentiality, integrity, and privacy-aware computations.

The findings of this survey will contribute to the existing body of knowledge by providing researchers, practitioners, and policymakers with a comprehensive understanding of the state-of-the-art in privacy-preserving blockchain solutions for secure and efficient MaaS in the transport sector. This knowledge will inform the development of robust privacy frameworks and support the advancement of trustworthy and user-centric MaaS platforms that prioritize privacy and data protection.

Organization: The paper is structured as follows: Section II provides a concise introduction and overview of key concepts related to the technologies above, including IoV, VANET, and Blockchain. Section III conducts a comprehensive survey of the relevant literature, while Section IV outlines the methodology adopted for this survey paper. Section V presents the findings and analysis derived from the study, and Section VI presents an in-depth exploration of the existing body of knowledge concerning blockchain-based privacy-preserving solutions for secure and efficient MaaS platforms in the IoV context. Section VII offers a comprehensive discussion of the findings, and finally, Section VIII presents the concluding remarks of this review paper.

II. Motivation

The motivation behind conducting this survey lies in the increasing adoption of Mobility-as-a-Service (MaaS) platforms in the context of the Internet of Vehicles (IoV) and the critical need to address privacy concerns within this evolving ecosystem. With the extensive collection and utilization of personal and sensitive data in MaaS systems, ensuring privacy preservation and data security has become a pressing issue. By exploring the potential of blockchain-based privacy-preserving solutions in the secure and efficient operation of MaaS platforms within the IoV, this survey aims to provide valuable insights for researchers, industry practitioners, and policymakers. By analyzing the existing body of knowledge, identifying key privacy challenges, and examining real-world implementations, this survey will contribute to a comprehensive understanding of the role of blockchain technology in safeguarding user privacy and enhancing the trustworthiness of MaaS platforms in the transport sector.

III. Overview

A. Blockchain Technology

Blockchain was first introduced by Satoshi Nakamoto [9] as the underlying technology behind Bitcoin, a digital cryptocurrency. Since its inception, blockchain has evolved beyond cryptocurrencies and garnered attention for its potential in various industries, including the transport sector's MaaS ecosystem within the Internet of Vehicles (IoV).

Blockchain combines various existing technologies such as digital signatures, public-key cryptography [11], and hash functions [12,13]. It aimed to establish a decentralized payment system where all participants maintain a copy of the same ledger containing past transactions and asset ownership [14]. In a blockchain system, transactions can be processed quickly and securely without the need for a trusted third party [15]. Transactions are grouped into blocks, validated, and added to the previous blocks, forming an immutable chain [16,17]. One notable feature of blockchain systems is their resistance to data modification once transactions are validated [18].

Today, the term "blockchain" does not refer to a single, uniform technology. Instead, there are numerous blockchain projects under development [19]. Hence, it is more appropriate to discuss "blockchains" or "blockchain technologies" rather than a singular blockchain technology.

There are many other definitions of blockchain such as in [10] that define blockchain as a ledger that is distributed and records transactions done by the members. It further says that once a transaction is done it cannot be erased. In the original implementation of financial blockchains, the ledger is responsible for recording currency transactions among various parties. Unlike traditional centralized systems, blockchain technology stores information on multiple distributed computers located in different parts of the world. These computers, known as ‘nodes’, hold replicated copies of the ledger and database. The blockchain database is organized into blocks, which are replicated and stored across all nodes in the network. Each block is generated and linked to the previous block using a cryptographic signature system, creating a sequential chain of blocks. These blocks contain transaction information, forming the foundation of the blockchain architecture.

The decentralized and immutable nature of blockchain provides a transparent and tamper-proof ledger of transactions, ensuring data integrity and enhancing trust among participants. With cryptographic techniques like homomorphic encryption, zero-knowledge proofs, and decentralized identity management, blockchain enables privacy-preserving mechanisms that can address the privacy concerns prevalent in MaaS platforms. By leveraging these features, blockchain technology offers the potential to establish secure and efficient MaaS platforms within the IoV, empowering users with control over their personal data and fostering a more privacy-focused transport experience.

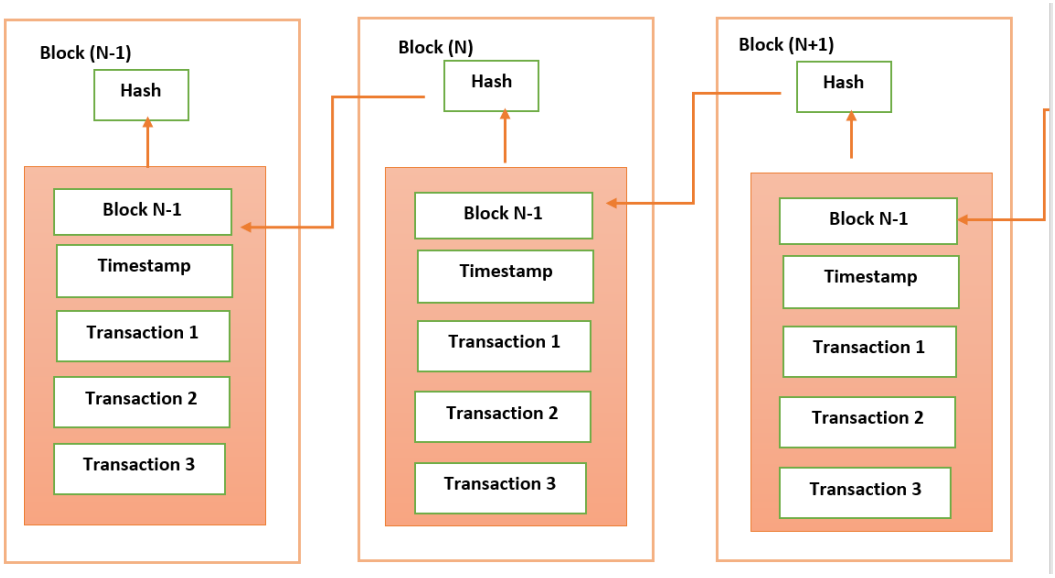

Figure 1. Blockchain Example

Different blockchains can vary in terms of achieving consensus, the type of currency used, and approaches to security and privacy [19]. The two commonly used criteria for classifying blockchains are transaction access and validation access as stated in [20,21]. In public permission-less blockchains, all participants can read, submit, and validate transactions. This are summarized in table 1; according to [20,21].

Table 1. Blockchain Systems according to (20,21).

	Participants' Access to Transactions	Participants' Access to Validation
Public Permission-less	**All participants can read, submit, and validate transactions**	**All participants can validate transaction**
Hybrid	**All network nodes can read and submit transactions**	**Only authorized nodes can validate transactions**
Private	**Only authorized nodes can read, submit, and validate transactions**	**Only authorized nodes can validate transactions**

The advantages of integrating blockchain in MaaS ecosystem in the concept of the Internet of Vehicles (IoV) is more extensive, as blockchain technology possesses key features that address various challenges in this domain

- Immutability: Block data cannot be tampered with or deleted, as any modification to a block's data alters its hash value, necessitating the replacement of subsequent blocks.
- Distributed Ledger: Participating nodes maintain a copy of the ledger, fostering trust among them.
- Consensus Algorithm: Mechanisms for verifying and validating blocks and ensuring agreement on the chain's current state.
- Smart Contract: Self-executing code that triggers when specific conditions are met, requiring consensus among all participants on the execution result.

By leveraging these characteristics, blockchain technology can effectively tackle security, trust, and distribution issues that may arise in vehicular networks.

B. Mobility-as-a-Service (MaaS)

Mobility as a Service (MaaS) is a concept that aims to transform the way people access and use transportation services. MaaS serves as a unified platform that brings together various transportation services to offer personalized journeys with a single ticket. The goal of MaaS is to establish a cooperative and interconnected ecosystem involving transportation services, transport information, and payment services, catering to the unique needs and preferences of customers [4]-[6]. By providing personalized bundles or packages that present the best travel options for each journey, MaaS presents a viable alternative to car ownership, encompassing options like taxis, public transport, rental cars, and bike shares, leading to reduced carbon dioxide emissions [7]-[9].

[10] identifies several key characteristics of MaaS, including the integration of transport modes, various tariff options, a unified platform, multiple actors, the utilization of technologies, customer-oriented demand, registration requirements, and personalization. However, one of the main challenges in implementing the MaaS business model lies in the willingness of public and private transportation providers to collaborate and interface with MaaS agents to serve the customers effectively.

C. Internet of Vehicles (IoV)

The concept of the Internet of Vehicles (IoV) is a comprehensive platform that integrates Internet of Things (IoT) technologies and intelligent transportation systems [29]. Building upon the structure and applications of Vehicular Ad hoc Networks (VANETs), IoV offers a wide array of services, including intelligent traffic control, autonomous vehicles, enhanced driving safety, reliable navigation, prompt crash response, efficient vehicle management, and convenient features such as remote door unlock and stolen vehicle recovery, as well as entertainment options like infotainment services. The combination of IoT and intelligent transportation systems in IoV brings forth transformative possibilities for the future of vehicular communication and transportation efficiency.

IoV encompasses diverse participants, including vehicles, drivers, passengers as users, sensors (e.g., on traffic lights), and On-Board Units (OBUs) installed on vehicles to provide intelligent features. A Central Authority (CA) is responsible for network access and maintenance, while cloud servers handle communications and storage. Additionally, Roadside Units (RSUs) are strategically placed along roads to facilitate communication between vehicles and infrastructures. These participants engage in multiple communication methods, such as Vehicle-to-Vehicle (V2V), Vehicle-to-Road (V2R), Vehicle-to-Human (V2H), Vehicles-to-Infrastructure (V2I), Vehicle-to-Devices and Vehicle-to-Sensor (V2S) interactions, collectively forming a social network of intelligent objects. These objects exchange traffic information through Safety Beacon Messages (SBM) [30]-[31].

As a heterogeneous network, IoV involves diverse participants and services, leading to various challenges due to its dynamic nature and real-time data requirements. For a visual representation of an IoV system, refer to Figure 2.

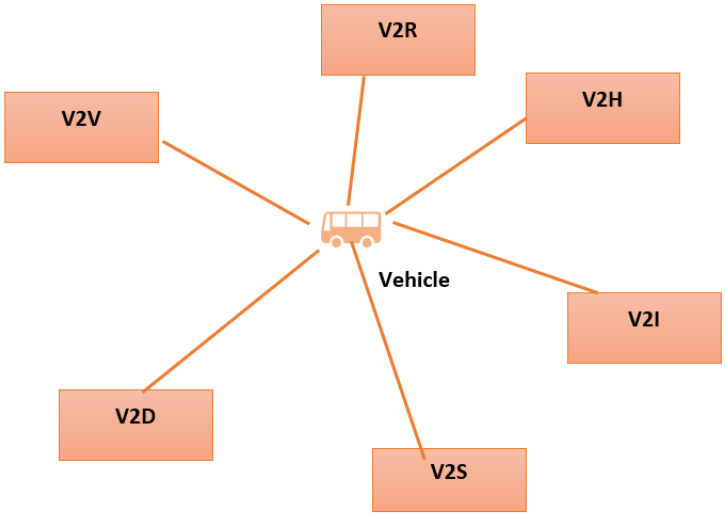

Figure 2: Sample Visual Representation of IoV

Layers of Internet of Vehicles (IoV)

The four layers of the typical Internet of Vehicles (IoV) architecture are described. Each layer serves a specific purpose, from gathering information through sensors in the environment sensing and control layer, managing communication in the network access and transport layer, accomplishing system management in the coordinative computing layer, to storing and analyzing data in the application layer. The application layer offers various services, categorized into open and closed services, catering to different needs and requirements. The centralized system relies on Trusted Central Authorities (CA) to ensure the system's integrity and security [32].

Table 1. The layers of Internet of Vehicles.

Layer	Description
Environment Sensing and control layer	**In this layer, information is gathered by sensors installed within vehicles. These sensors detect Safety Beacon Messages (SBMs), environmental conditions, and other vehicular data. They can also perceive radio frequency identification data like satellite position and road environment.**
Network access and transport layer	**This layer is responsible for node management, data analysis, processing, and communication between vehicles and other units within the vehicular system.**
Coordinative computing layer	**Management of the IoV system is accomplished in this layer. It also handles resource allocation and data processing.**
Application Layer	**The application layer stores and analyze information, making decisions about various risk situations. It includes several applications such as traffic safety and infotainment. The provided services are divided into two categories: open and closed services**

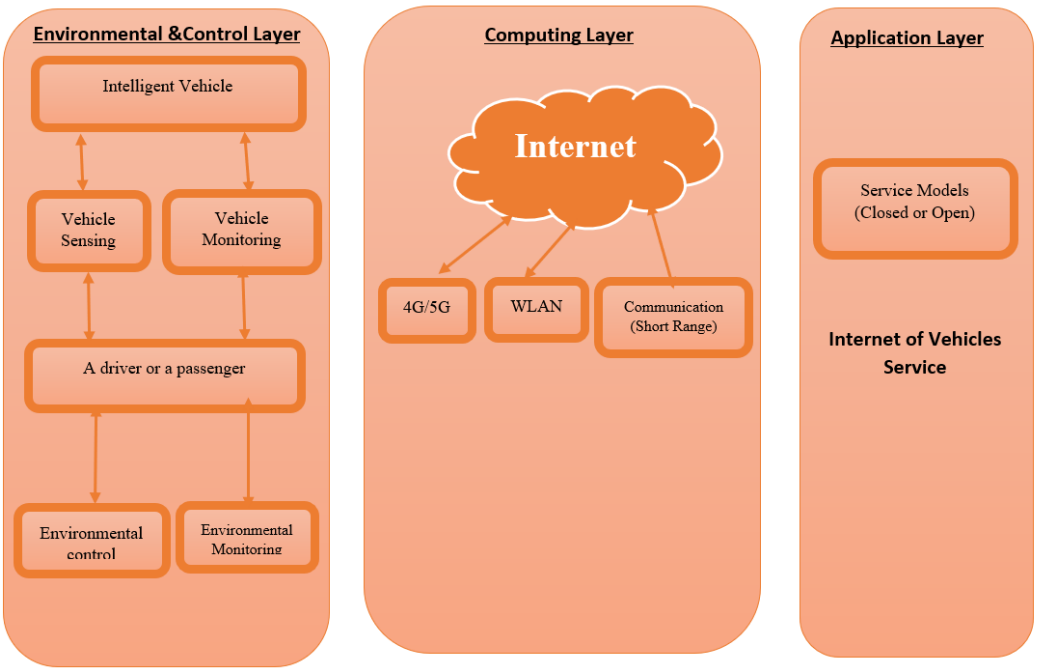

Figure 3: The components of IoV Architecture

D. Privacy in IoV ecosystem

Privacy is a crucial aspect that ensures individuals or groups can safeguard themselves and their confidential information from unauthorized access [33]. In the context of the Internet of Vehicles (IoV), which involves dynamic and heterogeneous systems with numerous participants who may not trust each other, preserving user privacy becomes paramount. Various technologies and strategies, such as pseudonyms, homomorphic encryption, k-anonymity via cloaking techniques, and zero-knowledge proofs, play a vital role in maintaining privacy [34]. As vehicular services expand and data exchange increases, privacy by design becomes a fundamental feature of any IoV technology [35]. The privacy of participants in the IoV ecosystem can be categorized into different types:

- **Privacy Identification:** Ensures the concealment of a user's real identity by employing pseudonyms during communication within a vehicular system [37].
- **Location privacy:** Safeguards the user's location data and can be achieved through techniques such as clustering [37].
- **Data privacy:** Protects the disclosure of personal data, such as vehicle trajectory, speed, and ad-hoc messages exchanged between vehicles. Techniques like homomorphic encryption or federated learning can be employed to achieve data privacy [36].

IV. Related Work

Over the recent years, numerous surveys have been conducted to address privacy concerns within the Maas ecosystem in the context of the Internet of Vehicles in the transport sector. Paper [38] explored the correlation between personal data, consent, and privacy in vehicular systems, while also analyzing existing proposals to mitigate security and privacy challenges related to data exchange. In [39], the authors concentrated on privacy and security solutions specifically designed for 5G vehicular networks. Additionally, [40] discussed prevalent security attacks and examined significant security mechanisms implemented to safeguard vehicular systems' privacy and counteract these attacks.

The researchers in [41] conducted an examination of existing applications with the goal of enhancing security and privacy in VANETs. Similarly, the authors in [42] addressed privacy and security concerns in IoV, particularly in relation to potential attacks. Several surveys have been conducted focusing on authentication schemes in VANET. For example, [43] conducted a survey on authentication methods to better preserve privacy, while [44] analyzed anonymous authentication mechanisms to protect privacy and discussed various trust management models for VANET. Another survey [45] concentrated on authentication and privacy issues during message dissemination in VANET, conducting a comparative study of proposed schemes over the past decade. They thoroughly analyzed and compared these schemes while discussing remaining challenges.

In the literature, a comprehensive survey addressing security and privacy aspects is discussed in reference [46]. Although the survey covers various aspects of IoV, including blockchain technology, its primary focus is not limited to privacy. Additionally, [47] provides a comparison of VANET-based authentication schemes, categorizing them into cryptography, signature and verification, and delving into some privacy-preservation considerations.

In contrast, there is limited research on blockchain solutions in the context of IoV. A survey conducted by the authors in [48] specifically explored the utilization and integration of blockchain technology in the Internet of Vehicles. The survey presented and compared various existing blockchain solutions applicable to IoV. Additionally, the study analyzed different requirements of blockchain-based applications in vehicular systems and highlighted open challenges that need to be addressed in this domain.

In the context of the Maas ecosystem in IoV, while extensive research has been conducted on privacy concerns within IoV, little attention has been given to exploring the privacy-preserving for secure and efficient blockchain-based solutions. Therefore, this study focuses on investigating blockchain technology's potential to address privacy concerns in IoV systems. Three primary privacy concerns in IoV are analyzed: the exposure of user privacy identity, vehicle location information, and the risk of data theft or unauthorized disclosure.

V. Research Methodology

In this survey paper, we analyse existing literature on the topic of blockchain-based privacy-preserving solutions for the secure and efficient implementation of Mobility as a Service (MaaS) in the context of the Internet of Vehicles (IoV) within the transport sector. The research methodology involves a comprehensive review of academic papers, conference proceedings, and relevant publications. By employing a rigorous selection process, we aim to provide a holistic and up-to-date overview of the current state of research in this field.

The methodology employed to establish privacy-preserving blockchain solutions in Maas Ecosystem in the context of the Internet of Vehicles (IoV) within the transport sector comprises three distinct steps:

1. String Searching

The string search was conducted on 15 July 2023, using Boolean operators to effectively retrieve relevant literature related to the study. The search query included the following keywords: "IoV," "Privacy-Preserving," "Blockchain-Based," and "MaaS." To enhance the search results, Boolean operators such as "OR" and "AND" were utilized. The "OR" operator was employed to broaden the search scope by retrieving articles containing any of the specified keywords. On the other hand, the "AND" operator was used to narrow down the search and obtain articles that included all the mentioned keywords, ensuring a more focused and specific selection of literature. This approach allowed for a comprehensive and systematic exploration of the literature related to privacy-preserving blockchain solutions within the IoV context for secure and efficient Mobility as a Service (MaaS) ecosystem in the transport sector.

2. Data Sources

The data sources for this research encompassed a selection of renowned academic databases, including IEEE Xplore, ScienceDirect, Springer, Hindawi, and PLOS. These databases were chosen for their extensive collection of scholarly papers and articles relevant to the study's focus on privacy-preserving blockchain solutions for the secure and efficient IoV ecosystem within the transport sector. Through a systematic search process using specific keywords and Boolean operators (IoV, Privacy-Preserving, blockchain-based, Maas), the search was conducted on 15 July 2023, to identify relevant literature. The papers were then carefully evaluated based on their titles, abstracts, and keywords to ensure their relevance and alignment with the research questions and objectives. The selected papers from these databases are listed in the table below:

Table 2: Selected Databases

Database	URL
ScienceDirect	**https://www.sciencedirect.com**
Springer	**https://www.springer.com**
Hindawi	**https://www.hindawi.com**
Wiley	**https://onlinelibrary.wiley.com/**
MDPI	**https://www.mdpi.com/**
Plos	**https://plos.org**

On 15th July 2023, a comprehensive search was conducted to identify relevant research papers for our study, resulting in a total of 497 papers. After removing 266 papers due to duplication, 231 papers remained. Subsequently, 119 articles were excluded based on the inclusion and exclusion criteria, leaving 112 articles for further analysis. During the abstract-based screening process, an additional 89 articles were excluded, resulting in 23 articles for in-depth review. After carefully reviewing these articles, four were excluded as they did not align with the scope and objectives of the current research, leaving a final dataset of 19 articles. After reading the full articles, four more were removed, resulting in a total of 15 articles that were ultimately included in the study. Figure 3 shows the selection and screening process.

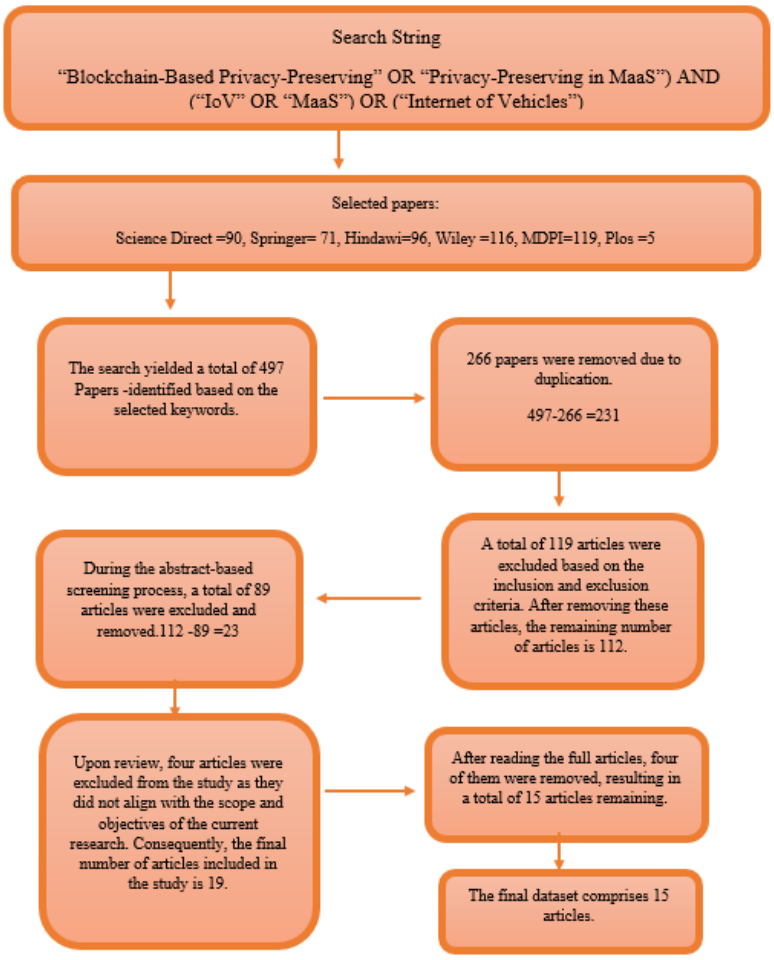

Figure 4: The selection and screening process

3. Screening of the papers

In this stage a screening process was applied to the papers identified from the data sources mentioned above. The initial step involved assessing the relevance of each paper based on their titles, abstracts, and keywords, ensuring they were aligned with the research area, which focused on privacy-preserving blockchain solutions for the secure and efficient IoV ecosystem within the transport sector. Papers that met the predefined criteria were then subjected to a more in-depth review to determine their suitability for answering the research questions and fulfilling the research objectives. During this process, papers that provided substantial insights into the integration of blockchain in the context of IoV privacy preservation and secure Mobility as a Service (MaaS) were retained for further analysis. In contrast, papers that did not closely align with the research area were excluded from the final selection. This meticulous screening process ensured that only highly relevant and valuable papers were included in the study, contributing to the robustness and credibility of the research findings.

Research Questions

In this survey, we aim to address the following research questions in table 3 and the corresponding questions.

Table 3: Research questions

	Research Question	Motivation
RQ 1	**What specific privacy protection are offered by the currently existing blockchain-based solutions within the MaaS ecosystem in the context of IoV?**	**To analyze the privacy features and mechanisms implemented in the current blockchain-based MaaS solutions in IoV**
RQ 2	**What types of blockchain technologies are commonly employed in privacy-preserving solutions within the MaaS ecosystem of IoV?**	**To explore the various blockchain technologies used to enhance privacy and security within the MaaS ecosystem in IoV.**

RQ 3	**Which service areas in the Internet of Vehicles (IoV) utilize blockchain-based privacy-preserving solutions in the Mobility-as-a-Service (MaaS) ecosystem?**	**To identify the specific applications of blockchain-based privacy solutions in the MaaS ecosystem within IoV.**
RQ 4	**Do the proposed schemes for privacy preservation and blockchain integration in the MaaS ecosystem include a comprehensive security analysis?**	**To evaluate whether the proposed schemes provide a thorough security analysis to ensure robust privacy preservation.**
RQ 5	**What are the privacy mechanisms inherent in blockchain-based IoV solutions that support secure and privacy-preserving Blockchain-based MaaS platforms?**	**To identify the privacy mechanisms within blockchain-based IoV solutions supporting secure MaaS platforms, aiming to enhance data protection and user trust.**

VI. Analysis of the results

In this section, we present a comprehensive analysis of the outcomes obtained from our research study on blockchain-based privacy-preserving solutions in the context of the Mobility-as-a-Service (MaaS) ecosystem within the Internet of Vehicles (IoV). The analysis delves into the data collected during the research process, aiming to answer the research questions posed in the earlier sections. By examining the results, we seek to gain valuable insights into the utilization of blockchain technology for privacy preservation in MaaS within the IoV domain. The findings will shed light on the specific service areas where these solutions are implemented, the privacy protection measures incorporated, the types of blockchain technologies and frameworks adopted, the underlying privacy mechanisms, the presence of a security analysis in the proposed schemes, and the current implementation maturity level of these solutions. Through a meticulous examination of the results, we aim to draw meaningful conclusions and contribute to the understanding and advancement of secure and efficient MaaS ecosystems within IoV. Table 4 shows a comparative analysis of Privacy-Preserving

Blockchain-Based Solutions in the Internet of Vehicles (IoV).

Table 4: Comparative analysis of Privacy-Preserving Blockchain-Based Solutions in the Internet of Vehicles (IoV)

	Proposed Sol.	Specific Privacy protection (RQ1)	Blockchain Technology (RQ2)	Comprehensive Security analysis inclusion (RQ4)	Privacy Mechanism employed (RQ5)
Akhter et.al [49]	**A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET**	**Privacy Identity**	**Permissioned – Multi-Level and Etherium**	**Informal**	**Access Control (Cluster-based Medium) Pseudonyms-Utilizing Public Keys**
Wang t.al [50]	**Privacy-preserving cloud-fog–based traceable road condition monitoring in VANET**	**Privacy Identity and Data**	**Permissioned**	**Not Available**	**Ciphertext Policy Attribute-Based Encryption**
Lu et.al [51]	**Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles**	**Data**	**Permissioned and permissionless**	**Not available**	**Group Signatures**
Benarous et.al [52]	**Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks**	**Location and privacy Identity**	**Both permissionless and permissioned - with public read access**	**Informal Security Analysis**	**Ring Signature, Temporal Pseudonyms, and One-Time Address (utilizing Hashes)**

Li.et.al [53]	**A blockchain-assisted intelligent Ttransportation system promoting data services with privacy protection**	**Data**	**Permissioned**	**Informal**	**Data Encryption,**
Liu et.al [54]	**A Blockchain-based Conditional Privacy-Preserving Traffic Data Sharing in Cloud.**	**Privacy identity and Data**	**Permissioned**	**Informal**	**Pseudonyms, Ciphertext Encryption**
Lu et.al [55]	**Toward Blockchain-Based Fair and Anonymous Ad Dissemination in Vehicular Networks.**	**Privacy identity and Location**	**Permissioned**	**Informal**	**Zero Knowledge Proof**
Wang et.al [56]	**A privacy-preserving trust model based on blockchain for VANETs.**	**Privacy identity**	**Permissionless**	**Informal**	**Uses public keys -Pseudonyms**
Qian et.al [57]	**Blockchain-based privacy-aware content caching in cognitive internet of vehicles.**	**Data**	**Not available**	**Not available**	**Broadcasting**
Chaudhary et.al [58]	**A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks.**	**Privacy identity and Location**	**Permissioned**	**Not Available**	**Pseudonyms & Random Encryption**
Lee et.al [59]	**A Privacy Preserving Blockchain-based Reward Solution for Vehicular Networks**	**Privacy identity Location**	**Permissioned**	**Informal**	**Pseudonyms -Utilizing Service Provider**
Guehguih et.al [60]	**Blockchain-Based Privacy-Preserving Authentication and Message Dissemination Scheme for VANET**	**Privacy identity**	**Permissioned**	**Informal Security Analysis**	**Trusted Authority - Pseudonyms**
Li et.al [61]	**A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles**	**Privacy identity**	**Permissioned**	**Informal Security Analysis**	**Combined-Public Keys, Ring Signature**
Li et.al [62]	**Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET**	**Privacy identity and Location**	**Permissionless**	**Informal**	**Zero Knowledge Proof**
Lai et.al [63]	**A Secure and Privacy-Preserving Incentive Scheme for Reliable Real-Time Map Updates**	**Privacy identity**	**Permissioned**	**Not Available**	**RSA-based, Pseudonyms**

.

VII. Discussion

Regarding specific privacy protection offered by the currently existing blockchain-based solutions within the MaaS ecosystem in the context of IoV, **(RQ1),** the survey of research papers indicates a predominant focus on privacy identity protection, with five papers addressing this aspect. Data privacy follows closely, with three papers addressing this aspect, as summarized in figure 4. Notably, many papers provide multiple privacy types simultaneously, exemplified by papers ensuring identity and location privacy, papers addressing identity and data privacy, and three papers covering all privacy types.

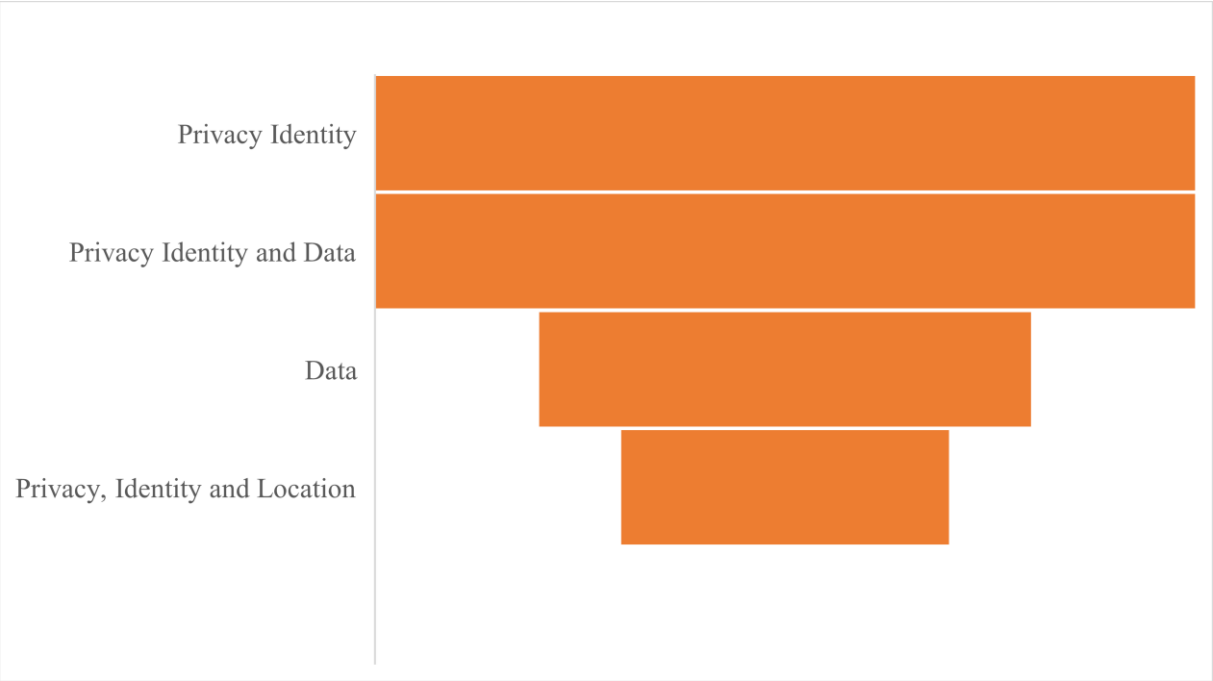

Figure 4: Specific Privacy Protection (RQ 1)

As per the NIST definition [64], the research question **(RQ2)** focuses on the types of blockchain used in the proposed schemes. The analysis reveals that the majority of the schemes utilize permissioned blockchains, while two schemes employ permissionless blockchains, and an additional two utilize both permissioned and permissionless blockchains. However, it is worth noting that one of the papers reviewed does not specify the type of blockchain used in their proposed scheme. Figure 4 shows a graphical representation.

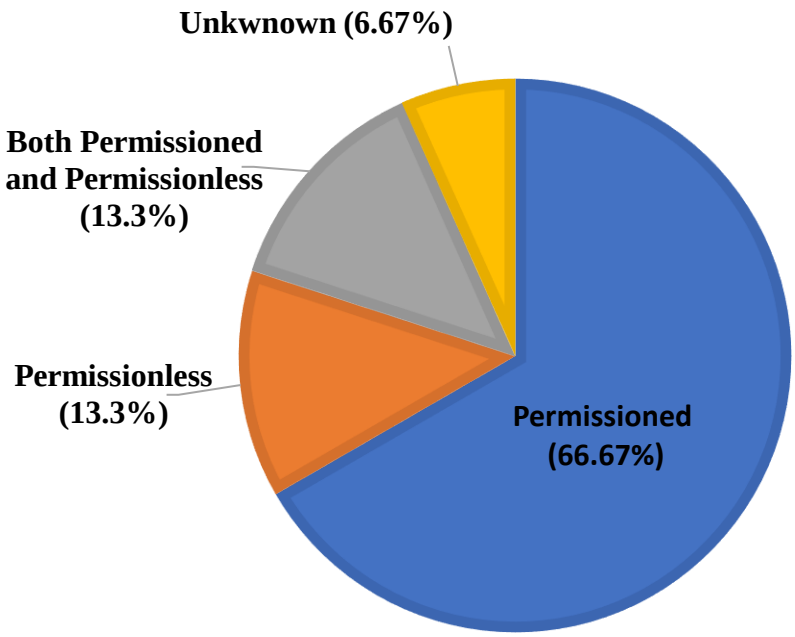

Figure 4: Blockchain Technologies (RQ 2)

The service areas covered by the proposed schemes are shown as summarized in the table 4, with a specific focus on the Blockchain-based MaaS ecosystem within the Internet of Vehicles (IoV). Most of the schemes encompass essential aspects such as authentication, identity management, data security, and location tracking, aligning with our research question **(RQ3).**

The findings regarding security analysis **(RQ4)** indicate that the majority of the proposed solutions lack formal analysis, while the remaining solutions do not offer any security analysis. This raises the question of whether the proposed schemes for privacy preservation and blockchain integration in the MaaS ecosystem include a comprehensive security analysis.

In response to research question **RQ5**, the analysis reveals that pseudonyms, incorporating various aspects, dominate the research papers concerning privacy mechanisms in blockchain-based IoV solutions. However, besides pseudonyms, several other significant mechanisms contribute to privacy preservation, such as zero-knowledge proofs, Combined-Public Keys, Ring Signature, access control, content broadcasting, and group signatures. These diverse privacy mechanisms collectively support the development of secure and privacy-preserving Blockchain-based MaaS platforms within the IoV context.

Research Gaps

Following an extensive review, our study identified several research gaps within the domain of secure and efficient privacy-preserving blockchain-based solutions for the Internet of Vehicles (IoV). While researchers have proposed numerous security measures to enhance privacy, significant privacy challenges in the IoV remain unaddressed. In this section, we delve into the research gaps that were identified and are detailed in Table 5. These gaps highlight the areas that require further investigation and attention to achieve robust and secure privacy-preserving mechanisms in the IoV context.

Table 5: Identified Research Gaps

Reference	Identified Gaps
[49]	**Further research is needed to critically assess the system's scalability when dealing with a substantial volume of registered vehicles and information exchange.**
[50]	**The current scheme guarantees privacy and anonymity for vehicles by utilizing pseudonyms during communication, and only the traceability authority possesses knowledge of their actual identities. However, it is essential to investigate the scalability of this pseudonym generation mechanism to ensure it can handle the increasing number of vehicles within the IoV ecosystem without compromising performance and efficiency.**
[51]	**A research gap lies in the exploration of privacy-preserving mechanisms to further enhance the security and efficiency of Mobility-as-a-Service (MaaS) ecosystems within the context of IoV. Another gap exists in evaluating and integrating additional privacy-preserving mechanisms like homomorphic encryption, zero-knowledge proofs, or privacy-aware data sharing protocols to further safeguard sensitive user information and enhance privacy in MaaS platforms.**
[52]	**Benarous et al. presents a decentralized blockchain-based solution for pseudonym management to ensure privacy and security in the context of the Internet of Vehicles (IoV), there's a potential research gap in evaluating the scalability and performance of this framework. As the IoV ecosystem continues to expand, accommodating a growing number of vehicles and Roadside Units (RSUs) could introduce scalability challenges for the blockchain-based pseudonym management system.**
[53]	**In this scheme, there's lack of in-depth exploration on the specific privacy-preserving mechanisms and techniques utilized within the proposed Ba-ITS intelligent transportation system**
[54]	**Liu et al. [54] proposed a protocol for traffic data sharing using CPHAS, a heterogeneous aggregate signcryption between Certificateless Cryptosystem (CLC) and Public Key Infrastructure (PKI), there is a need for further investigation into the effectiveness of this approach in ensuring robust privacy and security in the MaaS ecosystem. Specifically, the protocol's capability to protect sensitive vehicle identity information and ensure data integrity during data sharing and storage remains a crucial research gap.**
[55]	**The generation of anonymous credentials with zero-knowledge proof of knowledge techniques to prove the validity of the dissemination without revealing private information are included in the scheme, the paper lacks a comprehensive analysis of the effectiveness and robustness of these privacy measures**
[56]	**Blockchain-based anonymous reputation system (BARS) present an intriguing solution for secure message broadcast and user reputation management, there is a need to critically assess its cryptographic material's security, especially in terms of pseudonyms represented by public keys.**
[57]	**Qian et.al mentions the integration of blockchain technology to protect the security and privacy of involved vehicles and ensure the safety and immutability of content transactions. However, the type of blockchain used in this architecture is not specified, leaving room for further investigation and comparison of different blockchain frameworks with varying levels of privacy-preserving capabilities and efficiency.**
[58]	**The researcher proposed a privacy scheme for VANET called BELP, focusing on location and identity privacy. The existing work primarily addresses privacy concerns within VANETs, but there is a need to extend these privacy-preserving techniques to the broader MaaS ecosystem operating in the Internet of Vehicles.**
[59]	**The effectiveness of privacy protection mechanisms, user anonymity, and data confidentiality remains unexplored. Additionally, the vulnerability of pseudo-identities generated from public keys and random numbers, along with potential information leakage risks during registration and communication stages, requires further investigation.**

[60]	**Guehguih et al. scheme uses a permissioned geographical blockchain for vehicle authentication and a public blockchain for event message dissemination, but there is a need to critically assess and optimize the privacy-preserving aspects of this hybrid blockchain solution.**
[61]	**Specific privacy-enhancing features and cryptographic techniques employed to protect user identities and data remain relatively underexplored**
[62]	**A research gap can be identified concerning the scalability and performance of the proposed location cloaking system based on a dual-layer permissionless blockchain. While the system demonstrates promising features such as vehicle pseudonyms through certificates and clustering k-anonymity for location cloaking, its practical feasibility in a real-world MaaS ecosystem with a large number of vehicles and transactions remains unexplored.**

Future Directions

Moving forward, future research in blockchain-based privacy-preserving solutions for MaaS platforms within the Internet of Vehicles (IoV) should focus on several key directions. Firstly, investigating the scalability of blockchain technology in managing the vast data generated within the transport sector's MaaS ecosystem will be critical. Additionally, exploring the interoperability of blockchain systems with existing transportation infrastructure and technologies will pave the way for seamless integration and widespread adoption.

Advancements in cryptographic techniques and privacy-preserving mechanisms will be imperative to address evolving privacy concerns and ensure data security within MaaS platforms. Further research should delve into blockchain-based privacy-preserving and more efficient and secure techniques in MaaS ecosystem in IoV.

Moreover, real-world case studies and pilot implementations of blockchain-enabled MaaS platforms will provide valuable insights into practical challenges and opportunities for improvement. Collaborative efforts between researchers, industry stakeholders, and policymakers will play a pivotal role in driving innovation and establishing standardized frameworks for secure and privacy-enhanced MaaS ecosystems within the context of the Internet of Vehicles.

Conclusion

In conclusion, this survey explored the privacy and security concerns in Mobility-as-a-Service (MaaS) platforms within the transport sector, with a focus on the Internet of Vehicles (IoV). Blockchain technology emerged as a promising solution, offering inherent characteristics like transparency, immutability, and decentralization to ensure privacy preservation and security. Cryptographic methods, such as homomorphic encryption and zero-knowledge proofs, proved essential in enabling data confidentiality and integrity.

Blockchain technology, coupled with privacy-preserving measures, holds tremendous potential to revolutionize the transport sector's MaaS ecosystem within the Internet of Vehicles. Integrating blockchain into MaaS platforms empowers users, safeguards their sensitive information, and instils confidence in the secure and seamless mobility experience. As MaaS platforms continue to redefine urban transportation, embracing blockchain-based privacy mechanisms promises to create a future of privacy-aware and connected mobility, shaping a transport sector that prioritizes user privacy and data security. Collaborative efforts from researchers, industry experts, and policymakers are essential in realizing the full potential of blockchain technology to revolutionize the transport sector and advance the vision of privacy-preserving, efficient, and interconnected MaaS platforms within the IoV framework.

Declarations

Competing Interests: I declare that there are no competing interests as defined by Springer or any other interests that might be perceived to influence the results and/or discussion reported in this paper.

Ethical Approval: Ethical approval for this survey paper is not applicable.

Availability of Data and Materials: Data and materials used in this survey paper are either publicly available or referenced appropriately.

Funding: This survey paper received no specific funding support.

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. https://doi.org/10.1007/978-3-030-36938-5_20

[2] Sadiku, M.; Tembely, M.; Musa, S. Internet of Vehicles: An Introduction. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2018, 8, 11. https://doi.org/10.23956/ijarcsse.v8i1.512.

[3] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ‘‘A survey on the security of blockchain systems,’’ Future Gener. Comput. Syst., to be published.

[4] M. Vukolić, ‘‘The quest for scalable blockchain fabric: Proof-ofwork vs. BFT replication,’’ in Open Problems in Network Security, J. Camenisch and D. Kesdoğan, Eds. Cham, Switzerland: Springer, 016, pp. 112–125.

[5] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun,‘‘Evaluating user privacy in bitcoin,’’ in Financial Cryptography Data Security, A.-R. Sadeghi, Ed. Berlin, Germany: Springer, 2013,pp. 34–51.

[6] P. Koshy, D. Koshy, and P. McDaniel, ‘‘An analysis of anonymity in bitcoin using P2P network traffic,’’ in Financial Cryptography and Data Security, N. Christin and R. Safavi-Naini, Eds. Berlin, Germany:Springer, 2014, pp. 469–485.

[7] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, ‘‘Blockchain,’’ Bus. Inf.Syst. Eng., vol. 59, no. 3, pp. 183–187, Mar. 2017. https://doi.org/10.1007/s12599-017-0467-3

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), document 32016R0679, May 2016, vol. L119, pp. 1–88. [Online]. Available: EUR-Lex - L:2016:119:TOC - EN - EUR-Lex (europa.eu)

[9] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[10] S. Hietanen and S. Sahala, “Mobility as a service - the new transport model,” [Accessed on 16 July, 2023]. Available: https://silo.tips/downloadFile/sampo-hietanen-ceo-its-finland

[11]. Diffie, W.; Hellman, M. New directions in cryptography. IEEE Trans. Inform. Theory 1976, 22, 644–654. https://ieeexplore.ieee.org/document/1055638/

[12]. Merkle, R.C. Secrecy, Authentication, and Public key Systems. Doctoral Dissertation, Stanford University, Standford, CA, USA, 1979.

[13]. Rabin, M.O. Digitalized Signatures. In Foundations of Secure Computation; DeMillo, R.A., Ed.; Academic Press: New York, NY, USA, 1978; pp. 155–166, ISBN 0122103505.

[14]. Sedlmeir, J.; Buhl, H.U.; Fridgen, G.; Keller, R. The Energy Consumption of Blockchain Technology: Beyond Myth. Bus Inf. Syst.Eng. 2020, 62, 599–608. https://www.sciencedirect.com/science/article/abs/pii/S0167739X19316280?via%3Dihub

[15]. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. 2020, 105, 475–491. https://www.emerald.com/insight/content/doi/10.1108/SCM-01-2018-0029/full/html

[16]. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 14 July, 2023).

[17]. Raval, S. Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology, 1st ed.; O’Reilly Media: Sebastopol, CA, USA, 2016; ISBN 1491924543

[18] Treiblmaier, H. The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. SCM 2018, 23, 545–559. The impact of the blockchain on the supply chain: a theory-based research framework and a call for action | Emerald Insight (Accessed on 13,July 2023)

[19] Tasca, P.; Tessone, C.J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. Ledger 2019, 4, 1–39. https://ledger.pitt.edu/ojs/ledger/article/view/140

[20]. Peters, G.W.; Panayi, E. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. Available online: http://arxiv.org/pdf/1511.05740v1 (Accessed on 13 July 2023).

[21]. Ziolkowski, R.; Miscione, G.; Schwabe, G. Decision Problems in Blockchain Governance: Old Wine in New Bottles or Walking in Someone Else’s Shoes? J. Manag. Inf. Syst. 2020, 37, 316–348. https://www.tandfonline.com/doi/full/10.1080/07421222.2020.1759974

[22] S. Hietanen, “Mobility as a Service,” The New Transport Model, pp. 2–4, 2014.

[23] P. Holmberg, M. Collado, S. Sarasini, and M. Williander, “Mobility as a service-maas: describing the framework: final report maas framework,” 2016.

[24] J. Sherly and D. Somasundareswari, “Internet of things based smart transportation systems,” International Research Journal of Engineering and Technology, vol. 2, no. 7, pp. 1207–1210, 2015.

[25] F. Nemanu, J. Schlingensiepen, D. Buretea, and V. Iordache, “Mobility as a Service in smart cities,” Responsible Entrepreneurship Vision, Development and Ethics, p. 425, 2016.

[26] E. Gould, W. Wehrmeyer, and M. Leach, “Transition pathways of emobility services,” WIT Transactions on Ecology and the Environment, vol. 194, pp. 349–359, 2015.

[27] D. Konig, J. Eckhardt, A. Aapaoja, J. Sochor, and M. Karlsson, “Business and operator models for Mobility as a Service (MaaS) (Deliverable to the MAASiFiE project),” Brussels: Belgium, 2016.

[28] P. Jittrapirom, V. Caiati, A.-M. Feneri, S. Ebrahimigharehbaghi, M. J. Alonso Gonzalez, and J. Narayan, "Mobility as a service: A critical ´review of definitions, assessments of schemes, and key challenges," 2017.

[29] 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. https://doi.org/10.1007/978-3-030-36938-5_20

[30]. Sadiku, M.; Tembely, M.; Musa, S. Internet of Vehicles: An Introduction. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2018, 8, 11. https://doi.org/10.23956/ijarcsse.v8i1.512

[31] 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. https://doi.org/10.1007/s12083-019-00786-4

[32]. Sharma, S.; Kaushik, B. A survey on internet of vehicles: Applications, security issues & solutions. Veh. Commun. 2019, 20, 100182 https://doi.org/10.1016/j.vehcom.2019.100182

[33]. 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.

[34]. 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. https://doi.org/10.1007/978-3-030-29053-5.

[35]. 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. https://doi.org/10.2824/38623.

[36]. 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. https://doi.org/10.1007/s12083-019-00849-6

[37. 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. https://doi.org/10.1007/s12083-019-00786-4

[38] Akalu, R. Privacy, consent and vehicular ad hoc networks (VANETs). Comput. Law Secur. Rev. 2018, 34, 37–46. https://doi.org/10.1016/j.clsr.2017.06.006

[39] Sa ˘glam, E.T.; Bahtiyar, ¸S. 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. https://doi.org/10.1109/UBMK.2019.8907026

[40]. 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

[41]. 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

[42]. 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. https://doi.org/10.11591/ijece.v10i5.pp5409-5419.

[43]. Mathew, D.; Roy, H. A survey on different privacy-preserving authentication schemes in VANET. IOP Conf. Ser. Mater. Sci. Eng. 2018, 396, 012033. https://doi.org/10.1088/1757-899X/396/1/012033.

[44]. 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.

[45]. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). Veh. Commun. 2020, 25, 100247. https://doi.org/10.1016/j.vehcom.2020.100247.

[46]. Mikavica, B.; Kosti´c-Ljubisavljevi´c, A. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey. J. Supercomput. 2021, 77, 9520. https://doi.org/10.1007/s11227-021-03659-x.

[47]. 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. https://doi.org/10.1109/ACCESS.2021.3060046

[48]. Mendiboure, L.; Chalouf, M.; Krief, F. Survey on blockchain-based applications in internet of vehicles. Comput. Electr. Eng. 2020, 84, 106646. https://doi.org/10.1016/j.compeleceng.2020.106646

[49]. 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. https://doi.org/10.3390/su13010400

[50]. 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. https://doi.org/10.1002/nem.2096

[51]. 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. https://doi.org/10.1109/TVT.2020.2973651

[52]. Benarous, L.; Kadri, B.; Bouridane, A. Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks. Arab. J. Sci. Eng. 2020, 6033-6049. https://doi.org/10.1007/s13369-020-04448-z

[53]. 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. https://doi.org/10.3390/s20092483

[54]. 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. https://doi.org/10.1109/ICC40277.2020.9148864

[55]. 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. https://doi.org/10.1109/TVT.2019.2940148

[56]. 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. https://doi.org/10.1109/ACCESS.2018.2864189

[57]. 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. https://doi.org/10.1109/MNET.001.1900161

[58]. Chaudhary, B.; Singh, K. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. Peer-Peer Network. Appl. 2021, 3198. https://doi.org/10.1007/s12083-021-01079-5

[59]. 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. https://doi.org/10.1109/ICCE46568.2020.9043015

[60]. 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. https://doi.org/10.1145/3377458.3377466

[61]. 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. https://doi.org/10.1109/TITS.2017.2777990

[62]. 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. https://doi.org/10.1109/TITS.2020.3035869

[63]. 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. https://doi.org/10.1109/JIOT.2019.2953188

[64] 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; https://doi.org/10.6028/NIST.IR.8202