World Electric Vehicle Journal

Review

Using Blockchain in the Registration and Authentication of a Carpooling Application: From Review to Proposal

Lina Sofía Cardona Martínez [1], Cesar Andrés Sandoval Muñoz [1], Ricardo Salazar-Cabrera [1,*], Álvaro Pachón de la Cruz [2] and Juan Manuel Madrid Molina [2]

[1] Telematics Engineering Research Group (GIT), Telematics Department, Universidad del Cauca, Popayán 190003, Cauca, Colombia
[2] Information Technology and Telecommunications Research Group (I2T), CIS Department, Universidad Icesi, Cali 760001, Valle del Cauca, Colombia
* Correspondence: ricardosalazarc@unicauca.edu.co

Abstract: Today, transportation plays a crucial role in economic development and establishing strong social relationships. Primary mobility challenges in cities include high levels of traffic, accidents, and pollution. Improvements in road infrastructure, technological advancements at traffic light intersections, and the adoption of electric or hybrid vehicles are insufficient to resolve these issues. Maximizing the use of public transit and shared transportation is essential for this purpose. Strategies aimed at reducing the number of private vehicles on city roads are beneficial in this regard. Ridesharing, particularly carpooling, is an effective strategy to achieve such a reduction in vehicle numbers. However, safety concerns related to carpooling tools present a significant barrier to the growth of this mode of transportation. The measures implemented in these tools often lack appropriate technology for the authentication process, which is crucial for enhancing safety for both passengers and drivers. This proposed research explores the benefits of improving the authentication processes for passengers and drivers within a shared transportation system to minimize information security risks. A thorough literature review was conducted on shared transportation, user registration, authentication processes within these systems, and technologies that could enhance security, such as blockchain. Subsequently, considering the identified criteria in the literature review, a proposal was developed for creating a registration and authentication module based on blockchain that could be applied across various systems. Finally, an analysis was conducted on how this module could be integrated into a carpooling application and the benefits it would provide regarding safety and increased user adoption. The findings from the review were organized and assessed to identify key aspects for improving user authentication in a system based on intelligent transportation systems (ITSs) and utilizing blockchain, recognized for its security and data integrity. The registration and authentication module developed in this work allows increased security, scalability, and user adoption for any type of application, e.g., carpooling.

Keywords: carpooling; blockchain; shared transportation; intelligent transportation systems; sustainable mobility

check for updates

Academic Editor: Michael Fowler

Received: 9 December 2024
Revised: 16 January 2025
Accepted: 18 January 2025
Published: 20 January 2025

Citation: Martínez, L.S.C.; Muñoz, C.A.S.; Salazar-Cabrera, R.; Pachón de la Cruz, Á.; Molina, J.M.M. Using Blockchain in the Registration and Authentication of a Carpooling Application: From Review to Proposal. *World Electr. Veh. J.* **2025**, *16*, 49. https://doi.org/10.3390/wevj16010049

1. Introduction

Transportation has established itself as a crucial pillar for economic development and the creation of strong social relationships. The increasing recognition of transportation as a strategic industry has prompted the search for technological solutions that optimize efficiency and tackle critical safety and sustainability challenges. These advancements can be translated into intelligent systems and software applications that ensure efficiency and security in the exchange of information between users and transportation systems, improving control, management, and monitoring by users and various regulatory agencies [1]. Additionally, transportation must address its environmental impact. In recent years, air pollution levels have risen significantly, exceeding the World Health Organization (WHO) guidelines. The transportation sector has seen a notable increase in the number of vehicles, resulting in greater congestion and a corresponding rise in carbon emissions [2]. The implementation of electric and hybrid vehicles is a strategy aimed at reducing these pollution levels; however, it should be combined with other measures to decrease the overall number of vehicles. Figure 1 summarizes possible ways to reduce pollution levels on the roads.

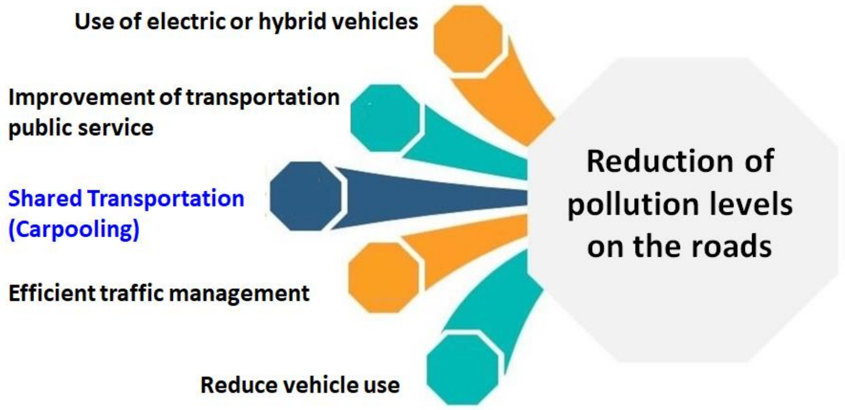
Use of electric or hybrid vehicles
Improvement of transportation public service
Shared Transportation (Carpooling)
Efficient traffic management
Reduce vehicle use
Reduction of pollution levels on the roads

Figure 1. Possible ways to reduce pollution on the roads.

Despite the remarkable technological advances that have transformed the transportation industry, significant challenges remain in safety, efficiency, and sustainability [3]. Growing concerns about pollution levels and safety issues in the transportation sector demand innovative solutions that exceed current conventions. This is a pivotal moment where technological innovation can significantly influence the conceptualization and execution of shared transport. Several alternatives have been proposed to enhance transportation efficiency and reduce environmental impact. One such alternative is shared transportation, commonly known as carpooling, where a private vehicle owner can offer available seats to those in need. This means that private vehicles utilizing this service operate with higher occupancy, thus reducing the number of vehicles on the road [4]. The adoption of this service alleviates vehicular traffic and reduces environmental impact due to greenhouse gas emissions [5].

Currently, transport apps such as Uber, Didi, and similar ones are illegal in countries such as Colombia, mainly due to inconveniences with the taxi union (related to additional costs that taxi drivers must incur to own and operate a taxicab, which is not paid by drivers linked to the apps). This makes strategies such as carpooling, which local and national governments encourage, a good completely legal transportation option for citizens. In 2021, more than 6500 vehicles were immobilized for providing illegal transportation services in Bogotá (the capital of Colombia), according to the mobility secretariat of this city [6]. Thus, it is very important to generate legal transportation strategies that help citizens move safely, sometimes acting as drivers and others as passengers, sharing their vehicles with technological tools that facilitate ride sharing.

In this context, this work focuses on proposing an innovative alternative for ridesharing, specifically carpooling, through the implementation of secured authentication technologies [7]. One of the issues with solutions proposed by shared transportation platforms is that passengers often cannot verify if the driver is the same person registered on the platform. Additionally, these solutions prioritize passenger safety while neglecting that of the driver, who can be the more vulnerable party in many cases. This is partly because passengers are not required to provide detailed information to use the platform. Often, the security measures implemented in these platforms do not employ appropriate technology for authentication, which is essential for enhancing safety for both passengers and drivers. Moreover, a significant risk emerges from the lack of transparency regarding the identities of both parties, fostering distrust due to the anonymity surrounding participants in the trip [8]. Furthermore, carpooling services utilize conventional technologies for storing user data, which makes them vulnerable to third-party attacks by exposing sensitive information [9]. Therefore, exploring new technological trends that can enhance data storage security, improve data verification, and ensure a secure and private authentication process is crucial.

In Colombia, the Superintendency of Industry and Commerce, SIC [10], is responsible for ensuring that the rights and privacy of the personal data of application users are respected. However, current regulations do not contemplate strict measures regarding the registration and authentication processes, which generates risks in this regard for the users.

The use of internationally recognized intelligent transportation systems (ITSs) architectures, implemented through blockchain technology, can effectively enhance security in authentication. Increasing carpooling security can improve users' perceptions of the service and boost its usage. Blockchain is a disruptive and innovative technology that emerged alongside Bitcoin as a decentralized finance solution [11]. Additionally, blockchain has gained significant recognition and has undergone rapid development, showing great potential in various fields, including ITS [12]. Figure 2 presents how improving a carpooling service using ICT is possible. Several authors have proposed applications of blockchain and ITS [12], including vehicular Ad-Hoc networks (VANET) [13], roadside units (RSU) [14], traffic management through priority scheduling [15], and alarm systems linked to national information networks [16]. In these studies, blockchain and ITS ensure security in information management for these applications. However, the proposed solutions for shared transportation issues do not utilize blockchain and fail to prioritize security within the system.

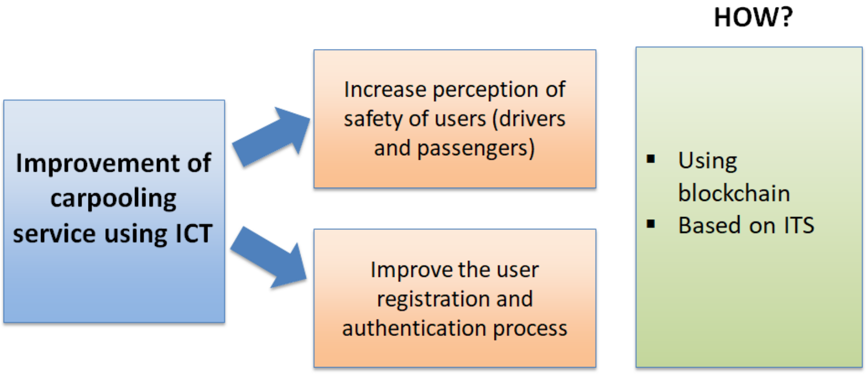
HOW?
Improvement of carpooling service using ICT
Increase perception of safety of users (drivers and passengers)
Improve the user registration and authentication process
▪ Using blockchain
▪ Based on ITS

Figure 2. Improvement in the carpooling service using ICT.

This proposed work delves into the advantages of enhancing the authentication process for passengers and drivers in a shared transportation system to reduce information security risks, emphasizing user registration and authentication. The study conducts a systematic literature review on the application of blockchain in shared transportation and general authentication processes. Based on this review's key findings, a registration and authentication module proposal was developed. Finally, the advantages of implementing this type of module, specifically in a carpooling solution, are assessed. The main contribution of this work, with respect to the state of the art, is the identification of a series of relevant criteria in blockchain-based authentication and registration processes for applications related to shared transportation, which are presented in summary form in Table 1. Additionally, the proposed Carpooling application represents another significant contribution.

Table 1. Summary of the evaluation of related work.

Proposal/ Criteria	Focused on Transportation	User Authentication	Device Authentication	Biometric Data Management	Environmentally Friendly	Security Testing	Use of Encryption Methods
[17]		X				X	X
[18]		X		X		X	X
[19]		X		X			X
[20]			X				X
[21]	X		X			X	X
[22]	X	X		X		X	X
[23]	X	X			X		
[24]	X		X			X	X
[25]		X				X	X
[26]		X				X	X
[27]		X					X

The subsequent sections of the article are organized as follows: Section 2 discusses the materials and methods utilized in the literature review as well as the development of the registration and authentication module. Section 3 presents the obtained results, including the literature review and the proposed development of the general authentication and registration module. Section 4 describes the adaptation of the registration and authentication module for a carpooling application, outlining the proposed design and its benefits. Finally, Section 5 presents the conclusions.

2. Materials and Methods

2.1. Literature Review Methods

The systematic review was performed using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology, version 2020 [28]. Scopus and ScienceDirect databases were selected as reliable reference sources for academic research. Two search strings were defined to address key aspects of the study: one focused on blockchain and shared transportation (String 1) and the other on blockchain and authentication (String 2).

The activities conducted during the three phases of the review recommended by PRISMA are outlined below.

2.1.1. Identification Phase

A database search was performed using the defined strings (String 1 and String 2). The results were filtered by type of document, prioritizing articles and reviews. The search with String 1 yielded 14 documents in Scopus and 2279 in ScienceDirect. The search with String 2 obtained 302 documents in Scopus and 1485 in ScienceDirect.

2.1.2. Detection Phase

Eligibility criteria were applied, discarding documents based on the title and abstract. Articles that did not align with the research objectives were excluded. The criteria applied in the review of the abstract were as follows:

- In the results from the String 1 search, articles not focused on shared transportation systems were excluded, regardless of the type of transport used;
- The results obtained from the String 2 search excluded articles that did not refer to user authentication, specifically those that mentioned blockchain-based authentication without emphasizing identity or human beings.

After filtering, the query results for String 1 yielded 17 articles, while the query results for String 2 yielded 203 articles.

Other filters related to the use of software and the achievement of the initially set objectives were applied to these 220 articles. Twenty-five articles were selected for the next phase.

2.1.3. Inclusion Phase

The 25 selected documents were grouped thematically into three main categories: medicine, vehicles and mobility, and authentication. Relevant documents in each category were highlighted, providing a comprehensive overview of the most significant contributions in each area. Section 3.1 presents the results of this phase in the three mentioned categories.

2.2. Tools and Methods for the Development of Registration and Authentication Module with Blockchain

The literature review was significant in identifying and selecting suitable tools and technologies for developing the registration and authentication module with blockchain. This review offered a thorough understanding of current trends, advancements, and best practices in the field, facilitating informed decision making. The chosen technologies for developing this module, which will incorporate encrypted biometric data and secure storage, are outlined below.

Ethereum was selected as the smart contract platform to implement business logic and store encrypted biometric data on a public blockchain [29]. It was chosen for its robustness as an open-source network that has been reviewed by a large community of developers, ensuring security and stability [29]. Utilizing an already-established blockchain streamlines the application implementation and management.

In addition to Ethereum, some other blockchain platforms were evaluated, such as Hyperledger Fabric [30], NEM [31], Stellar [32], and Tezos [33]. Hyperledger Fabric's main advantages are operational capability, no transaction costs, and microservice-adopted architecture. However, its disadvantages include implementation complexity, the relatively low number of proven use cases, and no token system [30]. The advantages of the NEM platform are high transaction throughput and delegated harvesting usage, while its disadvantages are a lack of community contribution, less decentralization, a reduced number of available tools, and a smaller development community than other platforms [31]. The main advantages of the Stellar platform are crypto-currency support, faster transaction processing time, enhanced security, and simplicity for developers. Its disadvantages include regulatory difficulties with the legal framework and a limited range of applications for the platform [32]. The advantages of the Tezos platform are security and simplicity, while its main disadvantage is vulnerability [33]. Finally, the main advantages of Ethereum (selected platform) pertain to the open-source system, availability of native cryptocurrency, availability in public and private mode, most stable nature, popular and reliable nature, and worldwide developer community support; its disadvantages include public ledger storage overheads, transaction approval time, transaction cost, and integration limitations [34]. The advantages of Ethereum are more relevant to the proposal, mainly because it is an open-source system with extensive developer support. Furthermore, its disadvantages are not significant compared to those of other platforms.

Solidity was chosen as a high-level programming language to develop smart contracts on the Ethereum platform [29]. Its ease of use, popularity, and ability to deploy contracts securely and efficiently on the Ethereum production and test networks support its choice [35]. In addition to Solidity, the Vyper language [36] was evaluated. Vyper, according to its official documentation, is a contract-oriented Python-based programming language targeting the Ethereum virtual machine [37]. Vyper claims to be designed to achieve the following three design goals: language and compiler simplicity, security, and auditability. Regarding vulnerabilities, Vyper presents some drawbacks, which have already been solved in Solidity. Additionally, the ease and security of development in Ethereum make Solidity the best option for the proposal.

The 256-bit Secure Hash Algorithm (SHA 256) was considered appropriate for the model integrity [38]. This cryptographic function is widely used to protect information by providing uniqueness and irreproducibility, which are critical in verifying the integrity and authenticity of biometric data [38].

React was the selected front-end development tool [39]. It is a JavaScript framework known for its efficiency and speed in creating user interfaces. While other options like Angular and Vue.js were considered, the decision to use React was based on its practicality, component-based approach, and rendering speed. React enables the creation of scalable and maintainable interfaces [39].

Ether.js is a comprehensive and compact library for interacting with the Ethereum blockchain [40]. It was selected for its intuitive application programming interface, which is ideal for working with smart contracts. Its compatibility and efficiency make it the right choice for this project.

These technologies were strategically combined to ensure the successful development of the registration and authentication module using blockchain. It employed an end-to-end approach, leveraging modern technologies and secure protocols. The development comprised two key applications: the user interface and the smart contract for interacting with the Ethereum blockchain.

2.2.1. User Interface Development of Module (Frontend)

The user interface was developed using React. This application manages user interaction during the registration and authentication processes. It has been integrated with the FaceIO API [41] for biometric authentication, providing each user with a unique facial identifier (FaceID). The FaceID serves as a key in the authentication process.

FaceIO is a facial authentication framework that can be implemented on websites or web applications using a simple JavaScript snippet to easily authenticate users via Face Recognition instead of the traditional login/password pair or OTP code [41]. The identification process comprises four stages: capture, extraction, comparison, and match/no match [42]. The implementation of FaceIO involves five main stages: image acquisition, image processing, distinctive characteristic location, template creation, and template matching [42]. Some successful implementations of FaceIO can be reviewed at [43–45].

The workflow started by capturing the user's facial image using the FaceIO API. The resulting FaceID was transmitted to the smart contract for secure storage on the blockchain. Ether.js was used as a library for interacting between the user interface and the blockchain, enabling the execution of functions in the smart contract.

2.2.2. Development of the Smart Contract (Backend)

The smart contract was developed using Solidity. It defines the rules and operations for securely storing and retrieving FaceIDs on the Ethereum blockchain. Instead of deploying the contract to the Ethereum mainnet, Hardhat was used to facilitate testing and tuning. This allowed exhaustive tests to be performed without requiring resource consumption on the Ethereum mainnet.

The smart contract includes specific functions to store and retrieve the FaceID. When a user registers, the contract receives the FaceID and stores it immutably on the blockchain. During the authentication process, the user provides his/her FaceID, which is compared to the FaceID stored on the blockchain to verify authenticity.

3. Results

3.1. Results of the Literature Review

In the identification phase, search strings were selected to obtain an initial number of articles. Later, in the detection phase, the obtained articles were filtered by title. Subsequently, the abstracts of the resulting articles were read.

A third filter was applied during the detection phase; only articles that discussed software development or some form of algorithm that clearly explained the implementation process of the proposed system were selected. Additionally, the conclusions of documents were reviewed to determine whether the authors had met their works' objectives or goals. As a result, works [46–50] were excluded.

Works [51–53] were excluded because they focus on Internet of Things (IoT) devices, which is not the emphasis of this proposal. The authors in [13,54–57] conducted research centered on transportation, specifically focusing on vehicle-to-vehicle communication. For this reason, these works were also set aside. Works [58–60] were excluded because, although they are user-centered, they propose an anonymous system, which differs from this proposal.

At the end of the detection phase, 25 articles were obtained. These 25 articles were reviewed in detail in the inclusion phase and grouped thematically into three categories. The most relevant works of each group identified are presented below.

3.1.1. Group 1: Medicine, Telehealth, and Service Providers

The first group corresponds to articles in the field of medicine, which has historically handled immense amounts of data that are not stored securely, so there is no adequate access control. With the advent of the digital era, this information began to migrate to databases and the Internet but continued to be "hacked" or intercepted when sent remotely. One option for introducing security in this area has been blockchain, due to its advantages in terms of privacy and anonymity.

The article "A Blockchain-based Decentralized Identifiers for Entity Authentication in Electronic Health Records (EHR)" presents an authentication model for managing patients and medical records, developed using verifiable credentials (VCs) and decentralized identifiers (DIDs) based on blockchain [17]. These identifiers are generated by an algorithm that stores the data on Hyperledger's Indy blockchain. The significance of this article lies in the decentralization of sensitive medical data hosted on the blockchain, as patients require access to their medical records only by themselves, their doctors, and the entities providing follow-up care for their health conditions. The authors successfully proposed a blockchain-based patient and entity authentication model, while maintaining privacy and consent management to access EHR records via VC and DID.

The authors of the article "A Permissioned Blockchain-Based Identity Management and User Authentication (PBBIMUA) Scheme for e-Health Systems" present a blockchain-based authentication and identity management system for e-health systems that addresses the security and privacy issues posed by online information systems [18]. The PBBIMUA system introduced by the authors employs a novel key distribution mechanism for authentication and management in electronic health systems. The keys are generated through encryption algorithms based on personal biometric data stored on the blockchain. This mechanism establishes a foundation for managing biometric data in the authentication process outlined in this work.

The article "Health-ID: A Blockchain-based Decentralized Identity Management for Remote Healthcare" outlines a solution in the context of the COVID-19 pandemic [19], during which numerous e-health services experienced significant growth. Yet, users had to depend on providers to manage their identity information. Consequently, the authors proposed a decentralized identity management system that identifies and authenticates both patients and healthcare providers. This system is transparent, secure, and decentralized, utilizing health identifiers (HealthID) stored on the Ethereum blockchain.

The authors of the article "A Decentralized Framework for Device Authentication and Data Security in the Next Generation Internet of Medical Things" introduced an authentication protocol based on Physical Unclonable Function (PUF) cryptographic techniques [20]. PUF employs complex mathematics that are difficult to replicate. Alongside this cryptographic method, the article incorporates blockchain for secure data exchange within the network.

3.1.2. Group 2: Vehicles and Mobility

The second group corresponds to articles focused on mobility and vehicles in the context of ITS. The Internet and IoT devices have influenced this area, generating data that can be shared between vehicles or between vehicles and intelligent transportation control systems.

The article "EASBF: An Efficient Authentication Scheme over Blockchain for Fog Computing-enabled Internet of Vehicles" proposes a blockchain-based authentication scheme for a secure fog computing-enabled Internet of Vehicles [21]. It uses elliptic curve cryptography, a one-way hash function, and a consensus Practical Byzantine Fault Tolerance (PBFT) algorithm to guarantee confidentiality, anonymity, privacy, and integrity.

The article "Towards Blockchain-IoT Based Shared Mobility: Car-Sharing and Leasing as a Case Study" presents a high-level architecture designed to promote shared mobility [22]. This architecture integrates car-sharing and leasing through a blockchain IoT platform. The article proposes a hybrid approach aimed at reducing resource consumption through a hash pointer, which grants users the right to be forgotten on the platform.

The authors of the article "Blockchain Empowered Cooperative Authentication with Data Traceability in Vehicular Edge Computing" present a group authentication system utilizing blockchain, incorporating secret sharing and mechanical proxies [23]. This article discusses a trusted entity, common vehicles, proxy vehicles, and Roadside Units (RSUs). A proxy vehicle and an RSU carry out the mutual authentication process, allowing multiple vehicles to connect to a proxy vehicle by forming authentication groups.

The article "Blockchain-enabled Shared Mobility for Sustainable Transportation" proposes a paradigm shift in the transportation sector by integrating blockchain technology into the carpooling network [61]. The authors present a discussion about the system architecture for a blockchain-enabled shared mobility network; however, they do not present a proposal using their proposed architecture.

The authors of the article "Smart Contract Based Carpooling Application for Secure and Efficient Ride Sharing" present a novel system designed to address the shortcomings of centralized ride-sharing services by leveraging smart contracts [62]. The article proposes some improvements to a carpooling service through the use of the decentralization provided by a Smart Contract. It should be noted that the proposed improvements are focused on the basic functionalities of a carpooling service (to publish rides or search for and book desired rides); they are not focused on improving the registration and authentication processes of an application in general.

3.1.3. Group 3: Authentication

The third group of articles focuses on the authentication of users or IoT devices, because data stored in information systems on the Internet must remain private, and users must be guaranteed that no one can impersonate them.

In the article "A zero-knowledge-proof-based digital identity management scheme in Blockchain" a traditional centralized digital identity management system (DIMS) is improved using smart contracts and Zero-Knowledge Protocol (ZKP) proof algorithms [24]. The scheme proposed by the authors is a claim system that decouples the user identity and can selectively reveal its attributes.

The article "PTAS: Privacy-preserving Thin-client Authentication Scheme in Blockchain-based PKI" presents a thin-client authentication scheme that allows the user to retrieve private information [25]. The authors also ensure security using a new PTAS(m-1) model and a certificate authority that acts as a trusted third party.

"AuthChain: A Decentralized Blockchain-based Authentication System" discusses the issue of centralizing user information in online services [26]. Users depend on identity management and authentication from their service provider, which puts their credentials at risk due to potential information leakage and hacking. To address this issue, the authors propose a system called Authchain. This secure and decentralized authentication system is hosted on the Ethereum blockchain for online service providers, allowing users to authenticate themselves through Authchain, thus reducing the likelihood of data breaches and attacks.

The authors of the article "A Secure End-to-End Verifiable E-Voting System Using Blockchain and Cloud Server" propose a cryptographic technique for an authenticated election by modifying the existing Direct Recording Electronic with Integrity and Enforced Privacy (DRE-ip) system. In this article, the voter registration and authentication process is conducted using the Fuzzy Vault algorithm and biometric encryption [27].

The article "STRade: Blockchain-based secure energy trading using vehicle-to-grid mutual authentication in smart transportation" proposes a framework that uses the blockchain-based decentralized, secure, and private vehicle-to-grid network mutual authentication and energy trading system using elliptic curve cryptography with a scheduling feature [63]. The proposed scheme is divided into four steps: registration, scheduling, mutual authentication, and consensus and energy trading. This proposal focuses on transportation (not necessarily shared) and presents an interesting option regarding the registration and authentication processes.

3.2. Summary of the Evaluation of Related Work

The systematic review allowed us to identify the technologies, methods, systems, and different points of view that were the basis for the solution proposed in this work. Table 1 summarizes the significant criteria concerning the related works. This table does not include the proposal presented by the authors, since the criteria identified as relevant in the majority of reviewed works were used to later develop an application that took them into account.

In total, 3 of the 11 documents focus on transportation but none on carpooling. Of the 11 works reviewed in detail, only 8 perform user authentication, while only 3 perform device authentication.

Few of the authentication models presented in the related works (Table 1) use biometric data for authentication (three of the eleven reviewed in detail). Some highlight the importance of this data collection method because it is difficult to imitate or falsify [19], [27]. Still, no system is infallible, and a certain level of risk or vulnerability is always present. Therefore, it is important to implement security measures and maintain appropriate data management in biometric authentication systems.

Data encryption is recognized as a crucial aspect of the system, as only 1 of the 11 reviewed works does not utilize it. It ensures the confidentiality of the data, meaning only authorized individuals can access it. Furthermore, encryption safeguards the integrity of biometric data by preventing unauthorized modifications or entries. Consequently, cryptographic techniques are employed in related works as a vital measure to ensure the privacy and protection of personal information. In most cases, the primary cryptography method, as seen in articles [18,19,22,24,27] in Table 1, is generated and used for secure information exchange. This approach is commonly adopted because it facilitates bidirectional communication and is adaptable based on the required level of security.

In terms of security testing, 7 of the 11 articles reviewed in detail present information related to this type of testing. Several articles merely state that blockchain provides adequate security to ensure privacy and data protection, but the authors do not specify any particular tests. However, other articles discuss certain attacks without detailing their complexity. Notable attacks mentioned include impersonation, phishing, and man-in-the-middle attacks. Based on the characteristics of these attacks in relation to security testing, it was deemed appropriate to conduct impersonation and brute force tests.

Finally, only one of the reviewed works can be considered “environmentally friendly” in the transportation sector, focusing on car rentals rather than a carpooling application. Furthermore, it does not conduct security tests, and its authentication is not biometric [22].

3.3. Development of a General Registration and Authentication Module Using Blockchain

This module was developed to allow users to register and authenticate themselves using biometric data. The criteria identified as relevant in the performed systematic review and in [64] were considered for the design and development of the module.

The biometric data needed to be managed through a smart contract that served as an intermediary between the application interface and the blockchain platform. Section 3.3.2 provides details about the smart contract’s development.

The module is presented using a component diagram. This type of diagram is a visual tool for modeling the structure of a software system in terms of components and interfaces. The Unified Modeling Language (UML) was used for this diagram, as it is an internationally standardized language commonly used for this type of graphic. This diagram represents how different modules and components of the system relate to each other [65].

Figure 3 presents the proposed module’s UML component diagram, including an approximation of the components used and their functionality within a blockchain authentication process. This module focuses on performing the registration and authentication process of any kind of application, not only an application related to mobility, such as carpooling.

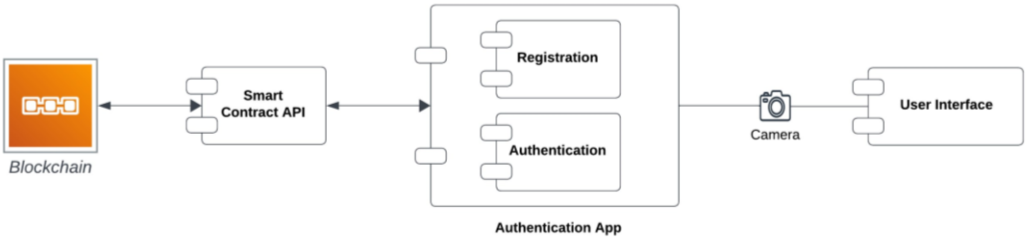

Figure 3. UML component diagram of registration and authentication model.

The Authentication App contains two components: registration and authentication. The User Interface, with the help of a Camera, uses these two components upon registration when the user enters the application for the first time; or authentication, when the user wants to use the application after registration. The Smart Contract API is responsible for storing the user identification information (FaceID) in the blockchain during registration and for verifying that the FaceID entered in the User Interface matches the one stored in the blockchain during authentication.

The Scrum framework was used for the development of the proposed module [66], specifying the functionality required through User Stories (US), which are available to readers upon request to the authors. For these US, the user interfaces were created, which are detailed in Section 3.3.1.

3.3.1. User Interfaces

The FaceIO API was used to capture the user's biometric information, which is used as a credential for authentication. FaceIO provides an application programming interface for interacting with the facial recognition platform. This API allows developers to easily integrate facial recognition functionality into their applications, enabling them to identify and authenticate users through facial images. The details of this API are presented in Section 2.2.1; more information can be consulted in [41].

A smart contract written in Solidity was developed to store the unique code generated by FaceIO, ensuring the security and privacy of the data stored in the Ethereum blockchain. To achieve integrity and authenticity, the SHA256 hash function was used to transform the biometric data before storing it in the smart contract. Below, Section 3.3.2 details the development of the smart contract.

3.3.2. Development of the Smart Contract

The smart contract was developed using the Hardhat platform, which provides tools for compiling, testing, and deploying them. The main reason for using Hardhat was the practicality of providing a fast and efficient smart contract development environment. In addition, this platform offers integrated security, auditing tools, and a wide range of features that significantly improve the smart contract development workflow. Other reviewed alternatives to Hardhat were Truffle, Ganache, Remix, and Brownie.

Initially, the smart contract was developed on a test network to avoid incurring additional costs. This helps to reduce errors and improve the security of smart contracts before deploying them on the main network. The available Ethereum networks include Ropsten and Mainnet. Ropsten was selected because it is a test network. Mainnet is the main network of Ethereum, which requires additional costs to implement a smart contract.

Hardhat was installed to integrate the blockchain authentication module into the frontend application implemented using the React library. Once the development environment was created, the smart contract was added to the contracts folder.

Figure 4 presents the smart contract structure; a constructor method that sets a time variable, "unlockTime," is defined. The "addString" function, presented in Figure 4, receives the biometric ID in string format and verifies whether it exists. If it does not, the storage process is executed in the local node of the Ethereum blockchain. This function is executed every time a passenger or driver registers in the application. Finally, the checkString function, presented in Figure 4, verifies the existence of biometric data in the Ethereum blockchain. When a user tries to log into this module, checkString is called and checks if the user has previously registered.

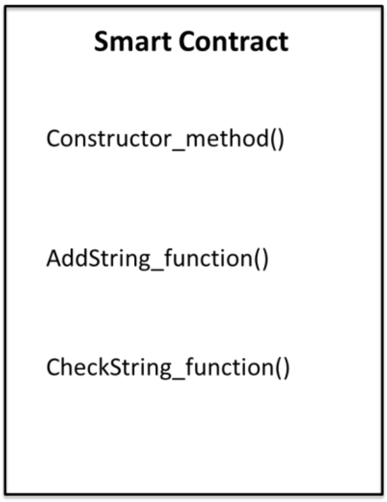

Figure 4. Smart contract structure.

Finally, the registration and authentication methods were modified for integration with blockchain. A React smart contract was called using Typescript. This call requires defining a "provider," which has an IP address, localhost (127.0.0.1), in this case.

4. Adaptation of the Registration and Authentication Module to a Carpooling Application, Proposed Design, and Benefits

For the application's development, a study was initially performed on the requirements of this type of shared transportation system regarding user typology and functionality. Subsequently, the application's functionality was determined. Then, the Scrum Framework was used to divide the functionality identified in the US into three defined user types.

4.1. Requirements Study

A review of the additional literature was performed to identify articles where carpooling applications had been made and to analyze their functionalities. The works [18,67–70] were selected. Although the works [67,69,70] focus on different implementations related to shared transportation, they have some functionalities in common, such as trip scheduling, which is essential in this type of service. The work [70] focuses on the safety of passenger users when using the application because its main contribution is sending alert messages to key contacts and the police in case the user is in danger. In this work, passengers can decide about the vehicle and its characteristics according to their requirements.

Work [69] is more specific about its intended users, focusing on two universities. This system allows a passenger user to schedule a set of trips, but the driver who enters his route and departure time decides the trip's passengers. To solve the carpooling problem, the authors of this work use a heuristic based on a guided Monte Carlo method. The algorithm minimizes an objective function, subject to user time windows and car capacity constraints. The objective function is a weighted sum of different terms in order to maximize the number of served users, minimize the total route length, and maximize the satisfied user preferences (e.g., friends). The work presents an interesting proposal to solve the challenges a carpooling-type application poses. However, it focuses on travel management rather than on the issue of security in registration and authentication, which is the objective of the proposed research.

In [67], the passenger can monitor the vehicle before the trip. Thus, the location of vehicles using this application is always shared, providing little safety to the driver, except for being able to observe the profiles of the people with whom they will share the vehicle. Implementing biometric authentication offers a security option for users to accept and adopt an application, as presented in the work [18]. Compared to other methods, facial authentication's ease of use and comfort make it an interesting option. Work [68] presents several aspects that justify facial-type authentication. This authentication offers high precision and robustness in identity verification. Due to the above, facial authentication is the most appropriate option to guarantee privacy and security. This work also reaffirms that the registration and authentication method proposed in the general module is a suitable option.

Considering the five related works reviewed, trip scheduling was selected as the principal functionality for the proposed carpooling application. The carpooling application users must be able to efficiently organize and plan their shared trips, deciding schedules, confirmations, reminders, and other settings. In addition, it was determined that it would be convenient to give drivers more flexibility in choosing the trip they want to do and the people they want to transport and to rate passengers at the end of the trip.

For the passenger user, functions for specifying the desired route and rating the driver after a trip were included.

4.2. Selected Functionality

Considering the analysis of Section 4.1, it was determined that the carpooling application would have three types of users: passenger, driver, and administrator. Below are the US selected for each user type.

Passenger US:

- Passenger registration;
- Passenger login;
- Passenger profile display;
- Driver rating;
- Passenger log out;
- Add trip as a passenger;
- Display of routes of interest to the passenger;
- Passenger route selection;
- Cancel trip as a passenger.

Driver US:

- Driver registration;
- Driver login;
- Driver profile display;
- Passenger rating;
- Driver log out;
- Specify the route by the driver;
- Passenger selection;
- Cancel driver user route.

Administrator US:

- Administrator login;

- User management;
- Administrator log out.

4.3. Architecture and Functionality of the Carpooling Application

Figure 5 presents the architecture diagram and functionalities of the developed carpooling application, GoTogether, based on the American ITS architecture, known as Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), proposed by the Department of Transportation (DoT) of the United States of America [71]. To determine the reference ITS architecture, ARC-IT, and European architecture, FRAME [72] was reviewed. ARC-IT was selected because it proposes the type of service most related to the required application. The ARC-IT service taken as a reference was Shared Use Mobility and Dynamic Ridesharing [73]. The application architecture presented in Figure 5 considered the mentioned service architecture and the analysis previously performed in the previous Sections of this document.

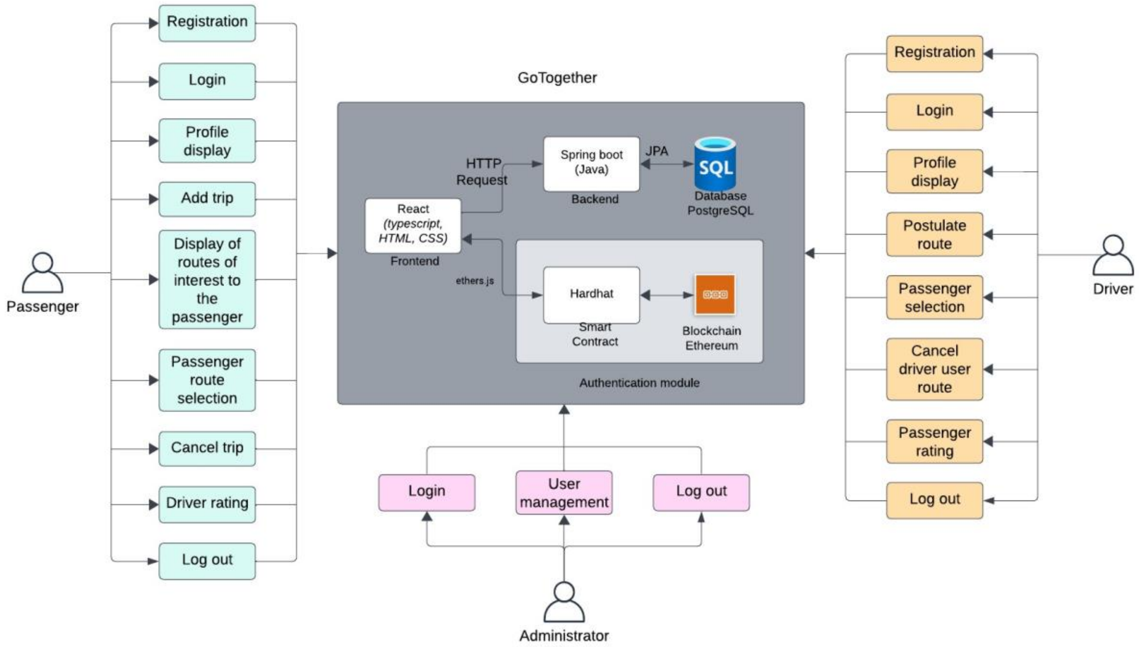

Figure 5. Application architecture.

Figure 5 presents the application's principal components: frontend, backend, authentication module, and database. It shows which tools were used in each component and their interactions. The three user types (administrator, driver, and passenger) and the functionalities available for each are also shown.

4.4. Integration of the Registration and Authentication Module in a Carpooling Application Using Blockchain

Figures 6 and 7 show the integration between the blockchain-based registration and authentication module and the carpooling application. These sequence diagrams detail the steps to be followed in both processes (registration and authentication), considering all the carpooling application elements (such as the Spring Boot backend responsible for storing the non-biometric data in the relational database).

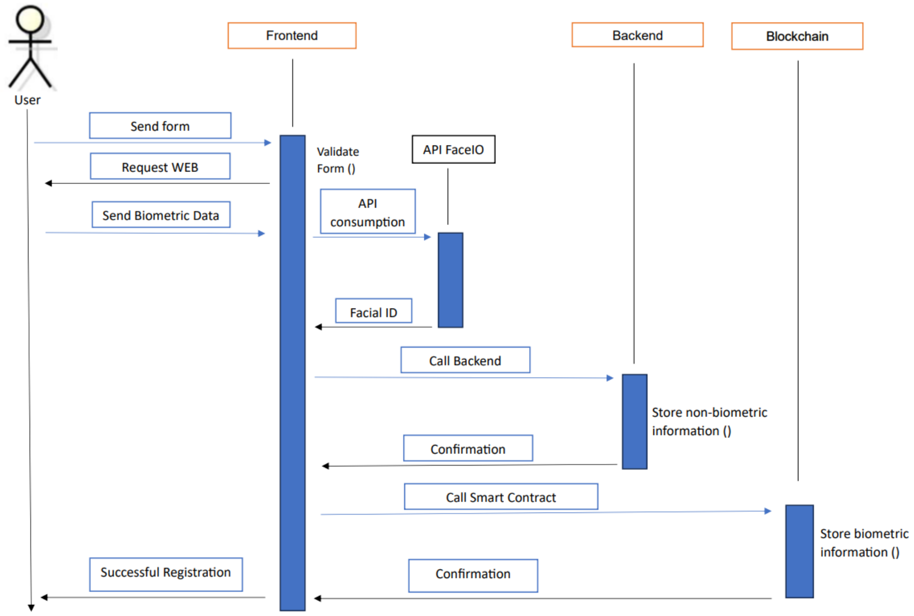

Figure 6. User registration sequence diagram.

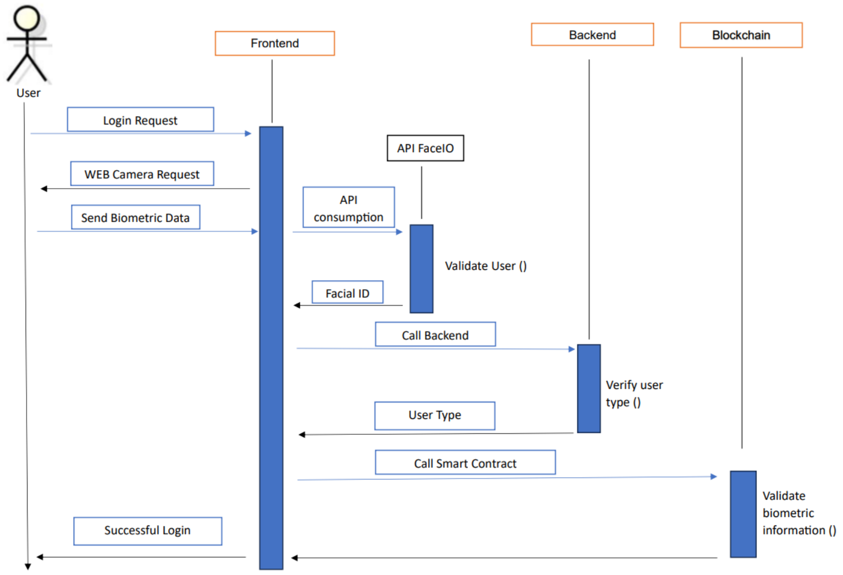

Figure 7. User login sequence diagram.

The communication between the "Frontend" and the "Blockchain" components in Figures 6 and 7 involves calling the developed Smart Contract. In the case of Figure 6 (registration), the call to the Smart Contract is made to store the biometric information. In contrast, in the case of Figure 7 (login), the call is made to validate that the biometric information captured matches that stored in the blockchain. By storing the biometric information in the blockchain at the time of registration and comparing it in the same blockchain at the time of login, security is considerably increased, compared to conventional carpooling applications that store biometric information in a database, in which case there are many possible vulnerabilities. Another relevant security aspect is the use of the FaceIO API because mobile phone applications usually do not request biometric verification to start their operation. Regarding scalability, it is clear that this type of registration and login could be used in any other mobility application or other application area.

FaceIO additionally improves security for the driver, guaranteeing that a login will not easily be performed by another person (possibly in another place and/or vehicle), generating trust for passengers and the service in general. It guarantees that the driver has previously verified his or her identity. It is also important to highlight that biometric verification is much more efficient than other types of verification, e.g., with a text key.

4.5. Discussion About the Benefits of Using Blockchain in the Registration and Authentication of a Carpooling Application

The successful incorporation of the authentication/registration module into the prototype carpooling application validates its applicability and evidences its ease of adaptation. Thus, the blockchain-based registration and authentication module can be integrated into various applications, providing flexibility for implementation in different contexts. Furthermore, its ability to operate in multiple environments demonstrates its scalability, as it can be integrated into both small applications and more complex systems.

One of the key advantages of integrating the authentication module lies in the decentralization inherent to blockchain technology, which makes applications more resistant to malicious attacks and ensures data immutability. Likewise, the implementation of blockchain promotes user privacy by allowing sensitive data, such as biometric information, to be stored securely and controlled by the users themselves. This, in turn, strengthens confidentiality and information security, crucial aspects in applications that handle sensitive data. Particularly in the mobility sector, security is one of the main concerns when using a transportation service. This type of authentication provides safety to the user, improving trust in the application and the user experience.

A carpooling application with the proposed module allows users (drivers and passengers) to secure registration and authentication. Security in this type of system has become a key priority in providing and receiving quality service.

The results showed that facial authentication can be a relatively secure alternative, especially when used as part of a two-step authentication process, as implemented in the prototype. In our approach, in addition to facial verification, the user must enter a PIN.

Concerning the limitations of a carpooling application with this type of registration and authentication, it is essential to highlight the importance of the required hardware. The camera used played a critical role in the operation of the application since its resolution had a direct impact on the application's facial detection capability. In cases where the camera did not have adequate resolution, the application faced difficulties in identifying and authenticating users' faces, resulting in the inability to register or authenticate users.

Another limitation of the work performed is related to using a test blockchain network. The main Ethereum network was not used because there was insufficient budget for the debug process required during development and testing. Although the prototype's operation on the main network is expected to be very similar, it is advisable to consider this aspect.

Regarding potential implementation challenges in real-world scenarios, it is important to consider two important aspects: the challenge of users agreeing to share their vehicle for free with certain passengers interested in their route and the monetization of the service. Most shared transportation services worldwide propose a payment scheme by passengers, which is why they are illegal in some countries because they are unfair competition for services such as taxis, which have additional costs (mainly quota payment to provide the service in the cities). The proposed scheme for the carpooling service in this work is based on a free service for passengers and drivers, with a user acting sometimes as a driver and sometimes as a passenger. This scheme requires a critical change in mentality about user mobility because it requires awareness of the problem of high traffic generated by the large number of vehicles on the roads with very few passengers. This awareness requires a considerable advertising effort and the support of government entities in charge of city mobility. Regarding monetization, it is important to take it into account because the proposed scheme uses a blockchain network, which generates continuous operation and maintenance costs. As mentioned, these costs could not be passed on to passengers. The most viable option would be for the government entities in charge of mobility to finance in some way the costs of the proposed service, considering the benefits that its implementation could generate.

Finally, it is essential to mention that these tools that aim to share vehicles are important in global efforts to reduce carbon emissions and promote environmentally friendly technologies. The number of vehicles in transit on the streets is reduced and several passengers sharing a vehicle reduces carbon emissions; however, the inclusion of blockchain technology requires computing power, which is important to consider. It would be necessary to guarantee that the carbon footprint of the blockchain application is much lower than the possible carbon emissions of the vehicles that are being prevented from traveling on the streets.

5. Conclusions and Future Work

The literature review identifies certain advances achieved in implementing blockchain in various areas, significantly strengthening traditional systems' security. However, these advances have yet to be extensively applied to shared transportation applications, such as carpooling. In this sense, a carpooling web application integrating a blockchain-based authentication module poses a novel approach, which could lay the foundation for providing users with a more secure experience.

The proposed user registration and authentication module, which uses blockchain, can be integrated into any related mobility solution that considers this type of process critical due to its flexibility. This is possible since the module was designed for general use, without determining a specific application on which to focus. Thus, the module can be adapted to any type of solution, even if it is not specifically focused on mobility.

Regarding the particular case of the proposal, improving registration and authentication incorporating blockchain, which minimizes security risks, can increase user confidence in this application and its use. Storing and verifying users' biometric data in a blockchain network instead of in a database means that such data are subject to fewer vulnerabilities and access issues. The use of biometric authentication, with the help of FaceIO and the device's camera, instead of the conventional use of passwords, increases the efficiency of the application and minimizes the possibility of unauthorized logins.

The most relevant limitations of this proposal are the need for an adequate camera on the users' devices to perform the registration and authentication procedures; the required evaluation with the selected blockchain network because the application has not yet been tested on the main Ethereum network (only on the test network); the required monetization of the proposed service; and finally, the acceptance of the proposed service by users, which requires the support of government entities in charge of mobility.

Regarding future research, the main pending work concerns implementing the proposed carpooling application. It would be advisable to evaluate this application with some users (passengers and drivers) to assess usability and perceptions of safety. This evaluation would involve a survey of user experience.

Another line of research could consider implementing a carpooling prototype based exclusively on blockchain technology as a data management system (not only for registration and authentication). This would guarantee an increase in security in the prototype operations after authentication, such as creating routes or requesting services.

Research on using blockchain technology in other mobility-related applications, such as public transportation, is also suggested. This is key to achieving better mobility in cities. Finally, integrating the general registration and authentication module developed with blockchain technology is proposed in other types of applications that require increased security in these processes.

Author Contributions: Conceptualization, R.S.-C. and Á.P.d.l.C.; methodology, R.S.-C., Á.P.d.l.C. and J.M.M.M.; software, L.S.C.M. and C.A.S.M.; validation, R.S.-C., L.S.C.M. and C.A.S.M.; formal analysis, R.S.-C., L.S.C.M., C.A.S.M. and Á.P.d.l.C.; investigation, R.S.-C., L.S.C.M. and C.A.S.M.; resources, Á.P.d.l.C. and J.M.M.M.; writing—original draft preparation, R.S.-C., L.S.C.M. and C.A.S.M.; writing—review and editing, R.S.-C., Á.P.d.l.C. and J.M.M.M.; supervision, R.S.-C., Á.P.d.l.C. and J.M.M.M.; funding acquisition, R.S.-C., Á.P.d.l.C. and J.M.M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

Acknowledgments: The authors thank Universidad del Cauca (Telematics Department) and Universidad Icesi (CIS Department) for supporting this research.

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

References

1. Jadhav, B.V.; Mujumdar, G.S.; Jadhav, N.A. Applications of artificial intelligence in machine learning: Review. *Int. J. Adv. Res. Sci. Commun. Technol.* **2022**, *2*, 19–23. [CrossRef]
2. Munoz, C.; Pineda, B.E.; Gil, H. Relevant aspects of the mobility and its relation with environment in the Valle de Aburrá: A review. *Ing. Desarro.* **2018**, *36*, 489–508. Available online: https://rcientificas.uninorte.edu.co/index.php/ingenieria/article/view/10403 (accessed on 10 January 2024).
3. Bai, C.A.; Cordeiro, J.; Sarkis, J. Blockchain technology: Business, strategy, the environment, and sustainability. *Bus. Strategy Environ.* **2020**, *29*, 321–322. [CrossRef]
4. Bresciani, C.; Colorni, A.; Costa, F.; Lue, A.; Studer, L. Carpooling: Facts and new trends. In Proceedings of the International Conference of Electrical and Electronic Technologies for Automotive, Milan, Italy, 9–11 July 2018. [CrossRef]
5. Asghari, M.; Al-e-hashem, S.M.J.M.; Rekik, Y. Environmental and social implications of incorporating carpooling service on a customized bus system. *Comput. Oper. Res.* **2022**, *142*, 105724. [CrossRef]
6. Secretaría de Movilidad de la Ciudad de Bogotá. Available online: https://www.movilidadbogota.gov.co/web/search/content/multas?page=6#:~:text=transporte%20ilegal (accessed on 23 May 2024).
7. Zafar, F.; Khattak, H.A.; Aloqaily, M.; Hussain, R. Carpooling in Connected and Autonomous Vehicles: Current Solutions and Future Directions. *ACM Comput. Surv.* **2022**, *54*, 218. [CrossRef]
8. Créno, L.; Cahour, B. Perceived risks and trust experience in a service of carpooling. In Proceedings of the 22nd ITS World Congress, Bordeaux, Francia, 5–9 October 2015.
9. Butler, L.; Yigitcanlar, T.; Paz, A. How Can Smart Mobility Innovations Alleviate Transportation Disadvantage? Assembling a Conceptual Framework through a Systematic Review. *Appl. Sci.* **2020**, *10*, 6306. [CrossRef]
10. Superintendency of Industry and Commerce, SIC. Available online: https://sedeelectronica.sic.gov.co/ (accessed on 11 July 2024).
11. Chen, Y.; Bellavitis, C. Blockchain disruption and decentralized finance: The rise of decentralized business models. *J. Bus. Ventur. Insights* **2020**, *13*, e00151. [CrossRef]
12. Singh, P.; Elmi, Z.; Lau, Y.Y.; Borowska-Stefańska, M.; Wiśniewski, S.; Dulebenets, M.A. Blockchain and AI technology convergence: Applications in transportation systems. *Veh. Commun.* **2022**, *38*, 100521. [CrossRef]
13. Daimary, S.; Kalita, H.K. An overview of Blockchain-based applications and architectures for VANET. *Int. J. Comput. Appl.* **2023**, *185*, 9–17. [CrossRef]
14. Akhter, A.F.M.S.; Ahmed, M.; Shah, A.F.M.S.; Anwar, A.; Kayes, A.S.M.; Zengin, A. A Blockchain-Based Authentication Protocol for Cooperative Vehicular Ad Hoc Network. *Sensors* **2021**, *21*, 1273. [CrossRef] [PubMed]
15. Janakbhai, N.D.; Saurin, M.J.; Patel, M. Blockchain-based intelligent transportation system with priority scheduling. In *Lecture Notes on Data Engineering and Communications Technologies*; Springer: Singapore, 2021. [CrossRef]
16. Ndri, A.; Bellamkonda, D.; Akalanka, B.M. Applications of Block-Chain Technologies to Enhance the Security of Intrusion Detection/Prevention Systems: A Review. In Proceedings of the Midwest Instruction and Computing Symposium (MICS)-2022, Milwaukee, WI, USA, 1–2 April 2022; p. 54.

17. Taleka, M.; Makkithaya, K.; Narendra, V.G. A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records. *Cogent Eng.* **2022**, *9*, 2035134. [CrossRef]
18. Xiang, X.; Wang, M.; Fan, W. A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems. *IEEE Access* **2020**, *8*, 171771–171783. [CrossRef]
19. Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-ID: A Blockchain based decentralized identity management for remote healthcare. *Healthcare* **2021**, *9*, 712. [CrossRef] [PubMed]
20. Satamraju, K.P.; Malarkodi, B. A decentralized framework for device authentication and data security in the next generation internet of medical things. *Comput. Commun.* **2021**, *180*, 146–160. [CrossRef]
21. Eddine, M.S.; Ferrag, M.A.; Friha, O.; Maglaras, L. EASBF: An efficient authentication scheme over Blockchain for fog computing-enabled internet of vehicles. *J. Inf. Secur. Appl.* **2021**, *59*, 102802. [CrossRef]
22. Auer, S.; Nagler, S.; Mazumdar, R.; Mukkamala, R.R. Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study. *J. Netw. Comput. Appl.* **2022**, *200*, 103316. [CrossRef]
23. Liu, H.; Zhang, P.; Pu, G.; Yang, T.; Maharjan, S.; Zhang, Y. Blockchain Empowered Cooperative Authentication with Data Traceability in Vehicular Edge Computing. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4221–4232. [CrossRef]
24. Yang, X.; Li, W. A zero-knowledge-proof-based digital identity management scheme in blockchain. *Comput. Secur.* **2020**, *99*, 102050. [CrossRef]
25. Jiang, W.; Li, H.; Xu, G.; Wen, M.; Dong, G.; Lin, X. PTAS: Privacy-preserving Thin-client Authentication scheme in blockchain-based PKI. *Future Gener. Comput. Syst.* **2019**, *96*, 185–195. [CrossRef]
26. Lim, S.Y.; Fotsing, P.T.; Musa, O.; Almasri, A. AuthChain: A Decentralized Blockchain-based Authentication System. *Int. J. Eng. Trends Technol.* **2020**, *1*, 70–74. [CrossRef]
27. Panja, S.; Roy, B. A secure end-to-end verifiable e-voting system using blockchain and cloud server. *J. Inf. Secur. Appl.* **2021**, *59*, 102815. [CrossRef]
28. Page, M.J.; Moher, D.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D. PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ* **2021**, *372*, 160. [CrossRef] [PubMed]
29. Ethereum. Introduction to Smart Contracts. Available online: https://ethereum.org/en/ (accessed on 24 March 2024).
30. Hyperledger Fabric. Available online: https://www.hyperledger.org/ (accessed on 11 July 2024).
31. NEM. Available online: https://docs.nem.io/pages/ (accessed on 11 July 2024).
32. Stellar. Available online: https://stellar.org/ (accessed on 11 July 2024).
33. Tezos. Available online: https://tezos.com/ (accessed on 11 July 2024).
34. Suvitha, M.; Subha, R. A survey on smart contract platforms and features. In Proceedings of the 2021 7th International Conference on Advanced Computing and Communication Systems, ICACCS, Coimbatore, India, 19–20 March 2021; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2021; pp. 1536–1539. [CrossRef]
35. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum, White Paper. 2014. Available online: https://ethereum.org/en/whitepaper (accessed on 25 May 2024).
36. Vyper. Available online: https://vyperlang.org/ (accessed on 11 January 2024).
37. Kaleem, M.; Mavridou, A.; Laszka, A. Vyper: A Security Comparison with Solidity Based on Common Vulnerabilities. In Proceedings of the 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020, Paris, France, 28–30 September 2020; Institute of Electrical and Electronics Engineers Inc.: New York, NY, USA, 2020; pp. 107–111. [CrossRef]
38. Azeez, N.A.; Chinazo, O.J. Achieving Data Authentication with hmac-sha256 Algorithm. 2018. Available online: https://www.researchgate.net/publication/332182220_ACHIEVING_DATA_AUTHENTICATION_WITH_HMAC-SHA256_ALGORITHM. (accessed on 6 June 2024).
39. React. React Documentation. Available online: https://reactjs.org/docs/getting-started.html (accessed on 18 May 2024).
40. Ethers. Documentation. Available online: https://docs.ethers.org/v5/ (accessed on 24 March 2024).
41. PixLab. Symisc Systems, FaceIO API Documentation. Available online: https://faceio.net/ (accessed on 2 April 2024).
42. FaceIO-New Age Face Authentication. Available online: https://www.analyticsvidhya.com/blog/2023/02/faceio-app-new-age-face-authentication/ (accessed on 2 April 2024).
43. Building an Attendance System with Face Recognition Using Nextjs and FACEIO. Available online: https://medium.com/@vshall/building-an-attendance-system-with-face-recognition-using-nextjs-and-faceio-d0dad93e0fd4 (accessed on 2 April 2024).
44. How to Build a Secure Voting Web App with FACEIO. Available online: https://blog.stackademic.com/how-to-build-a-secure-voting-web-app-with-faceio-76f0fb29c25d (accessed on 2 April 2024).
45. Building a Secure Event Booking App with FACEIO and Svelte. Available online: https://blog.stackademic.com/building-a-secure-event-booking-app-with-faceio-and-svelte-68e77b2625d6 (accessed on 2 April 2024).

46. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. *Veh. Commun.* **2022**, *34*, 100458. [CrossRef]
47. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Raymond Choo, K.K. Blockchain-based identity management systems: A review. *J. Netw. Comput. Appl.* **2020**, *166*, 102731. [CrossRef]
48. Mohsin, A.H.; Zaidan, A.A.; Zaidan, B.B.; Albahri, O.S.; Albahri, A.S.; Alsalem, M.A.; Mohammed, K.I. Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Comput. Stand. Interfaces* **2019**, *64*, 41–60. [CrossRef]
49. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C.A. A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]
50. Mundhe, P.; Verma, S.; Venkatesan, S. A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Comput. Sci. Rev.* **2021**, *41*, 100411. [CrossRef]
51. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized Blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
52. Li, F.; Yu, X.; Cui, Y.; Yu, S.; Sun, Y.; Wang, Y.; Zhou, H. An anonymous authentication and key agreement protocol in smart living. *Comput. Commun.* **2022**, *186*, 110–120. [CrossRef]
53. Zhang, J.; Wanh, Z.; Shang, L.; Lu, D.; Ma, J. BTNC: A blockchain based trusted network connection protocol in IoT. *J. Parallel Distrib. Comput.* **2020**, *143*, 1–16. [CrossRef]
54. Ali, I.; Gervais, M.; Ahene, E.; Li, F. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *J. Syst. Archit.* **2019**, *99*, 101636. [CrossRef]
55. Dwivedi, S.K.; Amin, R.; Vollala, S.; Chaudhry, R. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. *Comput. Electr. Eng.* **2020**, *86*, 106719. [CrossRef]
56. George, S.A.; Stephen, S.M.; Jaekel, A. Blockchain-Based Pseudonym Management Scheme for Vehicular Communication. *Electronics* **2021**, *10*, 1584. [CrossRef]
57. Ren, Y.; Li, X.; Sun, S.F.; Yuan, X.; Zhang, X. Privacy-preserving batch verification signature scheme based on blockchain for Vehicular Ad-Hoc Networks. *J. Inf. Secur. Appl.* **2021**, *58*, 102698. [CrossRef]
58. Lax, G.; Russo, A. Blockchain-Based access control supporting anonymity and accountability. *J. Adv. Inf. Technol.* **2020**, *11*, 186–191. [CrossRef]
59. Ra, G.; Kim, T.; Lee, I. VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things. *IEEE Access* **2021**, *9*, 75945–75960. [CrossRef]
60. Shao, W.; Jia, C.; Xu, Y.; Qiu, K.; Gao, Y.; He, Y. AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain. *Comput. Secur.* **2020**, *99*, 102069. [CrossRef]
61. Aswathy, M.; Arunkumar, J.; Samuel, R.M.; Sai Shibu, N.B. Blockchain enabled Shared Mobility for Sustainable Transportation. In *BlockSys 2023—Proceedings of the 5th ACM International Workshop on Blockchain-Enabled Networked Sensor Systems, Istanbul, Turkiye, 12 November 2023*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 34–36. [CrossRef]
62. Ramani Bai, V.; Sudhir, P.; Joshi, R.; Nair, V.; Anilkumar, V. Smart Contract Based Carpooling Application for Secure and Efficient Ride Sharing, 2023. In *RASSE 2023—IEEE International Conference on Recent Advances in Systems Science and Engineering, Proceedings, Kerala, India, 8–11 November 2023*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2023. [CrossRef]
63. Sharma, G.; Joshi, A.M.; Mohanty, S.P. STrade: Blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation. *Sustain. Energy Technol. Assess.* **2023**, *57*, 103296. [CrossRef]
64. Sharma, R.; Chakraborty, S. BlockAPP: Using Blockchain for Authentication and Privacy Preservation in IoV. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6. [CrossRef]
65. Hurtado, S.V. *Representación de la Arquitectura de Software Usando UML*; Facultad De Ingenieria Universidad Del Zulia: Maracaibo, Venezuela, 2023; Volume 1.
66. Scrum. Available online: https://www.scrum.org/ (accessed on 15 April 2024).
67. Akshay, B.; Asmita, G.; Kshetrapal, J. Car Pool'up–Real-time carpooling using GPS. In Proceedings of the National Conference on New Horizons in IT–NCNHIT, Mumbai, India, 15 September 2013.
68. Barra, S.; De Marsico, M.; Galdi, C.; Riccio, D.; Wechsler, H. FAME: Face Authentication for Mobile Encounter. In Proceedings of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, Napoli, Italy, 9 September 2013; IEEE: New York, NY, USA, 2013. [CrossRef]
69. Bruglieri, M.; Ciccarelli, D.; Colorni, A.; Luè, A. PoliUniPool: A carpooling system for universities. *Procedia-Soc. Behav. Sci.* **2011**, *20*, 558–567. [CrossRef]
70. Dangare, C.S.; Akila, G. IJARCCE An Android based application: Cab pooling. *Int. J. Adv. Res. Comput. Commun. Eng.* **2016**, *5*, 569–573.
71. U.S. Department of Transportation. Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT). Available online: https://www.arc-it.net/ (accessed on 15 March 2024).

72. FRAME. Frame Architecture. Available online: https://frame-online.eu/ (accessed on 6 May 2024).
73. U.S. Department of Transportation. Shared Use Mobility and Dynamic Ridesharing, ARC-IT. Available online: https://www.arc-it.net/html/servicepackages/sp17.html#tab-3 (accessed on 15 March 2024).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.