IJCI V9-02(2022) 45–63

International Journal of Computers and Information (IJCI)

Available online at https://ijci.journals.ekb.eg/

Ride-Sharing Services: From Centralization to Decentralization

Nesma Mahmoud[*, a], Asmaa Aly[*, b], Hatem Abdelkader[*, c]

[*]*Information Systems dept., Faculty of Computers and Information, Menoufia University, Shebin Elkom 32511, Egypt.*
[a]*nesma.1115@ci.menofia.edu.eg*, [b]*asmaa.elsayed@ci.menofia.edu.eg*, [c]*hatem.abdelkader@ci.menofia.edu.eg*

Abstract

Ride-sharing is a service that becomes basic and important for all communities due to its benefits for individuals like reducing travel cost and time and for societies like reducing gas emissions, congestions, and fuel consumption. Existing ride-sharing services are centralized and thus perform their functions through a central third party. Therefore, they suffer from various problems due to the centralized architecture namely single point of failure, lack of transparency, privacy violation, and many attacks such as distributed denial of service, etc. These problems urged the research community to shift to decentralization. Blockchain has revolutionized decentralization, which pushed the researchers to exploit it in ride-sharing and also other various fields. But what beyond implementing blockchain in ride-sharing? So, this paper answers the questions of where we are now in blockchain-based ride-sharing services and what is the next steps in them. It provides summary for previously proposed works in ride-sharing, specifically, blockchain-based. Followed by intensive analysis, comparison, and classification of these works. Finally, this paper provides guidance for future research with the promising and important directions in blockchain-based ride-sharing services.

Keywords: ride-sharing; intelligent transportation systems; blockchain; smart contracts;

1. Introduction

Nowadays, transportation represents an essential and important aspect of any society [1]. Intelligent Transportation Systems (ITSs) are the future of transportation [2, 3]. They aim to integrate all transportation elements with each other through information technologies and communication. These elements are roads, vehicles, traffics, and people. ITS's goal is to improve transportation and reduce its harmful effects. Ride-sharing is one of ITS's applications which helps it achieve its goal [1, 2]. It represents a prominent sharing economy example [4]. This economy encourages economic sharing activities in a peer-to-peer way. There is no doubt that ride-sharing becomes a basic part of any society. Due to its several advantages of congestion reduction, maintain the environment by reducing carbon dioxide emissions, saving time of users, etc. Recently, ride-sharing services (RSSs) become alternative transportation services which allow the use of personal cars wisely. They enable drivers or people owing private cars to share their free seats with other riders. RSSs have many benefits to the individual and the community as a whole including increasing rates of occupancy, travel costs sharing, and reducing fuel consumption, carbon emissions and air pollution [5, 16]. Across the world, many providers offer online RSSs such as Careem, Uber, Lyft Line and Blablacar etc., [16]. According to [6], the ride-sharing market was valued at USD 182.12 billion in 2018 and is expected to reach USD 212.60 billion by 2026.

RSSs run as a central system where service providers represent a middleman. Users must share their information with these service providers, including pickup times, locations, and destinations. But running these services as a centralized platform, makes any system vulnerable to many problems [1, 4]. These problems namely single point-of-failure, less transparency, inflexibility, dictation of policies and service conditions [1, 4, 7, 16]. Moreover, central server maintenance and management are expensive and highly vulnerable to several attacks including distributed denial of service (DDoS) [7, 16]. In addition to these issues, if the service provider's security is compromised, then its services will be interrupted and thus the data can be revealed, modified, or even deleted [7]. For example, in late 2016, a huge data leakage has occurred for Uber [8]. This leakage included data of 57 million users. As a results, Uber paid 148 million dollars to settle the investigation to this data leakage.

Recently, researchers suggested moving from central RSSs to decentralized ones [1, 2, 3, 5, 7, 16]. Blockchain is one of the recent, important, popular, and most attractive technologies which changing the centralization concept in various domain [2, 4, 9]. Decentralization, immutability, and transparency are the most attractive features of blockchain. These features help blockchain to achieve its goal of shifting from centralized to decentralized in various systems. Blockchain has brought many features to ride-sharing platforms as allowing direct connection between people and drivers who is wanting to transport them and thus cooperative management between them is facilitated [1, 7, 16]. Participants, drivers, and riders share transaction data across a large network of nodes rather than the agreement on one centralized trusted authority. This removes middlemen which performs any role of gatekeeping. Transactions are maintained in a data structure in a distributed and transparent manner. Moreover, they are accessed by all nodes and managed by computers network called miners which run peer-to-peer (p2p) protocol.

1.1. *Contributions*

The blockchain technology is particularly useful for ride-sharing applications based on two aspects. The blockchain's structural aspect - the technology is designed in a way which allows it to provide security services and data integrity without the dependency on a trustworthiness third-party. The other aspect is the smart contracts functionality, which provide a mechanism to perform complex tasks and allow intelligent interaction for many nodes or users. This paper goal is to give an in-depth look to the technical concepts and research developments in blockchain-based RSSs.

To the best of our knowledge, there is only one survey [14] which addressed p2p or blockchain-based RSSs. But this survey has not included several papers in the blockchain-based RSSs. It discussed only seven papers and didn't perform any analysis, comparison nor evaluation of them. Thus, The area of blockchain-based ride-sharing services lack to a comprehensive survey. So, the main contributions of this paper are as follow.

- A brief introduction to ride-sharing, intelligent transportation systems, blockchain with its related concepts, and smart contracts.
- Each research paper, in the area of blockchain-based RSSs, is studied intensively and then a summary of this study is presented.
- Then, all surveyed papers are analyzed, compared, and classified from various perspectives based on blockchain type and platform used, and finally evaluated.
- Finally, we highlight major research challenges and give future directions of research in the area of blockchain-based RSSs.

1.2. *Organization*

The organization of this paper is as follows. The introduction is presented in section 1. Section 2 presents the background knowledge required in this paper. Section 3 explains, studies, analyzes, and classifies the previously proposed blockchain-based RSSs. The discussion and future directions are explained in section 4. Section 5 concludes this paper.

2. Background Knowledge

This section gives a brief background on ITSs, RSSs, blockchain technology and smart contracts. Table 1 displays the abbreviations used in this paper.

Table 1. Abbreviations used in this paper

Notation	Meaning
DApp	Decentralized Application
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DPoS	Delegated Proof-of-Stake
ECDSA	Elliptic curve digital signature algorithm
GPS	Global Positioning System
IoT	Internet of Things
ITS	Intelligent Transportation System
P2P	Peer-to-Peer
PoA	Proof-of-Authority
PoM	Proof-of-Movement
PoS	Proof-of-Stake
PoW	Proof-of-Work
RSS	Ride-sharing service
SHA	Secure Hash Algorithm

2.1. *Intelligent Transportation Systems (ITSs)*

ITSs are the future of transportation [2, 3]. They have been emerged, in the last two decades, to improve transportation systems performance, to enhance travel security and mobility, and to reduce harmful effects of traffic such as road accidents and air pollution, etc., [5, 10]. They are a step towards smart cities and sharing economy and are considered to be part of internet of things (IoT) [1, 2, 11, 12]. ITS is defined as the implementation of information technologies and communications in the transportation systems [3, 12]. It integrates vehicles, people, and roads by utilizing advanced information and communication technologies. The "intelligence", in intelligent TS, refers to the transformation of the generated data from ITSs into meaningful information useful for individuals and the economy [13]. Smart cities, also called intelligent environments, exploit ITS to achieve their goal. They are defined as intelligent environment that embeds information and communication technologies to create interactive systems. ITS helps smart cities to provide comprehensive optimization of the urban mobility. In addition, it eases traffic flow in these cities by reducing travel time, bringing greater safety to drivers, and comfort and entertainment to passengers. ITS gives applications and services which address and solve transportation problems of smart cities.

ITS has various applications scenarios that can be enhanced with the blockchain. These applications are fall in eight categories which are [2]: (i) protection and management of data which aim to provide solutions to manage and protect generated data from ITS's elements of vehicles, users, and other devices; (ii) trading of resources and data which concern on facilitating data and resources trading of ITS with other businesses; (iii) sharing resources aims to sharing un-used computational resources among ITS's entities of vehicles, stationary, running entities, etc.; (iv) management of vehicles where smart parking and car platooning are popular examples of vehicle management; (v) forensics applications which includes traffic data analysis, in particular, for autonomous vehicles; (vi) content broadcasting aims to improve the services of in-vehicle and safety via propagate non-safety and safety contents through vehicles and other entities which may be semi-trusted, non-trusted, and attack-prone; (vii) traffic management and control which allows dynamic traffic control and management, traffic condition monitoring, and traffic congestion mitigation through data generated by vehicles and other entities; and (viii) ride-sharing which allows people having the same destination to share the same car. More details on ITS's categories can be found in [2]. The focus of this paper is on ride-sharing applications due to its importance in helping ITS to achieve its goal. Ride-sharing is explained in the following subsection.

2.2. *Ride-sharing*

Ride-sharing is one of the ITS's applications which helps it achieve its goal [1, 2]. Sharing rides represents a sharing economy example [16]. This economy promotes economic activities sharing in a p2p way [15]. Ride-sharing represents a decentralized decision-making model because users are often self-interested and only motivated to team up with each other based on individual objectives [15]. Improving ride-sharing has a great effect in improving ITS and consequently mitigating and overcoming its long-standing problems. These problems are traffic congestion, road accidents, delay, high operation costs, low efficiency, and security risks of data storage in traditional centralized systems [2, 3, 16, 17]. RSSs become popular via some noticeable service providers like Uber because of the convenient usage of travelling [7, 16]. They have received significant attention because of their importance in reducing the number of vehicles and consequently minimizing congestion and traffic overhead emission of gases etc.

Ride-sharing is also known as carpooling [15, 19, 20, 21]. In addition, ride-hailing (RHSs) and RSSs are interchangeable terminologies, but in fact, there is difference between them [18, 22, 23]. The ride-hailing term refers to companies such as Uber and Careem. It enables riders to request a specific ride from their current location to a specified destination. While the term ride-sharing describes situations where a rider accompanies a driver for a portion of a trip. This trip is pre-planned by the driver and it will being held with riders or without them. In ride-sharing, the vast majority of drivers plans a ride for themselves in the first place and then offer to share the ride with others. While in ride-hailing, drivers make on-demand rides based on riders’ requests; therefore, drivers have relatively strong origin constraints and no route or destination constraints.

Existing RSS can be categorized into centralized and decentralized [24 - 25]. Figs. 1 illustrates the general architecture for each of the centralized and decentralized RS. In centralized RSS [50], service provider represents a middleman which provides services namely handling incoming ride-requests, matching riders with available drivers, calculating and estimating fares, ride payment and reputation management. For these services, it charges a fee for each ride completed successfully e.g., Uber deducted around 25% from the fare [16]. Some service providers also sell data of rides or traces to third parties e.g., for planning for city or marketing. To use an RSS, riders and drivers need an account, a global positioning system (GPS) equipped smartphone with the service provider's installed app, web or mobile, and an active Internet connection. The steps involved in the process are as follows [25].

1) A rider looks for a ride via an app, web or mobile, of the corresponding service provider.
2) Then, the rider enters its request details namely pick-up and drop-off locations, time, persons number, car type, and payment mode.
3) The rider's request is received by the service provider. Then, this request is queued in the app and then is oriented to the nearby driver through matching.
4) The matched driver and rider exchange information with each other.
5) Once the trip is completed, the user will pay the trip fare to the service provider through the app. Then, the service provider will send the driver’s charge after discussed pre-specified commission value.

6) Also, all transactions and information exchange are performed via the service provider which has control over all processes and data.

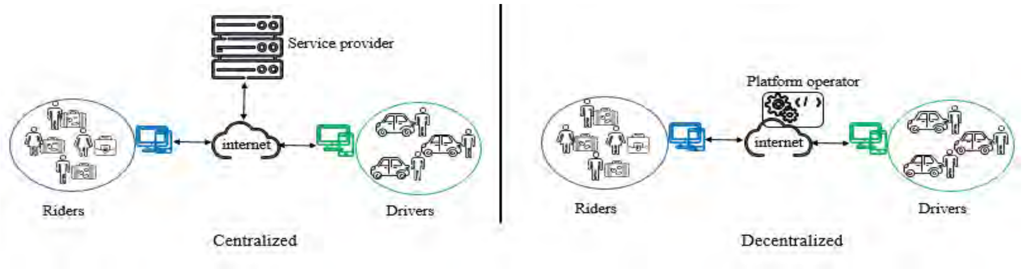

Fig. 1. Centralized vs. decentralized RSS

In contrast, decentralized RSS eliminates the role of the service provider and replaces it with a platform operator which enables p2p sharing of rides [21, 25]. Drivers and riders are directly connected through the platform operator. In p2p interaction, drivers provide their offers to riders and get fare from them after ride completed, while riders pay rides' fees to drivers directly. The platform operator operates like any third party to match drivers with riders and estimate trips fares.

Table 2 gives a comparison between centralized and decentralized RSS. In centralized RSS, the system is controlled by central authority, which leads to a high cost in providing services to end users. This rise in cost is due to the additional fees added to the actual cost by service providers which are about 20-25% [16]. While, in decentralized RSS, the additional fees from the service providers are eliminated and thus the cost is less. Users' data is not private in centralized RSS because this data is revealed to service providers and may also other users or companies. In contrast, in decentralized RSS, the privacy issues are less because of the absence of service providers. For security, the data stored in centralized RSS are not secure and vulnerable to attacks, while the data stored in decentralized RSS is stored cryptographically, tamper-resistance, and in integral way and thus more secure than the centralized RSS's data.

Table 2. Centralized vs decentralized RSS

	Centralized RSS	**Decentralized RSS**
Architecture	Centralized	Decentralized
Cost	High cost	Low cost
Privacy	No privacy	Less privacy issues
Security	No security	More secure
Transparency	lack transparency	Transparent
Safety	Not safe	Safe

Moreover, centralized RSS lacks to transparency as transactions can't be viewed or tracked, in contrast, decentralized RSS is transparent as all transactions are available to all users to view or track. Finally, centralized RSS is not safe for users, while decentralized RSS is safe because of DApps reliability, and the payment is done directly. Blockchain is one of the recent, and most attractive technologies which changing the centralization concept in various domain [2, 4, 9].

2.3. *Blockchain*

Blockchain is rapidly gaining attraction in fields such as transportation, finance, smart cities, supply chain management, and many others [1, 2, 4, 9]. It is a technology where its infancy in the Bitcoin's whitepaper [26] by Satoshi Nakamoto. It is known formally as a distributed ledger technology. Blockchain represents a data structure which holds records of digital transactions. Multiple different nodes, i.e., computing machines, store identical copies of the blockchain. They are connected in a p2p network. The blockchain structure is depicted in Fig. 2; Wherein, the fundamental units of blockchain are transactions and a group of them are stored in a block. A chain of blocks is formed by continuously appending them in sequence. The decentralization importance is emphasized in the blockchain by enabling most of the participating nodes to collectively take the decision through a process known as consensus mechanism.

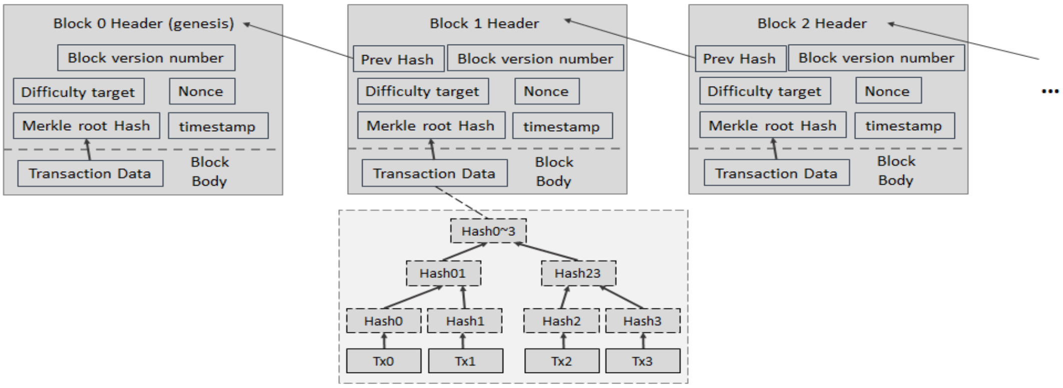

Fig. 2. Blockchain structure

The core ideas and concepts, where blockchain is built on, are briefly explained as follow [4, 9, 27].

1) *Hashing*. The blockchain backbone is the hashing algorithms which are exploited in hashing blockchain transactional data and blocks' headers. A hash function is a cryptographic algorithm which accepts inputs of variable sizes and returns an output of fixed length, called a hash. The popular hashing algorithms are the secure hash algorithm (SHA) family, i.e., SHA-1 and SHA-2. Two conditions which determine the good hash algorithm: a) non-invertible, i.e., it should not be possible to get the input from the output. b) very small chances or net of getting the same output hash from two different inputs. These two conditions are useful for security where a small input change will completely change the hash value, and that makes tampering evident.
2) *Blocks*. Blocks are the components of blockchain. They usually consist of a bodies and headers. The block's body contains transactions. The block header includes different information, namely Merkle tree root of transactions, timestamp, block version, and previous block’s header’s hash. These stored hash values provide transactions immutability. Wherein, the change in a transaction of any block will change the block header, and the hash value will not be the same as the stored in the successive block, and thus tampering is evident. A process called mining is applied to each block to validated it which works according to the consensus algorithm. The data immutability exists in blockchain because malicious nodes or users will not be able to meet the rules for this mining process. Therefore, they cannot change the hash values of subsequent blocks to achieve any tampering. Thus, the mining process needs to be done for all subsequent blocks if a certain block is modified after creation and added to the chain, which is impossible practically. The blockchain is public, so its nodes will be able to view but not modifying its contents.

3) *Node*. It is the basic part of the architecture of the blockchain. Nodes are users or highly configured computers. They play a major role in the transactions involved in the blockchain. Moreover, each node maintains a copy of the blockchain ledger.
4) *Mining*. Blocks addition to the blockchain is done through a process called mining. This process works according to the specified consensus protocol which specifies which miner's block added to the blockchain. For instance, in bitcoin, it works according to the proof-of-work (PoW) consensus protocol. In PoW, the first miner who solves the PoW puzzle will be permitted to add his block to the blockchain and be rewarded. For instance, a Bitcoin miner, currently, is rewarded 12.5 bitcoin for each new block addition to the blockchain.
5) *Consensus*. Group of rules which must be followed during the transactions in the blockchain is called as Consensus protocol [27]. The blockchain technology provides trust between end users through this protocol which guarantees a trust level in transferring or updating data. Transmitting data occurs anonymously in the form of a blockchain address and hence the trust between the end-users is preserved. Some well-known consensus protocols are PoW, proof-of-stake (PoS), etc., which are well-described in [27].
6) *Miner*. A special node with the ability of new blocks addition to the blockchain is called miner. Miners can perform several processes of validation, verification, and authentication of other nodes. They work according to the specified consensus protocol. Once miners validate and authenticate a transaction, the amount is transferred from the sender’s wallet to the receiver’s wallet.
7) *Digital Signatures.* The core concept in the blockchain is the public key cryptography which assigns two keys to each node, private and public. Private key encrypts anything which is decrypted only through the public key. The public key is considered as the address for each node, and each digital asset is associated with its owner’s public key. To transfer data, a node needs to sign it with its private key in order to authenticate this data. Bitcoin depends on the elliptic curve digital signature algorithm (ECDSA) in providing public and private keys to nodes.

Fig. 3 puts all blockchain related concepts together and demonstrates the lifecycle of blockchain, which works as follows. At any time, a user may create a transaction to transfer money or assets. Then, s/he signs this transaction with her private key and then broadcasts it to all nodes of the blockchain network. The nodes i.e., miners, group a set of new transactions into a block and then start verifying i.e., mining, them. Moreover, they will also create the header of the block and subsequently broadcast it to other nodes. Each node competes to verify the block first by performing a pre-decided consensus protocol. The miner who mines the block first broadcasts it urgently to all other miners on the blockchain network. Other miners check the validity of the broadcasted mined block. If this block is mined correctly, then other miners accept it as a valid block and add it to their blockchain replica by start mining the next block using the hash of the accepted block as the previous hash. Thereby, the accepted block is added to the blockchain, and all its transactions are confirmed to the corresponding users as completed successfully. This lifecycle of blockchain workflow starts again for other new transactions.

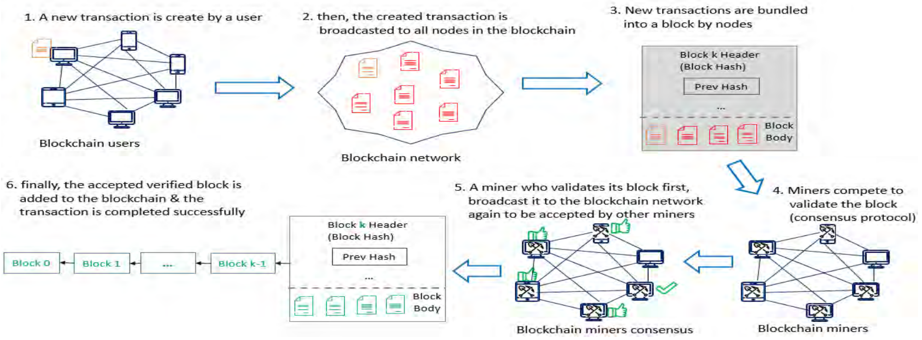
1. A new transaction is create by a user
Blockchain users
2. then, the created transaction is broadcasted to all nodes in the blockchain
Blockchain network
3. New transactions are bundled into a block by nodes
Block k Header (Block Hash)
Prev Hash
...
Block Body
4. Miners compete to validate the block (consensus protocol)
Blockchain miners
5. A miner who validates its block first, broadcast it to the blockchain network again to be accepted by other miners
Blockchain miners consensus
6. finally, the accepted verified block is added to the blockchain & the transaction is completed successfully
Block 0
Block 1
...
Block k-1
Block k Header (Block Hash)
Prev Hash
...
Block Body

Fig. 3. Blockchain lifecycle - how blockchain works

2.4. *Smart contracts*

The "smart contract" terminology was first introduced in the mid-1990 by Nick Szabo, a computer scientist and cryptographer who invented a virtual currency called "Bit Gold" in 1988. In his paper, Szabo defined a smart contract as "*set of promises, specified in a digital form, including protocols within which the parties perform on these promises*" [28]. Szabo's conception of the smart contract idea was based on the fact that those contracts could be built in a program form that would be executed exactly as designed. Then in [29], Szabo imagined that smart contracts can and be embedded in all sorts of properties. And thus, these properties are controlled by digital means which ensure that the associated contractual provisions are automatically executed. Nevertheless, the smart contracts didn't see the light except in the current era, thanks to the emergence of blockchain technology [30].

In general, smart contracts can be defined as a special-type computer program that is self-executed, self-verified, and self-enforced the conditions of agreement between two or more parties, e.g., seller and buyer [9, 30]. They differ from standard software programs because their execution is independent from any centralized or trusted third parties. Smart contracts programs are stored and executed on a blockchain. And with this, it is replicated across multiple nodes of the blockchain and benefits from the security, permanence, immutability, and traceability of blockchain. Smart contracts allow trusted transactions and agreements to be executed among distributed, anonymous parties without the need for submitting under control of central authority [35].

Table 3 demonstrates the differences between conventional or paper-based contracts and smart contracts [9]. A third party, like lawyer or government, must be exist in paper-based contracts, which is not required in the case of smart contracts. The processing of paper-based contracts may take days which is long compared to the time needed to process smart contracts, minutes. Smart contracts are transparent where all contract participants can view and track them at any time. This transparency is not available in paper-based contracts. The execution of paper-based contracts is manual, which is automatic in smart contracts. Thus, smart contracts are high accurate than paper-based contracts. Moreover, they are cheap than paper-based contracts. For security, paper-based contracts are limited in their security, which is high in smart contracts. Finally, smart contracts are signed digitally while paper-based contracts are signed manually.

Table 3. Paper-based contracts vs. Smart contracts [9]

Parameter	**Paper-based contract**	**Smart contract**
Third party	Lawyers, Government, etc.	Not required
Processing time	In days (slow)	In minutes (fast)
Transparency	Not available	Available at any time
Automation	Manual	Fully automated
Accuracy	Less accurate	Highly accurate
Security	Limited	Cryptographically secured
Cost	Expensive	Cheap
Signature	Manual	Digital signature

3. **Blockchain-based Ride-Sharing**

Blockchain-based ride-sharing services (RSS) are gaining traction because of allowing direction connection between people and drivers who is wanting to transport them [1]. They can mitigate the issues of privacy violation, security, and transparency lacks, etc., through cooperative management facilitation between passengers and drivers. Moreover, the agreement on one centralized trusted authority is replaced by shared transactional data between participants across a large network of nodes. Thus, intermediaries are eliminated who perform any role of gatekeeping. In addition, transactions are maintained in a ledger which is distributed and accessed by all blockchain nodes making it more transparent. Blockchain-based ride-sharing systems have a goal of building a worldwide, decentralized, private, anonymous, and auditable ride-sharing network to optimize empty seats and unused cargo spaces [3]. One of the main distinctive features of these applications from other ride-sharing networks like Uber is the decentralized authority.

Blockchain-based ride-sharing systems should satisfy various security requirements to increase their robustness [51]. Security requirements that should be addressed in blockchain-based ride-sharing applications were collected from papers such as [51], [52] and others. Then, these requirements were redefined to accommodate the RSS domain of this paper. Blockchain can provide some of these requirements implicitly [51] which are:

- *Decentralization*. Blockchain removes any third parties via enabling P2P networks where transactions are verified by some of its nodes. Thus, users' privacy is preserved through canceling the need for sharing their details with third parties.
- *Tamper-resistance*. It is difficult to tamper the recorded data in the blockchain due to the organization of these data in special structures. These structures are chain of hashes where the hash of each block is included in the previous block. Thus, irreversibility and immutability are ensured because data tampering in any block will change its hash value and then disconnected it from the blockchain.
- *Unforgeability*. It means the network ability to resist adversaries from forging users' digital signatures or data. The combination of decentralization with digitally signed transactions for blockchain guarantees and ensures that any adversary cannot pose as other user.
- *Traceability*. The cryptographic hash of each block is included in the previous block, thus achieving traceability. Any node can trace and verify data correspondence.
- *Public audit*. The consensus mechanism of blockchain helps in implementing public audits. Created blocks by miners must satisfy the used consensus mechanism criteria and then independently verified by other nodes in the network.

Apart from the above security requirements, other requirements are listed, and detailed as follow [51-52].

- *Security*. The proposed system must provide integrity of data, confidentiality of data, authentication anonymously, and authentication of location.
- *Privacy*. (1) Anonymity: during a ride, a user's location and identity should be protected from others. (2) Unlink-ability: a user's requests or responses should not be linked together. (3) Traceability: any node should not be able to know a user's real identity. (4) Transaction privacy: transaction details, i.e., sender, receiver, or transferred amount, should be protected from irrelevant users.
- *Auditability*. All users can maintain a copy of the ledger and rides' transactions in this ledger can be verified by any parties.
- *Fairness*. It guarantees that a rider will be matched with an appropriate driver, and a driver will receive a ride fare after a ride.
- *Efficiency*. Computational costs and communication overheads should be minimized as possible during all phases, such as matching, requesting a ride, and responding to ride.
- *Scalability*. It guarantees the ability of any proposed system to be efficient even in case of there are large number of riders and drivers. In blockchain-based ride-sharing systems, the scalability measure is the ability of the blockchain to manage large volumes of transactions. Some ways to achieve

scalability are minimizing the computational overhead and a dynamic consensus algorithm that adapts to the traffic volume.

3.1. *Blockchain-based ride-sharing state-of-arts*

For this paper, we perform intensive search on various research sources namely IEEE Access, Google Scholar, Semantic Scholar, and ResearchGate, and others. During the search on these sources, the used keywords are "*blockchain & ride sharing*", "*blockchain & ride hailing*", and "*blockchain & carpooling*". After search and filtering of result papers, the matched papers count thirty-one. These papers are categorized in subsections 3.2 and 3.3 and are analyzed in subsection 3.4. Table 4 provides a summary of these previously proposed ride-sharing papers, specifically blockchain-based ones. It includes thirty-one papers, twenty-nine papers are decentralized and blockchain-based while only two papers are centralized. These two papers, [18] and [33], are included in our survey because they had a great attention from the research community. Table 4 provides, for each paper, a brief description, the issue, and challenge which are addressed, the implemented consensus protocol and publication year, respectively. Some papers don't explain the used consensus protocol, so we leave it blank.

Table 4. Summary of blockchain-based ride-sharing state-of-arts

Paper	**Brief description**	**Main issue or challenge**	**Consensus protocol**	**Year**
[1]	Provided a preliminary study of blockchain-based ITS and given the base of the new ITS-oriented blockchain model. Proposed also a real-time blockchain-based ride-sharing platform called La'Zooz.	Centralization	PoM	2016
[7]	Exploited consortium blockchain along with smart contracts to overcomes the raised concerns of the current centralized ride-hailing services	Centralization	DPoS	2020
[16], [31]	Exploited public blockchain and smart contracts to allow users i.e., drivers and riders, to interact directly without the rely on a third party	Privacy, trust	PoA	2019, 2020
[32]	Proposed a scheme for ride sharing based on blockchain and vehicular fog computing. The proposed scheme allows fog nodes to match users locally.	Matching	PoS	2019
[15]	Highlighted on mechanisms of fair cost-sharing for decentralized ride-sharing systems.	Fair cost sharing, matching	____	2020
[33]	Proposed a practical solution for service provider which efficiently matches riders and rivers while preserving-privacy	Matching	____	2017
[18]	Proposed a new privacy-preserving protocol which protected users' privacy against service providers and curious users.	Matching	____	2018
[6]	Proposed reputation-enabled privacy-preserving decentralized P2P ride-sharing network.	Centralization		2016
[19]	Studied the benefits of utilizing blockchain features of decentralization and distribution to build ride-sharing application namely GreenRide.	Centralization		2019
[34]	Focused on utilizing blockchain inherits features, i.e., transparency, decentralization, and distribution, for ensuring fairness in car-sharing.	Centralization	PoA	2019

[35]	Illustrated that using blockchain, cryptocurrency, and smart contracts in ride-hailing services can preserve location privacy, pseudonym of users and also could be trust	Centralization	____	2018
[36]	Proposed Co-Ride which is a decentralized ride-hailing service which utilized fog computing, blockchain, and smart contracts. It targeted the collaboration of rides and commercial ride-hailing service like Uber, Lyft, Didi, etc.,	Information isolation, centralization	PoS	2019
[20]	Proposed a framework for securing ride-sharing via blockchain inherit features.	Centralization, privacy	Improved DPoS	2021
[37]	Proposed blockchain-based architecture based on proxy re-encryption scheme which then integrated with smart contracts to protect carpooling data and thus enhance privacy	Privacy	____	2020
[21]	Proposed the exploitation of blockchain smart contracts in ride-sharing systems to overcome its centralization problems	Centralization	____	2021

Table 4. (Continued) Summary of blockchain-based ride-sharing state-of-arts

Paper	**Brief description**	**Main issue or challenge**	**Consensus protocol**	**Year**
[38]	Proposed a novel secure billing protocol based on blockchain smart contracts for ride-sharing services which eliminate the presence of the online third party.	Payment	____	2019
[39]	Presented a novel identity verification system for existing ride-sharing systems. Privacy-preserving and safe digital identity verification was achieved through exploiting a permissioned blockchain and zero-knowledge proof.	Identity verification	____	2020
[25]	Proposed an improved version of existing blockchain-based framework which replaces centralized framework for an RSS. Then this framework is implemented as smart contracts-based decentralized application (DApp). To save riders' travel distance, this paper utilized a matching algorithm called min to match riders with drivers.	Centralization, Matching	____	2021
[22], [41]	Proposed a framework to develop a decentralized architecture for ride-hailing based on the blockchain and chaincode i.e., smart contracts in Hyperledger Fabric.	Centralization	____	2019, 2021
[24]	Proposed a Blockchain-based ride-sharing system with accurate matching and privacy preservation	Privacy and matching	PoS	2021
[40]	Introduced only the blockchain technology in ride-sharing to implement a new decentralized application (DApp).	Centralization	____	2021
[23]	Improved the security and intelligence of a ride-hailing system based on the integration of machine learning and blockchain into a proposed framework.	Mutable data, security	____	2022
[42]	Proposed a privacy protection scheme for carpooling service using fog `computing.	Security and privacy	____	2020
[43]	Proposed a way to ascertain the security of ride-sharing which is predicated on private blockchain	Security, centralization		2021
[44]	Presented a fully decentralized and privacy-preserving ride-sharing solution where the blockchain plays the role of the marketplace to	Centralization	____	2019

	compute the prices and provide proven trust between clients and providers.			
[45]	Proposed the utilization of the blockchain and an incentive mechanism in managing a decentralized ride-sharing system in a way trustworthy and transparent.	Centralization	____	2018
[46]	Presented a decentralized application for ride-sharing where all transactions, fare calculation, matching and information are stored on a Distributed Ledger.	Centralization	____	2021
[47]	Proposed a ride-sharing system, called SmaRi, which provided a more flexible management structure and enhanced the interactions between drivers and passengers.	Centralization	____	2018
[48]	Presented blockchain-based ride-sharing platform called ARCADE city.	Centralization	____	2015
[49]	Presented blockchain-based ride-sharing platform called DACSEE	Centralization	____	2018

3.2. *Categorization based on blockchain type*

Blockchain can be divided into two major categories, permissionless and permissioned [9, 22, 27]:

1) *Permissionless.* The permissionless blockchain enables every- and anyone to join it at any time where there is no authorization for joining and leaving. *Public blockchain* is the example of this blockchain type. It allows anyone to access the network with the ability to enter and exit it at any time. Its transactional data is visible for everyone to read and write. Whereas participant nodes can read, write, or validate on this public instance based on common rules and if they have a valid pseudonym (account address). Furthermore, everyone can have a copy of the blockchain, and data cannot be altered by anyone. In case of a change happened in the blockchain, all nodes notified and know this change.
2) *Permissioned.* This blockchain type requires that participants to be authorized before accessing or joining the blockchain network instance and their identities are revealed. Thus, only specific, and identifiable nodes can perform certain tasks. The identity revealing and the effective control the permission blockchain make it a perfect fit for internal or multi-party business application. Meanwhile, the limit size of the permissioned blockchain instance allows the use of efficient consensus protocol and thus achieving higher transactions processing and capacity. Permissioned blockchain is also classified into private and consortium.
    - *Private blockchain.* The governance of the private blockchain network and the consensus are under the control of a single private organization. It only allows for a selected nodes to access the blockchain. These restrictions provide advantages of quicker block creation where mining a block takes less than a minute. In this blockchain type, accessing transactions is allowed only for nodes who authorized to access the private blockchain network. Thus, a complete trusting and secure transaction occur. Moreover, the nodes involved in the transactions can be easily identified. In the case of any harmful occurred to the blockchain, the misbehaving node's identity can be traced. The speed and efficiency are not affected by the network growth, because transactions are performed by only a few authorized nodes. But the private blockchain suffers from the main disadvantage of centralization, as the network is controlled by only one organization.
    - *Consortium or federated blockchain.* In this blockchain type, the network is under the control of more than organization. Moreover, features of public and private blockchains are included in consortium blockchain types. Only the nodes of the consortium organizations are allowed to access the blockchain ledger. So, this blockchain type is considered as permissioned. It is called a “decentralized based consortium blockchain” because the validation process of any transaction is performed via the decision of multiple organizations.

Table 5 illustrates the categorization of the surveyed blockchain-based RSS papers based on the type of blockchain. It consists of two columns, one for the aforementioned three blockchain types and the other column contains the papers which exploited the corresponding category.

Table 5. Categorization based on blockchain type

Blockchain type	References
Public	[1], [16], [21], [24], [25], [31], [44]
Consortium	[7], [20], [22], [23], [36], [37], [39], [41], [42]
Private	[19], [23], [32], [34], [39], [43]

3.3. *Categorization based on platform*

Many platforms have been appeared as wider application scenarios of blockchain since Bitcoin release as open-source software in 2009. They come with various tools to enable the building of blockchain applications. Blockchain platforms are varied based on the options they offer - for instance, the Hyperledger platform offers several frameworks and is designed for different applications. Another platform is Ethereum which is popular and likes Bitcoin. Ethereum has its own cryptocurrency, called Ether, while Hyperledger is not associated with any token. Platforms, like Ethereum, are useful when blockchain is used for real-world market interactions. For example, in trading of energy application, Ether can be earned through the mining process, or the energy purchasing at charging stations. In general, the different criteria which differentiate between blockchain platforms are support of smart contract, scalability, crash fault tolerance, throughput, and consensus mechanism. Moreover, technical specifications are highly varied between platforms. The considered research papers are in the following two categories:

1) *Ethereum*. Ethereum platform enables the creation of smart contracts in Solidity, a Turing-complete language. In practical, Ethereum smart contracts represent accounts like normal users' accounts, but they contain executable bytecode rather than cryptocurrencies. This bytecode controls the smart contract behavior. During transactions, the stored code of the smart contract-owned account is executed, and its changes is recorded by the Ethereum Virtual Machine.
2) *Hyperledger Fabric*. Hyperledger Fabric platform is an open-source project which is maintained by the Hyperledger community. It is designed for the use in enterprises. It is the first platform to support smart contracts in general-purpose programming languages such as Java, Go, and Node.js. hyperledger is a permissioned platform where participants are known to each other unlike permissionless networks where participants are not known.

Based on that, table 6 illustrates the categorization of the surveyed papers based on the blockchain platform which was addressed. It consists of two columns, one for the blockchain platform and the other for the list of papers which fall in this platform category.

Table 6. Categorization based on blockchain platform

Blockchain platform	References
Ethereum	[1], [7], [16], [19], [21], [24], [25], [31], [34], [36], [40], [46]
Hyperledger Fabric	[22], [23], [32], [37], [39], [41], [43]

3.4. *Analysis of blockchain-based RSS state-of-arts*

This subsection analyzes, in detail, the blockchain-based RSS state-of-arts. Some security requirements are implicitly provided by the blockchain technology namely decentralization, traceability, auditability tamper-resistance of transactional data [51]. Other security requirements should be explicitly managed such as privacy, security, reputation, etc., [51-52]. Table 7 presents a detailed analysis and comparison of blockchain-based RSS papers. It is built based on the addressed security requirements in each paper. Table 7's columns refer to the security requirements which were addressed in each surveyed paper. These security requirements are described in section 3 (3. Blockchain-based ride-sharing). Table 7's columns description, in order, are:

- *Privacy (P)*. It indicates the privacy provided by the paper's proposal.
- *Security1 (S1)*. It refers to the security provided by the inherit feature of blockchain. This security is achieved through cryptographic hashing of blockchain data.
- *Security2 (S2)*. It represents the security provided by a paper beyond the blockchain security, such as authentication of locations and users, confidentiality.
- *Decentralization (D)*. it refers to the decentralization of storage and communication in the ride-sharing systems. It is implicitly provided by blockchain.
- *Trust (Ts)*. It refers to the trust level provided by ride-sharing service. This trust guarantees that a passenger gets his ride while a driver gets his fees.
- *Transparency (Tc)*. It refers to the ability of users to view their transactions and other related processes.
- *Reputation (R)*. It refers to that the ride-sharing system can provide a reputation for riders and drivers.
- *Auditability/traceability (A)*. It refers to the ability to audit and trace back the ride-sharing data.
- *Confidentiality (C)*. It refers to the ride-sharing system ability to keep its data secret.
- *Tamper-proof/Tamper-resistance (TP)*. It refers to the ride-sharing system ability to keep its data from any change.
- *Performance (Pr)*. It refers to the handling of the blockchain-based ride-sharing system performance, in terms of computational cost and communication overhead.
- *Verifiability (V)*. It refers to the ability to verify the ride-sharing data beyond blockchain verifiability.
- *Matching (M)*. It refers to the ride-sharing system ability to match users, i.e., drivers and riders.
- *Scalability (S)*. It refers to the ride-sharing system ability to scale with the increase of its data or nodes.
- *Fair payment (FP)*. It refers to the ride-sharing system ability to apply and calculate the payment in a fair way between users.

Table 7. Analysis of blockchain-based RSS's papers

	P	**S1**	**S2**	**D**	**Ts**	**Tc**	**R**	**A**	**C**	**TP**	**Pr**	**V**	**M**	**S**	**FP**
[1]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×
[7]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×
[16]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	✓
[31]	✓	✓	×	✓	×	✓	×	✓	✓	✓	×	×	×	×	×
[32]	✓	✓	✓	×	×	×	×	✓	✓	✓	✓	×	×	×	×
[33]	✓	×	✓	×	×	×	✓	×	✓	×	✓	×	×	×	×
[18]	✓	×	×	×	×	×	×	×	✓	×	✓	×	×	×	×
[6]	✓	×	×	✓	×	✓	✓	×	×	×	✓	×	×	×	×
[19]	×	✓	×	×	×	✓	×	✓	×	✓	×	×	×	×	×
[34]	×	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	×	×	×	×
[35]	✓	✓	×	✓	✓	✓	×	✓	✓	✓	×	×	×	×	×
[36]	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	×
[20]	✓	✓	✓	✓	×	×	✓	✓	✓	✓	✓	✓	×	×	×
[37]	✓	✓	×	✓	×	✓	×	✓	✓	✓	×	✓	×	×	×
[21]	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	×
[38]	×	✓	×	✓	✓	✓	×	✓	×	✓	×	×	×	×	✓
[39]	✓	✓	×	✓	×	✓	×	✓	✓	✓	✓	×	×	×	×

[25]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×
[22]	×	✓	×	✓	×	×	×	✓	×	✓	✓	×	×	×	×
[24]	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓	×	✓	×	×
[40]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×
[41]	×	✓	×	✓	×	✓	×	✓	×	✓	✓	×	×	×	×
[23]	×	✓	×	✓	×	✓	×	✓	×	✓	✓	×	×	×	×
[42]	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	×	✓	×	×
[43]	×	✓	×	×	×	×	×	✓	×	✓	✓	×	×	×	×
[44]	✓	✓	×	✓	×	✓	×	✓	✓	✓	×	×	×	×	×
[45]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×
[46]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	✓	×	×
[47]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×
[48]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×
[49]	×	✓	×	✓	×	✓	×	✓	×	✓	×	×	×	×	×

P: Privacy; S1: Security1; S2: Security2; D: Decentralization; Ts: Trust; Tc: Transparency; R: Reputation; A: Auditability; C: Confidentiality; TP: Tamper-Proof; Pr: Performance; V: Verifiability; M: Matching; S: Scalability; FP: Fair Payment;

In table 7, the mark (✓) means that the paper is addressed or achieved, partially or more, the corresponding requirement, while the mark (×) means that the paper was not addressed or achieved the corresponding requirement. For instance, the paper [4], of the third row, has the following:

- *Privacy (P)*. It addressed the privacy through cloaking algorithm which generalize location and times of users.
- *Security1 (S1)*. It addressed this security requirement via blockchain utilization.
- *Security2 (S2)*. It was partially addressed through anonymous authentication and data integrity of blockchain.
- *Decentralization (D)*. It was addressed through public blockchain employment.
- *Trust (Ts)*. It was addressed via the proposed time-locked protocol and zero-knowledge proof algorithm which guarantee that a passenger gets his ride while a driver gets his fees.
- *Transparency (Tc)*. It was addressed through blockchain.
- *Reputation (R)*. It was addressed via two indicators for evaluating each driver. One indicator is increased with every sent valid arrival proof to the pickup location. every time a driver sends a valid proof of arrival to the pickup location. While the other is increased with every ride completion.
- *Auditability/traceability (A)*. It was achieved through blockchain.
- *Confidentiality (C)*. It was addressed partially via privacy.
- *Tamper-proof/Tamper-resistance (TP)*. It was achieved via blockchain structure.
- *Performance (Pr)*. It is not measured in this paper.
- *Verifiability (V)*. It is not achieved.
- *Matching (M)*. It is not addressed.
- *Scalability (S)*. It is not addressed.
- *Fair payment (FP)*. It is not achieved.

4. Discussion and Future Directions

In this section, we discuss the presented details and comparisons of the surveyed RSS papers in section 3. Then, we present the future directions based on this discussion.

Based on our detailed survey and beyond blockchain inherit features such as decentralization, auditability, tamper-proof, and partial security, Fig. 4 illustrates the percent of addressing each parameter in the surveyed ride-sharing papers. This percent was calculated based on the thirty-one papers surveyed. For instance, privacy and performance requirement was addressed by fifteen different papers out of thirty-one. The confidentiality requirement was addressed by fourteen papers out of thirty-one. While scalability was not addressed anymore and thus count zero.

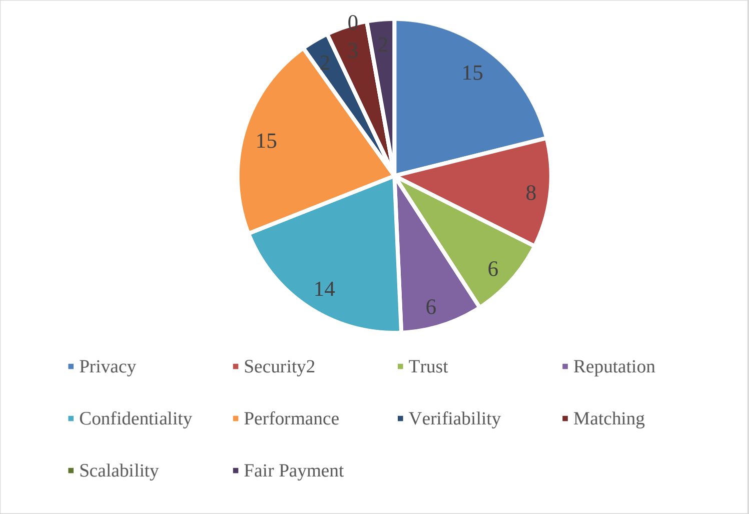

Fig. 4. Percent of security requirements addressed in RSS

From the performed detailed analysis, in this paper, and from Fig. 4, we deduce the following:

- Blockchain-based ride-sharing is still in its early stages.
- Most of the previous research has sought only to introduce the blockchain technology in the ride-sharing field in order to move it from centralization to decentralization. Refer to subsection 3.1.
- Some research papers addressed only the utilization of blockchain in ride-sharing, but others also enhanced their proposal beyond this utilization in privacy and confidentiality.
- The most usable blockchain platform is the Ethereum. Refer to subsection 3.3. The researchers are heading to the Ethereum because of its popularity, wider community, and usefulness in real-world transactions like ride-sharing.

Based on section 3, Fig. 4, and our discussion, we provide the following future directions in blockchain-based ride-sharing services:

- Intensive research and implementation in blockchain-based RSSs are still needed.
- Privacy and confidentiality are partially addressed in previous works. So, more improvements and contributions are still needed.
- In privacy, more techniques and algorithms need to be exploited and proposed in order to overcome high resources consumption of previously proposed works like [16], [21], and [31].
- Blockchain-based RSS application's performance needs to be addressed and measured in terms of computational cost and communication overhead.
- Trust, reputation, verifiability was addressed by very small papers, so they need more investigation.
- Matching users in RSS is a critical issue which affect application performance. So, more proposals and contributions are still needed.
- Despite of fair payment importance, it was addressed by only two papers. So, more contributions and scenarios for achieving fair payment in blockchain-based RSS are needed.
- Scalability, in terms of nodes and data, is never handled by any previous work.

- Exploiting other technologies, such as machine and deep learning, in blockchain-based RSS was only addressed by one paper [23]. Therefore, exploiting and integrating other technologies with blockchain for RSS still need more investigations.

5. Conclusions

Although centralized ride-sharing services are effective and popular, they still suffer from various deficiencies such as privacy violation, lack of security and transparency of transactional data, and users' safety. Blockchain-enabled ride-sharing services can help in mitigating these deficiencies. Besides, they provide more innovative functionality, ease of use and management. In this paper, we thoroughly reviewed, analyzed, classified, and discussed blockchain-based ride-sharing papers. We classify these papers based on the blockchain type they use and the blockchain platform they employ. We conclude that the blockchain-based ride-sharing is still in its early stages and still need intensive research. Moreover, this paper will act as a guide to the researchers who willing in blockchain-based solutions development for ride-sharing services.

References

[1] Y. Yuan and F.-Y. Wang, “Towards blockchain-based intelligent transportation systems,” in Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC), Rio de Janeiro, Brazil, 2016, pp. 2663–2668.

[2] M. B. Mollah et al., “Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey,” IEEE Internet Things J., vol. 8, no. 6, pp. 4157–4185, 2021, doi: 10.1109/JIOT.2020.3028368.

[3] M. T. Çaldağ and E. Gökalp, “Exploring critical success factors for blockchain-based intelligent transportation systems,” Emerg. Sci. J., vol. 4, no. Special Issue, pp. 27–44, 2020, doi: 10.28991/esj-2020-SP1-03.

[4] Y. Yuan and F.-Y. Wang, “Blockchain and cryptocurrencies: Model, techniques, and applications,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 48, no. 9, pp. 1421–1428, Sep. 2018.

[5] D. S´anchez, S. Mart´ınez, and J. Domingo-Ferrer, “Co-utile p2p ridesharing via decentralization and reputation management,” Transportation Research Part C: Emerging Technologies, vol. 73, pp. 147–166, June 2016.

[6] Ride sharing market. [Online]. Available: https://www.globenewswire.com/news-release/2021/12/01/2343775/0/en/Ride-Sharing-Market-Global-Statistics-2021-2028-Ride-Sharing-Industry-Size-Share-Growth-Factors-Forecast.html.

[7] S. Kudva, R. Norderhaug, S. Badsha, S. Sengupta, and A. S. M. Kayes, “PEBERS: Practical Ethereum Blockchain based Efficient Ride Hailing Service,” 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 422–428, 2020, doi: 10.1109/ICIoT48696.2020.9089473.

[8] Uber China data breach. [Online]. Available: https://www.nytimes.com/2018/09/26/technology/uder-data-breach.html.

[9] A. S. Rajasekaran, M. Azees, and F. Al-turjman, “A comprehensive survey on blockchain technology,” Sustain. Energy Technol. Assessments, vol. 52, no. PA, pp. 1–13, 2022, doi: 10.1016/j.seta.2022.102039.

[10] J. Zhang, F. Y. Wang, K. Wang, W. H. Lin, X. Xu, and C. Chen, “Data-driven intelligent transportation systems: A survey,” IEEE Trans. Intell. Transp. Syst., vol. 12, no. 4, pp. 1624–1639, 2011, doi: 10.1109/TITS.2011.2158001.

[11] Intelligent Transport Systems (ITS), chapter 13, in book: Recent Challenges in Science, Engineering, and Technology, 2021.

[12] S. R. Maskey, S. Badsha, S. Sengupta, and I. Khalil, “BITS: Blockchain based Intelligent Transportation System with Outlier Detection for Smart City,” 2020 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2020, 2020, doi: 10.1109/PerComWorkshops48775.2020.9156237.

[13] M. Zichichi, S. Ferretti, and G. D’Angelo, “A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems,” IEEE Access, vol. 8, pp. 100384–100402, 2020, doi: 10.1109/ACCESS.2020.2998012.

[14] R. Gupta, R. Gupta, and S. S. Shanbhag, “A Survey of Peer-to-Peer Ride Sharing Services using Blockchain,” Int. J. Eng. Res. Technol., vol. 10, no. 08, pp. 349–353, 2021.

[15] S. C. K. Chau, S. Shen, and Y. Zhou, “Decentralized Ride-Sharing and Vehicle-Pooling Based on Fair Cost-Sharing Mechanisms,” IEEE Trans. Intell. Transp. Syst., pp. 1–11, 2020, doi: 10.1109/TITS.2020.3030051.

[16] M. Baza, N. Lasla, M. Mahmoud, G. Srivastava, and M. Abdallah, “B-Ride: Ride-Sharing with Privacy-preservation, Trust and Fair Payment atop Public Blockchain,” IEEE Trans. Netw. Sci. Eng., vol. PP, no. c, pp. 1–16, 2019, doi: 10.1109/TNSE.2019.2959230.

[17] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang, and Y. Pei, “A Blockchain-Assisted Intelligent Transportation System Promoting Data Services with Privacy Protection,” Sensors (Special Issue Blockchain Secur. Priv. Internet Things), vol. 20, 2483, no. 9, pp. 1–22, 2020, doi: https://doi.org/10.3390/s20092483.

[18] U. M. Aïvodji, K. Huguenin, M. J. Huguet, and M.-O. Killijian, “SRide: A Privacy-Preserving Ridesharing System,” WiSec 2018 - Proc. 11th ACM Conf. Secur. Priv. Wirel. Mob. Networks, pp. 40–50, 2018, doi: 10.1145/3212480.3212483.

[19] S. Khanji and S. Assaf, “Boosting Ridesharing Efficiency Through Blockchain: GreenRide Application Case Study,” 2019 10th Int. Conf. Inf. Commun. Syst. ICICS 2019, pp. 224–229, 2019, doi: 10.1109/IACS.2019.8809108.

[20] D. Wang and X. Zhang, “Secure Ride-Sharing Services Based on a Consortium Blockchain,” IEEE Internet Things J., vol. 8, no. 4, pp. 2976–2991, 2021, doi: 10.1109/JIOT.2020.3023920.

[21] E. Vazquez and D. Landa-silva, “Towards Blockchain-based Ride-sharing Systems,” Proc. ofthe 10th Int. Conf. Oper. Res. Enterp. Syst. (ICORES 2021), pp. 446–452, 2021, doi: 10.5220/0010323204460452.

[22] R. Shivers, M. A. Rahman, and H. Shahriar, “Toward a Secure and Decentralized Blockchain-based Ride-Hailing Platform for Autonomous Vehicles,” arXiv:1910.00715v2, pp. 1–12, 2019, doi: 10.48550/arXiv.1910.00715.

[23] Z. Shahbazi and Y. Byun, “Blockchain and Machine Learning for Intelligent Multiple Factor-Based Ride-Hailing Services,” Comput. Mater. Contin., vol. 70, no. 3, pp. 4429–4446, 2022, doi: 10.32604/cmc.2022.019755.

[24] M. M. Badr, M. Baza, S. Abdelfattah, M. Mahmoud, and W. Alasmary, “Blockchain-Based Ride-Sharing System with Accurate Matching and Privacy-Preservation,” 2021 Int. Symp. Networks, Comput. Commun., 2021, doi: 10.1109/ISNCC52172.2021.9615661.

[25] S. A. Renu and B. G. Banik, “Implementation of a Secure Ride-Sharing DApp Using Smart Contracts on Ethereum Blockchain,” Int. J. Saf. Secur. Eng., vol. 11, no. 2, pp. 167–173, 2021, doi: https://doi.org/10.18280/ijsse.110205.

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

[27] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, “A Survey of Distributed Consensus Protocols for Blockchain Networks,” IEEE Commun. Surv. Tutorials, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.

[28] N. Szabo. (1996). "Smart Contracts: Building Blocks for Digital Markets". [Online]. Available:http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[29] N. Szabo. (1997). The Idea of Smart Contracts. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html.

[30] V. Buterin, “Ethereum white paper: a next generation smart contract & decentralized application platform,” First version, 2014, [Online]. Available:http://blockchainlab.com/pdf/Ethereum_white_paper_a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[31] M. Baza, M. Mahmoud, G. Srivastava, W. Alasmary, and M. Younis, “A Light Blockchain-Powered Privacy-Preserving Organization Scheme for Ride Sharing Services,” 2020 IEEE 91st Veh. Technol. Conf., pp. 1–6, 2020, doi: 10.1109/VTC2020-Spring48590.2020.9129197.

[32] M. Li, L. Zhu, and X. Lin, “Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing,” IEEE Internet Things J., vol. 6, no. 3, pp. 4573–4584, 2019, doi: 10.1109/JIOT.2018.2868076.

[33] A. Pham, I. Dacosta, G. Endignoux, J. R. Troncoso-Pastoriza, K. Huguenin, and J. Hubaux, “ORide : A Privacy-Preserving yet Accountable Ride-Hailing Service,” Proc. 26th USENIX Secur. Symp., 2017, [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-pham.pdf.

[34] P. Pal and S. Ruj, “BlockV: A Blockchain Enabled Peer-Peer Ride Sharing Service,” Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019, pp. 463–468, 2019, doi: 10.1109/Blockchain.2019.00070.

[35] Y. Kanza and E. Safra, “Cryptotransport: Blockchain-Powered Ride Hailing While Preserving Privacy, Pseudonymity and Trust,” GIS Proc. ACM Int. Symp. Adv. Geogr. Inf. Syst., pp. 540–543, 2018, doi: 10.1145/3274895.3274986.

[36] M. Li, L. Z. B, and X. Lin, “CoRide : A Privacy-Preserving Collaborative-Ride Hailing Service Using Blockchain-Assisted Vehicular Fog Computing,” Int. Conf. Secur. Priv. Commun. Syst. Springer, vol. 2, pp. 408–422, 2019, doi: 10.1007/978-3-030-37231-6.

[37] D. Zonda and M. Meddeb, “Proxy re-encryption for privacy enhancement in Blockchain : Carpooling use case,” Proc. - 2020 IEEE Int. Conf. Blockchain, Blockchain 2020, pp. 482–489, 2020, doi: 10.1109/Blockchain50366.2020.00070.

[38] H. Zhang, E. Deng, H. Zhu, and Z. Cao, “Smart contract for secure billing in ride-hailing service via blockchain,” Peer-to-Peer Netw. Appl., pp. 1346–1357, 2019, doi: https://doi.org/10.1007/s12083-018-0694-5.

[39] W. Li, C. Meese, H. Guo, and M. Nejad, “Blockchain-enabled Identity Verification for Safe Ridesharing Leveraging Zero-Knowledge Proof,” arXiv2010.14037v3 [cs.CR] 1 Nov 2020, 2020.

[40] R. Kumar, S. Balodia, R. K. Kedia, S. D. Suvvari, and D. Gowrishankar, “Decentralised Ride Sharing System,” Int. J. Innov. Sci. Res. Technol., vol. 6, no. 6, pp. 1347–1350, 2021.

[41] R. Shivers, M. A. Rahman, M. J. H. Faruk, H. Shahriar, A. Cuzzocrea, and V. Clincy, “Ride-Hailing for Autonomous Vehicles : Hyperledger Fabric-Based Secure and Decentralize Blockchain Platform,” 2021 IEEE Int. Conf. Big Data (Big Data), pp. 5450–5459, 2021, doi: 10.1109/BigData52589.2021.9671379.

[42] B. KOU, S. CAO, and J. LV, "A Privacy protection scheme for carpooling service using fog computing," J. Phys. Conf. Ser. Pap. (ICEMCE 2020), vol. 1601, pp. 1–8, 2020, doi: 10.1088/1742-6596/1601/3/032019.

[43] M. S. Hossan, M. L. Khatun, S. Rahman, S. Reno, and M. Ahmed, "Securing Ride-Sharing Service Using IPFS and Hyperledger Based on Private Blockchain," 2021 24th Int. Conf. Comput. Inf. Technol., pp. 1–6, 2021, doi: 10.1109/ICCIT54785.2021.9689814.

[44] Y. Semenko and D. Saucez, "Distributed Privacy Preserving Platform for Ridesharing Services," Secur. Privacy, Anonymity Comput. Commun. Storage, Springer, pp. 1–6, 2019, doi: 10.1007/978-3-030-24907-6_1.

[45] K. Kato, Y. Yan, and H. Toyoizumi, "Blockchain Application for Rideshare Service," 2018 8th Int. Conf. Logist. Informatics Serv. Sci., pp. 1–5, 2018, doi: 10.1109/LISS.2018.8593271.

[46] M. Richard Joseph, R. Sah, A. Date, P. Rane, and A. Chugh, "BlockWheels - A Peer to Peer Ridesharing Network," Proc. Fifth Int. Conf. Intell. Comput. Control Syst. (ICICCS 2021), pp. 166–171, 2021, doi: 10.1109/ICICCS51141.2021.9432188.

[47] S. E. Chang and C.-Y. Chang, "Application of Blockchain Technology to Smart City Service : A Case of Ridesharing," 2018 IEEE Confs Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. Congr. Cybermatics, pp. 664–671, 2018, doi: 10.1109/Cybermatics.

[48] Arcade city. [Online]. https://arcade.city/

[49] Dacsee platform. [Online]. https://dacsee.com/

[50] A. Pham et al., "PrivateRide : A Privacy-Enhanced Ride-Hailing Service," Proc. Priv. Enhancing Technol., vol. 2017, no. 2, pp. 38–56, 2017, doi: 10.1515/popets-2017-0015.

[51] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks," arXiv:2201.04803v1, pp. 1–29, 2022.

[52] L. Zhu, K. Gai, and M. Li, Blockchain Technology in Internet of Things. Springer Nature Switzerland AG 2019.