iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48842

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue I Jan 2023- Available at www.ijraset.com

Ride Sharing with Privacy, Trust and Fair Payment by using Blockchain

Ayush Kumar Singh[1], Ayushman[2], Abhisekh Kumar Yadav[3], Shivendra Mishra[4], Anju Joshi[5]
[1, 2, 3, 4]*IMSEC, Ghaziabad*

Abstract: ***The idea of sharing economy provides rise to distinctive concepts and develops innovative businesses. This text aims to relate the good town concept by introducing the good transport system and explores the opportunities of adopting blockchain technology in ridesharing services. Blockchain technology could be a distributed, suburbanized public ledger that allows peer-to-peer transactions in a very secure means with no third party. This proposes a blockchain-based framework from the prevailing centralized framework for a ride-sharing service and implements a similar as a suburbanized application (DApp) primarily based on good contracts on Ethereum Blockchain. exploitation good contracts facilitate the users with automated transactions, removes the intermediaries, and allows varied activities to be carried out safely and firmly. Implementation of good contracts is finished exploitation of the Solidity programming language. This DApp uses the min matching algorithmic program to match riders requesting rideshare to avoid wasting total travel distance. With the overwhelming growth in the usage of crypto currencies, good contracts usage in applications as projected during this paper will rework the sharing economy.***
Keywords: Blockchain, Peer-to-Peer, Decentralization, Ethereum, Ridesharing, Smart Contracts

I. INTRODUCTION

Ride sharing offerings have gained in popularity as a possible means of transportation in current years. services that permit purchasers everyday make better use of their private automobiles. A ride sharing driving force shares his journey with different passengers. Individuals can gain from experience sharing in a selection of methods as well as the network as a whole, inclusive of expanded occupancy charges, splitting trip expenses, extending social circles, and reducing both fuel utilization and pollution. Many organizations, including Flinc, UberPool, Ola and others, provide on-line ride sharing services all around the globe.

Cab carrier aggregators carry out their day to day activities by the use of a centralized technology. In addition, the payment method for cab bookings is handled with the aid of mediators or third party businesses. With more events engaged, this daily trouble due to the fact that a lack of transparency emerges. Most of the present ride sharing applications like Uber, Ola installation centralized third birthday party every day systems day-to-day offer experience sharing services daily day-to-day. The hassle with these conventional ride sharing systems is the centralization of statistics that can at instances result in failure of the whole machine if server failure is encountered. Furthermore, Centralized structures have an unmarried factor of corruption, a single point of failure and are fragile in nature when compared with decentralized structures. In decentralized ridesharing apps, passengers can have a look at how a ride sharing commercial enterprise works daily blockchain's capability to create responsibility. Clever contracts empower stakeholders to apply blockchain-enabled peer-to-peer renting of vehicles for 2 events actually involved daily on predetermined critical necessities. Hence, it consistently substances right fees, and the system develops confidence and transparency.

Peer to peer technology is a decentralized platform in which individual peers can directly engage with each other without any 3rd party managing the switch records, this is lots beneficial in terms of safety worries of the systems. For the reason that transactions take place peer to peer, they cannot be controlled or manipulated with the aid of third party day-to-day or even the developers that hooked up the gadget inside the first region. Now Blockchain comes into day-to-day use to help set up Peer to peer technology, making it decentralized, making it more comfy and extra proof against cyber attacks that are turning into a massive concern everyday technology because of the frequency and effect of those types of assaults.

II. LITERATURE SURVEY

Car-sharing systems were introduced to help solve transportation problems in urban areas, such as traffic congestion on the road, pollution from fuel combustion, and shortage of parking space from the increased number of vehicles. Car-sharing systems offer the benefits of private vehicle use without the costs and responsibilities of ownership to users and reduce private vehicle ownership. Rather than owning one or more vehicles, a household or business can access a fleet of shared vehicles on an as-required basis. With these advantages, car-sharing systems have proliferated.

The car-sharing system is classified as business models such as Business-to-Consumer (B2C) and Peer-to-Peer (P2P) car-sharing service models. In the B2C service model, companies have deployed their shared cars that are rented out to users. Unlike B2C, the P2P service model is a system in which car owners convert their personal vehicles into shared cars and rent them to other users on a short-term basis. In both car-sharing models, a service vendor assists the car owners and renters by acting as an intermediary and provides the resources needed to make the exchange possible, such as an online platform and customer support. Under this system, users can book and lease a shared car on an online service platform using their smartphones. The advent of car-sharing systems can alleviate transportation problems, but car-sharing systems have security problems.

Vaidaya and Mouftah [1] discussed security issues and the requirements of the car-sharing system. In their article, the connected and autonomous vehicles with external connectivity have security and privacy issues, such as eavesdropping, man-in-the-middle, replay, and denial-of-service attacks. Thus, secure communication and user authentication are essential for secure car-sharing systems. They also proposed a system overview of a personal vehicle sharing system.

Symeonidis et al. [2] specified the security and privacy requirements for a car-sharing system. They reported that entity authentication, data integrity, congeniality, non-repudiation, and authorization are required to design a car-sharing system to mitigate security threats. Furthermore, anonymity is needed to protect the users' privacy.

Busold et al. [3] suggested an authentication protocol for car access and rights delegation using a smartphone and access token.

Wei et al. [4] proposed a hierarchical carsharing system. Their system consisted of three entity levels: a key generation center was the top level; owners or sharing companies were the middle level; the users were the lowest level. Each level receives a key to access the vehicle from the upper level. Therefore, the user obtains the access key from the owners or companies and uses it to access the sharing vehicle through NFC communication.

Laurent et al. [5] proposed an authentication protocol for a car-sharing service, which addresses privacy-preserving using a pseudonym.

Dmitrienko et al. [6] proposed a secure free-floating car-sharing system. In their system, if a user wants to reserve the car-sharing service, the user is authenticated by the car-sharing provider to obtain an access token. The user can then access the vehicle using the access token and mobile device. However, their scheme did not consider the users' privacy. Moreover, these authentication schemes for car-sharing systems suffer from a single point of failure problem and bottleneck problem because they depend on a central node to manage the data and operate the system.

Xu et al [7] modeled the edge computing-based computation offloading approach to tackle privacy leakage problems with privacy preservation. After that, the Vehicle-to-Vehicle (V2V) network based on vehicle routing was designed for obtaining the origin vehicle, where the computing task was assigned at the destination vehicle.

Baza et al [8] developed and distributed firmware updates for Autonomous Vehicles (AVs) subsystems, leveraging smart contract, and blockchain technology. Here, the consortium of blockchain with various AVs are utilized for ensuring the integrity and the authenticity of firmware updates.

Kang Liu et al [9] developed a secure, decentralized data trading and debit-credit system for IoV using blockchain. In this scheme, the authors designed a mechanism to encourage borrowing and lending among vehicles by a motivation-based debit-credit mechanism.

Wang et al. [10] proposed a blockchain-assisted handover authenticated key agreement scheme in an edge-computing environment. In these schemes, the authentication servers, which maintain the blockchain, authenticate the user by employing the user's information stored in the blockchain. Therefore, there is no need for support by a registration authority in the authentication phase.

This concept has been introduced by Vitalik Buterin [11] and is called smart-contracts or decentralized autonomous organizations. A smart-contract can be described as an autonomous computer program running on a blockchain network. This program acts as a contract whose terms can be pre-programmed with the ability of self-executing and self-enforcing itself without the need for trusted authorities.

III. THEORY

A. Blockchain Technology

Blockchain is a statistics recording mechanism that makes it hard or not possible to adjust, hack, or cheat the gadget. A blockchain is basically a digit transaction ledger that is duplicated and disbursed on the blockchain through the entire community of pc devices. Blockchain is a database that saves all transactions grouped in blocks. Each block consists of a cryptographic hash of the previous block, a timestamp, and transaction records.

While a sparkling transaction is created, the sender pronounces in the peer to look community to all of the other nodes. As the nodes are getting the transaction, they verify and hold it in their transactional swimming pools. Confirm the transaction way the execution of predefined controls approximately the shape of the transaction and its movements. Unique varieties of nodes referred to as miners create a new block and group a number of their transaction pool's to be had transactions. Then the block is mined, that is a method of the usage of variable information from the header of the new block to locate the evidence of labor. The calculation of cryptographic hash that fits the given difficulty intention is to find the evidence of labor. Every block stores meta-facts and the hash fee of the previous block similarly to transaction. So each block has its figure block with a pointer. That is how the blocks are related, forming a block chain referred to as blockchain.

B. Decentralization

Decentralization is the technique of dispersing capabilities and energy far from the principal region or authority. Initially, the arena's huge net was installed as a decentralized discussion board. Examples of decentralized structure and systems are blockchain technologies, consisting of bitcoin and ethereum.

C. Web App vs DApp

Web applications use the central HTTP protocol to communicate on a centralized server. In contrast, DApps exist on decentralized blockchain technology hosted on a virtual machine.

TABLE I
WEB APP VS DAPP

Sr. No.	Web Application	Decentralised Application
1	Follows client-server architecture.	The client interacts through smart contracts.
2	Database connected to the backend server and is accessed by the client.	Backend code runs on a decentralized P2P network.
3	Needs central authority to set roles and permissions Security and Privacy are the concerns.	No central authority Secure, immutable, and autonomous.

D. Frameworks and Tools

For the ride sharing Dpp, we made use of Node and various Tools. The Frameworks and Tools used are mentioned below:

1) *Node*: A node framework is a workspace platform that supports the use of Node.js and which allows developers to use JavaScript for developing the front end as well as the back end of an application. Node frameworks are a wide collection of frameworks built on Node and that extend its properties and functionalities further.
2) *Sanity:* Sanity.io is the platform for structured content. With Sanity.io you can manage your text, images, and other media with APIs. You can also use the open-source single page application Sanity Studio to quickly set up an editing environment that you can customize.
3) *Vercel:* Vercel is a platform that enables frontend teams to do their best work, combining the best developer experience with a focus on end-user performance. We build products for developers, designers, and their collaborators that are easy to set up, and universally accessible
4) *Mapbox:* Mapbox is a location data platform for mobile and web applications powering navigation for people, packages, and vehicles everywhere
5) *Metamask:* MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

E. DApp architecture

DApp is two-tier design, one tier being the front-end client-side application and also the alternative being the back-end server-side tier wherever the good contract is deployed within the blockchain network. Figure 1. below shows the final design of the decentralized application and also the interaction between a consumer and a server-side application. The tools that area unit utilized in developing the ridesharing Dapp area unit mentioned within the later sections.

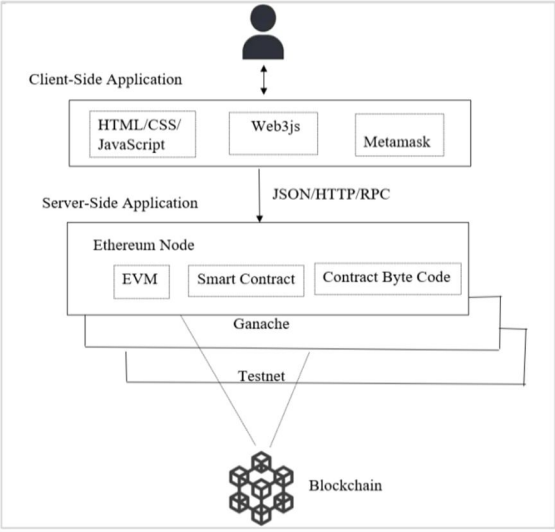


Fig. 1 DApp architecture

As mentioned on top of any DApp incorporates a backend and a frontend application unlike the centralized applications where the backend code runs on centralized servers, a DApp 's backend code is distributed through a suburbanised peer-to-peer network. The front-end code of a DApp is often written in any language and API calls are often created to the backend. Ethereum was the primary blockchain-based platform to make a mathematician complete language for writing good contracts and a DApp development platform. The quality language for building DApp on the Ethereum platform is solidity. In this project, the Ethereum Truffle suite was accustomed to develop and deploy good contracts.

IV. IMPLEMENTATION

A blockchain-primarily based machine is usually recommended to discover shared distributions made regionally. To maintain the privacy of passengers' travels, it uses cloaking, so the passenger sends the baggage choose-up point and pull-off time. After that, fascinated drivers use offline a corresponding process to check if the application falls into his or her binding shape and send it information of the precise experience encrypted with the passenger public key. After that, the rider can select the satisfactory driving force to percentage journey based on different sources.

This works as a transport to a blockchain-owned public sale to make sure transparency. To ensure acceptance as true with between the passenger and the selected driver, the paper recommends a delay deposit deposit for boarding services at the cross based totally at the set of information club. The main idea is to provide an explanation for a way to make a claim or first-rate that works as following:

1) The passenger ought to input into a smart contract and a deposit of finances as evidence of accepting motive force provided and a group of numerous included locations.

2) Time table for the targeted driving force ought to additionally set the finances within the contract as according to his dedication gift.

3) Upon arrival on the pick out-up factor, the driver acts as a proof and sends evidence of the taking area within the blockchain. Specifically, the motive force verifies that the document the place van falls into a predefined set of cells.

4) Eventually, a smart settlement acts as (evidence) through searching on the evidence in an incomprehensible manner and giving rewards driving if there's legitimate evidence or first-class the driving force in case he's unemployed or if no proof has been despatched before the agreed time period.

V. RESULT AND DISCUSSION

A. Main Page

The main page of the project Fig. 2, users have to log in before filling the box of "Where can we pick you up?" and "Where to?". After providing the location users can choose from a variety of car types, including traditional taxis, luxury vehicles, and carpool options. Once a ride is requested, a driver in the area will receive the request and can choose to accept or decline it. If accepted, the rider will receive updates on the driver's location and an estimated time of arrival.

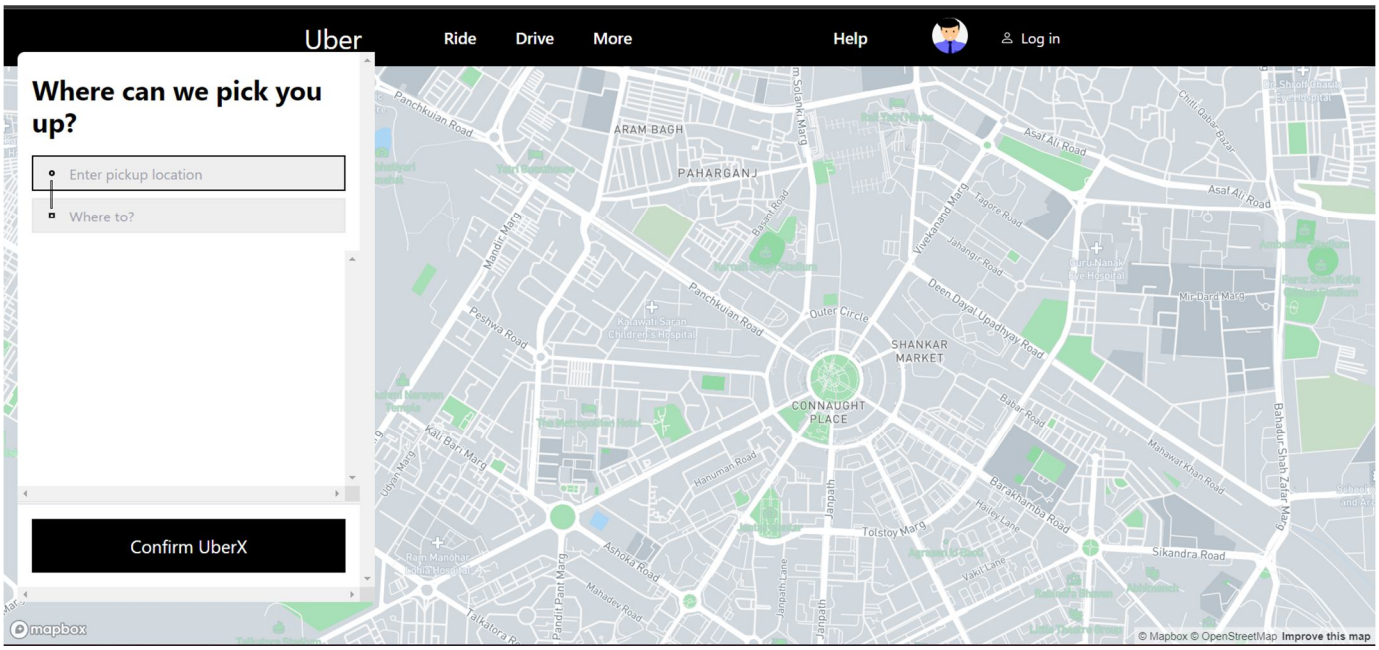


Fig. 2 The Main Page

B. Analysis of Average Price by cab type and Source

Fig. 3 gives the Avg Price & Count of surge multiplier by source. Which gives us an idea about when prices are surging, multiplier to standard rates, an additional surge amount, or an upfront fare including the surge amount will be shown on your offer card. This will vary depending on your city. Uber's service fee percentage does not change during surge pricing.

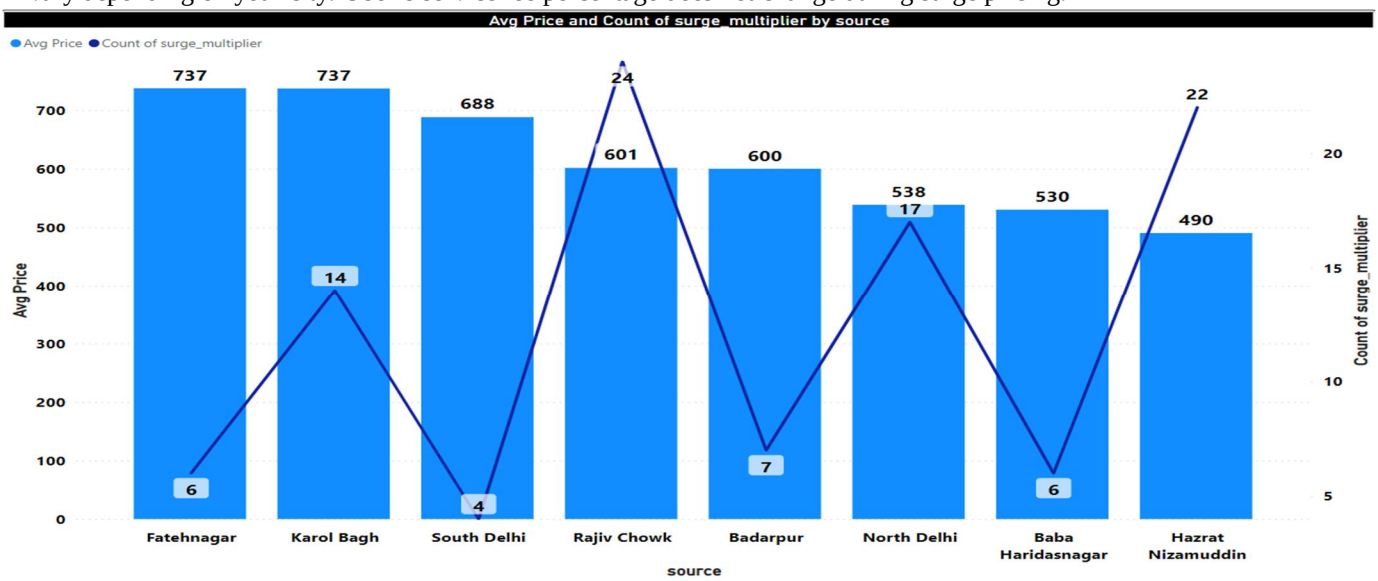


Fig. 3 Average Price and Count of Surge_Multiplier by Source

Fig.4 Average price of different car apps like Lyft and Uber. As shown in Fig.11 graph the Average Price of Lyft is 17.4 and the Average Price of Uber is 15.8. So, we can consider that the average price of Lyft is greater than that of Uber.

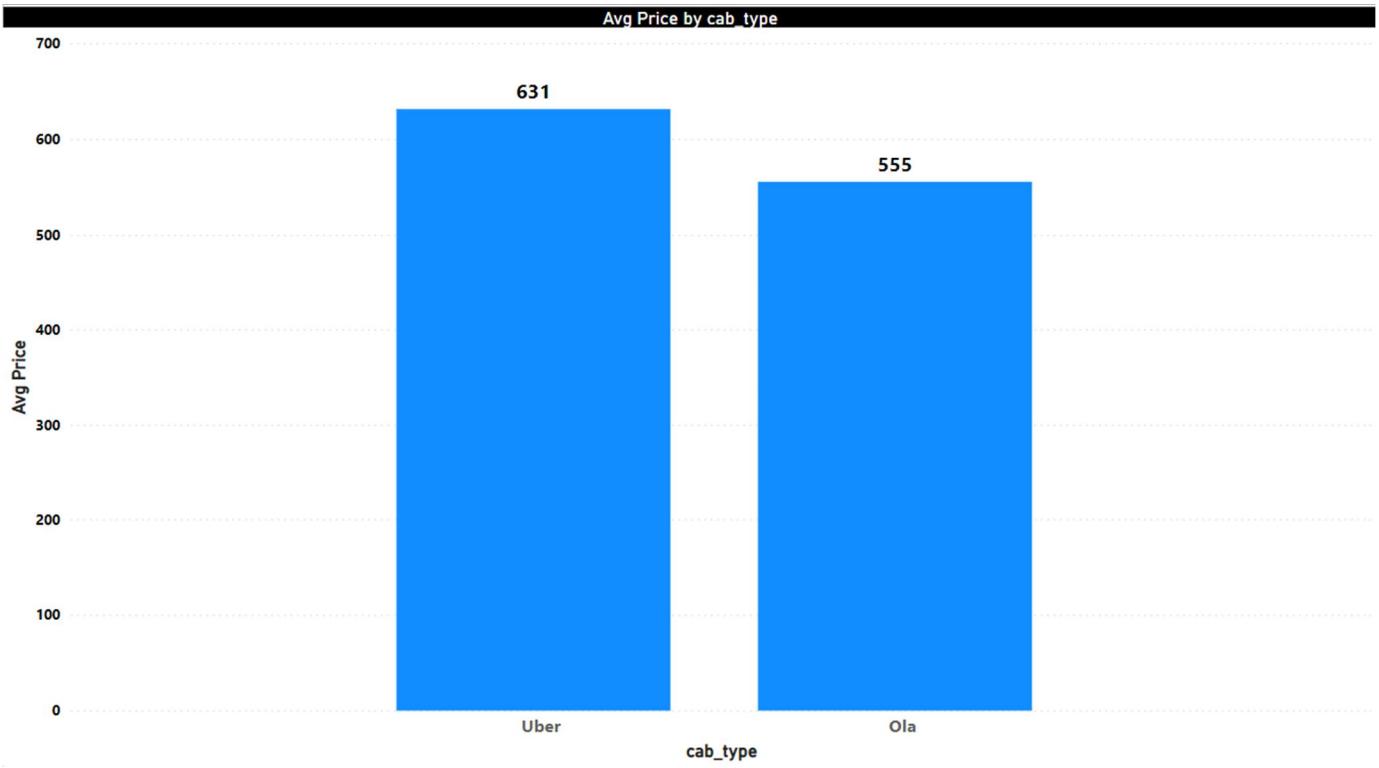


Fig. 4 Average Price by Cab type

C. The Proposed System Model

The proposed authentication scheme for a car-sharing gadget turned into a blockchain based on 5 entities: belief authority, stations, owner, car, and person. A belief authority sets up the system and issues the credential and pseudo-identification to the consumer and the vehicle owner as accepted as true with the entity. Stations have data storage and computing and arrange the consortium blockchain. The user sends the request for automobile-sharing to the proprietor through the station. After being authenticated, the person gets the right of entry to code to free up and control the automobile. The proposed machine version is depicted in Fig. 5.

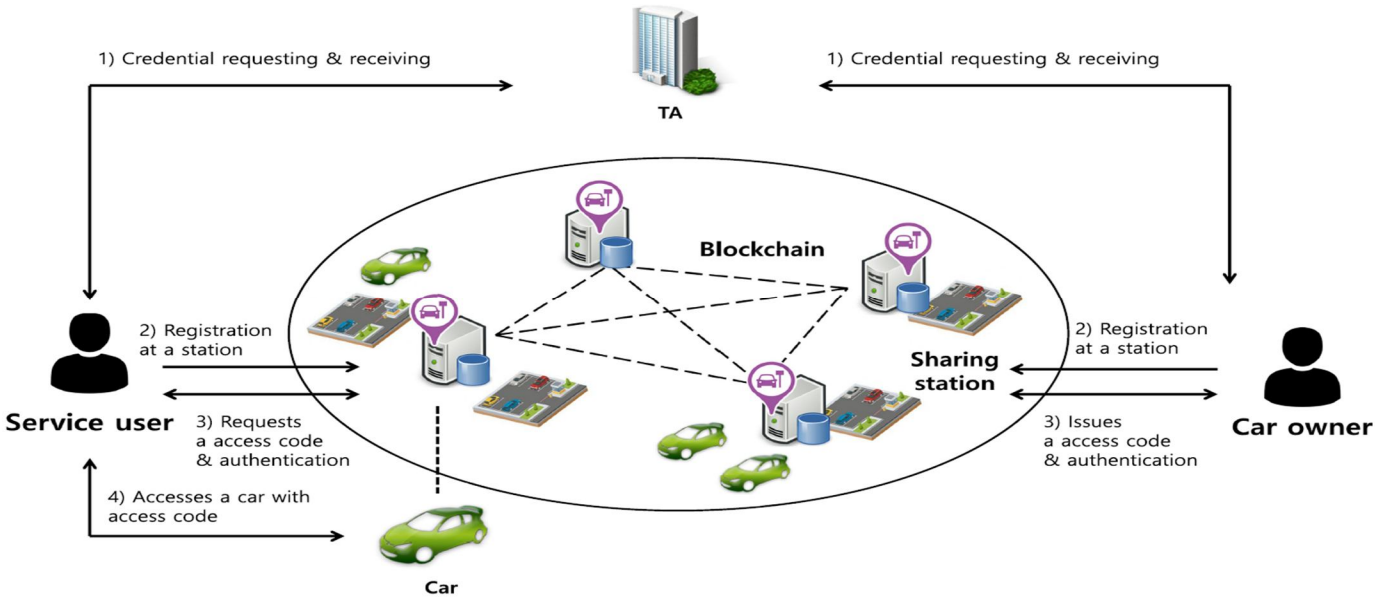


Fig. 5 Average Price by Cab type

VI. CONCLUSION

The main goal of this project is to see the revolutionary technology Blockchain and its use within the shared economy, which can function as a framework for the sensible town plan. This article presents an associate degree existing framework for suburbanized, P2P, blockchain-based ridesharing services and proposes an additional improved version for an equivalent. Further, to support this ridesharing framework, a suburbanized application (DApp) is developed. it'll act as a front-end program aided by blockchain. Ethereum, a permissionless public blockchain is used in this DApp and therefore the transactions and data exchange over the network are machine-controlled victimisation sensible contracts.

To summarise, blockchain may be wont to produce a system in which sensible contracts incorporated in digital code square measure are maintained in suburbanized and clear databases. The data in these information bases square measure thought of to be changeable. Every process and task is anticipated to own a digital record that may be known, valid employing a digital signature.

VII. FUTURE WORK

We will have a scheme wherever no additional intermediary square measure is required. Indeed, blockchain results in a metamorphosis of business models and governance however much it's still a few years away. Blockchain isn't a tumultuous technology meant to eradicate the standard business models by providing low cost solutions.

Rather, it may be seen as a foundational technology capable of giving birth to new frameworks for economic and social problems. Blockchain is not a band-aid resolution to a common technological drawback. Though it will facilitate the transition, a transparent arrangement supporting proof of ideas for opportunities should be established. However, whereas blockchain will have a large result, it'll take decades for it to perforate our socioeconomic infrastructure. As waves of technical and structural amendment win, acceptance is going to be incremental and steady, instead of abrupt. Although blockchain might be used on its own, it'd be more possible to have a bigger impact when integrated with other technologies just like the web of Things, Artificial Intelligence, and large information. This might cause higher solutions for location-based automotive services.

VIII. ACKNOWLEDGMENT

We are really thankful to Assistant Professor Ms. Anju Joshi from the IMS Engineering College in Ghaziabad's Computer Science and Engineering department for her assistance in assisting us with the application of our research to the real world. It's our privilege to express our sincere regards to our project guide, Ms. Anju Joshi for her valuable inputs, able guidance, encouragement, cooperation and constructive criticism throughout the duration of our project. We sincerely thank the Project Assessment Committee members for their support and for enabling us to present the project on
the topic. “Ride Sharing with Privacy, Trust and Fair Payment by using Blockchain.”

REFERENCES

[1] B. Vaidya and H. T. Mouftah, ``Security for shared electric and automated mobility services in smart cities," IEEE Secur. Privacy, vol. 19, no. 1, pp. 24-33, Feb. 2021.

[2] I. Symeonidis, M. A. Mustafa, and B. Preneel, ``Keyless car sharing system: A security and privacy analysis," in Proc. IEEE Int. Smart Cities Conf. (ISC2), Seattle, WA, USA, Sep. 2016, pp. 1-7.

[3] R. E. Haas and D. P. F. Moller, ``Automotive connectivity, cyber-attack scenarios and automotive cyber security," in Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT), May 2017, pp. 635-639.

[4] Z. Wei, Y. Yanjiang, Y. Wu, J. Weng, and R. H. Deng, ``HIBS-KSharing: Hierarchical identity-based signature key sharing for automotive," IEEE Access, vol. 5, pp. 16314-16323, 2017.

[5] M. Laurent, J. Leneutre, S. Chabridon, and I. Laaouane, ``Authenticated and privacy-preserving consent management in the Internet of Things," Procedia Comput. Sci., vol. 151, pp. 256-263, Dec. 2019.

[6] A. Dmitrienko and C. Plappert, ``Secure free-floating car sharing for ofline cars," in Proc. ACM Conf. Data Appl. Secur. Privacy, 2017, pp. 349-360.

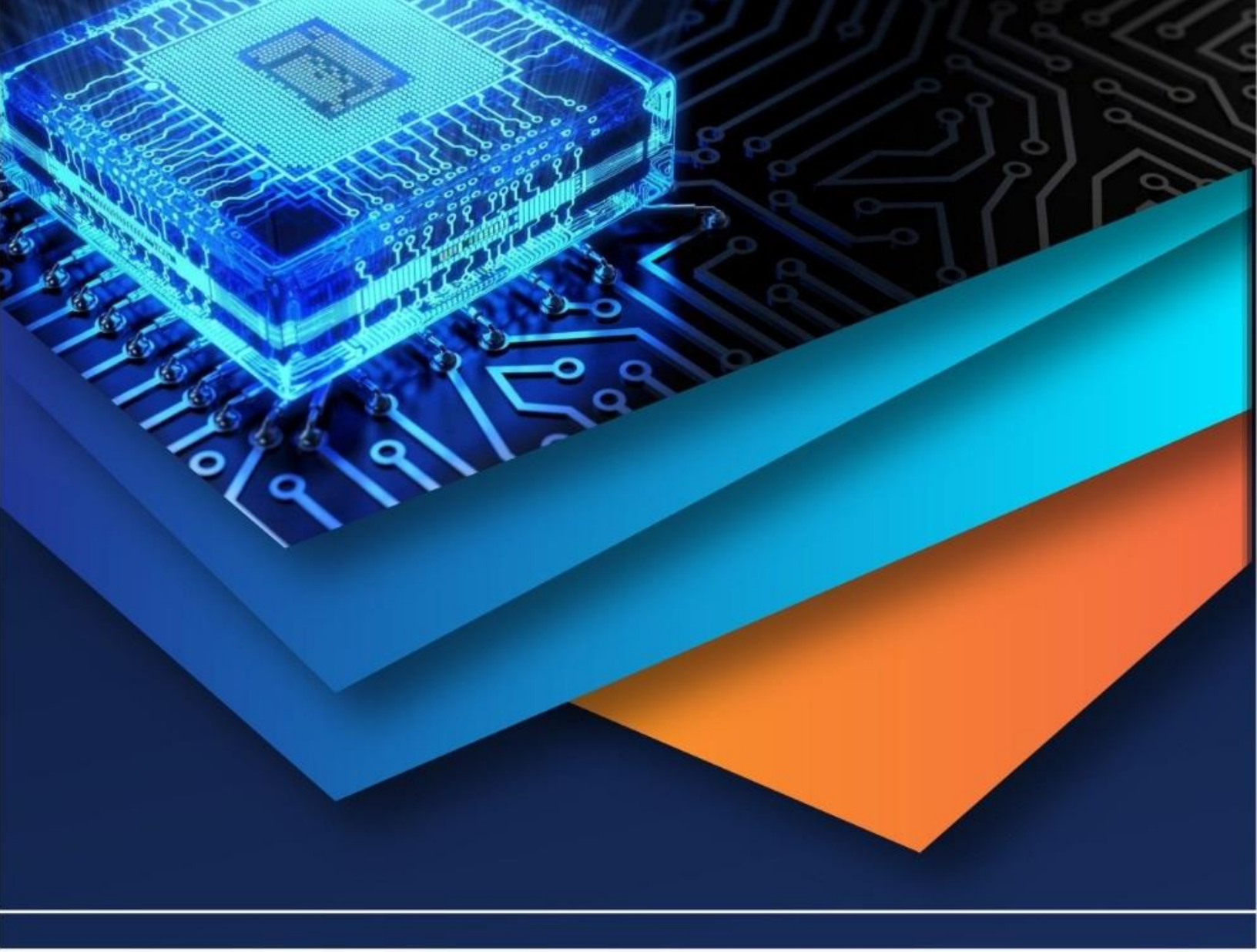
[7] Xu X, Xue Y, Qi L, et al. An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. Future Gener Comput Syst. 2019;96:89-100.

[8] Baza M, Nabil M, Lasla N, Fidan K. Blockchain-based firmware update scheme tailored for autonomous vehicles, Paper presented at: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC); 2019.

[9] Liu K, Chen W, Zheng Z, Li Z, Liang W. A novel debt-credit mechanism for blockchain based data-trading in the internet of vehicles. IEEE Internet Things J. 2019;6(5).9098–9111.

[10] W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, and Y. Zhang, ``Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environments," J. Syst. Archit., vol. 115, May 2021, Art. no. 102024.

[11] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY