

Privacy -preserving smart Ride Sharing Services system using blockchain & private information retrieval

Prof. S. B. Zanke¹, Ms. Shrushti Prashant Naphade², Ms. Rutuja Dilip Jaware³,
Mr. Abhishek Kishor Naphade⁴, Mr. Shivam Ramdas Kharat⁵

¹ Assistant Professor, Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur,
Maharashtra, India

^{2,3,4,5} Student, Department of Computer Science & Engineering, Padm. Dr.V.B.K.C.O.E.Malkapur,
Maharashtra, India

ABSTRACT

Lift sharing has seen a steep rise in fashionability in metropolitan metropolises to avoid destruction of coffers, business logjams and locks. This gave birth to a whole new trend which ride aggregator services went on to subsidize by furnishing the option of participating taxicabs to its druggies at a lower price. Although conventional lift sharing styles have proven to be relatively effective, there's always compass for enhancement in certain fields. This idea of vehicle sharing can be revolutionized by enforcing blockchain technologies. Blockchain is a decentralized record where all the information is stored on systems far and wide which can be recaptured and traced freely. There's a medium that allows peer to peer deals and brings the need for third parties to an absolute minimum. The system is no longer trust- grounded but simply grounded on concrete evidence that exists which is erected into the tally.

Keywords: Blockchain, decentralization, encryption, peer-to-peer network, ridesharing, intermediaries etc.

1. INTRODUCTION

Directly, hack indulgence aggregators are utilizing a centralized methodology to bear out their day-to-day missions. The programs, rules and regulations, terms and conditions that both the user and the automobilist must follow vary from company to company. Likewise, the booking of cabs requires brokers or third-party businesses to carry out the payment process. With further parties involved, this proves to be problematic with the creation of a lack of limpidity. These disadvantages have led to an extensive study of the blockchain technology and latterly several proffers of lift-participating armature erected atop the blockchain. This paper aims to compare and distinction between similar existent methodologies. The main ideal of this paper is to slip light on the colorful ways in which the decentralized, transparent ideas of blockchain have been executed and the reasons for doing so. In this work, we've stressed-out advantages as well as failings of these methodologies, along with information about how the blockchain modules and generalities are used in different phases of the system.

Blockchain is a public, inflexible tale for tracking resources, recording deals and erecting trust. Anything asset can be tracked and traded on a blockchain network, with the main advantage being the reduced trouble as well as significant cut in costs for all parties. Every sector in every field is erected on data. utmost businesses operate solely because of the transfer of information, the hastily this happens, the better. Blockchain is perfect for the movement of data because it can give prompt, participated and fully transparent information that will be kept on an tale that can be recovered only by those who are authorized to do so.

2. LITERATURE SURVEY

- The blockchain- grounded decentralized Lift participating System for smart metropolises” by M. Al-Jarrah et al. This paper presents a lift-sharing system grounded on blockchain technology that provides sequestration protection for druggies' sensitive information, similar as position data and payment details. The proposed system also ensures fair payment and trust among druggies.
- Lift-hailing using Blockchain Technology A Review of the Current Landscape and Research Directions” by Y. Chen et al. This paper provides an overview of being lift-hailing platforms that use

blockchain technology and identifies their strengths and sins. It also discusses the implicit exploration directions for perfecting the sequestration, security, and fairness of lift- participating systems using blockchain.

- " Blockchain- grounded Decentralized Lift participating System for Smart metropolises" by M. Al-Jarrah et al. This paper proposes a decentralized lift- sharing system that utilizes blockchain technology to give secure and effective lift- sharing services. The system ensures sequestration protection for druggies and fair payment for motorists while also promoting trust among druggies.
- " sequestration-Conserving and Secure Lift participating using Blockchain Technology" by S.S. Pandey et al. This paper presents a lift- sharing system that uses blockchain technology to cover druggies' sequestration and insure secure deals. The system uses a smart contract- grounded payment medium to insure fair payment for motorists and help fraud.
- " In the direction a Blockchain – grounded Lift participating Service “done by C. Li et al. This paper proposes a blockchain- grounded lift- sharing service that ensures sequestration, security, and fairness for druggies. The proposed system uses a combination of cryptographic ways, similar as zero-knowledge attestations and homomorphic encryption, to cover druggies' sensitive information.

3. PROBLEM STATEMENT

3.1 Problem Statement:

Ridesharing is a installation that arranges one- way transportation on short notice through mobile apps and websites. To make the overall lift more affordable and terrain friendly, the system groups druggies going in the same direction together and also splits the hack chow. The assiduity is roaring, with guests ready to pay on-demand providers for convenience and a lower figure. still, there are challenges too. The identification and posterior addressable of these grueling factors are of utmost significance to hack service providers, before consumers lose interest.

3.2 Goals & Objectives:

The main ideal of this system is It's a peer- to- peer networking system that offers a safe and trusted terrain for vehicle communication, furnishing an natural tally and secure data access. By equipping intelligent vehicles with digital coffers similar as pall computing, data storehouse, business guidance, and decision- timber, vehicular pall computing (VCC) has had a significant impact on business operation and road safety.

4. PROPOSED SYSTEM

Lift- sharing is a service that enables drivers to partake passages with other riders, contributing to appealing benefits of shared trip cost and reducing business business. still, the maturity of being lift-sharing services calculate on a central third party to organize the services, which make them subject to a single point of failure and insulation exposure enterprises by both internal and external attackers. also, they are vulnerable to distributed denial of service (DDoS) and Sybil attacks launched by vicious addicts and external attackers. either, high service freights are paid to the lift- sharing service provider. In this paper, we propose a decentralized lift- sharing service rested on public Blockchain, named B- Lift. B- Lift enables drivers to offer lift- sharing services without counting on a trusted third party. Both riders and drivers can learn whether they can partake lifts while conserving their trip data, including pick- up/ drop-off position, departure/ appearance date and trip price. still, vicious addicts exploit the obscurity handed by the public blockchain to submit multiple lift requests or offers, while not committing to any of them, in order to find a better offer or to make the system unreliable. B-Lift solves this problem by introducing a time- locked deposit protocol for a lift- sharing by using smart contract and zero-knowledge set class confirmation. In a nutshell, both a automobilist and a rider have to show their good will and commitment by transferring a deposit to the blockchain. subsequently, a automobilist has to prove to the blockchain on the agreed pick- up time that he she arrived at the pick-up position on time. To save rider/ automobilist insulation by hiding the exact pick-up position, the confirmation is performed using zero- knowledge set class confirmation. also, to ensure fair payment, a pay-as-you-drive methodology is introduced rested on the desisted distance of the automobilist and rider. In addition, we introduce a character model to rate drivers rested on their formerly geste without involving any third- parties to allow riders to conclude them rested on their history on the system. ultimately, we apply our protocol and fix it in a test net of custom blockchain. The experimental results show the connection of our protocol atop being real- world blockchain's.

4.1 SYSTEM ARCHITECTURE

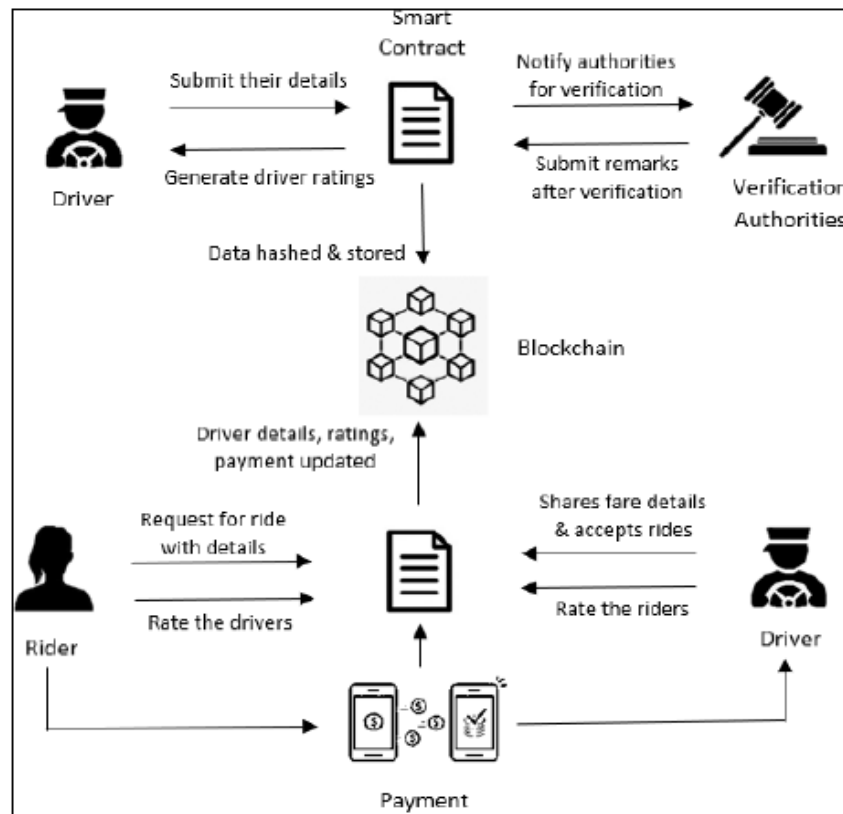


Fig.1: System Architecture

4.2 REQUIREMENTS SOFTWARE AND HARDWARE

4.2.1 Hardware Requirements Specification:

There should be required devices to interact with software.

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Ram : 256 Mb.
- IO Devices : Keyboard, Mouse, Monitor, etc.

4.2.2 Software Requirements Specification:

- Operating system : Windows XP/7.
- Coding Language : JAVA
- IDE : Eclipse Oxygen
- Web server : Apache Tomcat 8.5.

5. CONCLUSION AND FUTURE WORK

Riders can connect directly with motorists via blockchain's decentralized network, therefore reducing the fresh costs. Because there are no interposers, folks with a smartphone and secure ultramodern vehicles have further request prospects. Passengers can anatomize how a lift- sharing service functions thanks to blockchain's capacity to establish responsibility. Smart contracts encourage stakeholders to employ blockchain- enabled peer-to-peer leasing of buses for two parties directly involved predicated on the essential pre-decided specifications. As a result, it provides applicable pricing every time and the system gains credibility and translucency. The restrictions created insure that motorists don't engage in any illegal conduct by generating an applicable ranking for riders. For

case, blockchain technology can be developed to customize bus insurance grounded on particular data gathered about auto operation. likewise, statistical studies show that a auto stays idle for a significant period of its continuance. Blockchain offers a way of monetizing the capability of asset possessors to use it at a much advanced position and monetize deals.

REFERENCES

- [1] Baza, M., Mahmoud, M., Srivastava, G., Alasmay, W. and Younis, M., 2020, May. A light blockchain-powered privacy-preserving organization scheme for ride sharing services. In 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring) (pp. 1-6). IEEE
- [2] Yuan, Y. and Wang, F.Y., 2016, November. Towards blockchain-based intelligent transportation systems. In 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC) (pp. 2663- 2668). IEEE.
- [3] Wang, D. and Zhang, X., 2020. Secure Ride-Sharing Services Based on a Consortium Blockchain. IEEE Internet of Things Journal
- [4] Pal, P. and Ruj, S., 2019, July. BlockV: A Blockchain Enabled Peer- Peer Ride Sharing Service. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 463-468). IEEE
- [5] Abubhashim, A. and Tan, C.C., 2020, July. Smart Contract Designs on Blockchain Applications. In 2020 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-4). IEEE
- [6] Baza, M., Lasla, N., Mahmoud, M., Srivastava, G. and Abdallah, M., 2019. B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain. IEEE Transactions on Network Science and Engineering.
- [7] Chang, S.E. and Chang, C.Y., 2018, July. Application of blockchain technology to smart city service: A case of ridesharing. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 664-671). IEEE.11
- [8] Xu, B., Agbele, T. and Jiang, R., 2020. Biometric Blockchain: A Secure Solution for Intelligent Vehicle Data Sharing. In Deep Biometrics (pp. 245-256). Springer, Cham.
- [9] Zhang, X., Liu, J., Li, Y., Cui, Q., Tao, X. and Liu, R.P., 2019, October. Blockchain based secure package delivery via ridesharing. In 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP) (pp. 1-6). IEEE.
- [10] Sharma, P.K., Moon, S.Y. and Park, J.H., 2017. Block-VN: A distributed blockchain based vehicular network architecture in smart City. Journal of information processing systems, 13(1).
- [11] Khanji, S. and Assaf, S., 2019, June. Boosting ridesharing efficiency through blockchain: Greenride application case study. In 2019 10th International Conference on Information and Communication Systems (ICICS) (pp. 224-229). IEEE.
- [12] Kanza, Y. and Safra, E., 2018, November. Cryptotransport: blockchainpowered ride hailing while preserving privacy, pseudonymity and trust. In Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (pp. 540- 543).