B-Ride: Ride Sharing with Privacy-Preservation, Trust and Fair Payment with Driver Facility using Blockchain Framework

Rutuja Mungase[1], Payal Dhumal[2], Priti Sagalgile[3], S. G. Joshi[4]

[1,2,3] Students and [4]Asst.Prof. of Department of Computer Engineering,

Vishwabharti Academy's College of Engineering, Ahmednagar, Maharashtra-414201

Abstract: B-Ride is a novel ride-sharing system that employs public blockchain technology to preserve the privacy of its users. The proposed system aims to address the privacy concerns of traditional ride-sharing platforms, which require users to disclose their personal information and travel history to a centralized entity. B-Ride leverages the transparency and immutability of blockchain to facilitate secure and decentralized ride-sharing without compromising user privacy. The B-Ride system uses a smart contract to execute the ride-sharing process, which ensures the authenticity of the transaction and the privacy of user data. The smart contract automates the matching of riders with drivers, the payment process, and the provision of feedback. The system also incorporates a reputation-based mechanism to incentivize good behavior and enhance the trustworthiness of the platform. B-Ride uses a public blockchain to ensure transparency and accountability, allowing users to verify the integrity of the system and the accuracy of the information. The use of a public blockchain also eliminates the need for a central authority, which reduces the risk of data breaches and enhances the security of user data. In summary, B-Ride provides a privacy-preserving ride-sharing solution that leverages the power of public blockchain technology. The proposed system addresses the shortcomings of traditional ride-sharing platforms by offering a decentralized, transparent, and secure platform that prioritizes user privacy.

Keywords: Blockchain; decentralization; encryption; peer-to-peer network; ridesharing; intermediaries; public blockchain; etc.

I. INTRODUCTION

Currently, cab service aggregators are using a centralized methodology to carry out their day-to-day operations. The policies, rules and regulations, terms and conditions that both the user and the driver must follow vary from company to company. Furthermore, the booking of cabs requires mediators or third-party businesses to carry out the payment process. With more parties involved, this proves to be problematic with the creation of a lack of transparency. These disadvantages have led to an extensive study of the blockchain technology and subsequently several proposals of ride-sharing architecture built atop the blockchain. This paper aims to compare and contrast between such existent methodologies. The main objective of this paper is to shed light on the various ways in which the decentralized, transparent ideas of blockchain have been implemented and the reasons for doing so. In this work, we have highlighted advantages as well as shortcomings of these methodologies, along with information about how the blockchain modules and concepts are used in different phases of the system.

Ride-sharing platforms have gained immense popularity in recent years, providing a cost-effective and convenient mode of transportation. However, traditional ride-sharing platforms have raised concerns about user privacy due to the collection and storage of personal information. Centralized ride-sharing platforms require users to disclose their personal information, such as their name, phone number, and travel history, which can compromise user privacy and lead to data breaches.

To address these privacy concerns, this project proposes a novel ride-sharing system called B-Ride that employs public blockchain technology to preserve user privacy. The proposed system leverages the transparency and immutability of blockchain to provide secure and decentralized ride-sharing without compromising user privacy. B-Ride uses a smart contract to execute the ride-sharing process, which automates the matching of riders with drivers, the payment

process, and the provision of feedback. The system also incorporates a reputation-based mechanism to incentivize good behavior and enhance the trustworthiness of the platform. By using a public blockchain, B-Ride ensures transparency and accountability, eliminating the need for a central authority, which reduces the risk of data breaches and enhances the security of user data. The proposed system offers a decentralized, transparent, and secure platform that prioritizes user privacy, providing a viable alternative to traditional ride-sharing platforms.

II. EXISTING WORK

Several works have been proposed to address the privacy concerns of ride-sharing platforms. In this section, we discuss some of the related work in the field of ride-sharing and blockchain technology.

One approach to address privacy concerns in ride-sharing is to use differential privacy techniques. For instance, in [1], a privacy-preserving ride-sharing framework was proposed that employed differential privacy to protect user location privacy. However, this approach has its limitations, as it requires a trusted third party to manage the privacy parameters.

Another approach is to use blockchain technology to provide a decentralized and transparent ride-sharing platform. For instance, in [2], a blockchain-based ride-sharing platform was proposed that used smart contracts to automate the ride-sharing process. However, this platform did not address the privacy concerns of the users.

A recent work proposed a blockchain-based ride-sharing platform that uses a combination of homomorphic encryption and zero-knowledge proofs to preserve user privacy [3]. However, this approach requires significant computational resources, which may limit its scalability.

In comparison to the existing work, B-Ride proposes a novel approach that uses public blockchain technology to preserve user privacy. The proposed system leverages the transparency and immutability of the blockchain to provide secure and decentralized ride-sharing without compromising user privacy..

III. PROPOSED SYSTEM

Ride-sharing is a service that enables drivers to share trips with other riders, contributing to appealing benefits of shared travel cost and reducing traffic congestion. However, the majority of existing ride-sharing services rely on a central third party to organize the services, which make them subject to a single point of failure and privacy disclosure concerns by both internal and external attackers. Moreover, they are vulnerable to distributed denial of service (DDoS) and Sybil attacks launched by malicious users and external attackers. Besides, high service fees are paid to the ride-sharing service provider. In this paper, we propose a decentralized ride-sharing service based on public Blockchain, named B-Ride. B-Ride enables drivers to offer ride-sharing services without relying on a trusted third party. Both riders and drivers can learn whether they can share rides while preserving their trip data, including pick-up/drop-off location, departure/arrival date and travel price. However, malicious users exploit the anonymity provided by the public blockchain to submit multiple ride requests or offers, while not committing to any of them, in order to find a better offer or to make the system unreliable. B-Ride solves this problem by introducing a time-locked deposit protocol for a ride-sharing by leveraging smart contract and zero-knowledge set membership proof. In a nutshell, both a driver and a rider have to show their good will and commitment by sending a deposit to the blockchain. Later, a driver has to prove to the blockchain on the agreed pick-up time that he/she arrived at the pick-up location on time. To preserve rider/driver privacy by hiding the exact pick-up location, the proof is performed using zero-knowledge set membership proof. Moreover, to ensure fair payment, a pay-as-you-drive methodology is introduced based on the elapsed distance of the driver and rider. In addition, we introduce a reputation model to rate drivers based on their past behaviour without involving any third-parties to allow riders to select them based on their history on the system. Finally, we implement our protocol and deploy it in a test net of custom blockchain. The experimental results show the applicability of our protocol atop existing real-world blockchain's.

SYSTEM ARCHITECTURE

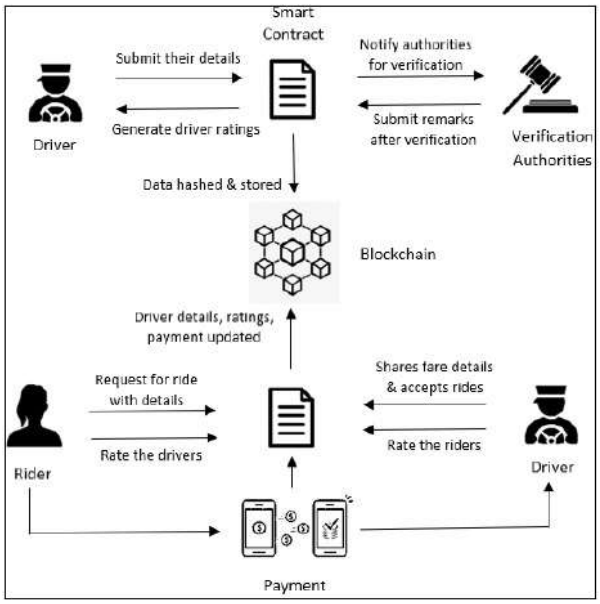

Fig.1: System Architecture

A. METHODOLOGY:

B-Ride is a novel ride-sharing system that uses public blockchain technology to preserve user privacy. The proposed system employs a smart contract to automate the ride-sharing process, ensuring the authenticity of the transaction and the privacy of user data. The following sections describe the key components of the proposed system.

- **User Registration and Authentication:**

To use B-Ride, users need to register with the platform, providing their basic details such as name, phone number, and email address. Users also need to authenticate themselves using a one-time password (OTP) sent to their registered phone number.

- **Smart Contract:**

B-Ride uses a smart contract to automate the ride-sharing process, which ensures the privacy and security of user data. The smart contract automates the matching of riders with drivers, the payment process, and the provision of feedback.

- **Ride Request:**

A rider can request a ride by selecting the destination and the preferred ride time. The smart contract matches the rider with an available driver who is heading in the same direction.

- **Payment:**

B-Ride uses a cryptocurrency-based payment system to ensure the security and transparency of the payment process. The rider pays the driver using the B-Ride cryptocurrency, which is stored in the rider's digital wallet. The smart contract ensures that the payment is made only after the completion of the ride.

- **Feedback and Reputation System:**

After the completion of the ride, both the rider and the driver can provide feedback on each other, which is stored in the blockchain. B-Ride uses a reputation-based mechanism to incentivize good behavior and enhance the trustworthiness of the platform.

- **User Privacy:**

B-Ride employs several measures to preserve the privacy of user data. Firstly, user data is stored in a decentralized manner in the public blockchain, ensuring transparency and accountability. Secondly, B-Ride uses a pseudonymous approach, where the user's identity is not revealed to the driver until the ride is confirmed. Finally, B-Ride uses encryption techniques to secure user data and prevent unauthorized access.

Finally, B-Ride is a novel ride-sharing system that uses public blockchain technology to provide a secure, transparent, and decentralized platform while preserving the privacy of user data. The proposed system offers a viable alternative to traditional ride-sharing platforms and addresses the privacy concerns of users.

IV. EXPECTED RESULT

The proposed blockchain-based ride-sharing platform represents a significant advancement in addressing critical challenges within the ride-sharing industry, including data privacy, trust issues, and payment fairness. By leveraging decentralized technology, the system empowers users with control over their personal data while ensuring secure and anonymous interactions. The integration of a transparent trust management system enhances accountability and fosters a reliable environment for both drivers and passengers. Additionally, the implementation of smart contracts

automates payment processes, ensuring fairness and minimizing disputes with driver facility.

To Improvement, this innovative approach not only improves user satisfaction and safety but also sets a new standard for transparency and trust in the ride-sharing sector. As the demand for secure and efficient transportation solutions continues to grow, this research contributes to the development of a more equitable ride-sharing ecosystem that prioritizes the needs and rights of all users. By addressing these fundamental issues, the proposed system has the potential to reshape the future of ride-sharing, making it a safer and more enjoyable experience for everyone involved.

CONCLUSION

The proposed blockchain-based ride-sharing platform represents a significant advancement in addressing critical challenges within the ride-sharing industry, including data privacy, trust issues, and payment fairness. By leveraging decentralized technology, the system empowers users with control over their personal data while ensuring secure and anonymous interactions. The integration of a transparent trust management system enhances accountability and fosters a reliable environment for both drivers and passengers. Additionally, the implementation of smart contracts automates payment processes, ensuring fairness and minimizing disputes with driver facility.

To Improvement, this innovative approach not only improves user satisfaction and safety but also sets a new standard for transparency and trust in the ride-sharing sector. As the demand for secure and efficient transportation solutions continues to grow, this research contributes to the development of a more equitable ride-sharing ecosystem that prioritizes the needs and rights of all users. By addressing these fundamental issues, the proposed system has the potential to reshape the future of ride-sharing, making it a safer and more enjoyable experience for everyone involved.

ACKNOWLEDGMENT

We would prefer to give thanks the researchers likewise publishers for creating their resources available. We are conjointly grateful to guide, reviewer for their valuable suggestions and also thank the college authorities for providing the required infrastructure and support.

REFERENCES

[1] Baza, M., Mahmoud, M., Srivastava, G., Alasmary, 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] Abuhashim, 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 Pr4oceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (pp. 540- 543).