Secure Decentralized Carpooling Application Using Blockchain and Zero Knowledge Proof

Saksham Goel[a], Sarvesh V. Sawant[b] and Bhawana Rudra[c]
Department of Information Technology, National Institute of Technology Karnataka, India

Keywords: Decentralized Application, Security, Privacy, Blockchain, Zero-Knowledge Proof.

Abstract: Blockchain extends its reach far beyond cryptocurrencies such as Bitcoin, encompassing a broader spectrum of applications. It acts as a transparent, distributed, and unchangeable ledger where every participant in the network possesses a copy of the blockchain. This decentralized system secures all data and transactions through encryption, ensuring reliability. The key components of blockchain-based applications include Smart Contracts, which house the application's logic and operate on the blockchain. In traditional carpooling systems, centralized authorities like Uber or Ola control the entire process, collecting and managing data from both drivers and riders. However, by leveraging blockchain and smart contracts, a more secure and private carpooling system can be established, allowing riders and drivers to connect directly without intermediaries. Blockchain applications encounter challenges, primarily related to scalability and privacy. Every node in the system processing transactions limits scalability. Moreover, the practice of publishing all data at each node for processing raises privacy concerns. To tackle these issues, an approach using non-interactive proofs for off-chain computations can enhance efficiency. This approach verifies correctness without exposing private data, thus improving privacy. ZoKrates, a toolbox, simplifies this process by providing a domain-specific language (DSL), compiler, and generators for proofs and verification of Smart Contracts, streamlining complex zero-knowledge proof tasks and promoting their adoption.

1 INTRODUCTION

PeerPool is an innovative carpooling application inspired by companies like Uber and Lyft, but with a significant difference (Schaller, 2021). It utilizes blockchain technology to establish direct connections between drivers and passengers, eliminating the need for any third-party applications. Uber and Ola, along with similar third-party agencies, possess comprehensive information about their drivers and riders, which raises concerns about potential privacy violations (Kapassa et al., 2021). There is a possibility that these companies could exploit the data to their advantage or even trade it with other firms. Unlike traditional ride-sharing platforms, PeerPool removes the middleman, represented by Uber and Lyft, thereby avoiding the 25% commission they charge (Ganapathy and Easaw, 2017). By decentralizing the process and employing trustless smart contracts, PeerPool ensures that user data is securely stored and accessible only by the respective individuals. This decentralized approach addresses the issues that large corporate ride-sharing services often overlook. PeerPool operates as a decentralized application (DAPP) with automated peer management, allowing for virtually no middleman fees. Additionally, the system's use of trustless contracts helps resolve disputes and shifts legal liability away from the gig workers (Prieto et al., 2022).

P2P carpooling technology leverages blockchain verification to establish trust among drivers and riders, guaranteeing the authenticity and authentication of all users (Prieto et al., 2022), (Houerbi et al., 2023), (Ben-Sasson et al., 2015). The concept of car-sharing systems has garnered significant interest as a potential solution to urban transportation challenges. However, conventional car-sharing systems encounter security issues due to their centralized structure and communication through public channels (Puthal et al., 2018). To tackle these concerns, this research introduces a secure and decentralized model for a car-sharing system, combined with a robust authentication method, providing a decentralized sharing service for genuine

[a] https://orcid.org/0009-0008-5280-658X
[b] https://orcid.org/0000-0002-6183-4653
[c] https://orcid.org/0000-0001-7651-3820

Goel, S., Sawant, S. and Rudra, B.
Secure Decentralized Carpooling Application Using Blockchain and Zero Knowledge Proof.
DOI: 10.5220/0012701400003705

In *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, pages 260-267
ISBN: 978-989-758-699-6; ISSN: 2184-4976

users (Kapassa et al., 2021). The proposed approach utilizes blockchain technology to ensure the accuracy of service information and deliver a decentralized car-sharing service. Furthermore, the system uses user pseudonyms to safeguard user privacy, rendering it challenging for potential adversaries to access actual user identities even if the stored information is compromised (Tafreshian et al., 2020). Although P2P using blockchain is effective in car-sharing rides, some private details must be shared leading to security breaches between users and drivers. Thus, in order to preserve the privacy of users consuming carpool services, we propose to use a Zero Knowledge Proof (ZKP) based Blockchain which will ensure that the privacy of the users' data is not compromised. Also, there might be a case where a passenger might cancel the ride when the driver arrives at the source. This will cause loss to the driver. To compensate for this loss, we propose a feature of security amount. This feature also covers the loss of the passenger if the driver cancels the ride.

This paper provides an update on the ongoing developments within the realm of Decentralized Carpooling. Furthermore, it outlines the approach we utilized, specifically the incorporation of Zero Knowledge Proofs in this Peer-to-Peer (P2P) Application. Following the presentation of our attained outcomes, the paper discusses the conclusions drawn, and it concludes with some recommendations for future research endeavors.

2 LITERATURE SURVEY

Peer-to-peer (P2P) ridesharing is an economical option for transportation, particularly suitable for those who prefer not to own a car or need to travel long distances (Rathee et al., 2019). This trend not only helps reduce traffic congestion and parking demands but also provides a more cost-efficient and eco-friendly alternative to traditional taxis or private vehicles (Morris, 2016). Blockchain technology brings about significant improvements in ridesharing services through various means. These include the creation of a decentralized ride-hailing platform, secure identity verification, smart contract-powered payments, transparent and traceable records, and the introduction of token-based incentives (Gupta and Shanbhag, 2021).

In a recent study, Uber revealed that in the combined years of 2017 and 2018, there were over 5,900 incidences of non-consensual sexual assault-related events on its ridesharing platform, including nine assault-related fatalities (Uber, 2019). Therefore, protecting ridesharing consumers' well-being is a crucial concern in the on-demand transportation industry.

Blockchain is used differently based on the application, leading to varying privacy-preserving techniques (Tran et al., 2021). Blockchain technology has the potential to revolutionize the ridesharing sector by offering improved transparency, security, and efficiency. By integrating blockchain into ridesharing services, decentralized networks can be created, connecting drivers and passengers directly and eliminating intermediaries. Despite the advantages, blockchain-based ridesharing platforms face challenges in scalability, data privacy, security, and interoperability with existing systems. Nevertheless, introducing blockchain technology has the potential to create a fair and efficient ridesharing system for the future (Dorri et al., 2017).

Numerous Peer-to-Peer Ride-Sharing Architectures based on Blockchain have been developed throughout time (Gupta and Shanbhag, 2021). The most well-liked Peer-to-Peer Ride Sharing Architecture concepts now in existence include Block-V, Block-VN, B-Ride, Green Ride, PEBERS, O-Ride, Ride Matcher, etc.

Smart contracts and digital currency offer a promising solution to streamline payment processes, reduce fraud risks, and eliminate the need for a centralized authority to oversee transactions (Puthal et al., 2018). Through self-executing agreements and a decentralized arbitration process, disagreements can be addressed efficiently and fairly. To ensure the secure storage and execution of these smart contracts, the Ethereum Ecosystem is employed. This ecosystem provides a robust platform for safely recording and managing the smart contracts designed to monitor each user's transactions and interactions(Jahan et al., 2023).

It has been suggested that blockchain technology might make decentralized, efficient two-sided sharing economies, like ridesharing services, possible (Chang and Chang, 2018). Originally used in Bitcoin: Blockchain technology, an emerging network technology that allows consensus among networked peers on a distributed, immutable digital record, is a Peer-to-Peer Electronic Cash System (Nakamoto, 2008). Future ridesharing systems might benefit greatly from the implementation of a secure, decentralized identity verification protocol thanks to blockchain's inherent provenance and immutability capabilities. However, when sensitive user data is included, public blockchain systems raise serious privacy issues. In a permissionless blockchain system like Bitcoin, any networked participant has access to the full ledger due to its transparency-by-design features. Although

blockchain technology provides assured execution and resistance to censorship, its scalability and privacy are limited. Zero-Knowledge Proof (ZK) technologies, however, can be used to overcome these restrictions (Vadhan, 1999).

For cryptographic attestations and in the context of blockchain-based ridesharing platforms, the zero-knowledge property of ZK proofs plays a crucial role in preserving users' privacy and personal data where sensitive information such as users' balances and transactions can be fully hidden from external observers (Kanza and Safra, 2018), (Ruch et al., 2020). For example, a technologically advanced government issues digital passports containing a person's name, date of birth, and both private and public keys, cryptographically signed. Now, consider a scenario where an individual needs to demonstrate to a system that they are a citizen of a specific nation and at least 18 years old. To achieve this, they can construct a function that takes the digital passport and a signature, signed with the passport's private key, as inputs (Bozdog et al., 2018). To maintain privacy and avoid revealing unnecessary personal information, the individual can create a zero-knowledge proof demonstrating that they possess an input that, when provided through the function, produces the validation. Importantly, they use a different private key for this proof, which they intend to use for future interactions with the algorithm. If the proof is accurate and valid, the service can verify it, and subsequently, messages signed with the individual's private key will be accepted as legitimate. This process ensures that the person's identity and age are proven without disclosing any other sensitive information, thereby preserving their privacy in the cryptographic attestation process (Bozdog et al., 2018), (Münzel et al., 2019).

Trusted setups play a crucial role in generating the proving and verification keys for zk-SNARKs. In a trusted setup, a group of individuals generates secret information, uses it to create the necessary data, and then publishes the data while discarding the secrets. The "trust" comes from the fact that once this data is generated, no further involvement from the creators is needed, ensuring the security of the system. Existing blockchain-based ridesharing platforms like Arcade City, DAV Network, Ridecoin and Jolocom exemplify the potential of blockchain technology to transform the ridesharing industry (Augot et al., 2022).

Currently, the Decentralized Carpool Applications have some security concerns (Gudymenko et al., 2020), (Li et al., 2019). For example, users have to provide their private sensitive data like Aadhaar Card Number (Aadhaar number is a 12-digit random number issued by the UIDAI ("Authority") to the residents of India after satisfying the verification process laid down by the Authority. Any individual, irrespective of age and gender, who is a resident of India, may voluntarily enroll to obtain an Aadhaar number), Driving License Number, etc. which is publically available to other users of the application. To deal with this, in this work, we have used Zero Knowledge Proof (ZKP) to hide these sensitive details from other users of the application. Also, many cases are there in current P2P carpool applications where after successful booking of a ride, either the driver or the passenger cancels the ride at the end moment. Due to this, either one of them has to suffer a loss in terms of time, etc. To compensate for this loss, we have proposed a way in which both parties have to deposit a security amount to the smart contract's address. On successful completion of the ride, both parties will get their security amount back but if one of them cancels the ride, then their security amount will be given to the other party involved as compensation. With these proposals, our work provides a solution to the loopholes present in the current implementations of the Decentralized Carpool Applications.

3 METHODOLOGY

The combination of smart contracts, digital currency, the Ethereum Ecosystem, and ZK Proofs has enabled the successful implementation of a robust and user-friendly application that revolutionizes payment processes and dispute resolution in the transportation sector.

As shown in Figure 1, drivers will first enter their details in the Driver Registration section of the application. These details include their name, contact number, car name, hash of DL number, and the fare they want to charge. After registration, these details will be stored via smart contract. Next, the drivers enter the ride details, i.e., the car name and the fare that the driver will charge to go from a particular source to the destination. Now, there are cases where after ride confirmation, either the driver or the passenger cancels the ride at the end moment. To avoid this, we introduced a security deposit concept where the passenger will not get into trouble after the confirmation of the ride. If the ride is confirmed and after that, it is being cancelled by the driver then the amount will be deducted from the security deposit and will be paid to the passenger which is not available with current riding apps. If the ride is a success, the security amount associated with the smart contract address will be returned as shown in Figure 1. We have considered not only the safety of the passenger but also

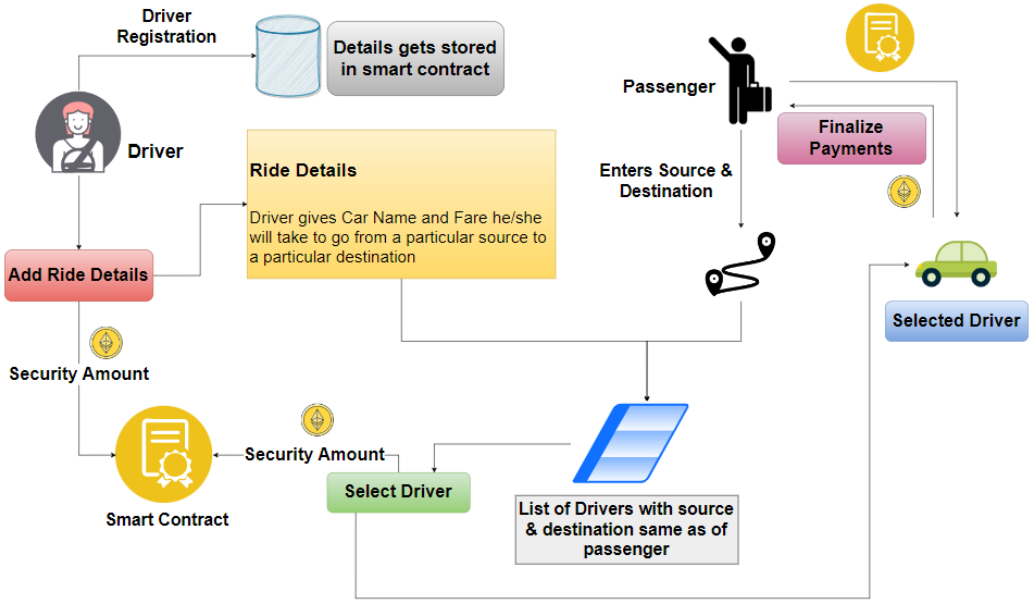

Figure 1: Decentralized Carpool Procedure (without ZKP).

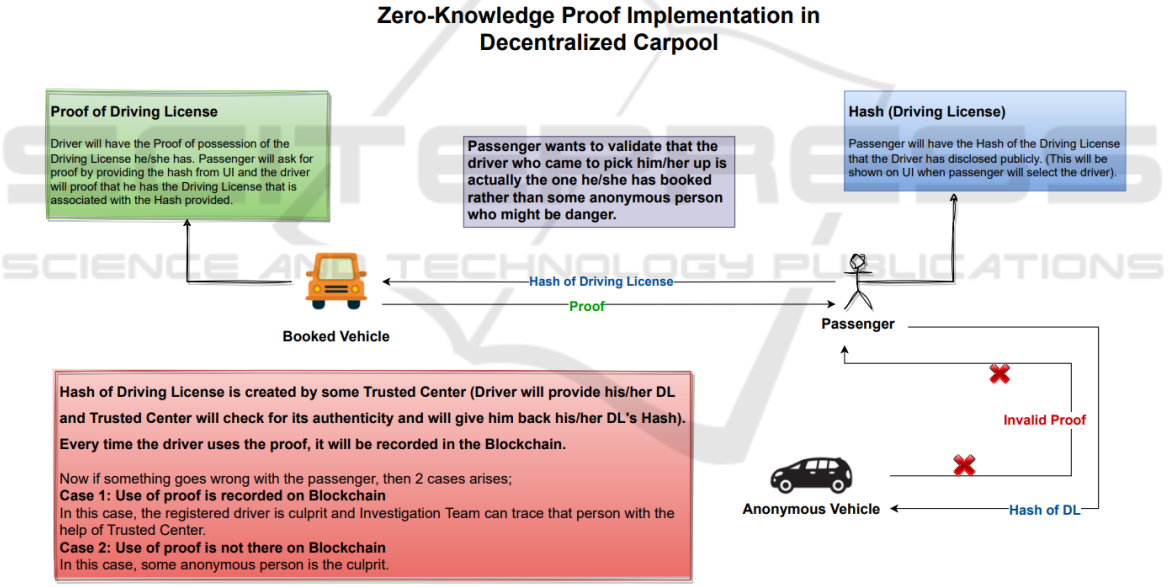

Figure 2: Zero-Knowledge Proof Implementation in Decentralized Carpool.

the safety of the driver, i.e., the passenger should not cancel the ride without any reason. For this, passengers also need to deposit the security amount to the smart contract at the time of booking the ride. If the ride is called off without any reason, then the driver will be compensated with the security amount. If the ride is successfully completed then the payments (including the security amounts that both parties have deposited) get settled between the passenger and the driver. The last step is to rate the driver based on the experience of the passenger.

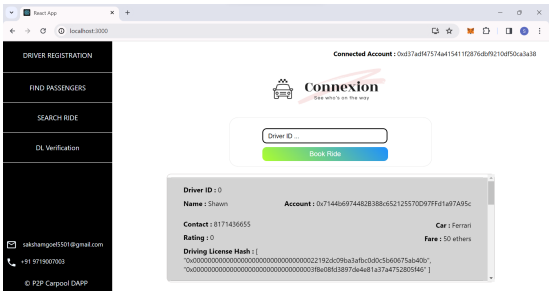

Figure 3: Only the Hash of Driving License Number will be shown on UI.

The use of ZKProof is to avoid impersonation attacks in the network as shown in Figure 2. In the passenger's UI, only the hash of the driver's Driving License number will be shown, i.e., the driver will hide his sensitive information from the public as shown in Figure 3. The hash of the Driving License will be created by some trusted authority. Only the divers who have hashes generated by trusted authorities can look for the passengers in the find passengers section of the application as shown in Figure 4. When the driver arrives at the pick-up location of the passenger, then the passenger would want to validate that the driver who came to pick him/her is actually the one he/she has booked rather than some anonymous vehicle, i.e., a vehicle that was not booked. For this, the passenger will give the hash of the driving license number to the driver and ask the driver for proof that the hash shown in UI is actually associated with the Driving License of the driver. For this, the driver will use their ZKP to show that the hash is actually associated with their DL number, i.e., the proof of possession of the Driving License number he/she has. If the driver who comes to pick up the passenger is actually the one who was booked, then a valid proof will be given, otherwise, an invalid proof will be given. Each time the driver uses the proof, it will be recorded in the blockchain. Now, if something goes wrong with the passenger and if the use of proof is recorded in the blockchain, then in this case, the registered driver is the culprit and the investigation team can trace that driver with the help of a trusted authority. If the use of proof is not there in the blockchain, then in this case some anonymous person is the culprit and appropriate actions will be taken by the investigation team.

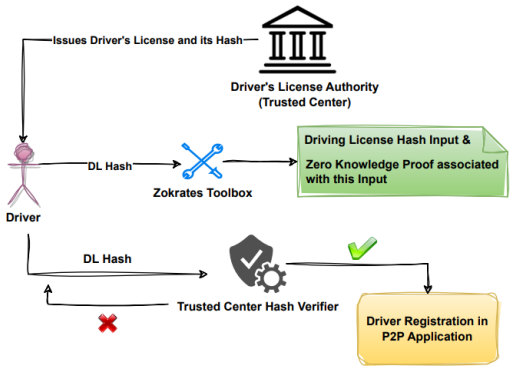

Figure 4: ZK Proof and DL Hash Input generation.

3.1 Passenger Safety Analysis

When a passenger books a ride then he/she will send the security amount to the smart contract but not to the selected driver. In this way, no one can predict (by looking at the blockchain), which driver will come to pick up the passenger. This avoids the case where some anonymous driver (like a kidnapper) will take over the vehicle along with the proof and kidnap the passenger. For example in OLA, Uber, etc., the selected driver may be guessed as they show in the map the nearby drivers, so there is a probability of guessing the correct driver. As the entire system works with ZP Proof, it solves identity theft and makes the entire system secure.

3.2 Driver Safety Analysis

A threat analysis is being performed towards the driver's end for the driver's safety. When the attackers know the whereabouts of the driver, then there is a chance of harming that person. To avoid this, we use random selection for example we have 50 available drivers, then only 20% of those, i.e., 10 random drivers will be displayed to the passenger. So, the probability of crime will be reduced. When the driver verifies ZK proof of the Aadhaar card number of the passenger. Passengers will provide the hash of the Aadhaar card number while booking the driver. Aadhaar Card proof and DL proof will be recorded in the blockchain which will help to trace the passenger as well driver for the real identity. Even the Blockchain Timestamps along with Gas will also help to investigate if any crime occurs.

If any or both the proofs are not used then the investigation team will look for blockchain timestamps at which gas transactions took place, etc. to find the criminal if some crime takes place.

As shown in Figure 4, using ZoKrates (a toolbox for zkSNARKS on Ethereum), drivers and passengers can get the Zero Knowledge Proof (ZKP) associated with their Driving License Number and Aadhaar Card respectively, i.e., each Driving License Number or Aadhaar Card Number has a unique proof mapped with it. This input and proof will be generated by the Driver/Passenger for verification using the Hash provided by the Trusted Centre. These proofs are used by the drivers as their identification when they reach out to the passengers and vice versa.

4 RESULTS

Decentralized Carpool, a ride-sharing platform leveraging public blockchain technology and Zero-Knowledge Proofs, anticipated several key benefits for its users. First and foremost, it upholds a strong commitment to privacy and confidentiality. By utilizing the inherent security features of blockchain, this

Carpooling application named *Connexion*, shielded the user data and ride history from unauthorized access and ensured that personal information remains hidden from third parties. By employing blockchain technology, the platform eliminated intermediaries typically found in traditional ride-sharing setups such as Uber, leading to reduced transaction fees. This reduction in overhead costs resulted not only in offering competitive prices for riders but also provided fair compensation to drivers. Another crucial aspect of Connexion's vision is an improved user experience. The platform has an intuitive and user-friendly interface, making it easy for users to register themselves, search, and book ride effortlessly. While delivering a seamless experience, Connexion emphasized safeguarding user privacy and security. Through diligent assessment and an unwavering focus on meeting user needs, Connexion attempted to revolutionize the ride-sharing industry while setting new standards for privacy, security, and affordability.

On successful completion of the ride, all payment transactions get finalized. This includes the settlement of the security amount. As shown in Figure 5, if the proof is associated with the driving license then the verification is successful as shown in Figure 6. But as we can see in Figure 7, if the proof is tampered with and used for identification purposes, then the verification fails as we can see in Figure 8.

The extensive security analysis shows that the proposed protocol is safeguarded against various threats, including impersonation, stolen mobile devices, offline password guessing, replay, and man-in-the-middle attacks. Key features of the protocol include anonymity, confidentiality, and mutual authentication, as confirmed through informal security analysis. A comparative analysis with related schemes demonstrates the efficiency of the proposed protocol, making it suitable for integration into blockchain-based car-sharing systems.

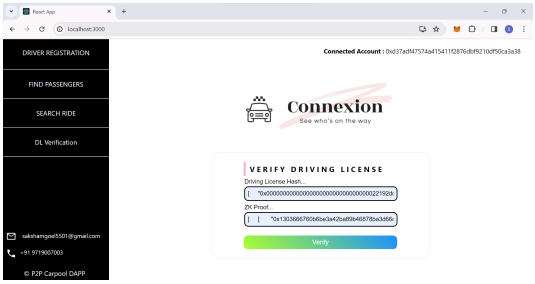

Figure 5: Driving License hash and its associated ZK Proof entered for the verification.

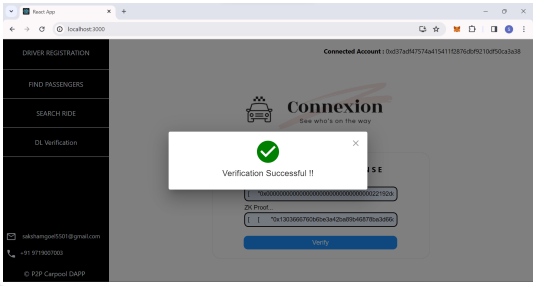

Figure 6: Successful Verification when hash and ZK proof are associated with each other.

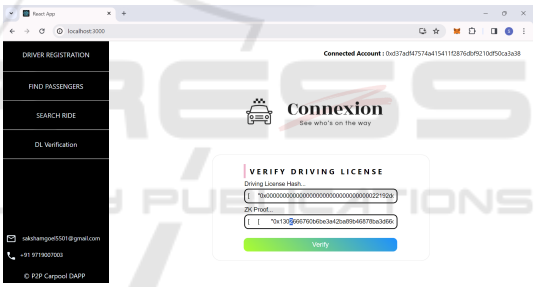

Figure 7: Driving License hash and altered ZK Proof entered for the verification.

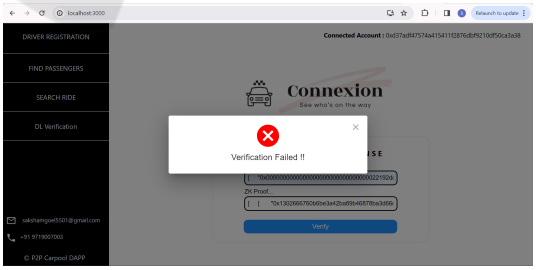

Figure 8: Failed Verification when hash and ZK proof are not associated with each other.

5 CONCLUSION

The future potential of Blockchain technology holds tremendous promise, particularly in revolutionizing the ride-sharing system by addressing its current challenges. One of the key advantages of this technology lies in its consensus-based approach and check instrument, which enables the creation of a permanent and verifiable blockchain record. By doing so, it effectively prevents issues like double-spending without the need for intermediaries, fostering a decentralized setup. By implementing a trustless and transparent system, P2P ridesharing using blockchain technology brings forth a more secure and trustworthy platform for both riders and drivers. An essential aspect of this technology is its ability to establish a decentralized network, eliminating the need for intermediaries and reducing costs for passengers while simultaneously increasing profitability for drivers. This shift to a peer-to-peer model with the implementation of

Zero Knowledge Proofs not only streamlines the payment process but also enhances data security and privacy for all participants. As this technology continues to evolve, its impact on the ride-sharing industry is expected to be transformative, reshaping the way we commute and enhancing the overall transportation ecosystem. While the tamper-resistant nature of Blockchain enhances security and reduces data revalidation time, it also comes with drawbacks. For instance, the presence of fake requests in the Blockchain system can disrupt communication and burden the organization, posing challenges to maintaining consistent security and privacy due to the large volume of Blockchain data. To ensure the successful implementation and widespread adoption of Blockchain technology in ride-sharing and ITS, careful consideration of its limitations and potential security concerns is imperative.

6 FUTURE WORK

An application can be developed that leverages the powerful Google Maps API to display optimal routes between two given points based on their latitude and longitude. Additionally, the application cleverly incorporates the Web Geolocation API, enabling it to determine the user's precise location on the decentralized web platform, thus enhancing user experience and convenience. Scalability is a key consideration in the system's design. As the application's popularity grows and traffic increases, the system needs to dynamically adjust various parameters to ensure smooth functioning. Market-related Trends can be shown to the users. One such feature is the implementation of a sophisticated price-suggesting algorithm, empowering users to gain insights into price ranges and compare them with the drivers' suggestions. This feature aims to provide greater transparency and convenience for users during their journey-planning process. Time-locked deposit contracts, bioinformatics security features, etc. can be further enhancements in this work. These additional features hold the potential to further enhance the system's integrity, security, and overall efficiency.

REFERENCES

Augot, D., Bordage, S., El Housni, Y., Fedak, G., and Simonet, A. (2022). Zero-knowledge: trust and privacy on an industrial scale.

Ben-Sasson, E., Chiesa, A., Green, M., Tromer, E., and Virza, M. (2015). Secure sampling of public parameters for succinct zero knowledge proofs. In *2015 IEEE Symposium on Security and Privacy*, pages 287–304. IEEE.

Bozdog, N. V., Makkes, M. X., Van Halteren, A., and Bal, H. (2018). Ridematcher: peer-to-peer matching of passengers for efficient ridesharing. In *2018 18th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pages 263–272. IEEE.

Chang, S. E. and Chang, C.-Y. (2018). 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)*, pages 664–671. IEEE.

Dorri, A., Steger, M., Kanhere, S. S., and Jurdak, R. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, 55(12):119–125.

Ganapathy, V. and Easaw, G. (2017). Urban mobility in the era of sharing economy: An empirical study of smartphone app based ridesourcing services. *J. Glob. Econ*, 13:268–289.

Gudymenko, I., Khalid, A., Siddiqui, H., Idrees, M., Clauß, S., Luckow, A., Bolsinger, M., and Miehle, D. (2020). Privacy-preserving blockchain-based systems for car sharing leveraging zero-knowledge protocols. In *2020 IEEE international conference on decentralized applications and infrastructures (DAPPS)*, pages 114–119. IEEE.

Gupta, R. and Shanbhag, S. (2021). A survey of peer-to-peer ride sharing services using blockchain. *Int. J. Eng. Res. Technol*, 10(08):349–353.

Houerbi, K. R., Machfar, D., and Ayed, H. K.-B. (2023). Blockchain for ridesharing: A systematic literature review. In *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, pages 1–6. IEEE.

Jahan, Z., Parween, N., Chauhan, M., and Chhabra, M. (2023). Peer-to-peer self-driving car rental: A case study on the development and limitations of a novel transport system. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 5–9. IEEE.

Kanza, Y. and Safra, E. (2018). Cryptotransport: blockchain-powered ride hailing while preserving privacy, pseudonymity and trust. In *Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pages 540–543.

Kapassa, E., Themistocleous, M., Christodoulou, K., and Iosif, E. (2021). Blockchain application in internet of vehicles: Challenges, contributions and current limitations. *Future Internet*, 13(12):313.

Li, F., Xie, R., Wang, Z., Guo, L., Ye, J., Ma, P., and Song, W. (2019). Online distributed iot security monitoring with multidimensional streaming big data. *IEEE Internet of Things Journal*, 7(5):4387–4394.

Morris, D. Z. (2016). Today's cars are parked 95% of the time. *Fortune, March*, 13:2016.

Münzel, K., Piscicelli, L., Boon, W., and Frenken, K. (2019). Different business models–different users? uncovering the motives and characteristics of business-to-consumer and peer-to-peer carsharing adopters in the netherlands. *Transportation Research Part D: Transport and Environment*, 73:276–306.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*.

Prieto, M., Stan, V., and Baltas, G. (2022). New insights in peer-to-peer carsharing and ridesharing participation intentions: Evidence from the "provider-user" perspective. *Journal of Retailing and Consumer Services*, 64:102795.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., and Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21.

Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., and Kumar, R. (2019). A blockchain framework for securing connected and autonomous vehicles. *Sensors*, 19(14):3165.

Ruch, C., Lu, C., Sieber, L., and Frazzoli, E. (2020). Quantifying the efficiency of ride sharing. *IEEE Transactions on Intelligent Transportation Systems*, 22(9):5811–5816.

Schaller, B. (2021). Can sharing a ride make for less traffic? evidence from uber and lyft and implications for cities. *Transport policy*, 102:1–10.

Tafreshian, A., Masoud, N., and Yin, Y. (2020). Frontiers in service science: Ride matching for peer-to-peer ride sharing: A review and future directions. *Service Science*, 12(2-3):44–60.

Tran, Q. N., Turnbull, B. P., Wu, H.-T., De Silva, A., Kormusheva, K., and Hu, J. (2021). A survey on privacy-preserving blockchain systems (ppbs) and a novel ppbs-based framework for smart agriculture. *IEEE Open Journal of the Computer Society*, 2:72–84.

Uber (2019). Uber's united safety report.

Vadhan, S. P. (1999). *A study of statistical zero-knowledge proofs*. PhD thesis, Massachusetts Institute of Technology.