RideShareX: A Decentralized Ride-Sharing Platform using Blockchain

Dr. Nazirkar S. B.[1], Dr. Shah S.N.[2], Dhanraj Natakale[3],
Adiraj Sanas[4], Aditya Saste[5], Vaibhav Salunkhe[6]
[1,2,3,4,5,6]*Department of Computer Engineering, Sharadchandra Pawar College of Engineering and Technology, Someshwarnagar, Pune, India*

***Abstract*—The emergence of ride-sharing services has revolutionized urban mobility, offering a seamless transportation experience via mobile applications. While existing solutions employ a centralized approach, leading to significant commission costs, lack of driver autonomy, and privacy challenges, blockchain-based decentralized ride-sharing systems have been suggested as possible alternatives but struggle with latency issues and scala-Bility constraints. In this study, we propose RideShareX, a novel hybrid decentralized ride-sharing system that utilizes WebSocket for real-time communication and Ethereum smart contract-based escrow payments. By decoupling ride discovery and payment settlement processes, RideShareX ensures the system's scala-bility and decentralization properties. The framework includes geospatial filtering through the Haversine formula, deterministic wallet creation to ensure Web3 integration, publish/subscribe ride announcements, and one-time password (OTP) validation via Keccak-256 hashing. The experimental results show that RideShareX is able to maintain ride broadcast latency below 100 ms while ensuring decentralized payment transactions' security.**

***Index Terms*—Ride-sharing, blockchain, smart contracts, Web-Sockets, decentralized applications, Ethereum, deterministic wal-lets**

I. INTRODUCTION

The emergence of ride-sharing platforms has had a sig-nificant impact on mobility. It allows riders to book rides by downloading the app on their smartphones. Ride-hailing applications such as Uber, Lyft, and Ola not only benefit riders but also improve the efficiency of vehicles and minimize traffic congestion in urban centers. Ride-sharing applications link riders with local drivers using mobile applications with the help of GPS technology. The popularity of ride-hailing services can be seen by the fact that these applications have contributed to the establishment of a global mobility network that enables millions of rides per day around the globe.

Despite being prevalent for several years now, all ride-sharing platforms utilize a centralized architecture wherein ride-matching, payments, validation, and pricing are managed by the platform itself. There are numerous disadvantages associated with the adoption of centralized architectures. First, the commissions charged by the ride-hailing firms for making the booking happen vary between 20% and 30% of the overall cost of the trip, which significantly reduces the income for drivers. Second, the centralization of operations restricts the freedom of action for drivers and reduces their options. Third, the centralization of information of the users creates risks for the privacy of the users. Cases where ride sharing information was stolen are proof of the danger associated with storing user information centrally.

With the development of blockchain technology, a suitable remedy has emerged in the form of decentralized mobility apps. The term blockchain can be described as a ledger system, which facilitates secure transactions between peers. The application of smart contracts enables the parties involved to conduct the transaction transparently without fear of fraud. Various studies have explored the implementation of the blockchain technology for solving trust, accountability, and decentralization problems in ridesharing apps. For instance, Arunkumar et al. suggested an innovative blockchain and smart contract system that tackles issues like data exploitations and privacy problems common in legacy systems [1]. Li et al. implemented a novel blockchain system that incorporated zero-knowledge proof to authenticate the driver and guarantee user anonymity [2]. Lu et al.

developed a decentralized audit model for recognizing disqualified drivers by implementing smart contracts [3].

Privacy is one of the key issues examined in decentralized rideshare models. For instance, Baza et al. created a rideshare protocol that applied blockchain technology that uses location cloaking and pseudonyms for preventing users from disclosing their actual location information [4]. In contrast, Hossan et al. developed a ridesharing protocol that employs the Hyperledger and Interplanetary File System technologies to securely record the complaint and rides transactions via tamper-proof methods [5].

However, there exist many disadvantages inherent to ride sharing based on blockchain technology. Firstly, public blockchain-based networks suffer from long transaction la-tencies. The confirmation of a block and establishing the consensus take a lot of time, which leads to large transaction latencies. For example, the process of confirming a block in the Ethereum network takes several seconds to minutes. Consequently, it is impossible to provide ride matchings, driver discovery, and GPS tracking in real time due to high transaction latencies.

Some studies have explored the possibilities of designing hybrid architecture, which can provide security guarantees provided by blockchain technology together with traditional computing infrastructure. For example, Abu Hashim and Tan explored the methods of indexing smart contracts, which can improve the performance of blockchain networks [6]. Also, Nama Sudra and Sharma offered a decentralized cab-sharing solution, which uses blockchain technology and access control based on encryption [10]. However, such solutions suffer from long transaction latencies.

In order to address these problems, RideShareX, a decentralized hybrid architecture for ride sharing which consists of two separate components - one for real time communication and other for managing payments, is proposed. In the proposed architecture, WebSocket communication protocol is going to be used for real time communication between the ride share service provider and users while Ethereum smart contracts are going to manage escrow payments. The combination of WebSocket communication and Ethereum smart contracts in the proposed architecture is helpful in combining the bene-fits of both technologies, providing low latency performance similar to that of conventional ride-sharing architectures but decentralized transactions.

The proposed Rideshare framework employs various tech-niques including geospatial filtering of drivers by applying Haversine formula, ride broadcasting through WebSocket, wallet creation based on identity of users, distance-based fare estimation, and OTP based authentication using Keccak-256 hashing function.

The remainder of the paper is organized as follows. In section II, we have provided a summary of literature review on ride sharing systems developed using the blockchain approach. In section III, we present the design of architecture for the proposed RideShareX framework. In section IV, there is an analysis of comparison between existing models for ride sharing system and proposed ride sharing system. In section V, the process flow of the system is explained. Section VI is related to the algorithm of the framework. Section VII is related to the security model of the framework. In section VIII, we provide the result of experimentation on the framework.

II. LITERATURE SURVEY

The main contributions of this work are summarized as follows:

- A mixed ride-sharing architecture utilizing real-time communication through WebSocket's combined with smart contract payments on the blockchain.
- Decentralized ride matching using pub/sub communication without ride matching from a center.
- An escrow payment system based on Ethereum smart contracts.
- A design focused on privacy and uses deterministic wallet generation to connect users without revealing any private keys.
- Comparison demonstrating the advantage of the proposed solution compared to blockchain ride-sharing solutions.

Many researchers have studied blockchain-enabled ride-sharing systems that lack intermediary participation. Arunkumar et al. created a ride-sharing platform using blockchains and smart contracts in order to increase security and integrity due to the elimination of data exploitation [1].

Li et al. came up with an identity verification

scheme on blockchain using zero knowledge proof for verifying the identity of the driver without exposing his/her personal data [2].
The decentralized auditing system was proposed by Lu et al., which uses smart contracts to verify if the driver is eligible to offer rideshare service and eliminate malicious users from utilizing the network [3].
As proposed by Baza et al., the ride-sharing framework sends cloaked ride request messages to avoid disclosing the actual locations of pick-up points of the riders [4]. The driver submits his/her ride proposal in ciphertext form to ensure safe ride matching.
An innovative ride-sharing security solution based on Hy-perledger and IPFS using blockchain technology was pre-sented by Hossan et al. The use of blockchain ensures that the transactions about rides and complaints remain immutable [5].
Additionally, Abuhashim and Tan have explored the in-dexing of smart contracts to secure ride-sharing data in a blockchain [6]. The authors discuss challenges related to blockchain-based query processing.
Despite the evidence that blockchain technologies can be used in ride-sharing systems, almost all of them rely heavily on blockchain transactions, which delay the process significantly. To address this challenge, the RideShareX system makes use of off-blockchain communication methods in matching rides. Design of RideShareX is that of a hybrid architecture that comprises three major layers.

III. SYSTEM ARCHITECTURE

The design of RideShareX is that of a hybrid architecture that comprises three major layers.

A. Client Layer

The client interface is built as a multiplatform mobile application using the React Native library alongside the Expo framework. This layer consists of two categories of users, namely riders and drivers. The interface has support for map visualization, rides request, navigation, and payments. Map-ping is done using Leaflet.js within a React Native WebView using OpenStreetMap tiles.

B. Communication Layer

Node.js and Express.js are used to build the backend server. Real-time communication is facilitated between drivers and riders using WebSockets from the Socket.io library.
WebSocket server is responsible for broadcasting rides offers to the nearest drivers.

C. Blockchain Layer

Finances are processed with the help of the Ethereum smart contract deployed within the Sepolia test network. Escrow payment handling is automated and the funds are released after successful completion of a ride. Wallets are created locally on the client-side by means of RPC nodes, allowing users to keep custody of their finances.

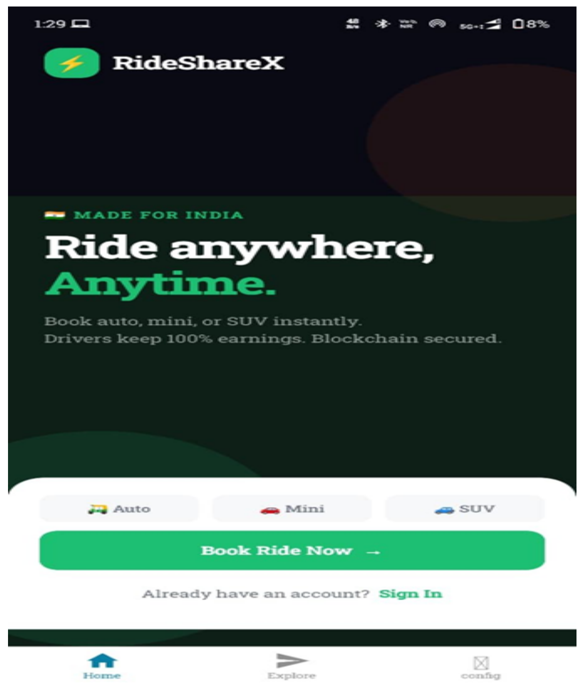

Fig. 1. RideShareX mobile application landing screen depicting decentralized ride-hailing platform user interface.

IV. COMPARATIVE ANALYSIS

Comparative analysis considers different blockchain-based ride-sharing solutions in terms of decentralization, privacy methods, payment structures, and system efficiency. Although existing ride-sharing systems have a strong emphasis on security or decentralization, they all lack some features regarding scalability. The RideShareX system incorporates a hybrid approach enabling high performance along with decentralized finance operations.
Comparison table between existing architectures of ride-sharing and RideShareX system in terms of

decentralization, privacy approaches, payment's structure, and limitations of the system is presented below.

V. SYSTEM WORKFLOW

The RideShareX system flow includes the following pro-cesses:

1) The rider creates a ride request.
2) Back-end computes available drivers through the use of the Haversine formula.
3) The ride request is communicated to the drivers using WebSocket channels.
4) A driver accepts the ride request.
5) Rider pays for the ride by transferring the fare into the smart contract.
6) Driver completes the ride.
7) Rider confirms the completion of the ride using one-time-password (OTP).
8) The smart contract pays out the ride amount to the driver.

VI. ALGORITHMS EMPLOYED

A. Haversine Distance Formula

The Haversine distance formula can compute the distance between any two coordinates

$$d = 2r \arcsin \sqrt{\sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_1)\cos(\phi_2)\sin^2\left(\frac{\Delta\lambda}{2}\right)} \quad (1)$$

The Haversine distance algorithm facilitates the efficient filtering of available drivers in close proximity

B. Publish-Subscribe Communication Paradigm

RideShareX adopts the publish/subscribe pattern whereby the ride requests will be pushed to those drivers who are nearby. The driver alone will decide whether he or she accepts the ride requests, which makes ride matching decentralized

C. Deterministic Wallet Generation

To circumvent the high entry barrier into Web3 technologies as well as the requirement for mnemonic, RideShareX makes use of a deterministic wallet

PrivateKey = Keccak256(SecretKey Username) (2)

which ensures wallet restoration on any other device with certainty, guaranteeing that the same identity is used across devices

D. Deterministic Pricing Model

Ride fare is calculated using a transparent and immutable fixed formula

Fare = BaseFare + (Distance × RatePerKM) (3)

VII. SECURITY ARCHITECTURE

The system integrates multiple security mechanisms.

- AES-256 encryption for driver identity documents
- HMAC-SHA256 authentication tokens
- Smart contract escrow payments
- Keccak-256 hashing for OTP verification

These mechanisms protect both rider and driver data.

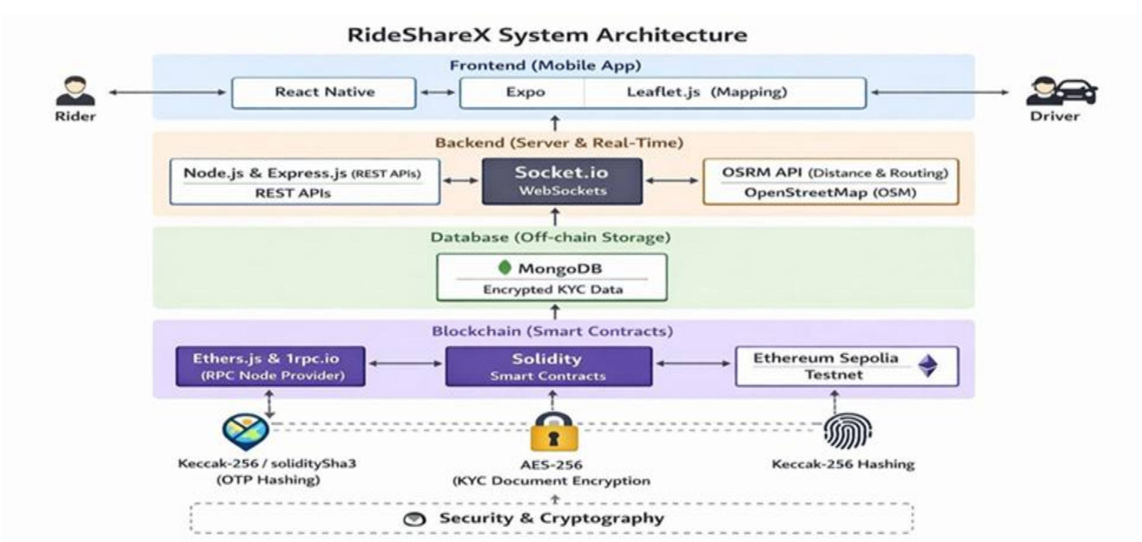

Fig. 2. RideShareX hybrid decentralized architecture integrating WebSocket communication, off-chain database storage, and Ethereum smart contract settlement.

Table I Comparison of Ride-Sharing Architectures

Reference/System		Year	Blockchain Used	Privacy Mechanism	Payment System	Remarks / Limitations
Arunkumar et al. [1]		2024	Blockchain Framework	Decentralized Structure	Smart Contracts	Focuses on mitigating data exploitation
						but lacks hybrid real-time mechanisms.
Li et al. [2]		2020	Hyperledger Fabric	Zero-Knowledge Proof	Not specified	Focuses on identity verification but does
						not address ride matching latency.
Lu et al. [3]		2021	Hyperledger Indy +	Decentralized identity au-	Smart contract incen-	Provides driver qualification verification
			Fabric	diting	tives	but lacks real-time ride discovery.
Baza et al. [4]		2020	Ethereum	Location cloaking,	Blockchain payments	Preserves rider privacy but introduces
				pseudonyms		blockchain latency during ride match-
						ing.
Hossan et al. [5]		2021	Hyperledger + IPFS	Secure complaint storage	Blockchain payment	Ensures transparent ride logs but lacks
					system	real-time communication mechanisms.
Abuhashim et al. [6]		2020	Ethereum	Data indexing smart con-	Smart contract trans-	Improves blockchain query efficiency
				tracts	actions	but does not address ride discovery.
Traditional	Platforms		None	Limited privacy protec-	Centralized payment	High commission fees and centralized
(Uber/Ola)				tion	gateway	control over ride allocation.

VIII. EXPERIMENTAL EVALUATION AND RESULTS

The design of the proposed RideShareX system was tested through implementation using a mixed Web2/Web3 architec-tural approach. Ride broadcasting in real time using WebSock-ets and decentralized payment transactions via Ethereum smart contracts running on the Sepolia testnet were incorporated into the framework for experimentation and testing of its performance and usability.

A. User Interface Implementation

In the proposed RideShareX system, separate user interfaces are available for both riders and drivers. In the case of riders, location for picking up passengers and their final destinations is selected by using Leaflet.js integrated into the interface through the use of React Native WebView. After the user makes the ride booking request, it gets broadcasted to the nearby drivers.

Fig. 3 illustrates the rider interface used for selecting pickup and destination locations.

B. Driver Request Dashboard

Ride requests are sent to drivers through the WebSocket publish-subscribe protocol. Drivers will not be forced to accept rides using an algorithmic approach; they can instead choose

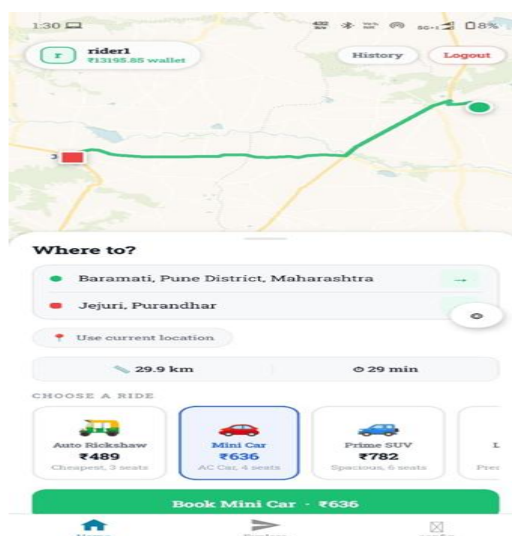

Fig. 3 illustrates the rider interface used for selecting pickup and destination locations.

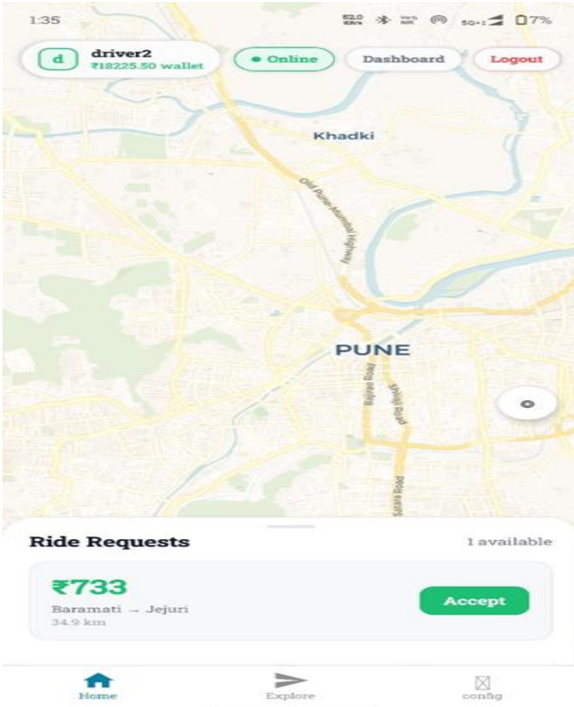

Fig. 4 shows the driver dashboard displaying incoming ride requests.

whether to accept the rides based on their own routes and prices

Fig. 4. Driver interface showing real-time ride requests broadcast using WebSocket communication.

C. Wallet and Deterministic Identity

The RideShareX wallet interface demonstrates the seamless integration of Web3 features, highlighting the user's total balance and deterministically generated Ethereum address.

D. System Performance Analysis

Performance evaluation was done considering latency fac-tors related to ride broadcasting, API calls, and blockchain transactions. The experimental results indicate that the pro-posed hybrid architecture is successful in implementing the low-latency ride matching process along with securing pay-ments through decentralization.

The findings have proven that the RideShareX system can still provide the same real-time capability for ride discovery compared to existing ride-hailing apps without sacrificing the benefits of blockchain-enabled transaction systems such as trust and transparency

Table II System Performance Evaluation

Metric	Result
Ride broadcast latency	< 100 ms
API response time	< 50 ms
Blockchain transaction confirmation	10 15 s
Driver discovery radius calculation	< 5 ms

E. Security Evaluation

The security features implemented within the system in-clude encryption using AES-256 for KYC document storage, tokenization using HMAC-SHA256 for session management, and hashing using Keccak-256 for one-time password (OTP) validation in the context of ride completion.

In summary, the findings from the experiments suggest that the proposed RideShareX architecture successfully combines decentralized characteristics with security and efficiency.

IX. DISCUSSION

From the experimental results, it can be concluded that the RideShareX framework effectively manages to integrate the benefits of conventional ride-hailing applications along

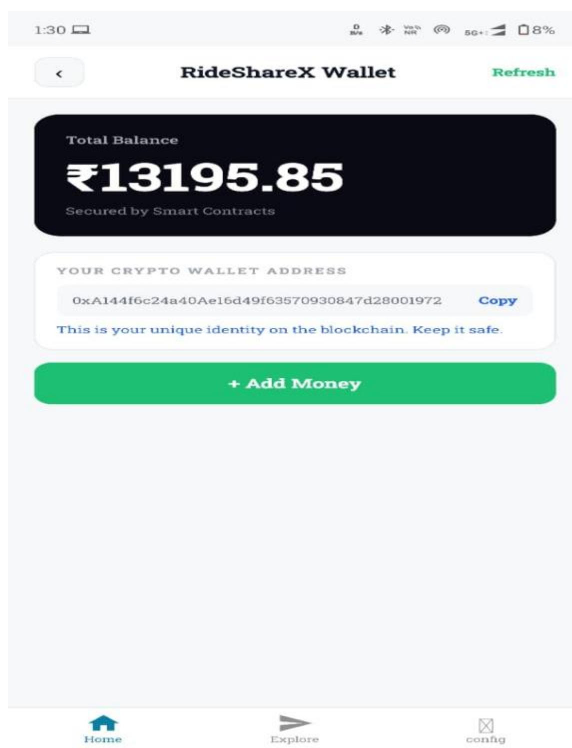

Fig. 5. RideShareX Wallet interface displaying deterministic identity and testnet ETH balance.

with the added advantage of blockchain-based transactions and transparency mechanisms. The hybrid approach allows the proposed application to achieve real-time ride discovery capabilities along with decentralized secure payments via smart contracts.

One of the major discoveries achieved in this research is that separating the communication module from the blockchain module improves performance dramatically. In the fully-decentralized approach, every action in a ride-hailing app needs to be written into the blockchain, causing noticeable transaction latencies due to block confirmation process times. RideShareX utilizes WebSocket communication for ride dis-covery and ride broadcasting resulting in less than 100 ms latency.

The absence of intermediaries in financial transactions is another significant advantage of the suggested framework. Traditionally, ride-sharing applications employ centralized in-termediary institutions that impose service charges averaging from 20% to 30% of the ride fee. RideShareX, on the other hand, utilizes Ethereum smart contracts to process payments using a decentralized escrow model. Thus, the drivers receive the full amount of the ride fee in RideShareX.

Concerning security and privacy, the solution is equipped with robust measures to safeguard sensitive information from potential security breaches. First, the driver KYC documents are secured using AES-256 encryption, guaranteeing safety even when a security breach occurs in the MongoDB database. Second, the Keccak-256 algorithm guarantees OTP verifica-tions without disclosing any ride completion codes to the blockchain network. Deterministic wallet generation further improves convenience by enabling users to work seamlessly with Web3 protocols without revealing their seed phrases.

In terms of scalability, the use of the hybrid architecture that combines Web2 and Web3 technologies is a viable approach to developing and implementing decentralized ride-hailing services in practical scenarios. Specifically, by excluding high-frequency actions (such as location updates, requesting rides, and finding drivers) from the blockchain, one can avoid high fees and ensure smooth service operation. Nevertheless, actions requiring transparency and reliability, such as pay-ment and transaction verification, will be conducted on the blockchain.

As compared with the blockchain-based ride-hailing ser-vices considered in literature and mentioned above, the sys-tem proposed here is characterized by a balance between decentralization, scalability, and performance. Previous models were more concerned about the aspect of decentralization but failed to provide a low-latency solution. Thus, the proposed hybrid approach helps solve this problem without sacrificing the benefits provided by blockchain.

Overall, the analysis of results shows that the proposed sys-tem is a viable solution that allows implementing decentralized ride-hailing services efficiently. The combination of communi-cation technologies and blockchain-based payments represents a promising trend in the development of decentralized mobility platforms.

X. CONCLUSION

In this paper, we discussed the development of a hybrid decentralized ride-sharing solution called RideShareX that combines WebSocket messaging with blockchain smart con-tract technology to provide real-time matching of ride offers and decentralized payments.

The experimental analysis revealed enhanced scalability and transparency in comparison with traditional ride-sharing solutions.

Further research will focus on incorporating Layer-2 blockchain services and AI for ride demand forecasting.

REFERENCES

[1] J. Arunkumar, S. Nair, and R. Menon, "Design of blockchain and smart contract enabled ride sharing platform," in *Proc. IEEE Int. Conf. for Women in Innovation, Technology & Entrepreneurship (ICWITE)*, 2024.

[2] W. Li, C. Meese, H. Guo, and M. Nejad, "Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof," in *Proc. IEEE Int. Conf. on Hot Information-Centric Networking (HotICN)*, 2020.

[3] Y. Lu, J. Zhang, Y. Qi, S. Qi, Y. Li, H. Song, and Y. Liu, "Safety warning! Decentralised and automated incentives for disqualified drivers auditing in ride-hailing services," *IEEE Transactions on Mobile Computing*, 2021.

[4] M. Baza, M. Mahmoud, G. Srivastava, W.

Alasmary, and M. Younis, "A light blockchain-powered privacy-preserving organization scheme for ride sharing services," in *Proc. IEEE Vehicular Technology Conference (VTC)*, 2020.

[5] 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," in *Proc. Int. Conf. on Computer and Information Technology (ICCIT)*, 2021.

[6] Abuhashim and C. C. Tan, "Smart contract designs on blockchain applications," in *Proc. IEEE Symp. on Computers and Communications (ISCC)*, 2020.

[7] L. A. D. Bathen, G. H. Flores, and D. Jadav, "RiderS: Towards a privacy-aware decentralized self-driving ride-sharing ecosystem," in *Proc. IEEE Int. Conf. on Decentralized Applications and Infrastructures (DAPPS)*, 2020.

[8] S. Chopra, B. Palanisamy, and S. Sural, "Credit-based peer-to-peer ride sharing using smart contracts," in *Proc. IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC)*, 2022.

[9] T.-M. Choi and X. Shi, "On-demand ride-hailing service platforms with hired drivers during coronavirus (COVID-19) outbreak: Can blockchain help?" *IEEE Transactions on Engineering Management*, 2022.

[10] S. Namasudra and P. Sharma, "Achieving a decentralized and secure cab sharing system using blockchain technology," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 15568–15577, 2023.