RESEARCH ARTICLE OPEN ACCESS

Decentralized Easyride using Smart Contracts

Meenu Shukla*, Ashish Kumar Singh, Pradyumn Kumar Shukla**, Ayush Singh Rawat****

Information Technology, Abdul Kalam Technical University Lucknow (U.P.)

ABSTRACT

As the technology is growing immensely in recent years, certain improvisation needs to be made in transportation sector too. As we know in today's world, we have options like cash and Online payment methods (like Paytm, Pi etc.) on the other hand we are also seeing the rapid growth of Cryptocurrency nowadays in the market to avail many goods and services, thus keeping in mind this we have decided to put the option of cryptocurrency on the cards for ride hailing and by using the concept of blockchain and combining with various modern technology. In this paper we are proposing our system PickupGenZ. This will be decentralized and will operate with the help of smart contracts and thus solving the current centralized ride hailing services anomalies like data tampering. We will use cryptocurrency (specifically Ethereum currently) as a method of payment along with regular payment modes. This is a step towards improving our current transportation system and aiding in building smart cities.

Keywords — PickupGenZ, Ride hailing, Cryptocurrency, Decentralized ride, Smart contracts

I. INTRODUCTION

Transportation is a very significant part of any country or state. It is the key through which all the development takes place. Ride hailing services are a vital part of this transportation [1] and thus in recent years these services have evolved a lot. Ride hailing applications are available now which are being used for availing on demand ride hailing services. These applications are centralized in nature and thus are vulnerable to data tampering and ransomware attacks. In addition, there are concerns about the safety and security of customer information [2]-[4] and their transnational data in relation to these centralized platforms. In distributed denial of service attacks maintaining and managing a central server is costly and highly vulnerable for attacks. In the stream of centralized systems response time to queries from a remote location the cloud server of the company result in an unavoidable increase in response delay due to high bandwidth usage. Due to this the current centralized Ride hailing systems are again questionable in terms of flexibility, accuracy, data integrity and stability. Blockchain technology has drastically changed various aspects of the information technology in recent times. Blockchain is a public database that records every transaction. A transaction can be as simple as sending someone money in the network. This is also introduced the usage of bitcoin by Satoshi Nakamoto. Bitcoin may have been the first to use blockchain technology, but there are many industries in which their applications have been emerged [5]-[8] except finance since 2009 app ideas are still being created, tested, and improved over time. Blockchain gains momentum while driving allowing people to connect directly with the drivers they want for their transport [9]. Blockchain based ride hailing platforms can alleviate the above problems by simplifying cooperative driving between drivers and passengers. Instead of agreeing on one trusted centralized authority, participants share transaction data across a large network of nodes. This eliminates the middlemen doing any monitoring role. This makes it more transparent as the transaction details are maintained in a distributed ledger to which all nodes of the blockchain network can access. What powers the blockchain, they work based on a timestamp a list of blocks about which data is recorded, shared, and aggregated transactions that have ever occurred within the blockchain network. When a block fills up, it is added to the blockchain. Each block is encrypted and associated with a hash code of the previous one, which prevents anyone from making changes to block. Thus, a transaction which is being shared are permanent records, irreversible, immutable, and highly secure. These are definitely the most interesting characteristic of blockchain which helps to build trust. What powers the blockchain, they work based on a timestamp a list of blocks about which data is recorded, shared and aggregated transactions which have ever takes place within the blockchain network. When a block fills up, it is added to the blockchain. Each block is encrypted and associated with a hashcode of the previous one, which prevents anyone from making changes to block. Thus, transactions are permanent records that they are shared, irreversible, immutable, and highly secure. These are undoubtedly the most interesting features of blockchain helps build trust [10]. In this paper, we have represented our idea of using this blockchain technology to make an efficient ride hailing system and to also provide cryptocurrency as a payment option. Use of smart contracts will enable automatic assets transfer and will also reduce the manual workload in the process. In addition, we are motivated by the protection of user's personal data to choose a private rather than a public blockchain. This feature allows you to limit the visibility of information in the network, but still decentralized. Further in contrast, it reduces the cost of creating a blockchain in traditional public blockchain.

II. LITERATURE REVIEW

Title	Author's Name	Year of Publication	Methodology Proposed	Summary
Boosting ridesharing efficiency through blockchain: GreenRide application case study	S. Khanji and S. Assaf [14]	2019	It utilizes decentralization and distribution nature of blockchain to create the GRT to reward users for their carbon emissions reduction. Users information along with application transactions are all conducted via Cloud to spare users time while locating their suitablerides	GreenRide, a smart ride sharing service incentivizes its users through token incentives. This research looks towards increasing ride sharing efficiency by leveraging the blockchain's benefits of decentralisation, trustlessness, and scalability. Also focussed on reducing carbonemissions.
SRide: A privacy-preserving ridesharing system	U. M. A¨ıvodji, K. Huguenin, et.al[15]	2018	Firstly generalized user spatiotemporal data is evaluated then a secure filtering algorithm is employed. For each viable combination, it computes a ridesharing score using an upgraded version of Priv-2SP-SP, a privacy-preserving protocol for computing meeting places for ridesharing.	This paper proposes a privacy preserving protocol for ridesharing that addresses matching problem for dynamic ridesharingsystems.
Co-utile p2p ridesharing via decentralization and reputation management	D. Sanchez, S. Mart ´ ´ınez, et.al [16]	2016	Decentralized P2P ride sharing system with protocols which are self-enforcing and mutually beneficial by relying on co-utility notion.	Paper proposes recently proposed notion of co-utility (essentially, self-enforcing, and mutually beneficial collaboration), which ensures that rational (even purely selfish) peers will find no incentives to deviate from the prescribed protocols.
Oride: A privacy- preserving yet accountable ride-hailing service	A. Pham, I. Dacosta et.al [17]	2017	Privacy preserving ride hailing system based on homomorphic encryption with optimizations such as ciphertext packaging and transformed processing.	Paper's goal is to design a Ride hailing service that provides stronger privacy guarantees to both riders and drivers, as well as better usability and accountability.

Pebers: Practical Ethereum blockchain based efficient ride hailing service	Kudva, Sowmya, et.al [18]	2020	Decentralized Ride hailing System based on Consortium Blockchain.	PEBERS: Practical Ethereum Blockchain based Efficient Ride Hailing Service, in which it is demonstrated how decentralized system based on consortium blockchain can be developed to keep track of ride data over blockchain network.
A Decentralized Ride-Hailing Mode Based on Blockchain and Attribute Encryption	Zhang, Yifan, et.al [19]	2022	Decentralized blockchain based ride hailing mode with attribute encryption.	In this paper a decentralized blockchain based ride hailing mode with attribute encryption is presented which has been simulated on test net of Ethereum.

III. DECENTRALISED SYSTEM

The traditional centralized model has to be improved to address the issues outlined in section 2. It is suggested that you employ a decentralized strategy. Blockchain as it is now understood is a peer-to-peer, decentralized public ledger that enables transactions to happen without the use of intermediaries. Additionally, every transaction on a blockchain network is safe, transparent, and immutable. The adoption of blockchain in ride-sharing services is a result of the elimination of the intermediary and the cost-effectiveness of transactions between users and drivers. This draws additional users on board and offers them financial advantages. According to S.E. Chang et al., blockchain incorporates new tech into the community and adds various social dimensions for efficient resource allocation, the delivery of high-value services, and the optimization of the general public's quality of life, the adoption of Blockchain technology in ride sharing services will bring us closer to the concept of a smart city [13]. Below is a summary of several advantages blockchain technology has over a centralized paradigm[14].

A. Transparency

Although Blockchain is anonymous at the same time, it ensures the transparency of transactions. As a result, in the event that something goes wrong, information can always be traced back. With the blockchain, data is accessible across the network and adversaries may see each other in fulltransparency.

B. Safety

Since all the data in a blockchain is cryptographically safeguarded, data authenticity is ensured. It is impossible for the network to contain any fake data.

C. Safe Payments

Users will be able to send a secure payment straight to thedrivers with the help of smart contracts.

IV. CRYPTOCURRENCY

A cryptocurrency is a type of digital currency that employs encryption to guard against fraud and double-spending. The decentralised networks of many cryptocurrencies are based on blockchain technology, a decentralised ledger enforced by a decentralised network of computers. Cryptocurrencies may be immune to government intervention or manipulation because they are frequently not issued by a centralized power.

V. PROPOSED METHODOLOGY

Taking current work in consideration, a decentralized P2P system is proposed. A decentralized Ethereum blockchain is used as the foundation of a decentralized application (DApp), which will serve as the front-end interface. According to this structure, the user and the driver will both be identified and then will get registered in the blockchain network. Each of their profiles has this required data attached, and every node in the network could view it.

The workflow is given below [17].

1. The driver sends his driver's license and other required documents to get registered in the network.

2. As soon as the driver submits the info, network-connected legal authorities will be notified. To the driver profile, a record and note check will be performed. A smart contract
[16] creates a driver review or rating that the rider can use todecide whether to ride with a certain driver.

3. Users who want a ride should register with the network by providing the appropriate details, such as their name, phone number, etc. Background checks will also be conducted in a similar manner. This promotes driver's safety.

4. The user may request cabs by entering his or her

location information as well as other trip details once verification is complete. The driver responds to the users' request and estimates the cost of the trip based on a number of factors, including the miles to travel, the type of vehicle, and a set fee per kilometer.

5. Riders can now select rides based on their level of comfort.

6. Payment can be transferred automatically through one wallet to another as a cryptocurrency payment after the ride is over.

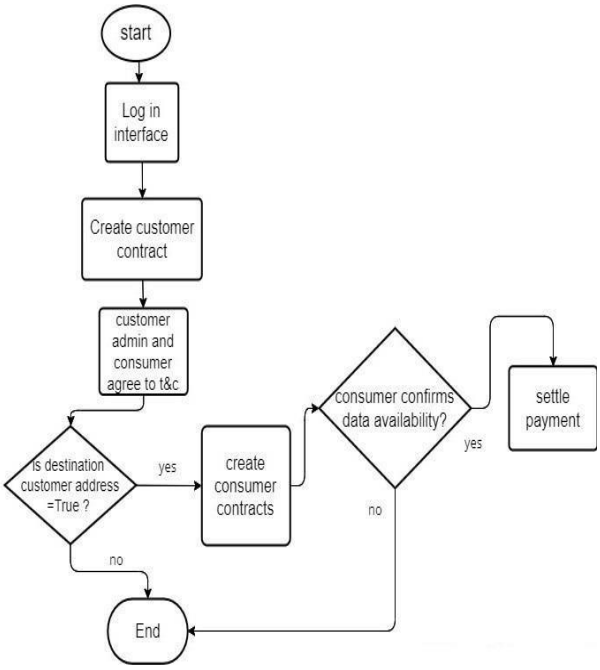

Fig. 1 Proposed blockchain-based carpooling architecture

A. MetaMask

MetaMask is a cryptocurrency wallet mainly used for the Ethereum blockchain.
As we need a crypto wallet to make a transaction with a blockchain, a wallet is a personal key to interact with the cryptographic world as it facilitates us to buy, sell or transfer assets on the blockchain. MetaMask is a well-known and trusted wallet for the most diverse Ethereum blockchain. It is available as an application for iOS and Android, we can also use this as an extension with a few web browsers: Chrome, Firefox, Brave, and Edge. MetaMask is a free, open-source and hot wallet to deal with Ethereum.

Some prominent features of this wallet:

1. Easy to Use

Starting the MetaMask is very easy, quick, and we don't even need an email address, just set the password and remember (store) the secret recovery phrase, and done.

2. High Security

Our information is securely encrypted in our browser and nobody has access to retrieve the lost password, we have the 12-word secret recovery phase (seed phrase) for recovery. It's necessary to keep the seed phrase safe because even MetaMask has no information about it, Once it is lost, it can't be retrieved again.

3. Ease of Backup and Restore

MetaMask stores our information locally. So, if we switch browsers, we can restore our MetaMask wallet with our secret recovery passphrase.

4. Well Established Community Support

As of now, MetaMask deals with 30 million monthly active users around the world, its simple and congenital user interface keeps pushing these numbers with a recorded 5x increase from past year.

5. Conclusively

MetaMask is reliable and trusted hot wallets for Ethereum, Various terms are used to facilitate the MetaMask like- Public and Private Keys, Multiple Accounts, Buy, Send & Swap, Buying Ether, Sending with MetaMask, Token Swap, Account Import etc.

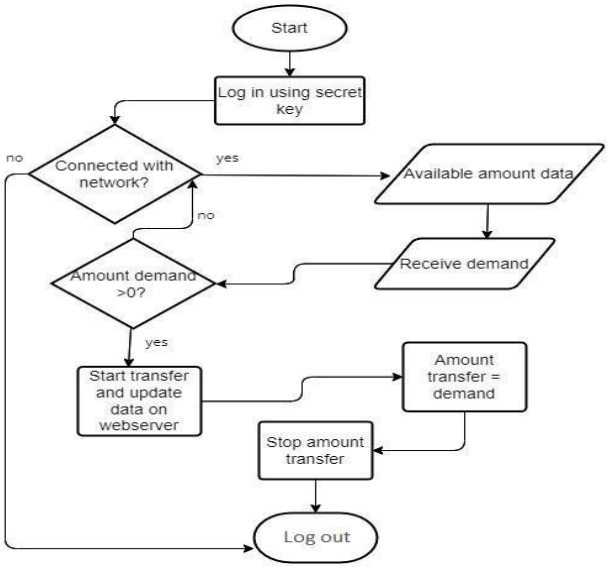

Fig. 2 MetaMask Transition flow diagram.

B. Block Diagram

Block diagram represents the overall structure where principle parts or functions are represented by blocks connected by lines which shows the certain kind of relationships among the blocks. Similarly, we have explained the relatedness between the various objects and technology in the below diagram.

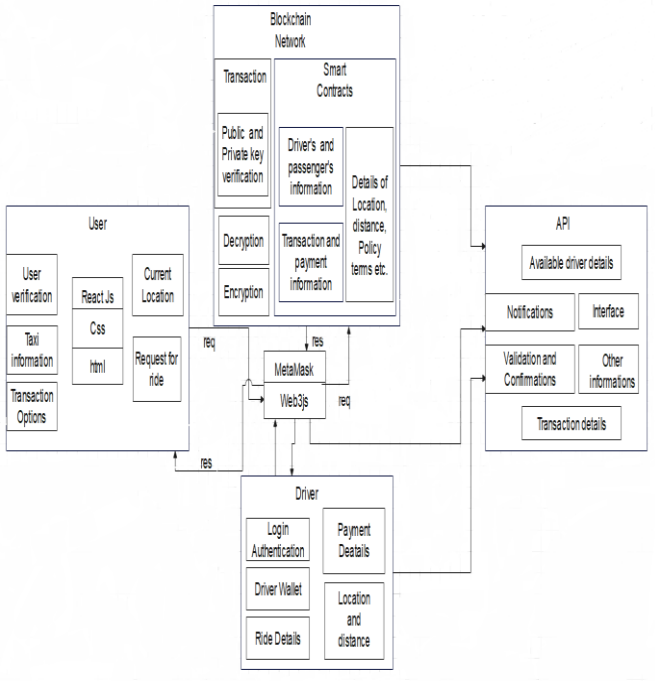

Fig. 3 Block diagram

C. User

The basic and initial process are performed initially at the user level like – location retrieval, UI/UX which internally created using the technologies like html, CSS, React etc

D. Blockchain Network

Blockchain network mainly deals with the functions performed at the machine or technical implementation level, here main concern is about how the process are exactly performed like handling of Transactions through blockchain using various public and private keys, Encryption, Decryption, smart contracts etc.

E. API

API (Application Programming Interface) is mainly responsible for the proper communication between the various components and shows the end results at user interface, like it represents the notifications, transaction details, validations and confirmations etc.

VI. IMPLEMENTATION

A. Tools And Libraries

For developing DApp, a variety of resources and libraries are available. However, a quick discussion of the resources and libraries used to create this ride-sharing DApp is provided under.

A. *Blockchain:* To resolve the problem of data security by forming a trusty chain.
B. *Cryptocurrency:* To use the cryptocurrency (Ethereum) for availing Ride Hailing Services.
C. *Web 3.0:* This technical dimension will help us to create a smart contract automated ecosystem and will also help us leveraging the power of blockchaintechnology.
D. *Ethers.js:* For communicating with the Ethereum blockchain and it's ecosystem.
E. *Sanity.io:* For Database.

B. Process flow For ridesharing DApp

With the help of the local Ethereum framework, MetaMask, Web3js, Nodejs, and Sanity.io, we are creating a prototype of the suggested framework. For this DApp, there are two different categories of stakeholders: drivers and riders. Each user has unique roles and responsibilities, which are provided by several DApp dashboards. The dashboard of the driver shows,

1. Information about user pick-up and drop-off
2. Fare
3. Payment Status

While rider dashboard shows,

1. Pickup and drop details
2. Fare

The DApp contains a frontend that runs on the backend and decentralized platform.

VII. CONCLUSION AND FUTURE WORK

This paper's main goal is to examine the revolutionary Blockchain and its application in the financial sector, which can act as a foundation for the concept of a modern city. A current architecture for decentralized P2P, blockchain-based ride-sharing systems is presented in this article, along with plans for further development of the same. A decentralized application (DApp) has also been developed to help this ride- sharing system. It will support blockchain by serving as the front-end user interface. In this DApp, transactions and exchange of information throughout the network are mechanized using smart contracts on Ethereum, the publicly permissionless blockchain. In conclusion, blockchain can be utilized to build a system with smart contracts stored in decentralized, transparent databases which are encoded in digital code. These databases' data is regarded as volatile. There should be a digital record for every procedure and task, which will be then identified and authenticated with the help of digital signature. We can create an ecosystem without the need for additional middlemen. Although the real implementation of blockchain is still many years away, it is undoubtedly changing business structures and governance.

Blockchain technology is not the revolutionary technology that will fully displace current business practices with less priced substitutes. Instead, it might be seen as a fundamental technology that can build new frameworks for issues in the market and society.. Blockchain is not a temporary fix for a persistent technological issue. A precise plan built on prospects that have been proven to work must be devised, but it can aid in the changeover. Although blockchain will have a significant impact, it will take a long time for it to permeate our socio-economic system. The acceptance of these waves of technological and structural change will be gradual and steady rather than abrupt.

In the future, we will

1. Examine the development's price and effectiveness.
2. Since blockchain is a trust-free system that enables consumers to trust data, it is important to investigate the technology from a computational standpoint. While integrating blockchain technology with a bigger software system, it is crucial to understand the data processing capabilities even though overall data quality has improved.
3. Adding other cryptocurrency as payment option.

REFERENCES

[1] J. W. Smith, “The uber-all economy of the future,” The Independent Review, vol. 20, no. 3, pp. 383–390, 2016.

[2] A. Kayes, W. Rahayu, and T. Dillon, “Critical situation management utilizing iot-based data resources through dynamic contextual role modeling and activation,” Computing, vol. 101, no. 7, pp. 743–772, 2019.

[3] J. M. Robbins and A. M. Sechooler, “Once more unto the breach: What the equifax and uber data breaches reveal about the intersection of information security and the enforecement of securities laws,” Criminal Justice, vol. 33, no. 1, pp. 4–7, 2018.

[4] A. Kayes, J. Han, W. Rahayu, T. Dillon, M. S. Islam, and A. Colman, “A policy model and framework for context-aware access control to information resources,” The Computer Journal, vol. 62, no. 5, pp. 670– 705, 2018.

[5] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, “Towards secure smart parking system using blockchain technology,” Proc. of 17th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las vegas, USA, 2020.

[6] M. Baza, M. Fouda, M. Nabil, A. S. Tag, H. Mansour, and M. Mahmoud, “Blockchain-based distributed key management approach tailored for smart grid,” in Combating Security Challenges in the Age of Big Data. Springer, 2019.

[7] S. Badsha, I. Vakilinia, and S. Sengupta, “Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control,” in 2020 IEEE 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020

[8] G. Chen, B. Xu, M. Lu, and N.-S. Chen, “Exploring blockchain technology and its potential applications for education,” Smart Learning Environments, vol. 5, no. 1, p. 1, 2018.

[9] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum white paper.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, 2017, pp. 557–564.

[11] M. Asghari, D. Deng, C. Shahabi, U. Demiryurek, and Y. Li, “Priceaware real-time ride-sharing at scale: an auction-based approach,” in Proceedings of the 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems. ACM, 2016, p. 3.

[12] Victor, F., Zickau, S. (2018). Geofences on the blockchain: Enabling decentralized location-based services. 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, pp. 97-104.

[13] Y. Yuan and F.-Y. Wang, “Towards blockchain-based intelligent transportation systems,” in 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016, pp. 2663– 2668.

[14] S. Khanji and S. Assaf, “Boosting ridesharing efficiency through blockchain: Greenride application case study,” in 2019 10th International Conference on Information

and Communication Systems (ICICS). IEEE, 2019, pp. 224–229.

[15] U. M. A¨ıvodji, K. Huguenin, M.-J. Huguet, and M.-O. Killijian, “Sride: A privacy-preserving ridesharing system,” in Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2018, pp. 40–50.

[16] D. Sanchez, S. Mart ´ ´ınez, and J. Domingo-Ferrer, “Co-utile p2p ridesharing via decentralization and reputation management,” Transportation Research Part C: Emerging Technologies, vol. 73, pp. 147–166, 2016.

[17] A. Pham, I. Dacosta, G. Endignoux, J. R. T. Pastoriza, K. Huguenin, and J.-P. Hubaux, “Oride: A privacy-preserving yet accountable ride- hailing service,” in 26th {USENIX} Security Symposium ({USENIX} Security 17), 2017, pp. 1235–1252.

[18] Kudva, Sowmya, Renat Norderhaug, Shahriar Badsha, Shamik Sengupta, and A. S. M. Kayes. "Pebers: Practical ethereum blockchain based efficient ride hailing service." In *2020 ieee international conference on informatics, iot, and enabling technologies (iciot)*, pp. 422-428. IEEE, 2020.

[19] Zhang, Yifan, Yuping Zhou, Yu Hu, and Hui Huang. "A Decentralized Ride-Hailing Mode Based on Blockchain and Attribute Encryption."In *Cyberspace Safety and Security: 14th International Symposium, CSS 2022, Xi'an, China, October 16–18, 2022, Proceedings*, pp. 301-313. Cham: Springer International Publishing, 2022.