International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

Decentralized Ridesharing System Using Blockchain

Anushka Priya[1], Ayush Chakladar[2], Divij Bahl[3], Devansh Baid[4], Jayakumar K[5]

[1234]*Student, School of Computer Science and Engineering, VIT University, Tamil Nadu, India*
[5]*Associate Professor, School of Computer Science and Engineering, VIT University, Tamil Nadu, India*

Abstract - *In today's world, the practice of ridesharing has been increasing steadily in popularity, moving outside of urban settings and into suburban and rural areas. Our proposed system aims to decentralize the ride-sharing system by maintaining the rider's trip and transaction details on the blockchain. Because the entire transaction would be publicly verifiable, trust issues would be minimum, and payment fraud issues will be easily checked and remedied. Due to the blockchain's anonymous nature, everyone's identity will be kept confidential. As a result, security and privacy standards will be reinforced. The transaction will be visible, secure, and efficient as a result of the entire system. Although various systems and methodologies have been proposed to decentralize the ride-booking systems, the concepts have been mostly theoretical and lack proper practical implementation.*

Key Words: **ridesharing, blockchain, privacy, security, transaction**

1. INTRODUCTION

The rise of digital technologies and cryptocurrencies over the past decade has brought significant changes in many industry sectors. The proposed decentralized ridesharing system is built on the Ethereum blockchain network. With most of the current ridesharing methods being controlled by central authorities and big corporations, there is a need for a decentralized system in public domain to make sure that ridesharing system becomes smoother. It's also necessary to make sure that the privacy of the user is not compromised and the data is not hackable. Therefore, it is best to use a blockchain network to carry out all these transactions to make them verifiable in the public domain. In this way the data is also secured and at the same time verified by the public. Smart contracts can be deployed on the blockchain network to make sure that the integration takes place properly. It is crucial that smart contracts are used to ensure that transparency and confidence is established in the system. To understand the emergence of blockchain technologies in the transportation industry and the various efforts made to make the system decentralized several methods have been reviewed.

2. LITERATURE REVIEW

In today's world, ride-sharing is becoming a popular mode of transport. [1] shows how ride-sharing can reduce traffic in a city to a great extent and potentially decrease the number of cars up to 31%. In ride-sharing, one of the most important aspects is the effective matching of riders to share rides and finding drivers for those riders [2]– [8].

With blockchain technology on the rise, significant efforts are being made to incorporate this technology in the transportation sector. Meshkani [9] suggested an empirical ride sharing method where individual users can share their ride with only a single user. Lei [10] and Abbas [11] have suggested decentralized data management systems that are integrated with blockchain and IoT to provide better transparency, data sharing and tracking.

Over the past few years, many attempts have been made to improve and better the existing ride-sharing and travel applications. According to a survey conducted in [12], blockchain technology and cryptocurrencies has the potential to dramatically change the working of the existing ride-sharing applications. [13] proposed a blockchain framework for connecting autonomous vehicles while [14] proposed further adding a credit based intelligent vehicle communication framework that includes biometric features.

Wang [15] introduced a secure and privacy-preserving decentralized collection system of traffic information on the blockchain, TrafficChain, by taking advantage of edge computing. For making payments and transactions easier in blockchain, [16] proposed a Decentralized conditional Anonymous payment (DCAP) method as an alternative to traditional currency and transaction method, furthering the concept of a cashless economy. A similar effort was made by [17] to ensure that the third party services in the travel industry are eradicated and a transparent system based on using smart contracts and blockchain can be implemented.

[18], [19] suggested using a decentralized application to share rides incorporating some privacy preserving algorithms to ensure more privacy to the users. Li [20] has also proposed a similar feature by proposing a blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof.

S. C. -K. Chau [21] sheds light on the principles of decentralized ride-sharing and vehicle-pooling mechanisms based on stable matching and showed how several fair cost-sharing mechanisms can achieve high social optimality. Taking this study further with practical implementation, this paper aims to create a decentralized ride-sharing system using blockchain.

3. PROPOSED METHODOLOGY

After reviewing the architecture of centralized ridesharing systems, our proposed system aims to tackle the various issues that riders and drivers face. It was observed how the presence of a centralized body controlling the ride-sharing application affects both riders and drivers. One of the primary reasons for this is the commission fee. In a centralized ride-sharing system, the middle man takes a commission fee from the rider leading to higher price values for riders and a lower amount (Payment done by riders - Commission) for drivers.

Centralized applications are also extremely vulnerable to hacking. If this application is somehow hacked millions of people's private information can be exposed. Decentralized cryptocurrencies and applications have a different approach. They allow users to carry their own data, as opposed to relying on centralized bodies and middlemen to secure that data in exchange for using their platforms.

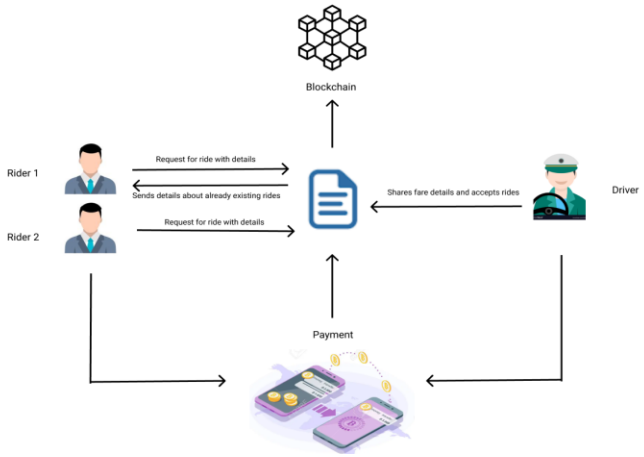

Fig -1: Architecture of Proposed System

Smart contracts are used to store the main details about the ride like the source, destination, price, and the public key of the user who is initiating the contract. By using this, the data is transparent, trackable and irreversible. At the same time this also ensures that the privacy of the user is not breached. The rider can share any rides from the available blockchain by paying for it via the cryptocurrencies. As soon as the transaction is complete, the changes are visible on the main blockchain and the ride can't be shared anymore.

4. IMPLEMENTATION

Our proposed system has been broadly divided into 3 modules: User interface, Smart contracts, and backend client. The user interface is meant for the user to enter the ride details and easily share the ride. The user interface also shows the ride history which is stored on the blockchain. This ride history is visible to any user who tries to share a ride.

The smart contracts are intended to make sure that the data being entered is traceable, transparent and irreversible. The details of the rides to be shared are stored on the blockchain with the help of the smart contract and cannot be changed at any cost. This ensures that the network is safe and secured. The backend client is used to transfer the data entered by the user to the smart contract and vice versa.

The rider/driver who wants to share the ride can enter the required details and can post it on the blockchain. He then has to pay a small amount of gas fees to make sure that the transaction succeeds. The other rider can just view it from his account. If he wants to share the ride at the given cost, he can just share the ride by paying the price of the ride and the required gas fees.

5. RESULTS AND DISCUSSION

This system is completely decentralized and is using blockchain. The blocks in blockchain are storing the following information: Gas fees used, the gas limit, the timestamp of the time when it was mined, and the hash of the previous block. The hash values are stored so that the block can be linked to the previous blocks.

It also stores the hash value of the current block and the to and from addresses of the transaction along with the amount transferred. All this information is stored on the blockchain and cannot be tampered with. If there is any change in the data then the hash value of the entire block changes and the blocks won't be connected. These values of timestamp and way of transaction can be determined using smart contracts.

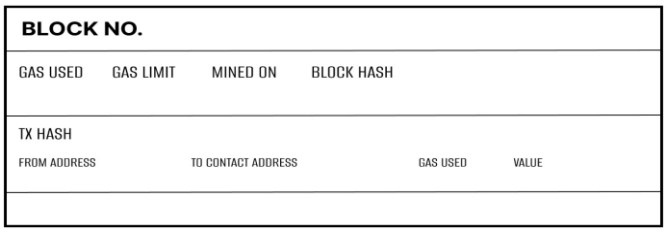

Fig -2: Block Diagram

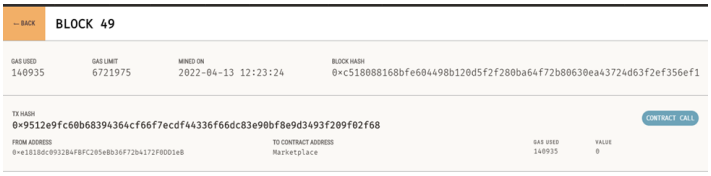

Fig -3: Block mined when user is creating the ride

This is the block (Fig -3) created when someone wants to put up a ride for sharing. As we can see this is the information stored on the block like the sender address, contract address, block hash, transaction hash, gas limit and gas used. Since this is used to create a ride that hence the value of ethers is 0.

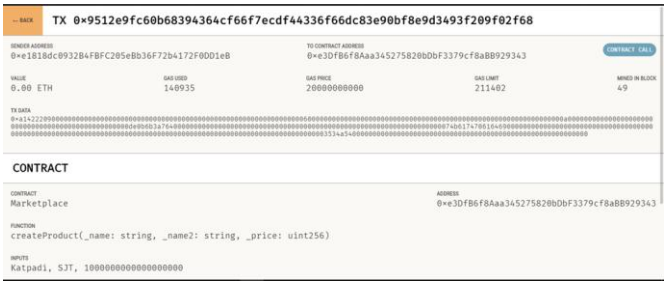

Fig -4: Snapshot of the transaction details when Block 49 was created

This is the transaction (Fig -4) created when the user put up the ride for sharing. The sender's address, gas value, gas limit, etc. are listed in the transaction. It also has the data of the transaction and other details related to the contract deployed.

Fig -5: Details of the smart contract stored on the Block

As we can see in the above figure (Fig -5), here the details sent by the user are stored. The to and from address along with price is stored and that's how the data is being stored on the blockchain.

Fig -6: Block mined when the user is sharing the ride

Similarly, this block (Fig -6) is the block mined when the user was sharing the ride. And similar to the above blocks this also stores information in a similar manner.

The below table (Table -1) lists the different transactions and the details of the transaction like the from address, to address, gas fees, price and the hash value of the block that has been mined. As we can observe when the user is putting up a ride to share the gas value is around 0.000000000000140000 ETH, however, when he wants to share the ride the gas fees comes down to 0.00000000000059000 ETH. In the first transaction, the user is putting up a ride to share. Since the data is being sent to the smart contract deployed, the address is to the smart contract's address. Hence the price is also 0.00 ETH. In the second transaction, the user is sharing the ride and has to pay 1.00 ETH with the gas fees. However the details are sent to the address of the smart contract and hence the address remains the same.

Table -1: Transaction Details

Transaction ID	From address	To address	Gas Fee	Price	Block Hash
0x9512e9fc60b68394364cf66f7ecdf443366f66dc83e90bf8e9d3493f209f02f68	0xe1818dc0932B4FBFC205eBb36F72b4172F0DD1eB	0xe3DfB6f8Aaa345275820bDbF3379cf8aBB929343	0.000000000000140935 ETH	0.00 ETH	0xc518088168bfe604498b120d5f2f280ba64f72b80630ea43724d63f2ef356ef1
0xd1dbc9953b158248015df64b4a66e3b7fb79b16707a583c65413ea06adbbf464	0xEE70573f59fFf6042a2a99599F12FE1c10247766	0xe3DfB6f8Aaa345275820bDbF3379cf8aBB929343	0.000000000000059174 ETH	1.00 ETH	0x012d200ddb97f51f5d9eaf3baf3979189fe5d43a791d5c3c5f85ee773a2e8b77
0x2dd59c1a685ac49c86a5092497c29ce341e955ac21e605ddec4013a9c5025228	0xEE70573f59fFf6042a2a99599F12FE1c10247766	0xe3DfB6f8Aaa345275820bDbF3379cf8aBB929343	0.000000000000140983 ETH	0.00 ETH	0xc315b17167561a06fadb6db1d806219619e6d422f1904628eb7c86d339e18fb0
0x0f5188849c5913f7aa8a93d5a913534b42a3d8f6e0b98d580e212097b56fe72f	0xe1818dc0932B4FBFC205eBb36F72b4172F0DD1eB	0xe3DfB6f8Aaa345275820bDbF3379cf8aBB929343	0.000000000000059174 ETH	1.00 ETH	0x42554f2098c1f311370a73c8c7b78732e176e5127fe2ff631629311842e309bc

Using smart contracts and the blockchain it has already been ensured that the data is secured and immutable. Hence it's enhancing the security, safety and privacy of the users. The middle man has also been removed in this system and it is more transparent. The blocks in the blockchain stores the time when the transaction was actually executed. Some of the improvements of the decentralized ridesharing system have been discussed below.

Table -2: Comparing Centralized and Decentralized Systems

Parameters	Centralized Ridesharing Systems	Decentralized Ridesharing systems
Security	All of the data is stored in a central server controlled by the big corporations and hence the data might not be safe.	The data is stored on the blockchain which is immutable and cannot be changed at any cost.
Safety	The safety of the rider depends on the person who is driving the vehicle. All of these details are with the central authority and hence it might be unsafe.	Since the blockchain is publicly verifiable, the safety of the riders is not compromised.
Privacy	The data of the rider and his/her personal details and bank account details are shared with the central authority and that can be misused.	Even though the blockchain is publicly verifiable the data of the user and the crucial details are kept safe and encrypted hence the privacy of the user is not breached.

6. CONCLUSION AND FUTURE WORK

This research pioneered a new field of study: decentralization of ride-sharing systems. Based on the results, it can be seen how the decentralized ride-sharing system can dramatically change and revolutionize the ride-sharing systems by providing fast, secure and efficient transactions without the interference of any centralized identity. Using this system, riders can connect directly with drivers via the blockchain decentralized network thereby reducing the additional costs incurred as a result of the use of several middlemen. Our proposed system also supports pseudonymous identities and provides users with a safe, permanent, and unbreakable link to their personal data. Our future work will include making this system more user-centric for wider adaptation and adding more safety protocols to ensure the safety of users as well as the driver.

REFERENCES

[1] Cici, B., Markopoulou, A., Frias-Martinez, E., & Laoutaris, N. (2014, September). Assessing the potential of ride-sharing using mobile and social data: a tale of four cities. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (pp. 201-211).

[2] H. Zhang and J. Zhao, "Mobility sharing as a preference matching problem," IEEE Trans. Intell. Transp. Syst., vol. 20, no. 7, pp. 2584–2592, Jul. 2019

[3] D. Pelzer, J. Xiao, D. Zehe, M. H. Lees, A. C. Knoll, and H. Aydt, "A partition-based match making algorithm for dynamic ridesharing," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 5, pp. 2587–2598, Oct. 2015.

[4] X. Wang, N. Agatz, and A. Erera, "Stable matching for dynamic ride-sharing systems," Transp. Sci., vol. 52, pp. 739–1034, Aug. 2017

[5] N. Agatz, A. L. Erera, M. W. Savelsbergh, and X. Wang, "Dynamic ridesharing: A simulation study in metro Atlanta," Procedia-Social Behav. Sci., vol. 17, pp. 532–550, Jan. 2011

[6] X. Wang, N. Agatz, and A. Erera, "Stable matching for dynamic ride-sharing systems," Transp. Sci., vol. 52, no. 4, pp. 850–867, Aug. 2018.

[7] S. Rasulkhani and J. Y. J. Chow, "Route-cost-assignment with joint user and operator behavior as a many-to-one stable matching assignment game," Transp. Res. B, Methodol., vol. 124, pp. 60–81, Jun. 2019

[8] Z. Peng, W. Shan, P. Jia, B. Yu, Y. Jiang, and B. Yao, "Stable ride-sharing matching for the commuters with payment design," Transportation, vol. 47, no. 1, pp. 1–21, Feb. 2020

[9] Meshkani, S. M., & Farooq, B. (2021). A Decentralized Shared CAV System Design and Application. arXiv preprint arXiv:2104.10022.

[10] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6), 1832-1843.

[11] Jabbar, R., Kharbeche, M., Al-Khalifa, K., Krichen, M., & Barkaoui, K. (2020). Blockchain for the internet of vehicles: A decentralized IoT solution for vehicle communication using ethereum. Sensors, 20(14), 3928.

[12] Gupta, R., Gupta, R., & Shanbhag, S. S. A Survey of Peer-to-Peer Ride Sharing Services using Blockchain.

[13] Xu, B., Agbele, T., & Jiang, R. (2020). Biometric blockchain: a secure solution for intelligent vehicle data sharing. In Deep Biometrics (pp. 245-256). Springer, Cham.

[14] Yoshida, N., Noda, I., & Sugawara, T. (2021). Distributed Service Area Control for Ride Sharing by using Multi-Agent Deep Reinforcement Learning. In ICAART (1) (pp. 101-112).

[15] Wang, Q., Ji, T., Guo, Y., Yu, L., Chen, X., & Li, P. (2020). TrafficChain: A blockchain-based secure and privacy-preserving traffic map. IEEE Access, 8, 60598-60612.

[16] Rahardja, U., Aini, Q., & Maulana, S. (2021). Blockchain innovation: Current and future viewpoints for the travel industry. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 3(1), 8-17.

[17] Wang, Y., Kim, D. K., & Jeong, D. (2020). A survey of the application of blockchain in multiple fields of financial services. Journal of Information Processing Systems, 16(4), 935-958.

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

[19] Baza, M., Mahmoud, M., Srivastava, G., Alasmary, W., & 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.

[20] Li, W., Meese, C., Guo, H., & Nejad, M. (2020, December). Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof. In 2020 3rd International Conference on Hot Information-Centric Networking (HotICN) (pp. 18-24). IEEE.

[21] Chau, S. C. K., Shen, S., & Zhou, Y. (2020). Decentralized ride-sharing and vehicle-pooling based on fair cost-sharing mechanisms. IEEE Transactions on Intelligent Transportation Systems.