RESEARCH ARTICLE OPEN ACCESS

Peer to Peer Ridesharing using Blockchain

Vivek Kekuda T U[1], Likitha P[2], Rekha B S[3], Sushmitha N[4]
1,2 (Final Year Students, Department of Information Science and Engineering, R. V. College of Engineering, Bengaluru
Email: vivekkekudatu.is17@rvce.edu.in[1], likithap.is17@rvce.edu.in[2])
3,4 (Professors, Department of Information Science and Engineering, R. V. College of Engineering, Bengaluru
Email: rekhabs@rvce.edu.in[3], sushmithan@rvce.edu.in[4])

Abstract:

Ridesharing is how drivers share trips with other riders, which not only has benefits that of a shared travel cost but also that of reduced traffic congestions. Existing ridesharing solutions rely on third parties which make them vulnerable at a single point of failure and attacks involving denial of service. It also raises privacy concerns.

The proposed solution to all this is via the use of blockchain technology. Blockchain, although is mainly associated with digital currency, the inbuilt distributed and decentralized nature of a blockchain is ideal to solve and overcome a lot of the problems facing traditional ridesharing services. The concepts related to architecture of a block for our use case, and the underlying implementation is discussed, along with the advantages and disadvantages.

Various features like booking a ride, confirmation of a ride, mining blocks and syncing the blockchain with all the nodes in a network is explored. Strong algorithms like SHA3-256 is used for hashing which is pivotal to validate the blockchain. In this paper, we explore registering peers to the same network which mimics a decentralized blockchain in the real world. The entire solution is deployed using the FLASK framework.

Keywords **— Blockchain, ridesharing services, Secure Hash Algorithm (SHA-3), peer to peer networks, Flask framework, decentralized application**

I. INTRODUCTION

Ridesharing and carpooling are becoming increasingly popular particularly in large cities having a lot of traffic jams and congestions. In ridesharing services, the vacant seats in a car could be shared by other people to make the prices of rides lesser, decrease the harm to the environment and make use of the driver's time judiciously. Many ridesharing services have gained monopoly in this space, like Uber with its UberPool, Lyft Line and Ola. They are traditional services, as in they have a single point of failure, and it is becoming increasingly difficult to trust these services and the data that we give to them.

This is where we can utilize the power of blockchains, which are one of the emerging fields of technology. Blockchains are nothing but a chain of peer-to-peer distributed blocks. They guarantee immutability as they contain a layer of cryptographic hashing. Once a block has been mined and added to the chain (post validation by all the nodes in the network), it is not possible to alter the data unless someone gains majority access (50%+1) of the network computing power, which is practically impossible, given the distributed nature and size of blockchains.

A request for a ride is considered a transaction. Each transaction has a source, a destination, the number of passengers and an ideal price which the rider can quote. Interested drivers nearby can reply to this request with their idea of an ideal price and the passenger can choose between drivers available, if any, based on the price they are offering. A block in the blockchain has one or more transactions, which is mined as and when the ride completes. A chain of blocks constitutes a blockchain which is shared between all the peers in the network.

This paper explores the use of blockchain for ridesharing, looking at all the requirements, considerations, assumptions, security, to come up with a simple implementation that captures the ideas presented.

II. LITERATURE SURVEY

A. Mohamed Baza, Mohamed Abdallah, Modhamed Mahmoud, Gautam Srivastava and Noureddine Lasla

This paper [1] proposes Blockchain based ridesharing service does not rely on a third party. Rider and driver can learn to share rides while ensuring sensitive information on trip data – pick up and drop off location, departure and arrival times, ride prices. It uses zero-knowledge set membership proof to preserve privacy.

B. Kosuke Kato, Yutong Yan and Hiroshi Toyoizum

This paper [2] proposes a blockchain solution that focuses on the profit of the driver. It offers a matching application to existing third party, but with added encouragement of drivers turning into miners. It calculates the static profit of every driver in the rideshare system, while finding the least probability to make drivers profit.

C. Panchalika Pal and Sushmitha Raj

This paper [3] discusses a system which also involves rating the driver post ride completion. It focuses on ensuring the fairness of the ride. The different events in the entire ride sharing process – booking, cancellation, completion, abortion – are investigated. This distributed ledger ensures the fairness of the reputation system.

D. Yaron Kanza and Eli Safa

This paper [4] explores the privacy aspects of both the rider and the driver – pseudonymity. This means that both the parties involved in a transaction use a pseudo entry and do not reveal their true identities to each other. It wraps up this concept in a blockchain which can ensure privacy, trust, pseudonymity, and trust.

E. Ryan Shivers, Mohammad Rahman and Hossain Shahriar

This paper [5] proposes Blockchain based solution that emphasizes on the decentralized architecture, fault tolerance and immutability. Performance analysis is also done under a heavy load.

III. METHODOLOGY

The methodology is explained as part of two separate modules:

Module 1 – Pre-Booking

Before a driver is interested in a rider's request, each rider must have to be logged in to the system and must have placed a ride request. We assume that all drivers and passengers are registered with their identities verified [10].

A passenger wanting a ride submits a transaction request via the single page dashboard, which is broadcasted and is viewable to all the people in the network. This request contains details information about the passenger's request. The passenger is needed to deposit his/her money into the system before requesting the ride.

The request for a ride made by a passenger contains the following details: starting point, destination, number of passengers, name under which the booking is done and his/her ideal price for the ride. This is just a placeholder. The request once made, is visible to all drivers in the network to which they can show their interest. This confirms the ride and finishes the transaction.

Module 2 – Mining and resyncing the blockchain

In the booking phase, a transaction is validated by mining the block and syncing the new block with all the nodes in the network. The validity of the block is verified before adding it to the network. The decentralized nature of the system ensures that privacy is maintained, and that the data is not hampered with by any malicious party.

A miner (not driver or passenger in this transaction) will verify this "transaction is processed and completed" by judging the following conditions [10]:

1. Driver arrives in time as promised

2. Passenger confirms he/she arrives at his/her destination

If both condition 1 and condition 2 satisfied, the driver gets the deposited money. If condition 1 is not satisfied but condition 2 is satisfied, the driver still gains some money but not the full amount. If neither of the conditions is satisfied, the driver will gain no money and the money is returned. The money is allocated by *smart contract* once this node is verified.

IV. IMPLEMENTATION AND RESULTS

The proposed system is divided into 2 modules:

1. Block module
2. Chain module

Block module

The block module demonstrates the fields considered in every block of the blockchain. It also showcases the hashing algorithms used.

Steps:

- A unique ID is generated for every ride and a UI is provided to enter ride details like starting location, destination, and number of passengers.
- Once the details are entered and a ride is booked, a block containing all pending transactions is mined.
- This is added to the current chain.

Here the block encryption is done using the SHA3 256 hashing algorithm. The data points considered are:

- Hash of previous block
- Transactions in the block. Each transaction internally includes the following:
    - ○ Name of the rider
    - ○ Number of passengers
    - ○ Starting point
    - ○ Destination
    - ○ Additional details/comments
    - ○ Fair price
    - ○ Actual price
    - ○ Timestamp
- Nonce
- Timestamp

All these fields encoded as a string in their dictionary representation and is fed as input to the hashing algorithm, and the hex digest of the hashed value is stored as the hash of the block.

Below are tables describing the structure of:

1. A transaction

2. A block

TABLE I
STRUCTURE OF A TRANSACTION T

Field	Type	Description
name	string	the name of the rider placing the request
message	string	additional note to the driver
start	string	coordinates of the starting point
end	string	coordinates of the destination
price	int	the actual price of the ride
fair_price	int	the fair price quoted by the rider
timestamp	datetime	the timestamp when the ride was confirmed

TABLE II
STRUCTURE OF A BLOCK B

Field	Type	Description
index	int	unique identifier of every block
nonce	int	a random number to prevent replay attacks
hash	string	the hex digest of the SHA256 hash calculated from all the other fields of the block
previous_hash	string	hash of the previous block
transactions	list <T>	the list of confirmed transactions to be mined
timestamp	datetime	the timestamp when the block was mined

Chain module

This module demonstrates the generation of a batch of transactions, the mining process, and the syncing of blocks with all the nodes in the peer-to-peer network. Before jumping into mining, let us understand how the network is first established.

All nodes in the network must share the same copy of the blockchain. This is the core concept of a decentralized application and in our case, a ridesharing application. All nodes in the network must be first registered with the main node to which the frontend will make its requests to. A list of peers is maintained in the application, to which this copy of the blockchain is shared. At any point of time, the copy of the blockchain can be verified, and before adding any block to the blockchain, validation is done to get a majority consensus on whether the block being added has not been tampered with.

The steps involved in creating the blockchain are as follows:

- Create a genesis block which acts as the first block in the blockchain.
- Each block is consistent with the hash of the previous block.
- On changing a minor field of a property in a block, its hash changes significantly [Avalanche property of hashing algorithms].
- The length of the block and the peers in the network are properties of the chain. It can be retrieved at any point after resyncing.

Major stages of the proposed system are:

1. Registering all the peers in the network
2. Ride booking by passenger – information
3. Ride confirmation by the driver – interest
4. Block Definition
5. Block Verification
6. Block Mining – of all pending transactions
7. Resyncing the blockchain to reflect and broadcast changes

Screenshots of the results obtained are shown below:

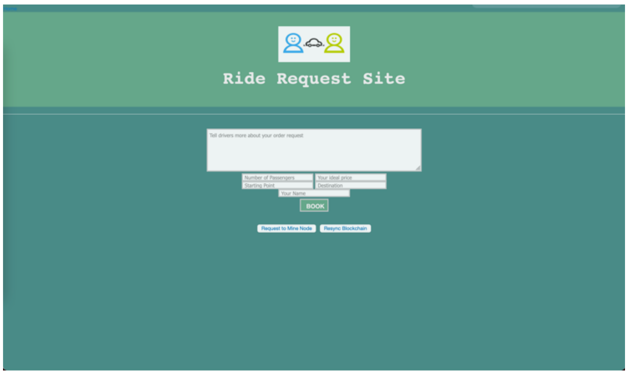
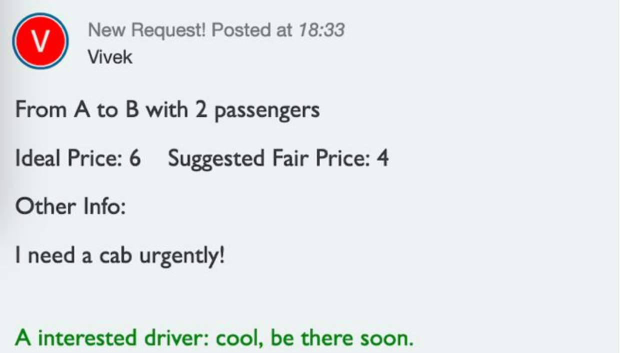


Fig. 1 Ride request form



New Request! Posted at *18:33*
Vivek

From A to B with 2 passengers

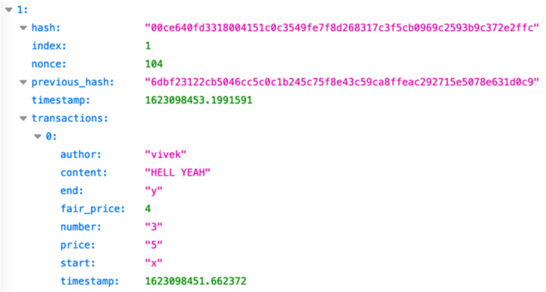
Ideal Price: 6 Suggested Fair Price: 4

Other Info:

I need a cab urgently!

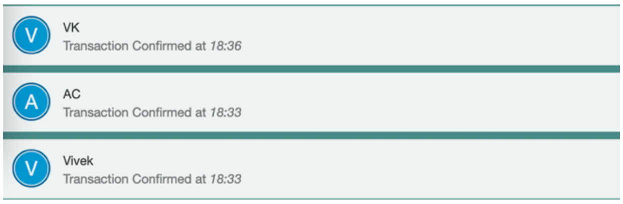
A interested driver: cool, be there soon.

Fig. 2 Ride details confirmation



```
▾ 1:
  ▾ hash:            "00ce640fd3318004151c0c3549fe7f8d268317c3f5cb0969c2593b9c372e2ffc"
    index:           1
    nonce:           104
  ▾ previous_hash:   "6dbf23122cb5046cc5c0c1b245c75f8e43c59ca8ffeac292715e5078e631d0c9"
    timestamp:       1623098453.1991591
  ▾ transactions:
    ▾ 0:
        author:      "vivek"
        content:     "HELL YEAH"
        end:         "y"
        fair_price:  4
        number:      "3"
        price:       "5"
        start:       "x"
        timestamp:   1623098451.662372
```

Fig. 3 Block definition

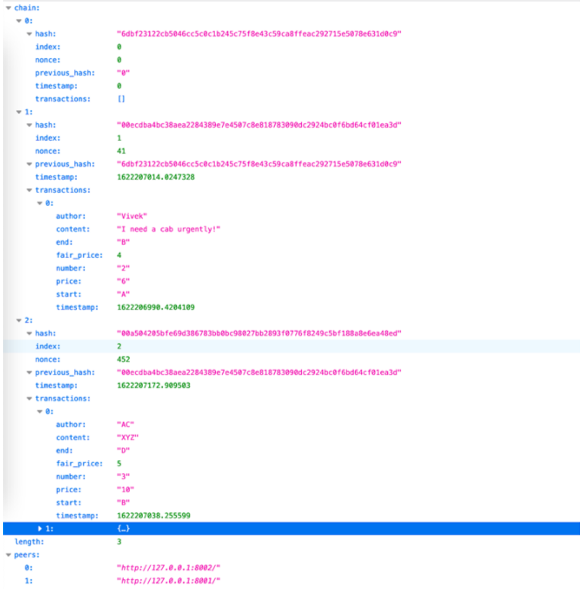


VK
Transaction Confirmed at *18:36*

AC
Transaction Confirmed at *18:33*

Vivek
Transaction Confirmed at *18:33*

Fig. 4 Transactions which are part of mined blocks



```
▾ chain:
  ▾ 0:
    ▾ hash:            "6dbf23122cb5046cc5c0c1b245c75f8e43c59ca8ffeac292715e5078e631d0c9"
      index:           0
      nonce:           0
      previous_hash:   "0"
      timestamp:       0
      transactions:    []
  ▾ 1:
    ▾ hash:            "00ecdba4bc38aea2284389e7e4507c8e818783090dc2924bc0f6bd64cf01ea3d"
      index:           1
      nonce:           41
    ▾ previous_hash:   "6dbf23122cb5046cc5c0c1b245c75f8e43c59ca8ffeac292715e5078e631d0c9"
      timestamp:       1622207014.0247328
    ▾ transactions:
      ▾ 0:
          author:      "Vivek"
          content:     "I need a cab urgently!"
          end:         "B"
          fair_price:  4
          number:      "2"
          price:       "6"
          start:       "A"
          timestamp:   1622206990.4204109
  ▾ 2:
    ▾ hash:            "00a504205bfe69d386783bb0bc98027bb2893f0776f8249c5bf188a8e6ea48ed"
      index:           2
      nonce:           452
    ▾ previous_hash:   "00ecdba4bc38aea2284389e7e4507c8e818783090dc2924bc0f6bd64cf01ea3d"
      timestamp:       1622207172.909503
    ▾ transactions:
      ▾ 0:
          author:      "AC"
          content:     "XYZ"
          end:         "D"
          fair_price:  5
          number:      "3"
          price:       "10"
          start:       "B"
          timestamp:   1622207038.255599
      ▸ 1:             {…}
  length:              3
▾ peers:
    0:                 "http://127.0.0.1:8002/"
    1:                 "http://127.0.0.1:8001/"
```

Fig. 5 Entire block chain – on any node in the peer-to-peer network

V. CONCLUSION

The need for the proposed system is rooted in the need for a transparent and decentralized system of peer-to-peer ridesharing that was secure and scalable. Blockchains can also be used for ridesharing, as presented. We believe that the proposed solution as part of this set up, is an application that can be built upon utilizing its great security aspects of decentralized blockchain systems involving strong cryptographic algorithms, peer to peer networks and game theory – the economic incentive mechanisms of validating transactions by consensus (Proof of work, proof of stake, etc.).

The current traditional systems such as Uber, Lyft and Ola are trusted third parties, but they are not transparent. Having systems built on the latest technologies which is transparent and decentralized, is much needed. It removes the necessity of a middleman altogether. Since it is a distributed network, data breaches or security concerns arising from the middleman involved is nonexistent. The fairness is ensured for both the rider as well the driver since no marketing strategies of the centralized company is involved.

ACKNOWLEDGMENT

We would like to mention our special thanks to our guides (Prof. Rekha.B.S and Prof. Sushmitha N) who have been a constant help in guiding us while working on this paper, which also helped us in doing a lot of research and helped us learn and explore new things.

REFERENCES

1. *Mohamed Baza, Noureddine Lasla, Modhamed Mahmoud, Gautam Srivastava and Mohamed Abdallah, "B-Ride: Ride Sharing with Privacy-preservation, Trust and Fair Payment atop Public Blockchain", arXiv:1906.09968v2 [cs.CR] 13 Nov 2019*

2. *Kosuke Kato, Yutong Yan and Hiroshi Toyoizumi, "Blockchain Application for Rideshare Service", 2018. Available: IEEExplore. DOI 10.1109/LISS.2018.8593271.*

3. *Panchalika Pal and Sushmita Raj, "BlockV: A Blockchain Enabled Peer-Peer Ride Sharing Service", IEEE International Conference on Blockchain 2019, DOI 10.1109/Blockchain.2019.00070.*

4. *Yaron Kanza and Eli Safra, "Cryptotransport: Blockchain-Powered Ride Hailing While Preserving Privacy, Pseudonymity and Trust", 2018. Available: Research Gate. DOI 10.1145/3274895.3274986.*

5. *E. Ryan Shivers, Mohammad Ashiqur Rahman and Hossain Shahriar, "Toward a Secure and Decentralized Blockcahin-based Ride-Hailing Platform for Autonomous Vehicles", arXiv:1910.00715v2 [cs.CR] 5 Oct 2019*

6. *L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announce- ment network for communications of smart vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2204-2220, 2018*

7. *Y. F. Hou, W. D. Zhou, L. Su, K. Hulme, A. W. Sadek, and C. M. Qi ao, "TAseT: Improving the efficiency of electric taxis with transfer-all owed rideshare," IEEE Transactions on Vehicular Technology, vol. 6 5, no. 12, pp. 9518-9528, 2016.*

8. *"How are Wait Time fees calculated?" Uber, 2021. [Online]. Avaliable: https://help.uber.com/driving-and-delivering/article/how-are-wait-time-fees-calculated?nodeId=7f41997f-a853-46ae-8001-8ab9dee504b0. [Accessed: 05-May-2021]*

9. *Somesh Kesarla Suresh, "Business & Engineering aspects of RideX" uxplanet, 2021. [Online]. Available: https://uxplanet.org/ridex-taxi-service-on-ethereum-blockchain-adb077fc818c. [Accessed: 06-May-2021]*

10. *"Blockchain-based-Ride-Sharing-System", github.com, 2021. [Online] Available: https://github.com/29vivek/Blockchain-based-Ride-Sharing-System/blob/main/algo.md. [Accessed: 27-May-2021]*

11. *"Developing a Ride-Sharing App like Uber with Blockchain", oodles blockchain, 2021. [Online] Available: https://blockchain.oodles.io/blog/developing-ride-sharing-app-uber-with-blockchain/. [Accessed: 07-May-2021]*