Blockchain and Stackleberg Game-based Fair and Trusted Data Pricing Scheme for Ride Sharing

Riya Kakkar*, Nilesh Kumar Jadav†, Rajesh Gupta‡, *Student Member, IEEE*, Smita Agrawal§, *Member, IEEE*, Sudeep Tanwar¶, *Senior Member, IEEE*
*†‡§¶Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, India
Email: *21ftphde56@nirmauni.ac.in, †21ftphde53@nirmauni.ac.in, ‡18ftvphde31@nirmauni.ac.in,
§smita.agrawal@nirmauni.ac.in, ¶sudeep.tanwar@nirmauni.ac.in

2022 IEEE International Conference on Communications Workshops (ICC Workshops) | 978-1-6654-2671-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCWORKSHOPS53468.2022.9814704

***Abstract*—This paper proposes a blockchain-based secure and optimal data pricing scheme for ride-sharing. It mainly focuses on securing the data transactions between vehicle owners and customers. It utilizes a communication network, i.e., 6G, to facilitate the low latency and high data rate transmissions between vehicle owner and customer. We applied a reverse Stackelberg game theory approach to yield the optimal payoff for vehicle owners and customers. The performance results of the proposed system over a 6G communication network is estimated by differentiating it with conventional networks such as 4G and 5G. The performance is evaluated considering the parameters latency, scalability, and the optimal payoff for the system. The performance results conclude that the proposed system is secure, reliable, and yields the optimal payoff for vehicle owners and customers.**

***Index Terms*—Blockchain, Smart contract, Stackelberg game, Optimum pricing, Ride sharing.**

I. Introduction

Nowadays, people have been fascinated by their private cars or vehicles to reach their work. Unfortunately, this incurs traffic congestion, pollution, and high energy consumption, due to which a person can lose his daily wages or even job [1]. Lately, on-demand ride-sharing schemes, such as Ola, Uber, Didi, etc., have attracted a lot of attention where users can share the ride to facilitate sharing activities, such as vehicle-pooling [2]. The ride-sharing scheme is a promising solution to enhance transportation services by improving traffic congestion, pollution quality index, and reducing energy consumption [3]. However, despite its indispensable advantages, ride-sharing schemes are vulnerable to security and privacy threats, such as denial-of-service (DoS), data forgery, spoofing, and injection attacks [4]. Moreover, the ride-sharing scheme uses a centralized system for data processing that is at a high stake of being exploited. In addition, the customers are sharing their personal information, such as government ID, address details, mobile number, payment details, etc., in the ride-sharing application [5]. Therefore, an attacker tries to collect personal information from the ride-sharing application to proliferate identity and authentication attacks.

Several researchers across the globe attempt to provide a feasible solution to tackle the aforementioned security issues [6]. For instance, the authors of [7] present a biometric-based authentication mechanism to verify the identity of the authentic drivers for on-demand ride-sharing services. Next in, [8] the customers are finding feasible partners to share the car-pooling services. However, one has to share his personal information to find viable partners; this raises privacy issues in the pooling services. Therefore, the authors embraced the privacy-preserving authentication mechanism to resolve the problem of finding genuine partners in the ride-sharing application. Nevertheless, the cryptographic solutions are not robust as modern computing can easily break them. With the advent of blockchain technology, it is incorporated in various applications to create trustworthy and privacy-preserving solutions. Baza *et al.* in [9] discussed that an attacker could forge and send multiple ride requests which are not committed by any of them. For that, they proposed a blockchain-based ride-sharing scheme that authenticates each request by using the smart contract [10][11]. Then in [12] the authors are ensuring the confidentiality, integrity, and privacy of the ride-sharing services by adopting consortium blockchain and encryption standards. However, the aforementioned work has not involved an interplanetary file system (IPFS) that can increase the scalability of the blockchain network.

The other constraint the ride-sharing scheme encounters is its price optimality. The price strategies are highly dynamic and complex under different ride-sharing schemes, such as high prices in the peak time, i.e., in the morning, and lower prices in the afternoon. There is a huge demand for ride-sharing platforms in a high peak time; however, it suffers from capacity issues that raise the prices. Therefore, there is a need for price optimality between drivers and customers in ride-sharing schemes. To confront the pricing optimality, the authors of [13] proposed a Stackelberg game between data proprietor, driver, and customer. The result shows that the proposed system has better convergence and the existence of game equilibrium. Then, in [14] the authors resolved the problem of territory allocation between drivers by embracing bargaining game theory. However, the aforementioned solutions have not discussed the price optimization between drivers and customers in ride-sharing schemes.

Thus, there is a requirement for a combinatorial framework that can solve the security and privacy issues and optimize the price in ride-sharing platforms. This motivates us to propose a secure and optimal framework by amalgamating the Stackelberg game and blockchain technology underlying 6G communication. First, we introduce the certificate authority that validates the vehicle owners and customers to become members of a blockchain network [15]. Then, we present a smart contract that verifies the credentials of vehicle owners and customers; only then they are authorized to share their data in the blockchain network. Once authenticated, the members can store their data inside IPFS, which is less expensive than ethereum-based blockchain. Furthermore, it generates hashes that can be stored securely in immutable, distributed blocks of the blockchain [16]. Moreover, to optimize the price between the blockchain members of ride-sharing platforms, we have

formulated a reverse stackelberg game that maximizes the payoff among each other. We also integrated the staggering benefits of a 6G network interface to increase the performance of the proposed framework in terms of data rates, latency, and scalability [17]. The blockchain technology blended with the reverse stackelberg game and a 6G network makes the proposed framework robust, reliable, and optimized for its better enactment.

A. Research contributions

- We propose a blockchain-based secure and optimal ride-sharing scheme over the 6G network. Furthermore, incorporated IPFS with blockchain ensures the cost-efficient data storage of the user's data about the rides.
- We formulate a reverse stackelberg game theory approach to provide users vehicle owners and customers with optimal payoff.
- Lastly, we evaluate the performance of the proposed system considering the parameters such as optimal payoff, scalability, and latency.

B. Organization

The rest of the paper is organized as follows. Section II presents the system model and problem formulation. Section III discusses a reverse stackelberg game theory approach. Section IV presents the security verification of the proposed system. Section V presents the results and discussion, and finally, the paper is concluded in Section VI.

II. System model and problem formulation

Fig. 1 shows the proposed framework of blockchain-based and reverse stackelberg game for ride-sharing applications. The proposed framework is divided into three layers, i.e., data acquisition, transaction, and blockchain layer. It mainly constitutes a group of vehicle owners (Δ_a), a group of customers (δ_c), and a group of certificate authorities Υ. The δ_c communicates over a 6G network with Δ_a in ride-sharing application to book a ride. From the viewpoint of security, the attacker can forge the car-sharing data $\mathcal{D}$, which adversely affects the performance of the ride-sharing system. Therefore, blockchain allows an immutable ledger where the $\mathcal{D}$ is stored securely. First, a certificate authority Υ gets the registration request from δ_c and Δ_a to become authentic blockchain members. Once they are authenticated, the smart contracts ψ execute upon a specified condition to verify the credentials obtained from the Υ and car-sharing data $\mathcal{D}$.

After verifying, the ψ permits the δ_c and Δ_a to store their $\mathcal{D}$ in IPFS. Incorporating IPFS-based blockchain technology in the proposed framework enhances blockchain scalability. This is because it stores hashes of the $\mathcal{D}$ instead of raw data. The second objective of this paper is to optimize the price between Δ_a and δ_c; for that, we have employed the reverse stackelberg game. Here, firstly follower player δ_c makes the strategy, and accordingly, Δ_a plans the strategy to get the optimized payoff in ride-sharing. A complete description of the game is described in Section III. Furthermore, each δ_c requires immediate service, i.e., a ride from a ride-sharing application. In this vein, we need low latency and a high data rate system to solve the high demands of customers. Toward this goal, a 6G network comprises high data rates (1 Tbps), high reliability (99.99999%), high scalability (10^99 devices/sqm), and low latency (1 ms) can enhance the communication between Δ_a and δ_c. A detailed explanation of each layer is as follows,

A. Data acquisition layer

In this layer, there are multiple vehicle owners $\{\Delta_1, \Delta_2, \ldots, \Delta_d\} \in \Delta_a$ and customers $\{\delta_1, \delta_2, \ldots, \delta_t\} \in \delta_c$, where each Δ_a and δ_c are associated with the hash function $\mathcal{H}$. The Δ_a fills the necessary information, such as ride fare, drop locations etc. for a δ_c to register the ride in the ride-sharing application. Similarly, the δ_c can also provide required data to register a ride, such as a pick and drop points, mobile number, etc. Consequently, the Δ_a and δ_c have stored the personal information in the centralized ride-sharing application that lures the attackers to manipulate it. To overcome this issue, a certificate authority Υ^{Φ} verifies the hash $\mathcal{H}$ and certificate phi of Δ_a and the δ_c. If both the entities are authenticated, then they can store the ride-sharing data $\mathcal{D}$ in the blockchain. If not, then the Υ assigns certificates ϕ to each Δ_a and δ_c to ensure the security and privacy of the ride-sharing system.

B. Transaction layer

This layer presents the data exchange between vehicle owner Δ_a, customer δ_c, and blockchain layer over the 6G network interface. Here, a smart contract psi is executed on specified conditions to vindicate the certificate phi assigned by the certificate authority Υ to each Δ_a and δ_c. If the certificates are valid, the vehicle owner and the customer can successfully store their data in the blockchain. Additionally, if both entities want to access the stored data from the blockchain. In that case, they still need to verify their certificate to the smart contract to access the data stored inside the blockchain. If the certificates are not valid, the smart contract declines the request and formally updates the data request status to the vehicle owner and customer.

C. Blockchain layer

In this layer, we introduce the ethereum-based blockchain to preserve privacy and improve the security of the proposed framework. In the previous layer, the smart contract has bifurcated the valid and invalid data requests from the vehicle owner Δ_a and customer δ_c. As a result, only authenticated data request is forwarded to the blockchain layer. This layer involves an IPFS technology proportionally fair compared to the ethereum-based blockchain. This is because to store 1MB of ride-sharing data $\mathcal{D}$ in an Ethereum block cost approximately 17,100 USD which is significantly high. The IPFS technology poses the same benefits as ethereum; however, it is cost-free, remarkably reliable, and competent. It generates unique hash values of $\mathcal{D}$ of Δ_a and δ_c and stores them inside the ethereum blocks. Then, transaction perfomed while generating the hashed data, i.e., Ξ_{Δ_a} for the vehicle owner and ξ_{δ_c} for the customer is forwarded to the blockchain network. The blockchain executes a proof-of-work consensus mechanism to verify the transaction between vehicle owner and customer. Finally, the miners solve the complex puzzle and get rewarded for validating the block of transactions. So, the transaction of the ride-sharing is stored inside the blockchain compels the proposed framework to be reliable and secure from data manipulation and injection attacks.

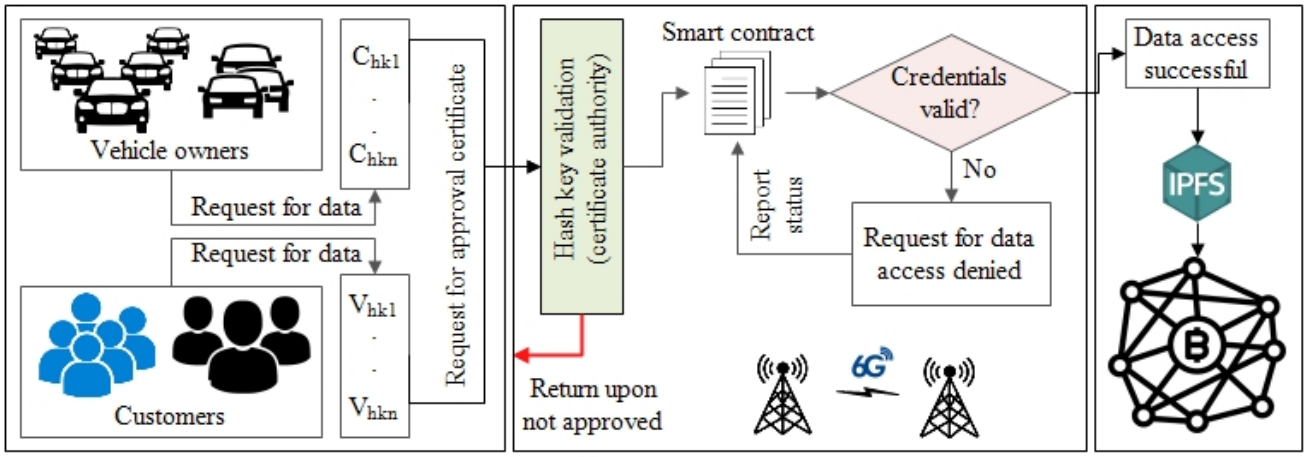

Fig. 1: The proposed system.

Algorithm 1 Blockchain data storage algorithm.

Input: $IPFS_{(h,k)}$, Υ, λ_{Δ_a}, Λ_{δ_c}, ρ_{br}
Output: Data added to the blockchain

procedure StoreData__blockchain(λ_{Δ_a}, Λ_{δ_c}, Υ)
  if $E \in E_{\Delta_a}$ **then**
    for $i = 1, 2, \ldots, d$ **do**
      $IPFS_{(h,k)} \leftarrow Rq\_for\_Data(\Delta_a)$
      $\Delta_a \xleftarrow{\Phi} \Upsilon$
      Smart contract executes
      if $\Phi == valid$ **then**
        $\Delta_a \xleftarrow{\lambda_{\Delta_a}} IPFS\_(h,k)$
        $blockchain \leftarrow$ Req_to_add(Δ_a)
        if $\lambda_{\Delta_a} \in \rho_{br}$ **then**
          Data added to Blockchain
        else
          Access denied
        end if
      else
        Invalid certificate
      end if
    end for
  else if $E \in E_{\delta_c}$ **then**
    for $j = 1, 2, \ldots, t$ **do**
      $IPFS_{(h,k)} \leftarrow$ DataReq(δ_c)
      $\delta_c \xleftarrow{\Phi} \Upsilon$
      Smart contract executes
      if $\Phi == valid$ **then**
        $\delta_c \xleftarrow{\Lambda_{\delta_c}} IPFS_{(h,k)}$
        $blockchain \leftarrow$ Req_to_add(δ_c)
        if $\Lambda_{\delta_c} \in \rho_{br}$ **then**
          Data added to blockchain
        else
          Access denied
        end if
      else
        Invalid certificate
      end if
    end for
  end if
end procedure

D. Problem Formulation

The proposed system include various elements E $\in \{E_\Delta, E_\delta, E_\Upsilon\}$ in which element E_Δ consists of d number of vehicle owners $\{\Delta_1, \Delta_2, \ldots, \Delta_d\} \in \Delta_a$ and element E_δ consists of t number of customers $\{\delta_1, \delta_2, \ldots, \delta_t\} \in \delta_c$ along with their hash keys λ_{Δ_a} and Λ_{δ_c} interacting with element E_Υ, i.e., u number of certificate authority $\{\Upsilon_1, \Upsilon_2, \ldots, \Upsilon_k\} \in \Upsilon_p$ to authenticate themselves for ride sharing with the help of approval certificate (Φ) . δ_c can request Δ_a to book a ride for a particular destination by paying the certain amount from their wallet. The above mentioned association between elements can be represented as follows:

$$\Delta_a(\lambda_{\Delta_a}) \xrightarrow{\eta} \sum_{c=1}^{t^{'}} \delta_c(\Lambda_{\delta_c}) \;\; and \;\; \delta_c(\Lambda_{\delta_c}) \xrightarrow{\eta} \sum_{a=1}^{d^{'}} \Delta_a(\lambda_{\Delta_a}) \quad (1)$$

$$\delta_c(\Lambda_{\delta_c}) \xrightarrow{\eta} \sum_{p=1}^{k^{'}} \Upsilon_p \;\; and \;\; \Delta_a(\lambda_{\Delta_a}) \xrightarrow{\eta} \sum_{p=1}^{k^{'}} \Upsilon_p \quad (2)$$

$$t^{'} \leq t; \;\; d^{'} \leq d; \;\; k^{'} \geq t^{'}; \;\; k^{'} \geq d^{'} \quad (3)$$

$$c, \;\; a, \;\; p \geq 0 \quad (4)$$

where η denotes the association between Δ_a, δ_c, and Υ_p. $\hat{t^{'}}$ number of customers and $\hat{d^{'}}$ number of vehicle owner are communicating with $\hat{k^{'}}$ number of certificate authority (Υ^Φ) for Φ.

Now, vehicle owners Δ_a and customers δ_c need to get authenticated to store their privacy information in the IPFS data storage protocol. Therefore, we have considered the certificate authority Υ to approve them for data storage in IPFS by providing them with Φ. Once Δ_a and δ_c get the approval certificate from certificate authority, smart contract executes to validate their data storage rights for IPFS with the help of Φ. If smart contract gives the approval to both the users, i.e., Δ_a and δ_c, then they can easily access and store their privacy information in the IPFS. IPFS can return the favor by sending them the hash keys $\Xi_{\Delta_a} \in \{\Xi_{\Delta_1}, \Xi_{\Delta_2}, \ldots, \Xi_{\Delta_d}\}$ for vehicle owners and $\xi_{\delta_c} \in \{\xi_{\delta_1}, \xi_{\delta_2}, \ldots, \xi_{\delta_t}\}$ for customers.

$$\Delta_a \xrightarrow{\beta} \sum_{a=1}^{d^{''}} \Xi_{\Delta_a} \;\; and \;\; \delta_c \xrightarrow{\beta} \sum_{c=1}^{t^{''}} \xi_{\delta_c} \quad (5)$$

$$d^{''} \leq d, r > 0, t^{''} \leq t \quad (6)$$

where β signifies the association of vehicle owner and customer with $d^{''}$ and $t^{''}$ number of hash keys.

Finally, users, i.e., vehicle owners Δ_a and customers δ_c contain the hash keys Ξ_{Δ_a} and ξ_{δ_c} that can be utilized further for storing their data transactions about the rides to the blockchain network. But, for that, they should satisfy a certain condition, i.e., hash keys Ξ_{Δ_a} and ξ_{δ_c} associated with the users should resonate with the hash of the blockchain. Hash

of the block header (ρ_{br}) in the blockchain can be determined using the previous hash of the block (Θ_{pv}^{br}) and data block (μ_{db}^{br}). The mentioned entities can be represented as follows:

$$\sum_{a=1}^{d''} \Delta_a(\Xi_{\Delta_a}) \xrightarrow{\vartheta} \rho_{br}(\Theta_{pv}^{b}, \mu_{db}^{br}) \tag{7}$$

$$\sum_{c=1}^{t''} \delta_c(\xi_{\delta_c}) \xrightarrow{\vartheta} \rho_{br}(\Theta_{pv}^{br}, \mu_{db}^{br}); \tag{8}$$

where ϑ denotes association of hash keys Ξ_{Δ_a} and ξ_{δ_c} of Δ_a and δ_c with ρ_{br}.

So, users, i.e., vehicle owners and customers can securely add the ride-sharing transactions to the blockchain. Now, δ_c can reliably book the rides made accessible by the vehicle owners Δ_a. Algorithm 1 explains the complete procedure to perform the data storage of vehicle owners and customers in the IPFS. So that transactions between users can be performed securely with the time complexity of O(d) and O(t).

Also, 6G network has been employed in the proposed system so that users can communicate with each other with high efficiency and reliability due to its various aspects such as high data rate (DR_H^{6G}), low latency (La_{Net}^{6G}), and high availability (Av_H^{6G}). It also improves the customer's traveling experience via ride-sharing. The features of 6G can be represented as follows:

$$La_{Net}^{6G} < 1ms \tag{9}$$

$$DR_H^{6G} < 10Gbps \tag{10}$$

$$Av_H^{6G} = 99.9999\% \tag{11}$$

Algorithm 2 Reverse stackelberg game for optimal data pricing.

Input: Δ_a, δ_c
Output: $N_{\Gamma_{\delta_c}}^{\Gamma_{\Delta_a}}$

procedure OPT_PAYOFF(Δ_a, δ_c)
  if $E \in \Delta_a$ **then**
    for $i = 1, 2, \ldots, d$ **do**
      $\Gamma_{\delta_c}^{op} \xrightarrow{\sigma} \Pi_{\Gamma_{\delta_c}}(Pf_{\Gamma_{\Delta_a}}^{op}(\Gamma_{\delta_c}), \Gamma_{\delta_c})$
      $Gamma_{\delta_c} \xrightarrow{k} min \sum_{d=1}^{b'} \sum_{u=1}^{h'}(\theta_d, \tau_u)$
    end for
  else
    for $j = 1, 2, \ldots, t$ **do**
      $Pf_{\Gamma_{\Delta_a}} \xrightarrow{n} \Pi_{\Gamma_{\Delta_a}}(Pf_{\Gamma_{\Delta_a}}(\Gamma_{\delta_c}^{op}(Pf_{\Gamma_{\Delta_a}}, \Gamma_{\delta_c}^{op}(Pf_{\Gamma_{\Delta_a}})$
      $\Gamma_{\Delta_a}' \xrightarrow{n} max \sum_{d=1}^{b'} \sum_{u=1}^{h'}(\theta_d, \tau_u)$
    end for
  end if
  for each players for optimal payoff **do**
    $(\Gamma_{\delta_c}^{op}, \Gamma_{\delta_c}) < N_{\Gamma_{\delta_c}}^{\Gamma_{\Delta_a}} < (Pf_{\Gamma_{\Delta_a}}, \Gamma_{\Delta_a})$
    $\{\Delta_a, \delta_c\} getmaximumpayoffN_{\Gamma_{\delta_c}}^{\Gamma_{\Delta_a}}$
  end for
end procedure

III. Reverse stackelberg game theory approach

The proposed system has introduced the reverse stackelberg game theory approach to provide Δ_a and δ_c with the optimal data pricing for ride-sharing. In the proposed system, a reverse stackelberg game consists of two players vehicle owner Δ_a and customer δ_c in which we have considered Δ_a as leader and δ_c as follower. The reverse stackelberg game works in such a way that initially δ_c as a follower decides upon the strategy Γ_{δ_c} in which customers prefer to travel shortest route from the number of routes $\{\tau_1, \tau_2, \ldots, \tau_h\} \in \tau_u$ available for rides and travel to the destination by paying the minimum price. The prices assigned to the number of routes are $\{\theta_1, \theta_2, \ldots, \theta_b\} \in \theta_d$. Based on the decided strategy of the follower, i.e., customer, vehicle owner as a leader takes the further action to choose its strategy Γ_{Δ_a} in such a way that ride-sharing should be favorable to them. Strategy Γ_{Δ_a} is chosen so that they want their cars to take from the longer path and want to charge high prices to the customers.

Now, strategies of Δ_a and δ_c can be defined in the form of variables such as $\Gamma_{\Delta_a} \in \Xi_{\Delta_a} \subseteq \mathbb{R}$ and $\Gamma_{\delta_c} \in \Xi_{\delta_c} \subseteq \mathbb{R}$ with the cost function considered as $\Pi_a : \Gamma_{\Delta_a} * \Gamma_{\delta_c}$ in which a lies between $\{\Gamma_{\Delta_a}, \Gamma_{\delta_c}\}$ and a path function $Pf_{\Gamma_{\Delta_a}} \in (\Gamma_{\delta_c}$ ¿ $\Gamma_{\Delta_a})$. So, optimal strategy of customer $\Gamma_{\delta_c}^{op}$ associated with the above mentioned entities can be represented as follows [18]:

$$\Gamma_{\delta_c}^{op} \xrightarrow{\sigma} \Pi_{\Gamma_{\delta_c}}(Pf_{\Gamma_{\Delta_a}}^{op}(\Gamma_{\delta_c}), \Gamma_{\delta_c}) \tag{12}$$

$$\Gamma_{\delta_c} \xrightarrow{k} min \sum_{d=1}^{b'} \sum_{u=1}^{h'}(\theta_d, \tau_u), \quad d \geq 0, \quad u \geq 0 \tag{13}$$

where σ denotes the customer's strategy based on which vehicle owners can try to optimize their payoff in the ride-sharing. k signifies the individual strategy of the customer, which will not affect any other users. So, according to the optimal strategy $\Gamma_{\delta_c}^{op}$ of the customer as a follower in the reverse stackelberg game, vehicle owner Γ_{Δ_a} as a leader adopt an optimal strategy defined in the form of function, which can be mentioned as follows [18]:

$$Pf_{\Gamma_{\Delta_a}} \xrightarrow{n} \Pi_{\Gamma_{\Delta_a}}(Pf_{\Gamma_{\Delta_a}}(\Gamma_{\delta_c}^{op}(Pf_{\Gamma_{\Delta_a}}, \Gamma_{\delta_c}^{op}(Pf_{\Gamma_{\Delta_a}}) \tag{14}$$

$$\Gamma_{\Delta_a}' \xrightarrow{n} max \sum_{d=1}^{b'} \sum_{u=1}^{h'}(\theta_d, \tau_u) \tag{15}$$

where n signifies the strategy of in vehicle owners Γ_{Δ_a} according to the strategy of the customer. So, we have discussed the strategies associated with the customer as a follower based on which leader can choose their strategy to maximize their payoff. So, we have to define a special condition in which both users can be satisfied with the pricing. As Γ_{δ_c} as a follower chooses to travel through the shortest route, they have to pay the minimum price for traveling. And, if Γ_{Δ_a} follow its decision to choose the strategy for their profit, then they prefer rides to travel through longer route and charge maximum prices from customers. Therefore, there is an existence of reverse stackelberg equilibrium between Γ_{Δ_a} and Γ_{δ_c} in which both the users can get the optimal payoff ($N_{\Gamma_{\delta_c}}^{\Gamma_{\Delta_a}}$) by adapting the strategy in favor of them, which can be mentioned as follows:

$$(\Gamma_{\delta_c}^{op}, \Gamma_{\delta_c}) < N_{\Gamma_{\delta_c}}^{\Gamma_{\Delta_a}} < (Pf_{\Gamma_{\Delta_a}}, \Gamma_{\Delta_a}) \tag{16}$$

So, in applied reverse stackelberg equilibrium game-based approach, customer considered as the follower firstly choose the strategy, then leader prepares the strategy by following the customer's decision [19]. But, both the users cannot be on the same level in terms of profit as one may suffer the loss due to route or pricing. This leads to the scenario of an equilibrium that assures profit for both the users making it convenient for utilizing the ride-sharing. Furthermore, Algorithm 2 describes

the procedure of obtaining optimized payoff between vehicle owners and customers during ride-sharing. The time complexity involved in the payoff can be computed in O(d) and O(t).

Fig. 2 shows the detailed procedure to optimize the payoff for vehicle owners and customers to enable secure ride-sharing in the blockchain-based proposed system. The procedure initiates with the system model considered as the input, which is further classified into three layers, i.e., Data acquistion layer, Transaction layer, and Blockchain layer. Moreover, a reverse stackelberg game theory has been applied to get the desired payoff for vehicle owners and customers at an equilibrium.

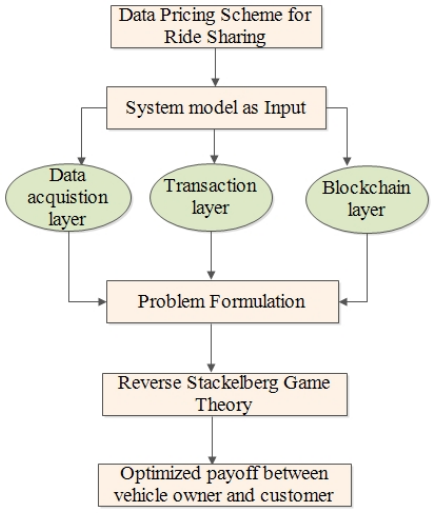

Fig. 2: Sequence flow of the proposed system.

IV. Security Verification of the Proposed System

In this section, security analysis of the smart contracts of the proposed system has been performed over the smartcheck tool. We have executed the source code from the Ethereum platform to detect the security issues in the proposed system. Fig. 3 depicts the working of the smartcheck tool in such a way that it verifies that the source code of the proposed system does not have any threat or vulnerability. But, smartcheck tool generates one severity in the source code by default as depicted in Fig. 4 [20]. We have also removed that identified severity from the source code as depicted in Fig. 3.

```
C:\Users\hp\Desktop\Parking.sol
jar:file:/C:/Users/hp/AppData/Roaming/npm/node_modules/@smartdec
```

Fig. 3: Security analysis of proposed system over smartcheck.

```
C:\Users\hp\Desktop\Parking.sol
jar:file:/C:/Users/hp/AppData/Roaming/npm/node_modules/@smartdec/smartcheck/
PRAGMAS_VERSION
patternId: 23fc32
severity: 1
line: 1
column: 23
```

Fig. 4: Security analysis over smartcheck by default.

V. Experimental Results of the Proposed System

In this section, the results of the blockchain-based proposed system have been evaluated for secure and efficient ride-sharing between vehicle owners and customers using a reverse stackelberg game theory approach to get the desired optimized payoff for users. For that, the simulation of the proposed system has been performed on Remix integrated development environment (IDE) by executing the smart contracts using a solidity high-level language. Finally, the simulation of the experimental results has been evaluated considering the communication latency, blockchain scalability, and payoff analysis, which can be represented as follows:

A. Communication latency

Fig. 5 illustrates the latency comparison between 4G, 5G and 6G network interface. The 6G-assisted base station operates on terahertz frequencies that bring ubiquitous high data rates and low latency communication [21]. Both the parameters data rates and latency are essential in enhancing the performance of the ride-sharing systems. From the graph,

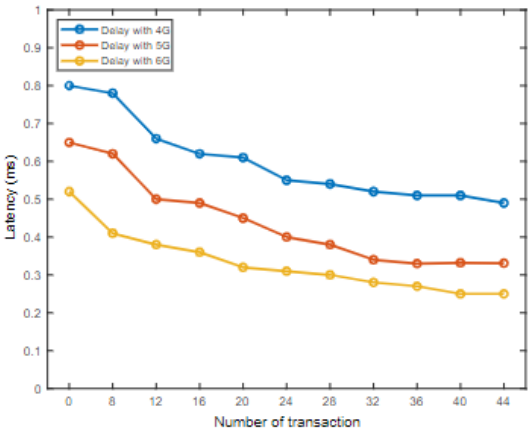

Fig. 5: Latency comparison.

we can depict that as the number of transactions increases, the latency of the 6G network decreases, ensuring faster communication between entities in the ride-sharing systems. On the contrary, the conventional cellular systems, such as the 4G and 5G networks, show severe delays as the number of transactions increases. Consequently, it deteriorates the performance of the ride-sharing system.

B. Blockchain scalability

Fig. 6 shows the scalability comparison between traditional blockchain and IPFS-based blockchain. It is evident from the paramount benefits of IPFS, i.e., cost expensive and storing hashed data instead of raw data makes this technology more scalable than the traditional blockchain layer. Moreover, the graph displays that as the number of transactions increases, the scalability of the IPFS technology increases. This happens because the IPFS is cost-free, and it processes the hashed data instead of raw data, due to which more users are incorporating it in their application.

C. Payoff analysis

Fig. 7 shows the payoff optimization of the proposed Stackelberg game with the increase in the number of transactions. It can be observed from the graph that as the number of transactions increases, the payoff of the game converges to an optimal point. The game has a reverse stackelberg equilibrium where players can optimize their payoffs. The output of the reverse stackelberg equilibrium is that player 1 plays a strategy on which player 2 depends. Hence, the graph highlights that

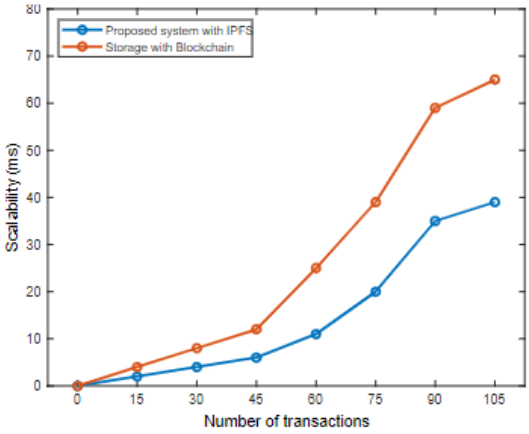

Fig. 6: Scalability comparison.

the payoffs remain the same between the players after a particular point, i.e., equilibria.

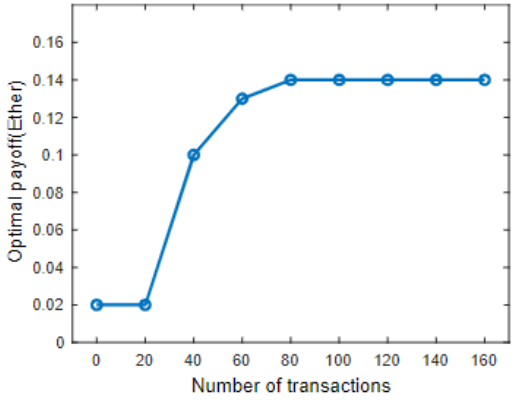

Fig. 7: Payoff analysis.

VI. Conclusion

In this paper, a blockchain-based secure and optimal data pricing system is proposed integrated with a 6G network. We have introduced the IPFS with blockchain to enable low-cost data storage for vehicle owners and customers. We explored the conventional systems to understand their trust, privacy, latency, reliability, payoff, and cost-efficiency issues. We have observed and analyzed that the employed IPFS with the 6G network ensures efficient and reliable data transmission in the system. Furthermore, we have formulated a reverse stackelberg game theory approach in the blockchain system to optimize the profit for users. Finally, the proposed system has been implemented on Remix Integrated Development Environment (IDE) by executing the smart contracts using the solidity programming language. At last, the performance of the proposed system has been evaluated considering the terms such as latency, scalability, and the optimal payoff for the system by differentiating it from the conventional systems. The results show that the proposed system is highly secure, reliable, and cost-efficient.

In the current scenario, we have applied a reverse stackelberg game theory between two players, i.e., vehicle owner and customer for optimizing the payoff. In the future work, we can apply a game theory approach for multiple number of users to enable the profitable and dynamic ride-sharing in the proposed system.

References

[1] H. M. Amar and O. A. Basir, "A game theoretic solution for the territory sharing problem in social taxi networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2114–2124, 2018.

[2] C. Huang, R. Lu, J. Ni, and X. Shen, "Dapa: A decentralized, accountable, and privacy-preserving architecture for car sharing services," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 4869–4882, 2020.

[3] A. J. Qarebagh, F. Sabahi, and D. Nazarpour, "Optimized scheduling for solving position allocation problem in electric vehicle charging stations," in *2019 27th Iranian Conference on Electrical Engineering (ICEE)*, pp. 593–597, IEEE, 2019.

[4] U. M. Aïvodji, 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*, pp. 40–50, 2018.

[5] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1314–1345, 2018.

[6] G. Guo and Y. Xu, "A deep reinforcement learning approach to ride-sharing vehicle dispatching in autonomous mobility-on-demand systems," *IEEE Intelligent Transportation Systems Magazine*, vol. 14, no. 1, pp. 128–140, 2022.

[7] "Driverauth: A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms," *Computers & Security*, vol. 83, pp. 122–139, 2019.

[8] Y. He, J. Ni, X. Wang, B. Niu, F. Li, and X. Shen, "Privacy-preserving partner selection for ride-sharing services," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5994–6005, 2018.

[9] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1214–1229, 2021.

[10] R. Kakkar, R. Gupta, S. Tanwar, and J. J. P. C. Rodrigues, "Coalition game and blockchain-based optimal data pricing scheme for ride sharing beyond 5g," *IEEE Systems Journal*, pp. 1–10, 2021.

[11] S. Tyagi, S. Tanwar, S. K. Gupta, N. Kumar, and J. J. Rodrigues, "A lifetime extended multi-levels heterogeneous routing protocol for wireless sensor networks," *Telecommun. Syst.*, vol. 59, p. 43–62, may 2015.

[12] D. Wang and X. Zhang, "Secure ride-sharing services based on a consortium blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2976–2991, 2021.

[13] C. Xu, K. Zhu, C. Yi, and R. Wang, "Data pricing for blockchain-based car sharing: A stackelberg game approach," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pp. 1–5, 2020.

[14] H. M. Amar and O. A. Basir, "A game theoretic solution for the territory sharing problem in social taxi networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2114–2124, 2018.

[15] P. Bhattacharya, S. Tanwar, R. Shah, and A. Ladha, "Mobile edge computing-enabled blockchain framework—a survey," in *Proceedings of ICRIC 2019* (P. K. Singh, A. K. Kar, Y. Singh, M. H. Kolekar, and S. Tanwar, eds.), (Cham), pp. 797–809, Springer International Publishing, 2020.

[16] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, "A secure data sharing platform using blockchain and interplanetary file system," *Sustainability*, vol. 11, no. 24, p. 7054, 2019.

[17] D. Reebadiya, T. Rathod, R. Gupta, S. Tanwar, and N. Kumar, "Blockchain-based secure and intelligent sensing for autonomous vehicles activity tracking beyond 5g networks," *Peer-to-Peer Networking and Applications*, 02 2021.

[18] N. Groot, B. De Schutter, and H. Hellendoorn, "Reverse stackelberg games, part i: Basic framework," in *2012 IEEE International Conference on Control Applications*, pp. 421–426, 2012.

[19] C. Xu, K. Zhu, C. Yi, and R. Wang, "Data pricing for blockchain-based car sharing: A stackelberg game approach," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pp. 1–5, 2020.

[20] A. L. Vivar, A. T. Castedo, A. L. S. Orozco, and L. J. G. Villalba, "An analysis of smart contracts security threats alongside existing solutions," *Entropy*, vol. 22, no. 2, 2020.

[21] S. Tanwar, S. Tyagi, I. Budhiraja, and N. Kumar, "Tactile internet for autonomous vehicles: Latency and reliability analysis," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 66–72, 2019.