# Cryptober: A Blockchain-based Secure and Cost-Optimal Car Rental Platform

Vikas Hassija, Mohd Zaid, Gurjot Singh, Amit Srivastava, Vikas Saxena
Department of CSE and IT, JIIT, Noida, India

***Abstract*—Blockchain is a growing list of records, stored in blocks, which are linked and secured using cryptography. Blockchain is important because it brings trust to peer-to-peer networks. Various blockchain applications from small to big are focused towards decentralizing different tasks and are trying to empower the masses to act without any intermediary in between. The existing and upcoming blockchain applications are highly promising to increase the level of comfort for everyone. Smart contracts can be thought of as self-executing contracts with the terms of the agreement between buyer and seller directly written into lines of code. In this paper, we present a detailed review of how blockchain and smart contracts can be used to create a platform for car rental services that will be beneficial for both the car owner and the renter. The platform is cost optimal because there will be no intermediary in between. This will also introduce high security, privacy, authentication, and safety in the car rental industry.**

***Keywords*—Blockchain, Smart Contracts, Cryptocurrency, Proof-of-Work, Proof-of-Stake, Digital Signatures, Hyperledger Fabric, Distributed Ledger Systems.**

## I. Introduction

A car rental service rents out vehicles to people who want a rented car for some time due to various reasons. The first known car rental service can be attributed to the German company Sixt in 1912. After World War 2, travel increased a lot which led to an expansion in car rental businesses. Car sales have significantly increased during the 20th century, but the trend seems to be slowing down due to many factors such as traffic, pollution, better public transport, etc [1]. So when people need a car for some reason, they prefer renting it for a short duration rather than buying it. With the advent of the digital era, these services have been infused with technology. Now users of this industry can look at various options on websites or mobile applications. Technology has also increased the ease of doing business in this field as owners can now track cars with Global Positioning Systems (GPS). The Internet has also increased the reach of such businesses. A lot of sharing companies such as ridesharing, house sharing have thrived due to the internet. Airbnb, Ola, Lyft, and Uber are some of the largest technology companies out there. Even after decades of technological advancements, the field is plagued with various issues such as lack of trust, centralization etc.

A lot of these problems can be solved using a distributed peer-to-peer network [2]. Such a network can significantly reduce the commissions charged by the middleman. This will also encourage a lot of people to rent out their car with ease when it is not in use. This is a significant problem with car rental services in the present times. If a person wants to rent a car, and his neighbor's car is not being used, he still has to go all the way to the rental service, to a middleman, to rent a car. Questions can be raised about the regulatory compliances in the absence of a central authority. The solution is smart contracts. Through the course of this paper, we will show how blockchain and smart contracts can be used to bring about a revolution in this industry.

### A. Motivation

The concept of leasing your assets when not in use with others for monetary benefit is in the market since decades. This allows the owner to fully utilize the asset. For instance, the use of tool libraries, a library where you lend tools instead of books. You do not need to buy your tools to get a job done, lend them instead. Blockchain technology allows secure peer-to-peer transactions. On current car rental platforms, an individual can rent a car on a daily basis or on kilometers basis but after a fixed charge only. But, in most cases, you just need to use the car for a few hours or a few kilometers. In case of centralized car rental services you also need to get to their local station. If your neighbor or someone next to you has the exact kind of service, than it can be availed easily in a peer-to-peer network. This would save time and other expenses including the hefty transaction fees. The platform also allows the user to avail the facilities only for the time for which the service is required. This is part of the problem we wish to address.

Figures 1, 2, 3 and 4 give us an idea of the growth of car rental industry in India.This is another motivating factor to propose this paper. According to revenue trends shown in Fig. 1, Car Rentals segment amounts to US $338 million in 2019[3] and this is expected to grow rapidly in upcoming years.

The active user-base is increasing every year as shown in the Fig. 2. The average revenue per user is also increasing - i.e., the amount of money each user spends in car renting process, as shown in Fig. 3. The percentage of population from a selected market using car rental services for each year is also showing a positive slope as shown in Fig. 4[**?**]. Hence, we can see that introducing a peer-to-peer network in this industry can be highly promising.

As we have seen through the stats provided above, the car rental industry in India is still in its growing phase. With an increase in the size of any industry, its structure becomes more

978-1-7281-3591-5/19/$31.00 ©2019 IEEE

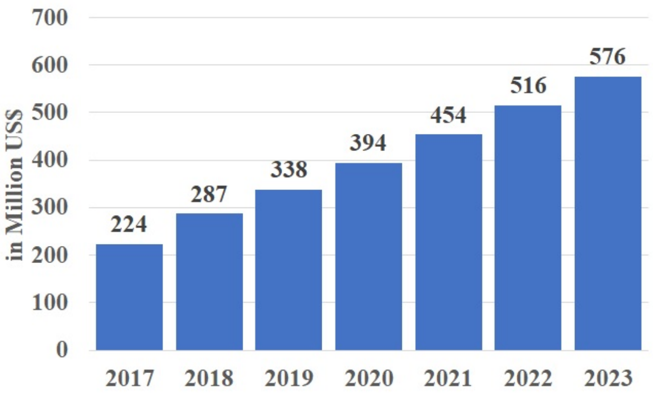

Fig. 1. Revenue trends

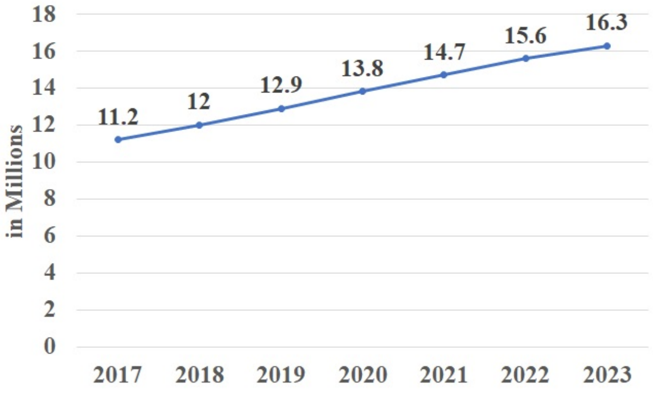

Fig. 2. Users

and more complex. It is always better to tackle the shortcomings of any system when it is not fully grown and still simple and easy to comprehend.

### B. *Organization of this paper*

This paper is organized in the following fashion:

- Section 2 describes the drawbacks in existing platforms.

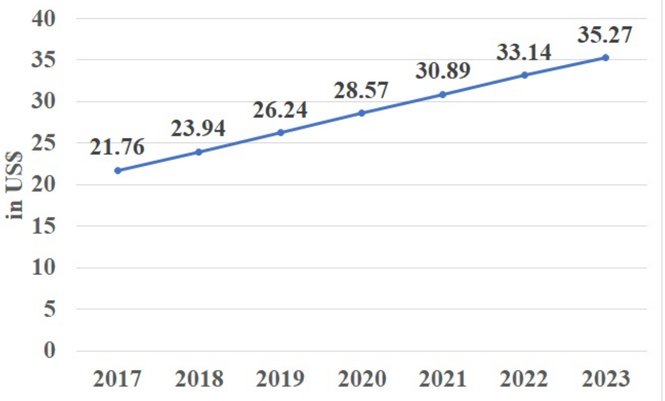

Fig. 3. Average Revenue Per User

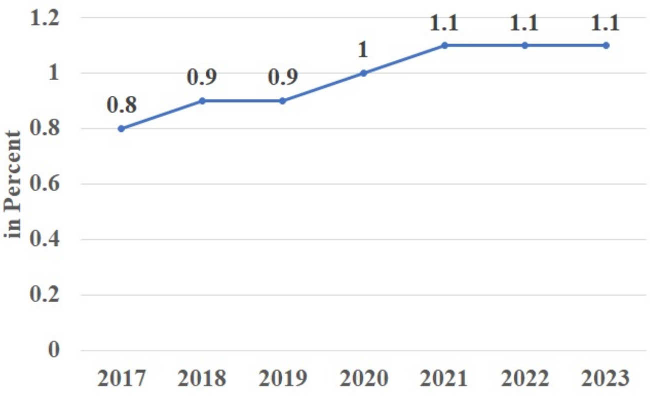

Fig. 4. Penetration Rate

- Section 3 describes the utility of blockchain and smart contracts in this industry.
- Section 4 describes our proposed approach.
- Section 5 elaborates on the algorithms used in the smart contract.
- Section 6 is for the conclusion of this paper.

## II. Drawbacks In Existing Platforms

In this section we introduce the major drawbacks in the existing car rental systems and sharing businesses.

- **High expenses** - A lot of sharing businesses have flourished in recent decades, but these businesses are plagued with high costs as the companies tend to take a high rate of commission, ranging to 30% [4]. This puts a heavy burden, both on the true owners and users of the service. These businesses do not have any assets, they just act as intermediaries who take a big chunk of profits from the true owners.
- **No transparency** - Transparency, in this case refers to everything being open to the public, not only the source code. This includes the people responsible, documents, reports, etc. In traditional cases for example zoom car, there is a lack of transparency in terms of documents or reports.
- **Centralized Structure** - The centralized structure of the existing services ends up into a heavy loss to the owners and users of the service. The middlemen, who have no real stake in the business, call the shots and decide the prices, charging high commissions. They drive out small businesses and generate a false monopoly in the market. These companies also take advantage of their monopoly by selling the user data to other third parties for monetary reasons.
- **Absence of trust** - There is a genuine absence of trust in the rental business. Proprietors frequently expect leaseholders to pay robust sums immediately, yet neglect to keep their pledge when these deposits are made. On the other hand, the leaseholders misuse the vehicle and do not agree to pay the appropriate bills [5].

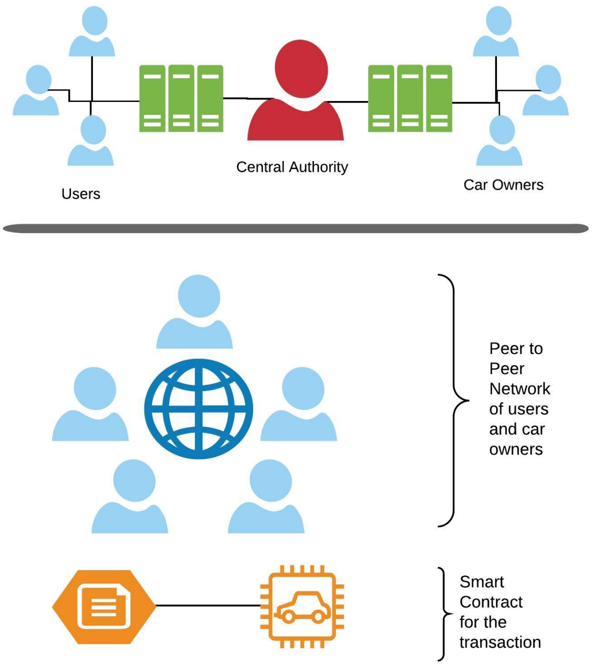
Users
Central Authority
Car Owners
Peer to Peer Network of users and car owners
Smart Contract for the transaction

Fig. 5. Differences - Above : Traditional systems, Below : Proposed car rental service

- **Safety and security** - There are no provisions for the safety of the users of the present car rental services. In case the user unfortunately encounters an accident and becomes incapacitated to call for help, the platform will be of no use.

## III. Why Blockchain and Smart contracts?

As we have noted, there are a lot of drawbacks in existing car rental platforms. Each of those can be solved using blockchain and smart contracts. The problem of trust can be solved using blockchain [6]. Once a transaction is recorded in a block, it cannot be tampered as the hash computed for a block contains the previous block hash [7]. So if transaction is tampered, then all the subsequent block hashes will have to be recomputed which requires a tremendous amount of computation power. Blockchain is completely decentralized, so the money and power will remain in the hands of the masses [8]. Over and above, there will be no unnecessary commissions going to big corporations. User's information will be secured using cryptography and will not be shared with third parties as the traditional companies do for monetary benefits [9]. This will result in less spamming to the users of the platform. There will be complete transparency of transactions as all the transactions will be recorded on the public ledger [10] and everyone will be able to see where the money is going.

Smart contracts will take the place of intermediaries in ensuring that the terms of the deal are being followed by both the parties. Money on both ends will be locked until the successful completion of the transaction. Smart contracts will also have a direct link to the GPS which will monitor the ride. Mishappenings such as accidents will be monitored and the authorities will be informed immediately with the location details. This will ensure more security than the existing platforms. Blockchain will employ a lot of people in the form of miners who will get incentives in the form of transaction fees (a lot less than existing services).

## IV. Proposed Approach

The basic data structure of this project is the blockchain which is a growing list of records called blocks, which are linked using cryptography [11],[12]. Blocks in our blockchain will represent the transaction made during the renting of the car. Each block will have data stored in the form of Merkle trees. It is a tree structure in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its children [13].

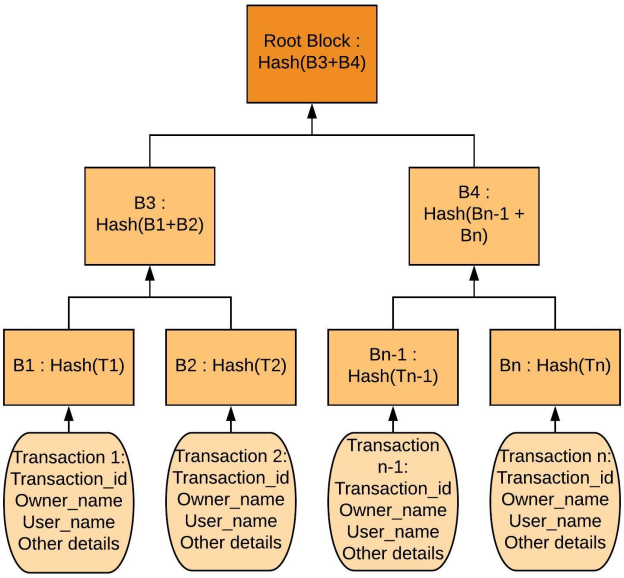
Root Block : Hash(B3+B4)
B3 : Hash(B1+B2)
B4 : Hash(Bn-1 + Bn)
B1 : Hash(T1)
B2 : Hash(T2)
Bn-1 : Hash(Tn-1)
Bn : Hash(Tn)
Transaction 1: Transaction_id Owner_name User_name Other details
Transaction 2: Transaction_id Owner_name User_name Other details
Transaction n-1: Transaction_id Owner_name User_name Other details
Transaction n: Transaction_id Owner_name User_name Other details

Fig. 6. Merkle Tree

The Merkle tree has up to 2 children on each node, i.e., the balancing factor is 2. This technique provides a security measure against unwanted modification of data by hackers. The hashing technique used for the encoding purpose is SHA-256 [14]. This technique works with information broken down into pieces of 512 bits (or 64 bytes in other words). It produces its cryptographic ”mixing” and then issues a 256-bit hash code. The algorithm includes a comparatively simple procedure, which is repeated 64 times. The SHA-256 algorithm is based on the Merkle-Damgard construction method, according to which the initial index is divided into blocks immediately after the change is made, and those, in turn, are divided into 16 words [15].

All transaction will take place in a permissionless network where the miners will be paid an incentive. These incentives will be in the form of transaction fees on each transaction on the network. The transaction fees will be very less compared to other car rental platforms [16].

We will use Proof of Work to achieve consensus. A Proof-of-Work (PoW) system is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester [11]. The miner will have to calculate the hash value such that first $D$ (difficulty) characters of the hash are ’0’ [17]. Whichever miner is the first to generate this hash value and add the transaction in a block to the blockchain, will get the incentive.

The Global Positioning System on the vehicle will track the user throughout the ride (or transaction). It will store data such as distance travelled, top speed reached, accidents, etc. and will compile a report on the condition of the car which will also be stored in the blockchain [18]. There will be a QR code attached to the car which will store all the previous transactions or trips on that car. When a new user wants to rent the car, he/she can scan the QR code and can know about the state of the car. The user will also verify the physical state of the car before renting it from the owner. If he decides to rent the car, the transaction will start.

Each transaction will contain 2 blocks - *start* and *finish*. Both parts will be stored on separate blocks in the blockchain. In the *start*, the user and the owner will set a few rules such as the time for which the vehicle will be rented, the top speed that the user can reach, the furthest the user can go, etc. All this will be in the form of a *Smart Contract* which will get executed based on the information from the GPS device on the vehicle [19] ,[20]. Both will also decide the price of the transaction which will then be floated for the miner to add in the blockchain. In the *finish* part, when the user returns the vehicle to the owner, the smart contract will check whether all the predefined rules were followed by the user and the transaction will be completed. This second part will then be added to the blockchain, and the whole transaction will be over.

The smart contract will also monitor the ride and check for accident or collisions using the Global Positioning System and the Collision Detection System of the vehicle. If this happens, the contract will immediately inform the owner and the concerned authorities for immediate assistance.

## V. Algorithms

In this section we present the structure for the smart contract that will be running during the process of the transaction (ride) in Algorithm 1. The inputs will be the start location, the end location, the total distance allowed to the user, the total time for which the user can rent the car and the maximum speed the user can reach. The smart contract will lock the price from the user and will only release the amount after the completion of the trip.

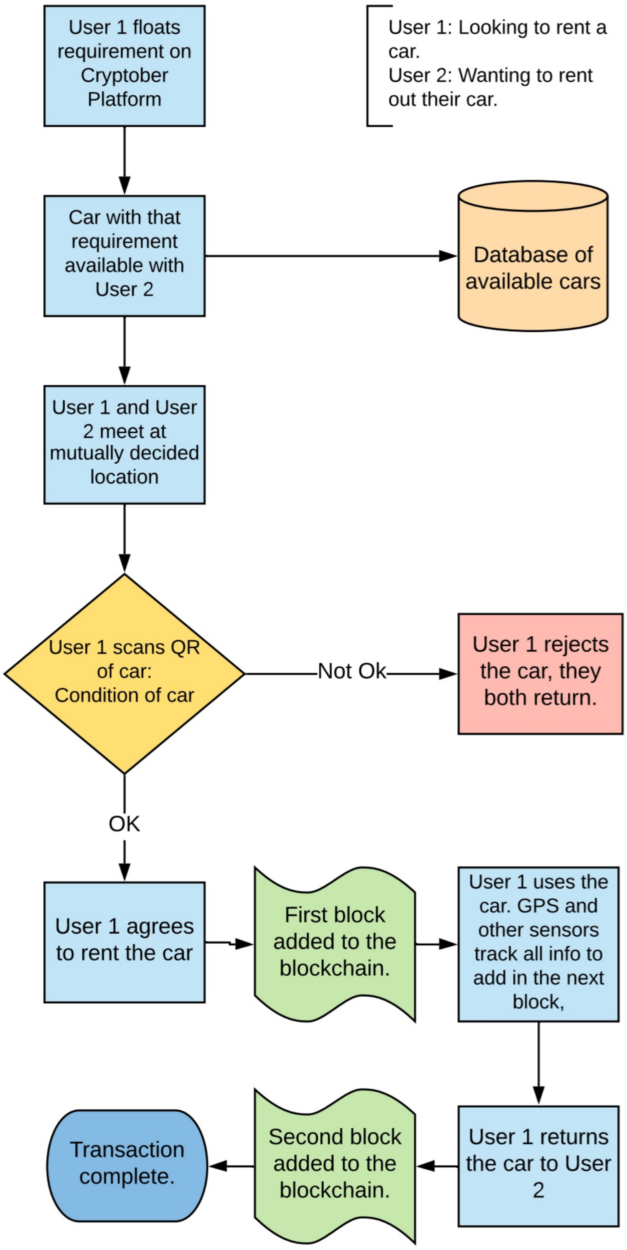
User 1 floats requirement on Cryptober Platform
User 1: Looking to rent a car.
User 2: Wanting to rent out their car.
Car with that requirement available with User 2
Database of available cars
User 1 and User 2 meet at mutually decided location
User 1 scans QR of car: Condition of car
Not Ok
User 1 rejects the car, they both return.
OK
User 1 agrees to rent the car
First block added to the blockchain.
User 1 uses the car. GPS and other sensors track all info to add in the next block,
User 1 returns the car to User 2
Second block added to the blockchain.
Transaction complete.

Fig. 7. Steps involved in renting a car.

The contract will also lock a certain security deposit from the user and give it back to the user only after the successful completion of the trip. The smart contract will have a direct link to the Global Positioning System and will receive the current location of the vehicle and the speed of the vehicle. The smart contract will monitor the trip and check if the top speed by the user has exceeded the top speed allowed by the owner. If that has happened, the contract will pop up a warning on the GPS

**Algorithm 1** Designing Smart Contract for the basics of the ride

```
function $Contract1($
$startLoc, endLoc, dist, time, topSpeed)$
    Creating block for transaction
    Set : $Global\_Positioning\_System$
    Set : $Current\_Location$
    Set : $Distance\_travelled$
    Set : $Top\_speed$
    Set : $Trip\_Time$
    Set : $Price\_Finalized$
    Set : $Trip\_Normal$
    if start of trip then
        Lock Price_Finalized from user
        Lock Security_Deposit from user
    end if
    if Distance_travelled greater than dist then
        initialize :$send\ location\ to\ owner$
        SendLocationOwner()
    end if
    if Top_speed greater than topSpeed then
        initialize :$Warning:\ top\ speed\ reached$
    end if
    if Trip_Time greater than time then
        initialize :$Warning:\ time\ limit\ exceeded$
        SendLocationOwner()
    end if
    if end of trip and Trip_Normal then
        Release Price_Finalized to owner
        Release Security_Deposit to user
    end if
    Encrypt block using the public key of both customer
        and sender. % Block is propagated to all the nodes.
end function
function $SendLocationOwner$
    set : $Owner$
    Set : $Global\_Positioning\_System$
    Set : $Current\_Location$
    Send Current_Location to Owner
end function
```

screen. Apart from warnings, a fine can also be charged in case of repeated violations. The smart contract will also look if the user has exceeded the time limit of his ride and if so, will send the location of the car to the owner. If the user travels further than the allowed distance (might be due to malicious intent), then the contract will send the car's location to the owner.

Now we present the smart contract structure for emergencies in the Algorithm 2. As has been shown, smart contracts will be linked to the Global Positioning System of the vehicle. If the contract detects that there has been a sudden drop in the speed of the vehicle, it will assume that an accident might have happened, and so it will immediately inform the owner and the authorities for immediate assistance. The same will happen if

**Algorithm 2** Designing Smart Contract for emergencies

```
function $Emergency($
$startLoc, endLoc, dist, topSpeed)$
    Creating block for transaction
    Set : $Global\_Positioning\_System$
    Set : $Current\_Location$
    Set : $speed$
    Set : $Road\_Location$
    Set : $Collision\_Sensor$
    if sudden drop in speed detected then
        Warning: Sudden drop in speed detected
        initialize :$send\ location\ to\ owner\ and\ authorities$
        SendLocation()
    end if
    if vehicle goes offroad then
        initialize :$Warning:\ Vehicle\ not\ on\ road$
        SendLocation()
    end if
    if collision detected then
        initialize :$Warning:\ Collision\ detected$
        SendLocation()
    end if
end function
function $SendLocation$
    set : $Owner$
    set : $Police$
    set : $Ambulance$
    Set : $Global\_Positioning\_System$
    Set : $Current\_Location$
    Send Current_Location to Owner
    Send Current_Location to Police
    Send Current_Location to Ambulance
end function
```

the GPS detects that the vehicle has gone off-road. The smart contract will also have a link to the Collision Detection System of the vehicle. If the collision detection system goes off, the contract will immediately inform the concerned authorities and the owner.

## VI. Conclusion

In this paper we present a decentralized platform for car rental application with minimum transaction charges. The enforcing is done by smart contracts, and the ledger will be in the form of a blockchain which is tamper-proof. The proposed platform will employ a lot of people (in the form of miners) and give a lot of people an opportunity to earn money by renting out their cars securely, without a need of giving commissions to the intermediaries. In terms of security and safety, as soon as the GPS detects an accident (sudden stop of a car after a high speed, or leaving the road), the smart contract will inform the authorities. The money will only be transferred to the respective parties on successful completion of the transactions unbiased (judged by the unbias smart contract). There will also be a provision for a security deposit which will be locked by the smart contract, until the successful completion of the ride. Thus we can see how this system can resolve some of the shortcomings of the car rental industry efficiently.

## References

[1] S. A. Shaheen, D. Sperling, and C. Wagner, "A short history of carsharing in the 90's," 1999.

[2] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proceedings First International Conference on Peer-to-Peer Computing*. IEEE, 2001, pp. 101–102.

[3] statista-The Statistics Portal, "Car rental stats - india," 2018. [Online]. Available: https://www.statista.com/outlook/270/119/car-rentals/india

[4] B. G. Edelman and D. Geradin, "Efficiencies and regulatory shortcuts: How should we regulate companies like airbnb and uber," *Stan. Tech. L. Rev.*, vol. 19, p. 293, 2015.

[5] P. Kamal and J. Q. Chen, "Trust in sharing economy." in *PACIS*, 2016, p. 109.

[6] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, July 2019.

[7] 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.

[8] S. Raval, "Decentralized applications: harnessing bitcoin's blockchain technology," pp. 14–16, 2016.

[9] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *Journal of Network and Computer Applications*, vol. 127, pp. 43–58, 2019.

[10] R. Maull, P. Godsiff, C. Mulligan, A. Brown, and B. Kewell, "Distributed ledger technology: Applications and implications," *Strategic Change*, vol. 26, no. 5, pp. 481–489, 2017.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[12] E. Staff, "Blockchains: The great chain of being sure about things," *The Economist*, vol. 18, 2016.

[13] G. Becker, "Merkle signature schemes, merkle trees and their cryptanalysis," *Ruhr-University Bochum, Tech. Rep*, 2008.

[14] W. Penard and T. van Werkhoven, "On the secure hash algorithm family," *Cryptography in Context*, pp. 1–18, 2008.

[15] R. Merkle, "Secrecy, authentication, and public key systems," *Ph. D. Thesis, Stanford University*, 1979.

[16] A. Chepurnoy, V. Kharin, and D. Meshkov, "A systematic approach to cryptocurrency fees," in *International Conference on Financial Cryptography and Data Security*. Springer, 2018, pp. 19–30.

[17] A. Back, "Hashcash-a denial of service counter-measure," vol. 2, pp. 3–6, 2002.

[18] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "Blockcom: A blockchain based commerce model for smart communities using auction mechanism," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[19] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[20] G. Brambilla, M. Amoretti, and F. Zanichelli, "Using blockchain for peer-to-peer proof-of-location," *arXiv preprint arXiv:1607.00174*, 2016.