Secure Blockchain Model for Vehicles toll Collection by GPS tracking: A case study of India

Sujit Sangram Sahoo*
Dept. of IT
IIIT, Allahabad
Prayagraj, India
rsi2018005@iiita.ac.in

Aravind R Menon
Dept. of IT
IIIT, Allahabad
Prayagraj, India
mit2020049@iiita.ac.in

Vijay K. Chaurasiya
Dept. of IT
IIIT, Allahabad
Prayagraj, India
vijayk@iiita.ac.in

***Abstract*—This paper aims to implement a blockchain-based, fully decentralized vehicle toll collection model. The resultant scheme uses a Global positioning system to track the vehicles, and the payment module is fully decentralized and uses Ethereum blockchain. Ethereum blockchain uses immutable documents called smart contracts to carry out business logic. It ensures that every transaction between vehicle owners and the authorities is traceable, immutable, transparent, and trustworthy. The Global Positioning System provides the location of an object using coordinates measured using satellites. The data from GPS is recorded constantly to ensure that the vehicle has traveled to the correct location and is stored in a publicly verifiable blockchain. The other vehicle owners work as location verifiers except for the particular vehicle. An automatic payment system is to be developed, which gets triggered when necessary conditions are met by the vehicle. Our proposed model is authentic and secure, ensuring penalties for malicious participants. The experimental results are based on the Gas consumption of all the smart contracts. This model can improve the current toll collection model of the National Highway Authority of India to make it more profitable and corruption-free.**

***Index Terms*—Blockchain, Smart Contract, GPS, Fastag, Ether.**

I. Introduction

In the advent of information technology, the fundamental challenge is transparency and technology-based data management that needs public verifiable. The data should be authentic and social acceptance with solving different technological challenges. Corruption is not a part, and that guarantee provides the decentralization technology called Blockchain. It should be essential that auditable data and the system not be a single-point failure. It is good to discuss the current toll collection model of the Indian economy. The current model for toll collection by the National Highway Authority of India (NHAI) is fully centralized. The model may fail because of single-point failure, and corruption is not avoidable at any moment. There are many corruption cases regarding toll collection, important data leaks, particular scams, and many more. Except this, handling transactions has always been a challenging task. It is challenging to maintain accurate records of all transactions carried out by millions of people daily. In the example of a toll booth payment, various middle parties are involved, such as the cash collector and toll booth operating station. With such a large number of people using vehicles nowadays, it has become impossible to maintain records manually and use a centralized system model.

The Blockchain is necessary to make the system faster and fully decentralized to avoid all the above problems. Blockchain is an emerging technology used initially in 2008 to facilitate bitcoin by Satoshi Nakamoto. It uses a decentralized ledger to store data in blocks connected one after the other in the form of a chain. Blockchain guarantees that the participating users remain anonymous in the network [1]. The Blockchain cannot be altered once a valid transaction block is added to the decentralized ledger. Therefore, this guarantees that people who have conducted a transaction cannot deny details about it at a later point in time. It started as a technology to transfer bitcoin, the cryptocurrency used. Now, it is used in a variety of fields. Blockchain guarantees user anonymity, data immutability, and traceability with the help of cryptographic methods and consensus mechanisms such as proof of Work, Proof of Stake, Proof of Burn, and Proof of Authority [2]. Particular nodes called miners perform block validation in Blockchain and get rewarded with bitcoin current upon achieving consensus and successful data entry into the Blockchain. In 2014, a new blockchain model named Ethereum was introduced, which uses smart contracts to carry out transactions. Ethereum [3] uses a cryptocurrency called Ether. We will be looking into Ethereum based Blockchain for this project. Our model is based on smart contracts, and the overview of the proposed model is available in fig.1.

A. Failure of current toll collection model

Toll collection involved direct cash transactions in toll plazas from the very beginning and then cashless transactions using credit and debit cards. The bar-code scanning process also fails. The current process is Fastag based system. Joshi et al. [9] discussed the different methods of toll payment, including Electronic Toll Collection, Fastag, and BookMyToll. The Fastag system is used in India, operated by the NHAI. It uses Radio Frequency Identification (RFID) technology for making automatic payments from the vehicle owner's bank account linked to the Fastag card. Automatic toll payment and Fastag are good improvements to the traditional manual toll payment method. The above techniques help reduce traffic

978-1-6654-6601-1/22/$31.00 ©2022 IEEE

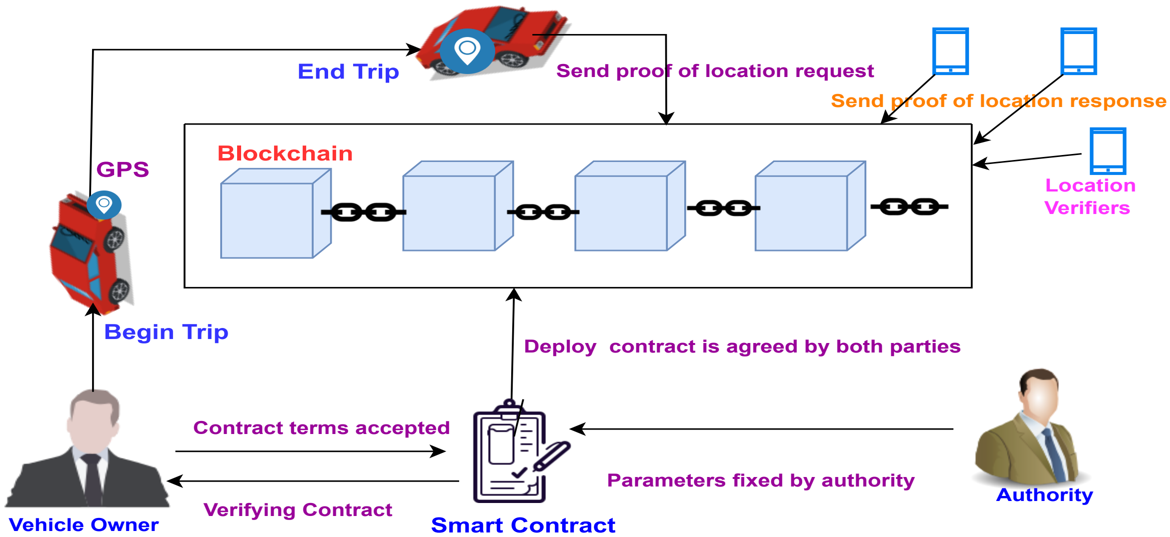

Fig. 1. Overview of proposed model

jams, wastage of fuel, and time. Sontakke et al. [10] explains how the process of automatic transaction takes place with Fastag and RFID.

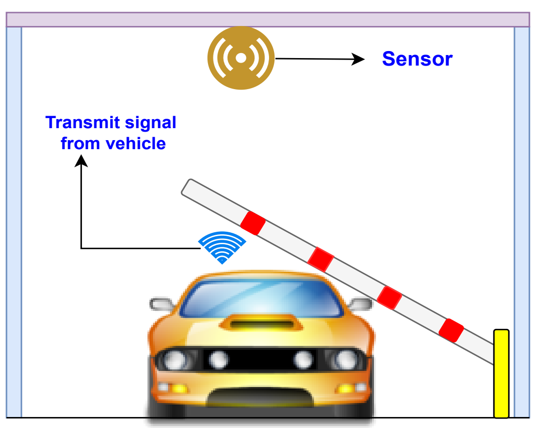

Fig. 2. Fastag based toll payment system

The automatic payment methods have addressed many issues, but there are specific challenges. Satao [11] assessed the benefits and challenges of Fastag based toll payment system. Fastag may charge users incorrectly due to technical issues. Fig.2 shows the graphical view of the fastag based model. NHAI is not involved in Fastag transactions. Bank and credit card companies handle payment and other transactions. These third parties can charge users excessively and mistreat their software to benefit themselves. Again all the above models are centralized, which shows single point failure. If we discuss data authenticity, auditable transaction, and data immutability, the current system shows disability.

Our proposed model is fully decentralized and authentic. Blockchain is publicly available and provides immutability data. It assures the authority, participants, and public that no corruption is feasible as the current system. The model uses the Global positioning system (GPS) to track the vehicles when they travel from source to destination. Smart contracts use to create a contract between the vehicle owner and NHAI authority. When a vehicle starts a trip, it deploys a smart contract on Ethereum Blockchain, including the vehicle's current and destination location. The vehicle also agrees with the price per kilometer before the contract deploys. The vehicle owner can register for more than one vehicle. After reaching the destination, the vehicle signs the location and requests the location verification to the blockchain. The blockchain is public verifiable so that the other participants or vehicles nearest to the area can verify by using their location signature. The successful verification automatically executes the smart contract, and unsuccessful verification concludes the penalty. The malicious participants penalize as per the smart contract rule, which shows our system is secure.

B. Global Positioning System

GPS has many applications nowadays, starting from vehicle navigation, tracking, measuring the distance from one point to another, speed, and many more. It is a satellite-based navigation system used to identify an object's location. Satellites transmit signals so that GPS devices can decode and find the correct location of things. GPS device needs data from at least three satellites to calculate position accurately. This process is called trilateration. Cheung et al. [12] discussed the technique of performing trilateration. The signal coming from satellites has a spherical coverage. The point of intersection of the spherical ranges of all satellites is computed to pinpoint the

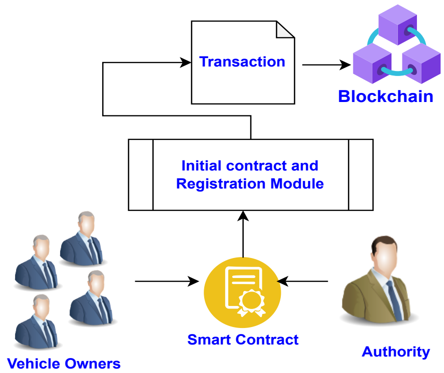

Fig. 3. Entities involved and the modules of smart contract

object's location. Since the location of the satellites is known, the distance from the satellite to a vehicle can be calculated using time and speed of received signal. The satellites use atomic clocks to calculate time. The receiver takes input from at least three satellites to accurately calculate longitude, latitude, time, and altitude.

Algorithm 1 GPS co-ordinate Calculation

Require: Input: x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3, x, y, z, c, t_1, t_2, t_3, t_{r1}, t_{r2}, t_{r3}

1:

2: $c*(t_1 - t_{r1}) = \sqrt{(x-x_1)^2 + (y-y_1)^2 + (z-z_1)^2}$

3: $c*(t_2 - t_{r2}) = \sqrt{(x-x_2)^2 + (y-y_2)^2 + (z-z_2)^2}$

4: $c*(t_3 - t_r3) = \sqrt{(x-x_3)^2 + (y-y_3)^2 + (z-z_3)^2}$

Algorithm 1 shows the calculation of GPS coordinates of vehicle x,y,z, and time correction of GPS receiver t_c. Variables x_1,y_1,z_1 and x_2,y_2,z_2 and x_3,y_3,z_3 are the coordinates of satellite one, satellite two and satellite three respectively. The speed of light is the variable c. Variables t_1,t_2 and t_3 are the transmission time and Variables t_{r1},t_{r2} and t_{r3} are data receiving time of satellite 1,2 and 3 respectively. Each satellite sends its location coordinates and transmission time to the GPS receiver, and the receiver stores the data receiving time from each satellite. The distance between the vehicle and each satellite is calculated using the euclidean distance formula. The above equations corresponding to each satellite are formed using distance = speed * time.

C. Smart Contract

A smart contract is a piece of code stored in the blockchain and executed when certain conditions are met. Smart contracts are linked with some transactions and automatically updated in the blockchain after completing the transaction. The contract account of the ethereum blockchain performs this task. The transactions on the smart contract are immutable, and relative entities can view their transaction. The smart contracts are authentic, immutable, and secure, making our model more reliable.

Fig.3 explains the function of a smart contract between Vehicle owners and NHAI Authorities. A formal agreement takes place between the parties at the time time of vehicle trip start. Both the parties deploy the contract in the blockchain. The successful verification of location concludes the execution of the smart contract automatically. Execution takes place in seconds, and the participating entities do not need to trust each other. Smart contracts do not require a physical exchange of documents or other third parties to conduct transactions. Entities can authenticate themselves using their digital signatures.

II. Literature Survey

Blockchain technology has been a subject of interest for many researchers recently. Blockchain has transcended various domains such as supply chain management, business transactions, medicine, payment, voting, and the Internet of Things in the past decade. It is also flexible and can be combined with other technologies such as Artificial Intelligence big data analytics, which further helps the blockchain analyze data faster and more accurately. Blockchain has the ledger that keeps all the transactions. Automatic payment is an important area of blockchain application. The sensors can gather data from the environment and send it to the network for analysis and storage. These details can be used for many purposes, including payment and bill generation. Hasan et al. [6] uses an ethereum blockchain that uses the Proof of Delivery consensus algorithm and immutable smart contracts to track digital assets.

Tracking the things relating to various research areas discussed in Different models. Jabbar et al. [4] proposed a parking system payment model based on the ethereum blockchain. It consists of three layers, the perception layer, the network layer, and the application layer. Finally, a few testing techniques are applied to find drawbacks and suggest improvements for the model. Chen et al. [5] discussed IoT for blockchain and their future research possibilities. The access control methods deal with organizing and managing data. Data integrity deals with securing data and correctly describing the source. Blockchain's role as a trusted party is assessed by reviewing logistics management and product traceability. Saurabh et al. [7] aims to study blockchain usage in a sustainable agriculture supply chain. RFID-based tracking module is analyzed, and the technology used is explored in a P2P system. Helo et al. [17] describes a model to conduct real-time supply chain management using blockchain. All the items involved in the supply chain are tracked using RFID and other IoT devices and look at various case studies in which attacks related to blockchain are explored. All the above models discussed RFID and tracking management differently, but there is no clear competition towards our proposed model.

Many kinds of research are carried out for vehicles to the blockchain, but they discussed the improvement in vehicles only. The models also show the smart vehicles and smart roads, but they have not addressed the future regarding the whole system by considering any government or the entire country. Kazi et al. [13] discussed smart vehicles considering road accidents and used a vehicular ad-hoc network. Again Sharma

TABLE I
DRAWBACKS AND RESEARCH POSSIBILITIES OF EXISTING MODELS

Paper	Description	Limitations
Chen et.al [5]	IoT model Discusses various applications of IoT in blockchain such as asset tracking, security and payment	IoT devices are low-power operating machines. They need to be close to the blockchain network for fast computing and exchange of information. Throughput of such devices are to be improved.
Saurabh et al. [7]	RFID based tracking. Discusses asset tracking with RFID and blockchain to achieve transparency and data immutability	RFID tags can get damaged. Hence, the scanner or sensing device may not detect it. Applying RFID tracking with Proof of Work(PoW) algorithm can consume large amount of time and resources.
Feng et al. [8]	IoT tracking to improve food traceability. Discussed the relevance of food supply chain traceability. A blockchain based framework is proposed. Various challenges related to IoT and blockchain are discussed.	IoT has many legal and regulatory challenges. Blockchain and IoT do not have certain set of clear rules and standards for implementation in the country. IoT based applications also have stability and security issues.

et al. [14] explained heavy automatic vehicles and their management. Hasnain [15] discussed the road toll collection model in a decentralized manner. The smart road model for toll collection and vehicle communication was also discussed. It is a very costly model, and resource availability is challenging. It is impossible to smart road every area and more appropriate for urban areas. Our model is more suitable for every location and less costly using GPS devices. All the above models are discussed as proper solutions for their models. But no one has a precise matching with our model and techniques. Many schemes use blockchain and smart devices, but they are also more costly. The proposed method is innovative and unique to the best of our knowledge. There are no similar models available.

III. PROPOSED MODEL

Our proposed model is fully decentralized and automated for vehicle toll collection. It uses GPS for location tracking. The main issue that this project tries to solve is the removal of third parties for conducting transactions. The problem of having intermediaries and the cost and time associated with maintaining them is solved with the help of blockchain. It also aims to make the system more transparent and avoid data loss or modification. The vehicle's location makes transactions automatic if certain predefined conditions are met. These conditions can be previously agreed upon and stored in immutable smart contracts. It includes:

1) Type of payment
2) Location of the vehicle
3) Amount to be debited for payment

Vehicle owners and authorities agree upon predefined terms for the trip using a smart contract. The vehicle begins to trip after the contract is deployed on the blockchain. The vehicle's location authenticity is verified using the Location verification algorithm; When the vehicle arrives at the destination and updates the location to the blockchain. The nearest location verifiers have confirmed the location and updated it to the blockchain. Payment will complete after the correct location verification. The proposed model categorizes into four layers depending on the flow of work. Fig.4 shows the workflow of the proposed model. They are (i) Registration Layer, (ii) Data collection Layer, (iii) Data Updation Layer, and (iv) Blockchain Layer.

A. Registration Layer

The first layer is the registration layer, where vehicle owners and authorities register in the system. One owner registers for different vehicles. The vehicles work as a location verifier for other vehicles. Participants must have an ethereum blockchain wallet to participate in this model. The vehicle owner creates a smart contract in the blockchain before making the trip. During this phase, the vehicle owner agrees to various terms of the journey as given in the smart contract. The information is taken from the vehicle owner and stored in an immutable smart contract. After the details are collected, the highway authorities deploy the smart contract on the blockchain. The vehicle is ready to start a trip.

Algorithm 2 Contract between vehicle owner and authority and registration

Require: Input: $price$, $start$
if $vehicleMapping[address]$=1 **then**
    Multiple registration is not allowed
else
    $vehicleMapping[address].price\_per\_km.Penalty$ = $price$;
    $vehicleMapping[address].start$=$start$;
end if

Algorithm 2 shows the business logic to register a vehicle and contract between the authority and vehicle owner. Vehicle owners use the Ethereum account to set initial values of price to be charged per Kilometer and starting point of the journey. Therefore, the distance to a particular location is the destination value. It can be written in a smart contract and committed to the blockchain before the trip begins.

B. Data Collection

The data collection phase sends the vehicle's location and current timestamp to the network. GPS is used to identify the vehicle's position. The GPS technology is not faultless since the measurement approximates the intersection of signals coming from distant satellites. Many factors can cause deviation in the final value obtained. Changle et al. [16] proposed a Deep Neural Network-based GPS error detection and correction method. The method uses blockchain as well for storing and sharing positional errors. A smart contract is used for recording and sharing information. Our proposed

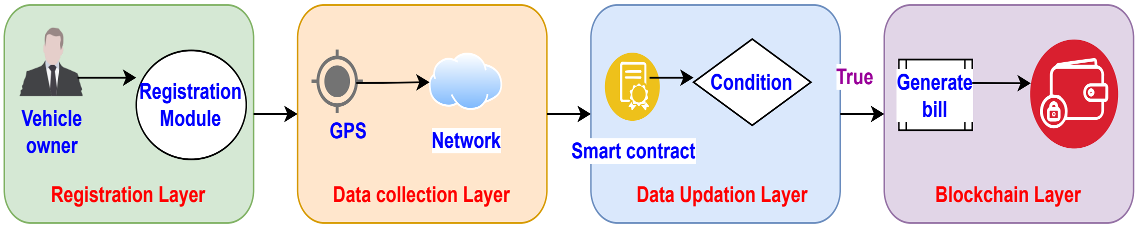

Fig. 4. Work Flow of proposed method

model uses public-private key authentication to ensure that location information comes from a trusted source. The data is signed with the vehicle owner's private key. Any person in the network verifies the vehicle owner's location public.

Algorithm 3 Location Contract

Require: Input: $address$,$locations$

$vehicleMapping[address].location[locations[0]]$=1;
$vehicleMapping[address].distances(locations[0])$;
$vehicleMapping[address].location[locations[1]]$=1;
$vehicleMapping[address].distances(locations[1])$;
$vehicleMapping[address].location[locations[2]]$=1;
$vehicleMapping[address].distances(locations[2])$;
$vehicleMapping[address].location[locations[3]]$=1;
$vehicleMapping[address].distances(locations[3])$;

Algorithm 3 shows the smart contract between the vehicle owner and the authority. A list of locations is agreed upon by both parties and added to a map corresponding to the owner's address. Distance from the start point to each location calculate. If the vehicle stops before the destination, the location is verified, and the contract executes also. In each case, the location verifiers confirm the location data.

C. Data Updation

The data from the previous phase gives the time and location of the vehicle. The data updation phase uses that information to verify whether the vehicle has reached a destination point or not. If not, the details are updated. Otherwise, a bill is generated using the distance and price per Kilometer values.

Algorithm 4 Update Vehicle details

Require: Input: $current\_location$, $current\_time$

if $current\_location$!=$destination(dest)$ **then**
  $statusMapping[address].location$=$current\_location$
  $statusMapping[address].time$=$current\_time$
else
  $distance$=$vehicleMapping[address].distance(dest)$
  Generate_bill($distance$)
  $statusMapping[address].location$=$current\_location$
  $statusMapping[address].time$=$current\_time$
end if
Update done successfully

Algorithm 4 is the method to update vehicle details. At regular intervals, the vehicle coordinates are received through GPS and checked with the previously agreed list of destinations. If the vehicle is not at any location in the list, the details are updated. Otherwise, the distance is retrieved from the smart contract method corresponding to the user address by giving the destination as an argument. After this, a bill is generated, and the details are updated.

D. Blockchain Layer

The data from the data updation phase send to the blockchain layer. The vehicle owner sends a Location verification request to the blockchain. The location verification request is visible publicly, and other vehicles verify the location using a location signature. The smart contract between the vehicle owner and authority is automatically executed. If the location demonstrates successfully, a bill will generate—payment transfers from the vehicle owner to authority. Algorithms 5 and 6 show the location signature generation and verification, respectively. The user uses a private key for the location signature generation, and the verifier verifies the location using the user's public key.

Algorithm 5 Location Signature

Require: Input: $location$

$signed\_data$=$vehicleMapping[address].privatekey$ ($location$)
return $signed\_data$

Algorithm 6 Location Signature Verification

Require: Input: $data\_1$,$data\_2$,$address\_1$,$address\_2$

$location\_1$=$vehicleMapping[address\_1].publickey($ $data\_1$)
$location\_2$=$vehicleMapping[address\_2].publickey($ $data\_2$)
if $location\_1$==$location\_2$ **then**
  Location of $address\_1$ verified successfully
end if

Algorithm 7 is the method to generate a bill by calculating the distance. When the vehicle reaches a location present in the smart contract, the vehicle owner is charged a certain amount. It is calculated by multiplying the price per Kilometer and distance from source to the location, retrieved from the smart contract. The malicious vehicle owners lose the total contract money and penalties as per the smart contract rule.

Algorithm 7 Generate bill

Require: Input: $distance$

1: $price$=$vehicleMapping[address].price\_per\_km*$ $distance$

2: $vehicleMapping[address].price$=$price$

3: Bill generated successfully

IV. Experiment Results

We analyze the resultant work and all the smart contracts. The experiments have been conducted on i3-10th gen 8GB RAM 3.2GHz. We use solidity programming language and truffle suite along with Ganache with Metamask. The contracts deploy on the ethereum framework, and all are working at their highest possibilities.

TABLE II
Gas consumption of each module use in this project

Modules	Gas Consumed	Cost in Ether
Registration	23236	0.000023236
DataCollection	103067	0.000103067
DataUpdate	95562	0.000095562
GenerateBill	33418	0.000033418

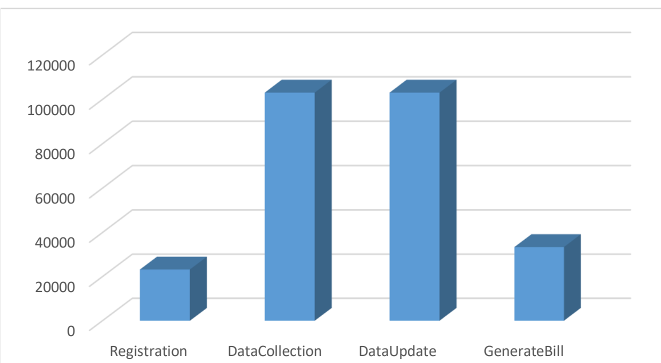

Fig. 5. Smart Contracts vs gas consume

Table II shows the gas consumption of the smart contracts along with the cost in ether. Fig.5 represents each module, and gas consumed is plotted. All detail of transactions is calculated and stored on the blockchain. The model is working fine, and To the best of our knowledge, It is the first blockchain-based, fully decentralized model in toll collection.

V. Conclusion

The proposed public blockchain-based model ensures that any person can be a part of the network and will be able to conduct automatic payment. This successful model depends on blockchain and GPS along with smart contracts. All smart contracts work better and provide fully secure transactions to focus users. The data generation model uses GPS that is publicly available and immutable. Blockchain stores all the generated data and performs location verification using other vehicle owners. This model also collects penalties from malicious participants to ensure security. The experimental results show less gas consumption for the smart contracts. In India, many states have many vehicles, increasing the chance of inefficient toll payment tracking and ambiguity in the process. This system will undoubtedly be a huge step in solving those problems.

References

[1] Zhang, R., Xue, R. and Liu, L., 2019. Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3), pp.1-34.

[2] Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R., 2020. A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), pp.147-156.

[3] Buterin, V., 2014. A next-generation smart contract and decentralized application platform. white paper, 3(37).

[4] Jabbar, R., Krichen, M., Shinoy, M., Kharbeche, M., Fetais, N. and Barkaoui, K., 2020, June. A Model-Based and Resource-Aware Testing Framework for Parking System Payment using Blockchain. In 2020 International Wireless Communications and Mobile Computing (IWCMC) (pp. 1252-1259). IEEE.

[5] Chen, F., Xiao, Z., Cui, L., Lin, Q., Li, J. and Yu, S., 2020. Blockchain for Internet of things applications: A review and open issues. Journal of Network and Computer Applications, 172, p.102839.

[6] Hasan, H.R. and Salah, K., 2018. Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access, 6, pp.65439-65448.

[7] Saurabh, S. and Dey, K., 2021. Blockchain technology adoption, architecture, and sustainable agri-food supply chains. Journal of Cleaner Production, 284, p.124731.

[8] Feng, H., Wang, X., Duan, Y., Zhang, J. and Zhang, X., 2020. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. Journal of cleaner production, 260, p.121031.

[9] Joshi, B., Bhagat, K., Desai, H., Patel, M. and Parmar, J.K., 2017. A comparative study of Toll Collection Systems in India. International Journal of Engineering Research And Development, 13(11).

[10] Sontakke, A., Diwakar, A. and Kaur, G., 2019. Intelligent Automatic Traffic Challan on Highways and Payment Through FASTag Card. Indian Journal of Science and Technology, 12, p.44.

[11] Satao, S., An Introduction to Fastag: Advantageous and automatic mode of toll collection system in India.

[12] Cheung, K.M. and Lee, C., 2017. A New Geometric Trilateration Scheme for GPS-Style Localization. Interplanetary Network Progress Report, 42, pp.1-9.

[13] Shakib, K.H., Neha, F.F. and Shazib, K.H., 2022. Smart vehicle accident detection for flash floods. In Autonomous and Connected Heavy Vehicle Technology (pp. 391-416). Academic Press.

[14] Sharma, G., Kumar, A. and Gill, S.S., 2022. Applications of blockchain in automated heavy vehicles: Yesterday, today, and tomorrow. In Autonomous and Connected Heavy Vehicle Technology (pp. 81-93). Academic Press.

[15] Tanveer, H. and Javaid, N., 2019. Using Ethereum Blockchain Technology for Road Toll Collection on Highways.

[16] Li, C., Fu, Y., Yu, F.R., Luan, T.H. and Zhang, Y., 2020. Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework. IEEE Transactions on Intelligent Transportation Systems, 22(2), pp.898-912.

[17] Helo, P. and Shamsuzzoha, A.H.M., 2020. Real-time supply chain—A blockchain architecture for project deliveries. Robotics and Computer-Integrated Manufacturing, 63, p.101909.