Mansoura Journal of Computers and Information Sciences

Traffic Violations Management System Using Blockchain Technology

Zahraa Tarek
Faculty of Computers and Information systems, C.S dep.
Mansoura University, Egypt
Zahraatarek@mans.edu.eg

Mohamed AL-Rahmawy
Faculty of Computers and Information systems, C.S dep.
Mansoura University, Egypt
mrahmawy@mans.edu.eg

A.S. Tolba
Faculty of Computers and Information systems, C.S dep.
Mansoura University, Egypt
ast@astolba.com

ABSTRACT

This paper presents the implementation of a traffic violation management system. A vehicle tracking system uses the GPS, GSM and a microcontroller to detect speed violations on roads. Any violation is sent to a central database.

Payments can be performed off-line; without involving a third party during payment, or on-line; contacting an intermediate server for each payment. In this paper, we focus on using on-line payment without third party by using a new technology called blockchain for the authentication and authorization purposes in case of traffic violations payment. The contribution of this paper is providing a model of electronic payment for traffic violations to enhance two important factors; trust and security of the e- payment system.

Blockchain as a shared ledger holds a many set of entities that faithfully records a series of transactions combined together by using a smart contract platform for embedding scripts that run across the network and enables adding new entries to that ledger. Blockchain technology is used in this paper for securing traffic violations management. Using the Blockchain guarantees highly secured traffic violations payment as no hacker can change the balance in driver's wallet or a vehicle property papers in a network around the world without the requirement for a central management, as all transactions are recorded in all copies distributed among all parties in the network, where each party has the same copy of the ledger. The proposed model should reduce the response times of violation requests and payment at any time and from any place.

Keywords

Internet of Things, Fog computing, Blockchain, Smart contract, Traffic violations.

1. INTRODUCTION

Traffic violations recording and processing is one of the traffic management issues that need to be managed in a quick and secure way. In this paper, traffic violations processing is done using a smart contract based on the Blockchain technology to ensure security, integrity and validity of vehicle information in order to increase the efficiency of violation processing by both the driver and the government with mitigation from fraud risks.

Because of the rapid technology advancement and the digital disruption, enterprises face critical business challenges including securing product data and supporting the move to connected smart products and service business models, so Blockchain and smart contract are proposed. Blockchain is distributed not centralized, inclusive not exclusive, open not hidden, immutable and secure. Blockchain gives us new capabilities to make value in society. Blockchain technology's core component is a protocol that enables data exchange among multiple parties inside a network without the need for third party, as network members act with encrypted identities and directly with each other using peer-to-peer communication. Each transaction in the network is added to an immutable transaction chain that is distributed to all network nodes [1].

A Blockchain can be described as a distributed transaction ledger that allow adding new information, while the previous information, kept in blocks, cannot be edited or modified. This is often accomplished by exploitation cryptography to link the contents of the recently added block with every block added before it, such that any modification to the contents of a current block in the Blockchain would affect the data in all blocks coming after that [2]. The Blockchain is used to record financial transactions and everything of value, so it is considered an incorruptible digital ledger of transactions [3].

Figure 1 is a detailed diagram that describes the Blockchain transactions. Blockchain wallet is a concept based on the Blockchain, where participants can deal with their balances by using Blockchain cryptocurrencies. Each user of a Blockchain wallet is provided with a Wallet ID when the wallet is created, this ID is a unique identifier similar to a bank account number. Wallet holders can access the electronic wallet whether by logging into the Blockchain website, or by downloading and accessing a mobile application related to it. The receive/send method is similar to receiving or sending funds through PayPal, however it uses cryptocurrency instead of real currencies [4].

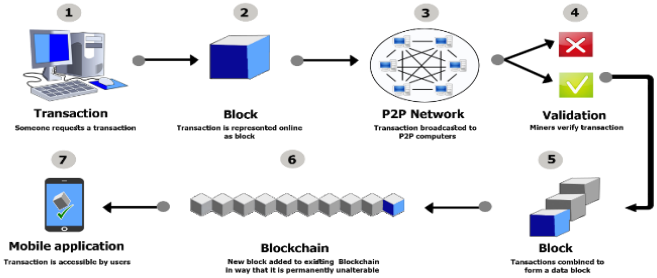


Fig 1: Blockchain Transactions

In this paper, traffic violations are recorded in an electronic way using the Blockchain ledger rather than using a notebook, where fog servers are distributed across roads with cameras attached to them to detect and record each violation. The violations may be: speed limit violation, accidents or lack in vehicle property papers. These violations are saved in decentralized network that enable all police men to see the violations of each driver to help them in payment of violation fees, or driver can pay for violation from any place at any time in his country as electronic payment using Blockchain.

The remainder of this paper is addressed as follows: Section II presents the related works of real time applications using Blockchain technology. Section III describes the process of speed violation detection. Section IV lists the techniques used for traffic violations payment system. In Section V, the framework of the proposed traffic violations model is provided. In Section VI, experiments and results are discussed. In the end, Section VII addressed the conclusions of our work and presented the future work.

2. RELATED WORKS

Yong and Wang conducted an early study of Blockchain based on Intelligent Transportation Systems (ITS). They discussed the Blockchain as one of the trusted and ensured architectures for building PTMS (parallel transportation management systems]; they conjointly bestowed a case study for real time ride-sharing services based on Blockchain [5].

Maher and Aad presented a use case of smart contracts based on Blockchain to enable nodes to share data through Internet to access or share completely different digital features without a trusty third party. Numerous corporations examine this use case. For instance, Slock.it is a German company that uses Ethereum on smart contracts for marketing, renting or sharing something like marketing a car without a reliable third party in this process[6].

Kristin Houser wrote about Porsche who researched many uses for Blockchain through the work with Berlin-based startup called XAIN: Blockchain is used to unlock vehicles of drivers. In addition, vehicle owners pay the electricity invoices using Blockchain to charge electric vehicles as a smart contract on the Blockchain took the suitable amount of cash money from your account and sent it to the charging station. It is noted that autonomous driving systems could be boosted using Blockchain and eco-friendly driving is encouraged [7].

Oberlandesgericht Stuttgart discussed that the use of video material from dashboard cameras is permissible as evidence to prosecute traffic violations after the ruling of a German appellate court to accept video evidence for prosecuting traffic violations. Given this development, it is more crucial than ever to have secure means for proving that the video footage has not been manipulated after the accident [8]. So B. Gipp and others presented an application that converts a video camera enabled smartphone into a cost-effective tamperproof dashboard camera (dash cam), the video file's hash is permanently secured in the tamperproof decentralized public ledger that is the Blockchain [9].

Ali Dorri proposed analysis study about decentralized Blockchain methodology that is used to form IoT system safer and privacy. The idea of Blockchain in smart houses for the primary time is conferred. The purpose to produce the Blockchain based mostly security so as to get rid of the unskillfulness of the present strategies. Simulation results showed that the overheads (in terms of processing time, traffic and energy consumption) produced by the projected approach are insignificant compared to its security and privacy requirements [10].

W. Egbertsen and others introduced recording the ownership rights of a music that is used as a potential use case in the Blockchain. The payment for music owners is enforced using the smart contract once a music is used for commercial or industrial purposes. It further ensures the distribution of payment between the music's owners. Ujo is a company that explores the use of Blockchain based on smart contracts within the music business [11].

Thabit and others introduced a model for reduction of traffic congestion using fog computing and its relevancy to each cloud computing and the internet of things (IoT). Obtaining, analyzing, and processing traffic information at traffic junctions are tasks assigned to fog nodes. The results show that additional reliable traffic is carried out when reducing congestion through symmetric traffic distribution by concerning average rate of traffic flow among the fog nodes [12].

Emily Su spoke about recording patient data on a distributed ledger using Blockchain technology that will enable completely different stakeholders conditional access to one source of truth. As every interaction with a patient's health information are often recorded on a ledger as a transaction seen by all in the network. This makes access to a patient's health data safer (patient information is encrypted). The smart metering of electricity generated from an individual's solar panels is enabled using Blockchain technology, these measures are recorded, listed and settled on a ledger and there are different cases in [13].

Nitin Narkhede discussed how traffic police could prevent many of 'unknown' violations if violation-reporting rights are provided to the public by adopting Blockchain. Based on mobile application, anyone can notify a proof of traffic violation and time of happening to Blockchain even in an absence of Traffic policeman [14].

One of the first flight delay insurances is given exploitation using smart contract. This insurance covers flight delays. The terms of the insurance are clear, and the compensation procedure is automatically. The client will select for what best fit with his needs. Flight and traffic databases that record flight's standing, are connected to the smart contract. The refund method in this procedure is triggered once the system notices a delay of 2 hours or more [15].

According to all these applications that illustrate the uses and importance of blockchain, so blockchain is used as a shared repository among different parties in the proposed platform and contains a permanent immutable log of events and processes for the future analysis and accountability. Also, Smart Contracts are used in the proposed platform to manage relationships among different parties of the platform.

3. SPEED VIOLATION DETECTION

In this paper, vehicle speed tracking system is benefit for the smart traffic management in providing the necessary data of vehicles for electronic violation payment. Since the proposed system can show the positions of vehicles in owners mobile phone, so that they can expect the future processes such as

violation payment in case of recording penalty. This tracking system can store the whole data where the vehicle had gone, what speed it runs, how much time it takes for them to come to a particular stop, and can create whole data analysis. This system is used to data capture, data storage, data analysis and finally data transfer.

The proposed system uses Arduino, GPS and GSM to track and provide speed information to user and to blockchain database. Vehicles speeds are updated minute by minute by GPS module. Microcontroller is the central processing unit CPU to measure vehicle speed. Arduino gets the coordinates from GPS modem and compute speed, then send Text SMS to the driver in case of violation recording. GSM modem is used to send this information via SMS to the owner of the vehicle.

Figure 2 illustrates HW-based violation detection using IOT devices; Satellite Global Position System (GPS), Global System for Mobile communication (GSM). The speed is calculated using ready library called TinyGPSPlus, The computed speed is compared with standard speeds saved in fog server. If the computed one is larger than standard speed, then this speed is traffic violation, else it is valid speed.

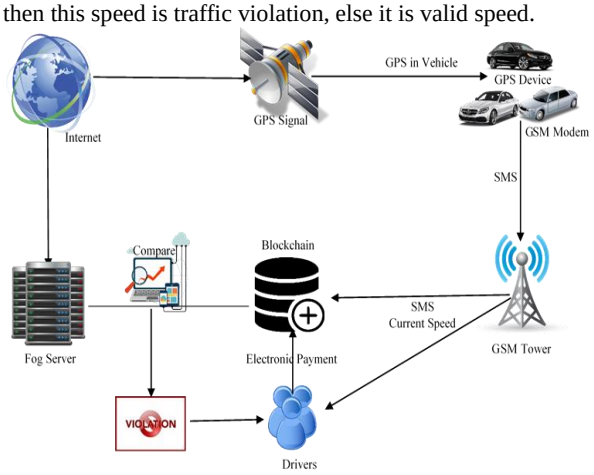


Fig 2: Violation Detection System Layout

Violation is recorded in blockchain decentralized database to be used after that in the proposed automated violations payment system in this paper, as each record in blockchain can record the whole history of each vehicle from speed capturing until violation payment. Also, stored Violations in blockchain are useful for further uses like vehicle licenses, property transfer and so on. Figure 3 describes the block diagram of the proposed module to measure speed using IOT devices.

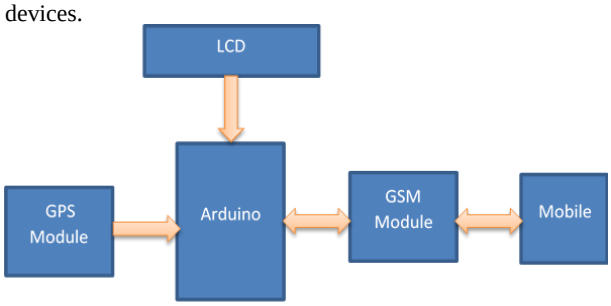


Fig 3: Block diagram of the proposed methodology

In the proposed system, Arduino is used for controlling whole the process with a GPS Receiver and GSM module. GPS Receiver is used for detecting speeds of the vehicle, GSM module is used for sending the speeds to user by SMS. And an optional 16x2 LCD is also used for displaying status messages or speeds. GPS consists of a network of 24 satellites located into orbit. Once the vehicle position has been determined, the GPS unit can determine other information like, speed, distance to destination, time and other. GPS module sends the data related to tracking position in real time, and it sends so many data in NMEA format. NMEA format consists of several sentences, in which we only need one sentence. This sentence starts from $GPGGA and contains the coordinates, time and other useful information as shown in Figure 4.

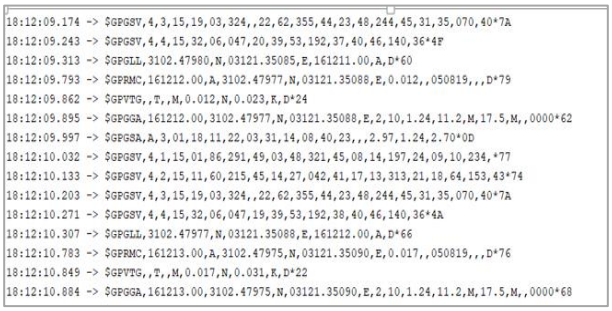


Fig 4: GPS satellites

Arduino reads speed messages and compare it with predefined speed message in Arduino. If any match occurs then Arduino reads speeds by extracting $GPGGA string from GPS module. This message contains the speeds of vehicle to driver mobile .The GSM modem is a specialized type of modem which accepts a SIM card operates on a subscribers mobile number over a network. Software Serial is a library of Arduino which enables serial data communication through other digital pins of Arduino. Figure 5 shows an example of SMS message using sim 900 of the GSM module.

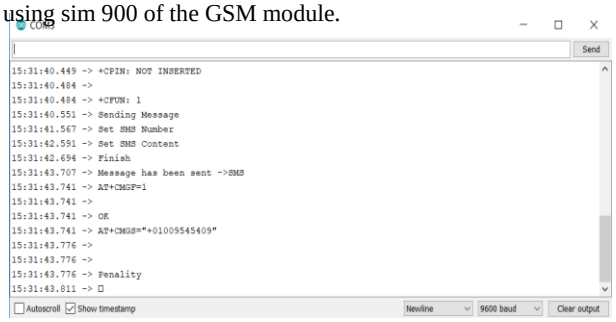


Fig 5: Sent message using GSM

The GPS, GSM, LCD and Arduino connections of proposed methodology to calculate speed in real time experiment for vehicle tracking system are shown in Figure 6.

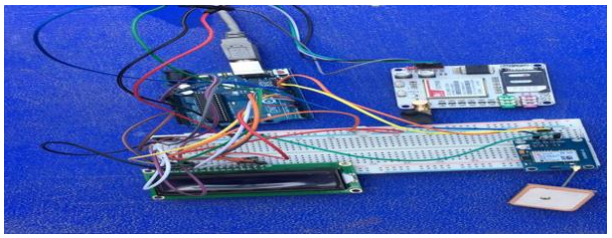


Fig 6: Proposed system

The proposed system shows the speed of vehicle on the LCD connected to it to make sure the working condition of the microcontroller. If the speed captured by GPS is larger than 50 then this speed is recorded as penalty speed on LCD screen, else it is valid speed as shown in Figure 7.

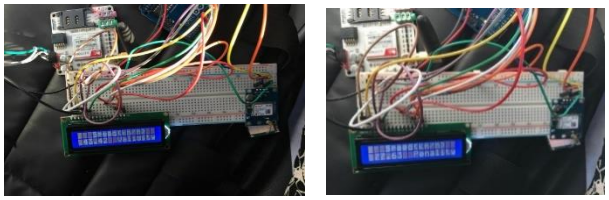


Fig 7: Speed measurements results

The history of vehicle is uploaded in website for applying in real time environment for traffic management. NodeMCU is ESP8266 based development board that is used to connect with GPS module and to send data to website. The proposed GPS Interfacing with NodeMCU is shown in Figure 8.

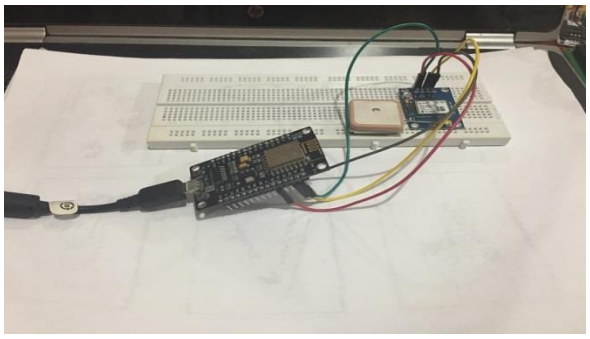


Fig 8: GPS with NodeMCU

Figure 9 shows the WiFi connections with server for saving the sensor data into database using TinyGPSPlus and ESP8266WiFi libraries as declared in Arduino code.

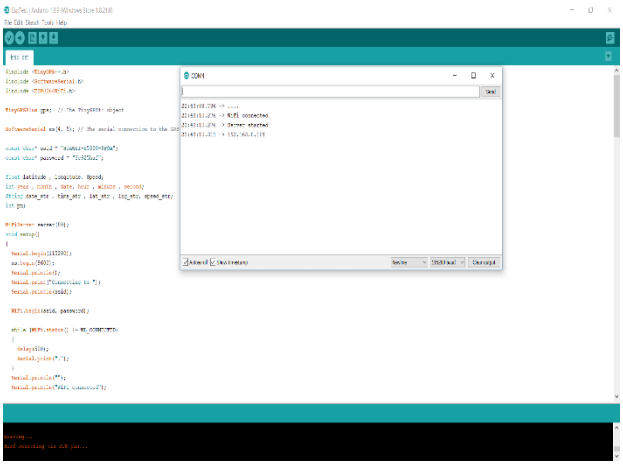


Fig 9: Sending data to server

The sensor readings is stored in the database, so that it can be accessed later. There are two types of data about vehicle that is needed to store; fixed data and varied data. Fixed data represents information about vehicle such as vehicle no, style, chassis no, capacity, color, license start, insurance company, manufacturing year, motor no, license end, document no, vehicle shape, model, owner's name, address. Varied data represents GPS readings such as latitude, longitude, date and time. All these data are uploaded to webserver for further process by traffic management department. Tables 1,2 lists the driver line of two trip; trip 1 from Mansoura to Mahalla with speed limit=60 and Trip2 from Kafr El-Sheikh to Mahalla with speed limit=90.

Figures 10, 11 shows the changes of speed along each trip. It is noted that speeds increase in high away roads where there is no monitoring of speeds. The proposed system can be used to track vehicles in high away roads as there are no cameras or traffic men, as violation is recorded in time of exceeds the

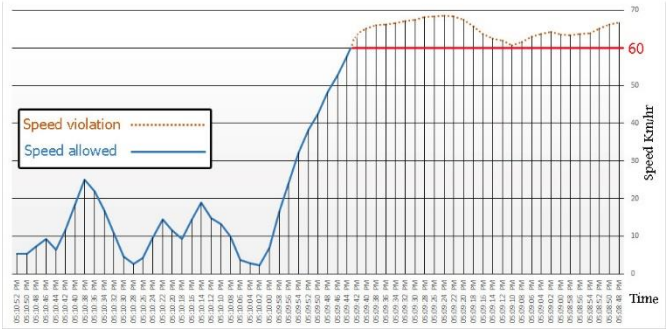


Fig 10: Speed violation and speed allowed of trip 1

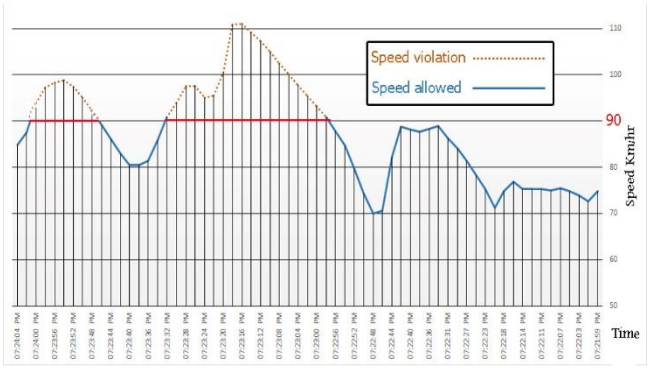


Fig 11: Speed violation and speed allowed of trip 2

The benefits of speed tracking system for traffic department and public security are:

- Reducing accidents when following speed limit
- Protecting vehicle from stealing as storing locations and times of vehicle movement
- Reducing cheating during selling in-use vehicles using full history of vehicle
- Showing the reckless behaviour of driving in inside and highways roads.

Vehicle speed tracking system both in case of personal as well as business purpose improves safety and security, communication medium, performance monitoring and increases productivity. The aim of the proposed methodology is generating the adequate data for arriving to right results for secure electronic violations payment system in next sections using blockchain technology in next sections.

The speed violations will be managed using Blockchain technology. The main objective of a Blockchain e-payment system is to use a decentralized network to enhance financial settlement and payments using the rapid, private, secure, and acceptable payment transactions. Therefore, Blockchain technology is needed for easier and faster payments.

Table 1. Trip1 from Mansoura to Mahalla (speed limit=60)

Latitude	Longitude	Speed in Km/hr	Time	Date	Speed Status
31.030801	31.315643	66.80	17:8:48	6/8/2019	Violation
31.030557	31.315378	66.14	17:8:50	6/8/2019	Violation
31.030317	31.315111	65.11	17:8:52	6/8/2019	Violation
31.030084	31.314849	63.89	17:8:54	6/8/2019	Violation
31.029848	31.314594	63.69	17:8:56	6/8/2019	Violation
31.029619	31.314332	63.43	17:8:58	6/8/2019	Violation
31.029388	31.314077	63.45	17:9:0	6/8/2019	Violation
31.029155	31.313819	64.19	17:9:2	6/8/2019	Violation
31.028923	31.313560	63.71	17:9:4	6/8/2019	Violation
31.028694	31.313302	62.90	17:9:6	6/8/2019	Violation
31.028469	31.313051	61.59	17:9:8	6/8/2019	Violation
31.028244	31.312807	60.69	17:9:10	6/8/2019	Violation
31.028017	31.312559	61.90	17:9:12	6/8/2019	Violation
31.027788	31.312307	62.36	17:9:14	6/8/2019	Violation
31.027555	31.312053	63.65	17:9:16	6/8/2019	Violation
31.027318	31.311790	65.71	17:9:18	6/8/2019	Violation
31.027076	31.311519	67.48	17:9:20	6/8/2019	Violation
31.026826	31.311243	68.38	17:9:22	6/8/2019	Violation
31.026575	31.310968	68.48	17:9:24	6/8/2019	Violation
31.026325	31.310689	68.37	17:9:26	6/8/2019	Violation
31.026079	31.310411	68.20	17:9:28	6/8/2019	Violation
31.025829	31.310140	67.52	17:9:30	6/8/2019	Violation
31.025583	31.309869	67.17	17:9:32	6/8/2019	Violation
31.025339	31.309598	66.60	17:9:34	6/8/2019	Violation
31.025096	31.309331	66.21	17:9:36	6/8/2019	Violation
31.024856	31.309061	66.03	17:9:38	6/8/2019	Violation
31.024621	31.308788	65.22	17:9:40	6/8/2019	Violation
31.024385	31.308528	63.74	17:9:42	6/8/2019	Violation
31.024166	31.308284	57.74	17:9:44	6/8/2019	Legal
31.023963	31.308071	52.75	17:9:46	6/8/2019	Legal
31.023780	31.307868	48.24	17:9:48	6/8/2019	Legal
31.023614	31.307689	42.48	17:9:50	6/8/2019	Legal
31.023468	31.307525	38.26	17:9:52	6/8/2019	Legal
31.023342	31.307382	32.22	17:9:54	6/8/2019	Legal
31.023242	31.307277	24.05	17:9:56	6/8/2019	Legal
31.023172	31.307197	16.68	17:9:58	6/8/2019	Legal
31.023130	31.307159	6.92	17:10:0	6/8/2019	Legal
31.023118	31.307142	2.28	17:10:2	6/8/2019	Legal
31.023113	31.307134	2.74	17:10:4	6/8/2019	Legal
31.023103	31.307123	3.81	17:10:6	6/8/2019	Legal
31.023075	31.307090	10.03	17:10:8	6/8/2019	Legal
31.023027	31.307041	13.18	17:10:10	6/8/2019	Legal
31.022977	31.306987	14.79	17:10:12	6/8/2019	Legal
31.022916	31.306915	19.02	17:10:14	6/8/2019	Legal
31.022855	31.306840	14.49	17:10:16	6/8/2019	Legal
31.022817	31.306795	9.30	17:10:18	6/8/2019	Legal
31.022779	31.306753	11.69	17:10:20	6/8/2019	Legal
31.022726	31.306699	14.38	17:10:22	6/8/2019	Legal
31.022680	31.306653	9.63	17:10:24	6/8/2019	Legal
31.022655	31.306631	4.25	17:10:26	6/8/2019	Legal
31.022647	31.306621	2.60	17:10:28	6/8/2019	Legal
31.022634	31.306600	4.57	17:10:30	6/8/2019	Legal
31.022607	31.306570	10.97	17:10:32	6/8/2019	Legal
31.022554	31.306512	16.76	17:10:34	6/8/2019	Legal
31.022476	31.306440	22.06	17:10:36	6/8/2019	Legal
31.022380	31.306352	24.95	17:10:38	6/8/2019	Legal
31.022302	31.306276	18.52	17:10:40	6/8/2019	Legal
31.022249	31.306215	11.64	17:10:42	6/8/2019	Legal
31.022218	31.306179	6.44	17:10:44	6/8/2019	Legal
31.022188	31.306140	9.22	17:10:46	6/8/2019	Legal
31.022155	31.306110	7.35	17:10:48	6/8/2019	Legal
31.022129	31.306087	5.25	17:10:50	6/8/2019	Legal
31.022109	31.306068	5.28	17:10:52	6/8/2019	Legal

Table 2. Trip2 from Kafr El-Sheikh to Mahalla (speed limit=90)

Latitude	longitude	Speed in Km/hr	Time	Date	Speed Status
31.022451	31.087524	74.79	19:21:59	11/8/2019	Legal
31.022148	31.087766	72.66	19:22:1	11/8/2019	Legal
31.021862	31.088039	73.94	19:22:3	11/8/2019	Legal
31.021593	31.088342	74.85	19:22:5	11/8/2019	Legal
31.021345	31.088672	75.44	19:22:7	11/8/2019	Legal
31.021120	31.089027	75.01	19:22:9	11/8/2019	Legal
31.020919	31.089399	75.29	19:22:11	11/8/2019	Legal
31.266666	0.716667	75.29	19:22:11	11/8/2019	Legal
31.020679	31.090002	75.36	19:22:14	11/8/2019	Legal
31.020549	31.090421	76.96	19:22:16	11/8/2019	Legal
31.020441	31.090848	74.79	19:22:18	11/8/2019	Legal
31.020364	31.091262	71.24	19:22:20	11/8/2019	Legal
31.020259	31.091899	75.34	19:22:23	11/8/2019	Legal
31.020181	31.092342	78.27	19:22:25	11/8/2019	Legal
31.020103	31.092802	81.38	19:22:27	11/8/2019	Legal
31.020021	31.093278	84.13	19:22:29	11/8/2019	Legal
31.019937	31.093770	86.34	19:22:31	11/8/2019	Legal
31.019809	31.094530	88.93	19:22:34	11/8/2019	Legal
31.019727	31.095041	88.38	19:22:36	11/8/2019	Legal
31.019647	31.095544	87.64	19:22:38	11/8/2019	Legal
31.019567	31.096050	88.18	19:22:40	11/8/2019	Legal
31.019485	31.096561	88.84	19:22:42	11/8/2019	Legal
31.019401	31.097051	82.19	19:22:44	11/8/2019	Legal
31.019330	31.097484	70.63	19:22:46	11/8/2019	Legal
31.019266	31.097883	69.95	19:22:48	11/8/2019	Legal
31.019193	31.098299	74.37	19:22:50	11/8/2019	Legal
31.019115	31.098745	79.91	19:22:52	11/8/2019	Legal
31.019031	31.099220	84.70	19:22:54	11/8/2019	Legal
31.018941	31.099716	87.81	19:22:56	11/8/2019	Legal
31.018848	31.100229	90.76	19:22:58	11/8/2019	Violation
31.018756	31.100759	93.20	19:23:0	11/8/2019	Violation
31.018665	31.101305	95.32	19:23:2	11/8/2019	Violation
31.018569	31.101861	97.71	19:23:4	11/8/2019	Violation
31.018472	31.102434	100.02	19:23:6	11/8/2019	Violation
31.018373	31.103019	102.43	19:23:8	11/8/2019	Violation
31.018270	31.103614	104.88	19:23:10	11/8/2019	Violation
31.018167	31.104225	107.22	19:23:12	11/8/2019	Violation
31.018060	31.104850	109.20	19:23:14	11/8/2019	Violation
31.017953	31.105485	111.08	19:23:16	11/8/2019	Violation
31.017845	31.106126	110.94	19:23:18	11/8/2019	Violation
31.017740	31.106727	100.48	19:23:20	11/8/2019	Violation
31.017644	31.107286	95.60	19:23:22	11/8/2019	Violation
31.017551	31.107831	95.05	19:23:24	11/8/2019	Violation
31.017457	31.108386	97.62	19:23:26	11/8/2019	Violation
31.017360	31.108951	97.59	19:23:28	11/8/2019	Violation
31.017269	31.109500	94.03	19:23:30	11/8/2019	Violation
31.017177	31.110031	90.85	19:23:32	11/8/2019	Violation
31.017093	31.110538	85.99	19:23:34	11/8/2019	Legal
31.017013	31.111015	81.38	19:23:36	11/8/2019	Legal
31.016935	31.111478	80.50	19:23:38	11/8/2019	Legal
31.016855	31.111940	80.43	19:23:40	11/8/2019	Legal
31.016778	31.112409	82.95	19:23:42	11/8/2019	Legal
31.016698	31.112899	86.17	19:23:44	11/8/2019	Legal
31.016616	31.113405	89.17	19:23:46	11/8/2019	Legal
31.016529	31.113929	92.26	19:23:48	11/8/2019	Violation
31.016443	31.114467	95.03	19:23:50	11/8/2019	Violation
31.016351	31.115022	97.46	19:23:52	11/8/2019	Violation
31.016256	31.115589	98.76	19:23:54	11/8/2019	Violation
31.016162	31.116155	98.32	19:23:56	11/8/2019	Violation
31.016069	31.116718	97.25	19:23:58	11/8/2019	Violation
31.015977	31.117267	94.00	19:24:0	11/8/2019	Violation
31.015890	31.117784	87.61	19:24:2	11/8/2019	Legal
31.015800	31.118276	84.86	19:24:4	11/8/2019	Legal

4. TECHNIQUES USED FOR TRAFFIC VIOLATIONS PAYMENT

The proposed model is depended on two techniques; these techniques are Blockchain and smart contract. This paper is depending on the data presented from manufacturer about basic details, and data collected by fog servers on different locations about traffic violations to be managed by smart contract on blockchain network for electronic violation payment.

4.1 Blockchain

DEFINITION. Blockchain technology is the backbone of the technologies proposed in this paper to enable secure and trusted sharing of traffic records across companies, governments, drivers and autonomous vehicles. Blockchain technology provides security of proposed system against hackers through its built-in encryption features, and simultaneously creates transparency of the data history about vehicles, owners and violations.

COMPOSITION. Sequence of blocks is the composition of blockchain structure; these blocks are linked together by their hash values. Hash of the previous block, set of transactions and proof-of-work are contents of the block. The random value found by the miners is behind the term 'proof-of-work' when hashing the block contents is compared with many such random values to achieve the cryptographic hash of block [16]. The blockchain composition is shown in Figure 12.

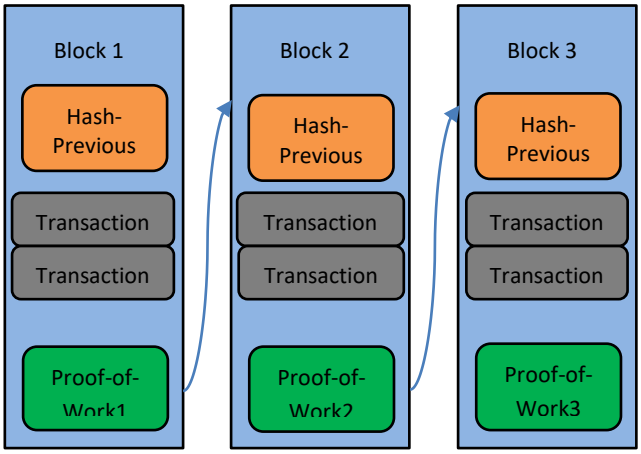


Fig 12: Blockchain composition

This structure is coded by java script in section 6 with simple example of violation payment between driver and traffic department without third party.

HASH FUNCTION. A hash function is one of the mathematical functions. It is used to convert input of letters and numbers into an encrypted output in a fixed length. Hash function has many types , the most common one is called SHA-256 which stands for Secure Hash Algorithm – 256 bit. This type is used in this paper. To replace the need for a trusted third party, a hashes of block in an interdependent sequence is the solution. Duplicate a hash is nearly impossible by using the SHA-256 function because there are too many combinations of
2^256 probabilities to try and process[17]. The details of hash function is described in [18].

TRADITIONAL WAYS. The process of vehicles and owners data registration has always been very tiring, time consuming since multiple parties are involved, and it causes a risk of data duplication and various errors of these data. In this case, important information can be without protection against frauds or even become non-traceable. In traditional system, some persons pay money to change vehicle property papers of other drivers or delete violations from system, so vehicle property papers and violations are stored in blockchain network and distributed to all members on the network. Blockchain in its role will decrease a risk of data duplication and various errors of these data like change or delete some documents of specific drivers.

BENEFITS. By using Blockchain, many of these issues can easily be solved by reducing the average response time. Blockchain will enable manufacturers, governments, drivers to push data within a smart contract that ultimately becomes a single source of fixed data not immutable to all parties. Using Blockchain in vehicle registration system will help also in reducing the danger of attacks and frauds, as data updates are only changeable by authorized personnel using a private key. In fact, any tampering of data can also be easily tracked on Blockchain. Not only this, Blockchain will provide an easy and single view of the vehicle history that is not available [19].

In this paper, Fog mining is introduced by using fog servers to confirm transactions related to violations of vehicles. violations are saved for long time in distributed ledger for further access in punishing violations offenders or for vehicle transfer, buying and selling. The goal of fog computing is to boost efficiency and cut back the quantity of data required for analysis, processing and storage that has to be transported to the Blockchain. A service provider deploys local data centers and servers at the edge of networks in different locations to store violations

These are many forms of violations such as clashes in traffic junctions, one-way driving, rush driving, drunken driving, hit & run cases, papers lack, pedestrian driving, speeding exceed etc. Some violations are handled by traffic officers and other violations by cameras and sensors. For example, sensors are used for speeding exceed violations. Traffic officers record papers lack violations and traffic junctions, one-way driving, rush driving, drunken driving, hit & run cases and speeding exceed violations. Cameras are used to verify violations handled by traffic officers except papers lack which listed only by officers.

4.2 Smart Contract

Smart contracts are agreements between participants without a third party. Each transaction about adding new information or executing specific functions are called contracts. These contracts contain agreed processes such as payment request as violation penalty, pay it and accept payment with reliable electronic invoice depending on available balance in driver's wallet. These processes are coded inside smart contract.

To activate this contract, vehicle owner should display his balance to check if it is enough for violations payment or not. Then this contract will distribute to all nodes on the Blockchain network and no one can Tamper with his balance, add or delete violation. This copy of contract contains address of vehicle owner, vehicle id and contract rules.

Miners are responsible for verifying vehicle life history for traffic violations. The miners are traffic department for irregularities, driver wallet for verification of the balance of vehicle owner, and customers and other owners on network.

Those miners can confirm each transaction and ensure each partner is responsible for his individual roles in the overall transaction of traffic violation for preventing disputes in the Blockchain network.

The smart contracts are saved on Blockchain as a contract address (ID) that is impossible to change by hackers across all people in network. The contracts are distributed to all nodes on the Blockchain network and no one can change or access balance of drivers as each driver has fake name and no one know his private information, each transaction is rejected o accepted according to the verification from miners on the network.

5. FRAMEWORK of the PROPOSED TRAFFIC VIOLATIONS MODEL

In this paper, Fog computing is used for saving database of speeds that are standard for all drivers to follow. There are many types to detect violation. Violations can be detected by cameras, or traffic men or using IOT devices. There are fog servers in different location; traffic signal, junctions, roundabouts, highways, and any other locations that vehicle may go. In the case of congested area with thousands of cars, cloud servers can be used rather than fog servers.

Cameras and sensors are IOT elements which check the vehicles speeds and violations are stored on the distributed blockchain. Sensors are used to register vehicles speed. And cameras are used for signs, accidents and speed violations. Traffic officer in streets is responsible for vehicle property papers violations. All data violations from sensors or cameras and officers are collected, classified as violations or not and then send to the blockchain network to prevent these data from duplication or various errors.

Blockchain is used to record the traffic violations, which are captured by cameras or officers and compared with standard speeds in by fog servers in different locations. Blockchain is considered the backbone technology used in the framework to enable secure and trusted sharing of traffic violations records between traffic departments, government and vehicle owners.

Smart contracts are used as the agreements between partners on the blockchin network. The smart contract is responsible for validation of transactions. Each transaction need to be verificied by the miners on Blockchain. In the proposed framework, the miners are traffic department to print violations list and driver wallet to check and accept the value of violation from its owners.

Transaction is represented as a payment record or a request about traffic violation. Blockchain and smart contract technologies are used for preventing disputes and making certain that individual roles of each partner is under control in the overall transaction in order to verify these transactions.

This combination of Blockchain and smart contract technologies permits secure and transparent tracking of traffic violations' transactions between drivers and government partners. This dramatically reduces delays, costs, and human errors in data registration.

In the proposed framework, the basic details like vehicle model, name, color are stored on a Blockchain by manufacturing companies. After that, the vehicle owners ask for their violations which are stored as transactions in the Blockchain embedded within the smart contract and needed to be verified by all miners on the Blockchain. The miners of the Blockchain embedded within the smart contract is responsible for confirming or rejecting the transactions of violation payment. The contract acknowledges that the traffic department has the right to withdraw the fine from the driver's wallet in the event of a violation of the allowed speed limits. What if there is no balance in drivers account? His driving licence could be withdrawn as a part of the smart contract.

Blockchain in the proposed framework contains information about all partners on the network including vehicles, owners and their wallets and any one on the network, in addition to records the information about each transaction between drivers and traffic department. The following steps are taken into consideration in the process of paying traffic violations in the proposed framework:

-A vehicle owner wants to request or pay his vehicle's violations as there is driver's wallet which deals with digital currencies only, and this is presented as a first transaction.

-The transaction is distributed online as a new 'block'.

-The block is broadcasted to every device in the network.

-The transaction is checked for validation from those miners in the network.

-The block is added to the Blockchain by creating a hash that depend on the information of the transaction, time block created and previous block hash.

-The violation certificate is modified after payment and broadcasting the new transaction.

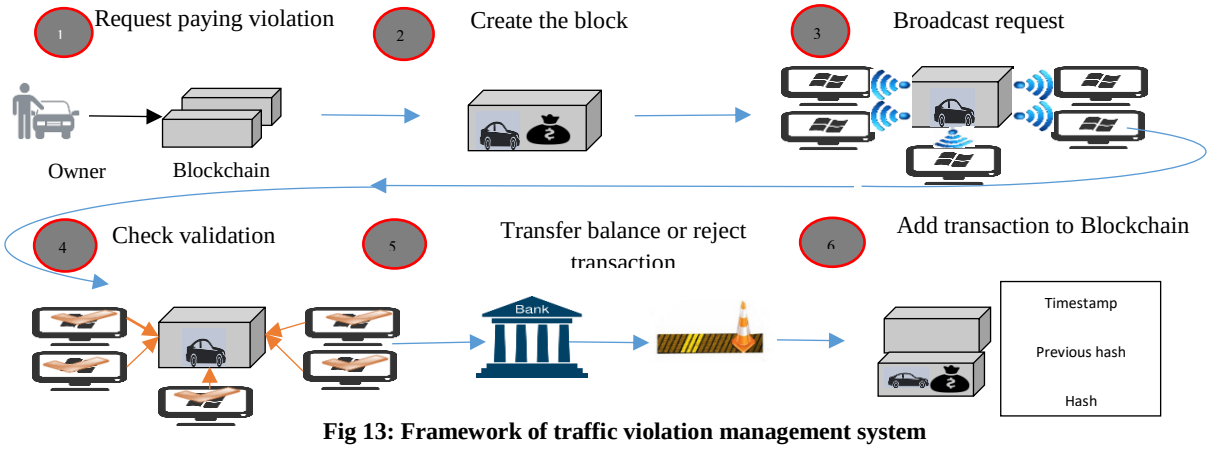


Fig 13: Framework of traffic violation management system

Figure 13 shows that there are a vehicle owner who ask the Blockchain system for violation payment. The owner starts to create a block with some information about the transaction, the time that block is created and the previous and current hash. Then, block is added to a Blockchain after check validation from all other devices in the same network and reply to the owner with the modified violation certificate by accepting payment or rejecting transactions. Each owner will have a wallet that contain real name and fake name that is appeared to the other people on the network. Owners store their information with fake name; vehicle information is stored by manufacturer in one ledger seen by all people accessing the system.

Each transaction on the Blockchain network pass by two steps: First, to be validated by other miners on the network and then accept or reject, then new records will be sorted with the accepted transactions. Therefore, we can say that there is amount of money that is deposited before the start of the sale process to ensure the credibility; vehicle owner who makes invalid transactions loses the money.

This paper depends on two transaction. The first one when owner request to know if he has violations on his car or not. The transaction are broadcasted to all devices on the network and the miners will check if vehicle's owner has violations or not by the help of full history provided by traffic department to blockchain network. These violations are collected by cameras and traffic men as mentioned in section 3. The receipt with violation whether there are violations or not is sent to the network and is available to all users. This transaction is saved on the Blockchain that could be used for the second transaction of violation payment. The second transaction is when owner send transaction that he want to pay his violation.

All persons on the Blockchain network around the world check the ledger if this owner has enough balance or not by the help of driver's wallet of his fake name, if he hasn't the enough balance then the transaction is rejected and this owner who make the false transaction will be penalized by paying fees to persons who access the transaction. If the owners has already the enough balance, people across network will confirm the transaction and accept payment from driver's wallet to traffic department. The owner balance will be reduced and the violation will be deleted. The violation certificate will be modified as a new transaction and this transaction is stored on Blockchain for further processes.

6. EXPERIMENTS AND RESULTS

In this section, the proposed violation payment system based on Blockchain has been validated using a simple simulation written by java script programming language using visual studio program.

In this simulation, the parameters used in the proposed violation payment system are four parameters. These parameters are address of traffic department, address of bank, balance of driver on traffic department, balance of driver on bank. Every system user has a wallet which contains the address and the balance of each driver. The two basic partners on the network are the driver's wallet and traffic department. Figure 14 is the result of our system that shows wallets of the system.

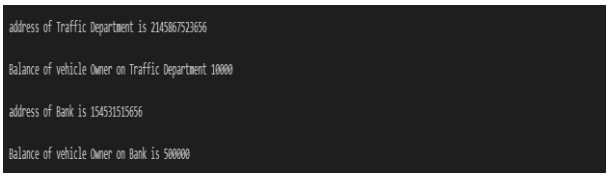


Fig 14: User wallets

Each vehicle owner has two accounts for their balance; one is driver's wallet and another is in traffic department.

If any documents from traffic department like violations on the vehicle and its related information like basic data stored by manufacturer or other documents are needed, the traffic department should transfer these documents by transaction from vehicle owner. The system checks the balance of the owners from his wallet and other miners on the network ensure if the owner has the enough balance in driver's wallet of paying the violations as specified by the traffic department, the transaction is accepted and Blockchain starts to create a new block and add it to the Blockchain to ensure security.Figure 15 shows block creation by a violation owner and accepting transaction.

Fig 15: Accepting transaction

When the transaction of ckecking balance is accepted, the system creates the block and hashes it by using the information of transaction and previous hash, then the traffic department starts to reply with the modified violation certificate by accepting value of violation and deleting violation. Figure 16 shows the traffic department's reply with violation value to be payed from bank to traffic department.

Fig 16: Transaction of violation value

When the balance of owners accounts on his wallet and traffic department is checked, the owners's balance on driver's wallet must be decreased with the balance in driver's wallet and the owners's balance on traffic department must be increased by the same amount. Figure 17 shows the users wallets.

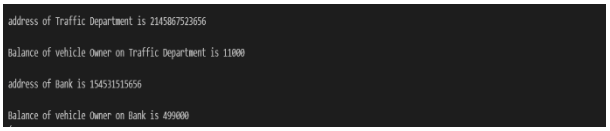


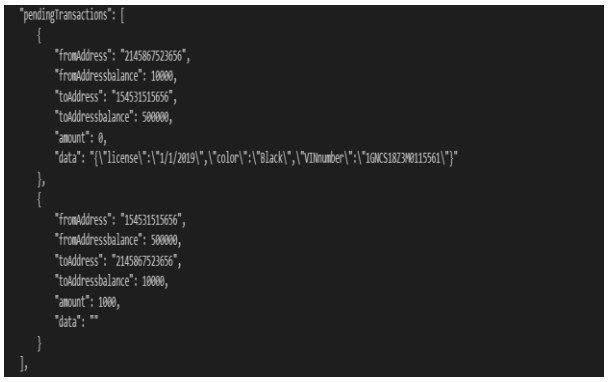
Fig 17: User wallets after applying transaction

Assuming that the amount of violation fees is 100 pound so the balance of owner's wallet on traffic department is increased by 100 pounds and becomes 11000 pounds because his wallet had 10000 pound before the transaction. And the balance of owner on his wallet become 49000 because it decreases by the amount of transaction. Figure 18 shows the status of the Blockchain.

```
"chain": [
    {
        "previousHash": "0",
        "timestamp": 1483228800000,
        "transactions": [],
        "hash": "ff2da8cbc6c99d6846c88baaece037f5c627405f1a577944b651a3a2b9863348",
        "nonce": 0
    },
    {
        "previousHash": "ff2da8cbc6c99d6846c88baaece037f5c627405f1a577944b651a3a2b9863348",
        "timestamp": 1542736881127,
        "transactions": [
            {
                "fromAddress": "2145867523656",
                "fromAddressbalance": 10000,
                "toAddress": "154531515656",
                "toAddressbalance": 500000,
                "amount": 0,
                "data": "{\"license\":\"1/1/2019\",\"color\":\"Black\",\"VINnumber\":\"1GNCS18Z3M0115561\"}"
            },
            {
                "fromAddress": "154531515656",
                "fromAddressbalance": 500000,
                "toAddress": "2145867523656",
                "toAddressbalance": 10000,
                "amount": 1000,
                "data": ""
            }
        ],
        "hash": "00ee40354e8775108c28760f934646d01366c0c141ab8ad3c63361d47c6284ec4",
        "nonce": 124
    }
],
```


Fig 18: Blockchain status

The first block is called genesis block and don't have any transaction but it is used to create the hash of the second block Every block has the transaction from driver's wallet to traffic department by the vehicle owners and from department to driver's wallet. If the driver's wallet hasn't the enough balance in his wallet, the transaction becomes a pending and block and hash aren't created. Figure 19 shows the pending transaction.



```
"pendingTransactions": [
    {
        "fromAddress": "2145867523656",
        "fromAddressbalance": 10000,
        "toAddress": "154531515656",
        "toAddressbalance": 500000,
        "amount": 0,
        "data": "{\"license\":\"1/1/2019\",\"color\":\"Black\",\"VINnumber\":\"1GNCS18Z3M0115561\"}"
    },
    {
        "fromAddress": "154531515656",
        "fromAddressbalance": 500000,
        "toAddress": "2145867523656",
        "toAddressbalance": 10000,
        "amount": 1000,
        "data": ""
    }
],
```


Fig 19: Pending transaction

The system checks the Blockchain after some time if any change is made to it. Transactions are usually settled in just a few seconds, leaving an immutable, transparent record for both bank and traffic department. In the proposed system, Blockchain create a new block as frequently as every 10 minutes. The 10 minute window is just an average which is taken to mine a block as the hashing algorithm used in the proposed system is SHA-256 like Bitcoin that takes10 minutes. Figure 20 shows the reply of the system if there is an error.

```
Changing a block...
Blockchain valid? false
```


Fig 20: Checking block information

The Blockchain is hard to hack because it is decentralized so the hacker must change all the ledgers to hack the Blockchain and for a large number of blocks that it's even harder to hack or change.

Also, the hash of the new block is produced with the transaction information and the hash starts with fixed number of zeros that is difficult to get any information, so the data is secured. Certain amount of transactions are reordered in one block and this block will be connected to next and previous blocks to prevent manipulation and falsification of records. Each transaction can be tracked through previous blocks stored and distributed in the network which ensure security.

Without full traffic history, drivers could waste money and time in searching and verifying violation like patients who waste time and money on tests they don't need or be unable to get the best treatment. The full traffic history for each driver is provided by blockchain and accessed by smart contract on blockchain technology for payment or just Inquiry.

Table 3 contains a comparison between some types of e-payments methods and features of blockchain technology for these methods as an evaluation of the proposed technology.

Table 3. Types of e-Payment methods and Blockchain features

Feature / E-payments	Definition	Distributed Ledger	Cost	Decentralized Network	Data theft & Corruption	Enhanced Security
Electronic checks	Institution settles transactions between the buyer's bank and the seller's bank in the form of electronic checks using digital signature.	Not Supported	Extra Fees for third party	Unavailable	High	Supported
Credit cards	Buying goods and services with a credit line and the amount will be settled at a later date.	Not Supported	Extra Fees for third party	Unavailable	High	Supported
Debit cards	The transaction amount is deducted directly from the cardholder's bank account upon authorization.	Not Supported	Extra Fees for third party	Unavailable	High	Supported
Pre-paid card	Customers use it for a specified amount by making an entry of the unique card number on merchant sites.	Not Supported	Extra Fees for third party	Unavailable	High	Supported
Electronic cash	transactions are settled via the exchange of electronic currency, need to purchase at points of sale (Bitcoin)	Supported	No third party	Available	Low	Supported

7. CONCLUSIONS

Our search can focus on the validation of factors that can contribute to the successful adoption of electronic payment methods around the world such as achieving trust and security of violations payment using blockchain technology. In this paper, we proposed a speed violation detection system using GPS, GSM, Arduino devices as speed is one of the violations that needs to be detected for electronic payment in Blockchain.

The proposed model aims to increase efficiency of electronic violation payment system using Blockchain technology with mitigation from fraud risk of traditional payment by hackers. The efficiency of the proposed automated violation payment depends on the time and cost that can be consumed by the drivers on the blockchain network as there is a few fees for miners to verify transactions rather than depending on third parties that consume more money in the traditional payment systems, as the transaction are distributed to all nodes on Blockchain network and any hacker should access all computers of all partners on the network. The presented technology guarantees the features of blockchain such as trust, security, distributed ledger, lower cost of the third party that are not found in the other methods.

Future Work

The proposed model can be used also for insurance companies in the case of accidents, also for transferring the fine to the judgement in case of refusal of violation payment. Driver behavior can be analyzed from the proposed vehicle tracking system of this paper.

The idea of registering traffic violation using consensus public people in the street at any time is proposed as a future work. As violation can be recorded using mobile applications, then the violation is verified by rapid response of police to the place of violation or by GPS satellite.

REFERENCES

[1] P.Wiedmann et al., "IoT powered by Blockchain," Deloitte, 2018, [Available: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/IoT-powered-by-Blockchain-Deloitte.pdf] [Accessed 1/3/2019, 11:20 PM].

[2] L. Fortney, "Blockchain Explained," Investopedia, 2019, [Available: https://www.investopedia.com/terms/b/Blockchain.asp#ixzz5DyJN7WHE] [Accessed : 11/4/2019, 1:00 AM].

[3] A. Rosic, "What is Blockchain Technology? A Step-by-Step Guide For Beginners," Blockgeeks, 2017, [Available: https://blockgeeks.com/guides/what-is-Blockchain-technology/] [Accessed : 24 /4/ 2019, 4:15].

[4] J. Frankenfield, "Blockchain Wallet," Investopedia, 2018, [Available: https://www.investopedia.com/terms/b/Blockchain-wallet.asp#ixzz5DyFWFDJs] [Accessed: 28 /3/ 2019, 10: 40 PM].

[5] Yong and Wang, "Towards Blockchain-based Intelligent Transportation Systems," IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Brazil, 2016.

[6] Maher and Aad, " Blockchain Based Smart Contracts : A Systematic Mapping Study," 3rd International Conference on Artificial Intelligence and Soft computing, Medina, KSA, 2017.

[7] Kristin Houser, "Blockchain is ready to transform personal transportation," Futurism, 2018, [Available: https://futurism.com/cars-Blockchain-six-ways/], [Accessed: 28/ 4/ 2019, 10:15 PM].

[8] Oberlandesgericht, "Recordings used basically to prosecute serious traffic offenses," Higher Regional Court, Stuttgart, 2016, [Available: www.olgstuttgart.de], [Accessed: 29 /11/ 2018, 1:00 AM].

[9] B. Gipp et al., "Securing Video Integrity Using Decentralized Trusted Timestamping on the Blockchain", in Proceedings of the 10th Mediterranean Conference on Information Systems (MCIS), Paphos, Zypern, 2016.

[10] Ali Dorri et al., "Blockchain for IoT security and privacy: The case study of a smart home," EEE International Conference on Pervasive Computing and Communications Workshops, Kona, HI, USA, 2017.

[11] G. Hardeman et al., "Replacing paper contracts with ethereum smart contracts," Semantic Scholar, 2016, [Available: https://www.semanticscholar.org/paper/Replacing-Paper-Contracts-With-Ethereum-Smart-Hardeman/24f74dd678bcac203d8bb0687f60e03e6222c455], [Accessed: 8 /12/ 2018, 11:10 PM].

[12] T. Sultan et al., "Fog Computing-Based Model for Mitigation of Traffic Congestion," International Journal of Simulation: Systems, Science & Technology, vol. 19, no. 3, 2018.

[13] Emily Su, "Top 5 most compelling use cases for Blockchain technology", Medium, [Available: https://medium.com/bitfwd/top-5-most-compelling-use-cases-for-Blockchain-technology-d198e500e3d3], [Accessed: 29 6/ 2018].

[14] N. Narkhede, " Blockchain: Control Un-Noticed Traffic Violations with Help of Blockchain," Mphasis, 2018, [Available: https://www.mphasis.com/home/thought-leadership/blog/blockchain-control-un-noticed-traffic-violations-with-help-of-blockchain.html], [Accessed: 19 /11/ 2018, 12:10 PM].

[15] V. Osetskyi, "What Is Smart Contracts Blockchain and Its Use Cases in Business," DZone, 2018, [Available: https://dzone.com/articles/what-is-smart-contracts-blockchain-and-its-use-cas-1], [Accessed: 23 /5 / 2018, 3:10 PM].

[16] D. Puthal et al., "The Blockchain as A Decentralized Security Framework," IEEE Consumer Electronics Magazine, vol. 7, no. 2, pp. 18-21, 2018.

[17] Emily Kotow, " What is Blockchain Hashing?," HEDGETRADE, 2019, [Available: https://hedgetrade.com/what-is-blockchain-hashing/], [Accessed 20/7/2019, 2:50 PM].

[18] C. Veness, "SHA-256 Cryptographic Hash Algorithm," Movable Type Scripts, 2019, [Available: https://www.movable-type.co.uk/scripts/sha256.html], [Accessed: 22/7/2019, 12:30 PM].

[19] A. Sidhu, "Blockchain Technology to Streamline the Vehicle Registration Process," TOTHENEW, 2018, [Available: http://www.tothenew.com/blog/Blockchain-technology-to-streamline-the-vehicle-registration-process/], [Accessed: 19 Nov 2018].