Blockchain Traffic Offence Demerit Points Smart Contracts: Proof of Work

Aditya Pradana, Goh Ong Sing, Yogan Jaya Kumar, and Ali A. Mohammed
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka
76100 Durian Tunggal, Melaka, Malaysia

***Abstract*—In Malaysia, a new regulation of traffic offences demerit points has been over a debate. Therefore, a blockchain model is formulated to solve this issue. It serves a purpose to be a Proof of Work (PoW) of a blockchain system. This model contains application layer and blockchain layer with smart contract inside. The smart contracts act as a conditional filter which follows the regulation rules. It contains three contracts starting from the declaration of each offence's demerit points and fines until the penalties when a certain amount of demerit points is collected, including revocation of driver license. The contracts will be automatically executed when such conditions are fulfilled. A transaction schema is also designed to match the schema of a traffic offence system. This model is deployed in online environment with two servers synced to each other to prove the decentralized characteristic of blockchain. It is developed using NodeJS while preserving JSON format for transaction between server and client. A user interface is also provided as a simulation media where a traffic officer can input offences and send it to blockchain server while public users or the driver itself can check the status of the driver license recorded on the blockchain. Government officer can monitor the records through a dashboard analytics provided which contains graphs and charts based on the records. This interface is used as media to do evaluation which produces satisfying results. The evaluation shows that the smart contracts are executed properly as compared to real regulations.**

***Keywords*—Blockchain; proof of work; smart contract; demerit points; decentralized system; distributed ledger**

I. Introduction

A revolution of peer-to-peer trust-free systems has been rising with blockchain technology on its core. This technology provides robust interactions among the peers which previously was maintained by third-party providers. It is able to replace the role of third-party providers by utilizing its smart contract which rules have been agreed by the involved parties. It opens up possibilities to be implemented in crucial party including government. Government policies which involve public as its object has been questioned with the existence of corruption by other parties. As new regulation is being implemented, it is better to see if blockchain technology can assist the regulation to be transparent and clear of any trust issues.

A case in Malaysia where a new regulation has been over debate by public is considered as an opportunity to test the capability of blockchain technology over the existing system. The regulation stated that road traffic offenders will be punished after a certain amount of demerit points reached. According to The Sun, driving licenses will be revoked when road traffic offenders reached 100 Kejara demerit points [1]. The details of each offences are shown in Table 1. A blockchain Proof-of-Work (PoW) is developed based on this regulation.

A blockchain or sometimes referred as trust-free technology [2] is a distributed ledger system with decentralized consensus mechanism. The ledger is cryptographically secured to avoid security issues on the records [3]. In technical perspective, it is also considered as a shared database to perform transactions among users without interference of an intermediary. The database contains transactional data stored in an encrypted infinite chain of blocks or ledgers. Each block contains the transaction along with timestamping algorithm to order it in time sequence [4]. The consensus mechanism requires a set of programmable rules dependent to the specific system to be developed. Nowadays, it is projected as the core of an alternative approach for trust-free systems. It has main characteristics such as distributed, immutable, trust-less, and decentralised. With its characteristics, it enables a verification of a record by public users without a need of intermediary institution [5]–[7]. These characteristics suit the main purpose of having an automated trust-less traffic offence system. Looking at its distributed characteristic, blockchain provides a wide variety of nodes or computers to be involved in a network in order to distribute the computing power. For example, Amazon AWS and Ethereum are two contrasting model. AWS is a private set of computing power bought and maintained by Amazon so only Amazon can contribute on the computers. Meanwhile, a blockchain organisation called Ethereum provides freedom by allowing anyone to install their software, so they can contribute to their network. Distribution helps to reduce risk of tampering, fraud and cybercrime [8]. Systems are more difficult to attack and taken down since more nodes are connected. Blockchain will provide transparency to the system since all parties involved have access to view the status of a driving license.

This research work is sponsored by UTeM Zamalah Scheme from Universiti Teknikal Malaysia Melaka.

TABLE II. KEJARA DEMERIT POINTS [1]

No.	Offence	Points	Fines
01	Driving under the influence of alcohol or drugs / Intoxication.	15 points	RM 300
02	Driving dangerous / reckless.	15 points	RM 300
03	Illegal racing on the road / Street Racing.	15 points	RM 300
04	Inconsiderate driving.	15 points	RM 300
05	Failure to provide breath, blood or urine sample when requested by a police officer, without a justifiable reason.	15 points	RM 300
06	Failed to follow traffic light.	10 points	RM 200
07a	Driving over the speed limit By 40 km/h	10 points	RM 200
07b	Driving over the speed limit By 26 km/h – 40 km/h	8 points	RM 150
07c	Driving over the speed limit By 1 km/h – 25 km/h	6 points	RM 100
08	Fail to give priority to ambulance, firefighter, police, custom, or Road Transaction Department car (with siren)	8 points	RM 150
09	Fail to stop at junction	8 points	RM 150
10	Offences related to overtaking and obstructing an overtaking vehicle.	8 points	RM 150
11	Offences committed at a pedestrian’s crossing.	8 points	RM 150
12	Offences related to driving left lane.	8 points	RM 150
13	Careless driving.	8 points	RM 150
14	Ignore traffic sign or regulation.	5 points	RM 80
15	Using exhausted tire.	5 points	RM 80
16	Operating a motor vehicle on a cordoned off roadway.	5 points	RM 80
17	Overtaking at a double line.	5 points	RM 80
18a	Failure to keep the probationary license on one’s person while operating a motor vehicle.	5 points	RM 80
18b	Failure to display identification at an easily-accessible place, according to the diagram in the sixth table of the rules.	10 points	RM 200
18c	Failure to keep the alcohol level in one’s breath, blood and urine at 0.00.	5 points	RM 80

In trust-less characteristic, parties who involved in blockchain are able to perform digital transactions even if the parties do not trust each other. For example in the current system, central authorities like banks act as ledgers without the involvement of other parties with a purpose of avoiding the problem of duplication. They are not able to record or duplicate any transactions since central authorities have full control of it. Different with blockchain, it distributes the ledgers to may nodes and synchronise the ledgers using consensus method. It allows involving parties who don’t trust each other can trust that the transaction is happening and valuable. It won’t stop only to this kind of trust since the processes are shared among the parties and the records of transactions are immutable. It opens a massive range of potential digital transactions and possibilities that couldn’t have happened with the current management style of central authorities. In a traffic offence system, government, police departments, and citizen might not have full trust in each other. It might even reduce a decision affected by political reason. Therefore, having blockchain is important.

Another important characteristic is its immutability. Removing or updating a transaction is impossible in blockchain because the transaction has been agreed upon and shared across the distributed network. Over time, when the transactions are increased, it becomes even harder to undo since the transactions are also shared across the network. Bitcoin as a public ledger provider allows everyone to explore the blockchain registered in Bitcoin and check the amount of Bitcoins in anyone’s account. It also allows tracking of any transactions happened, thus it can be used to track supply chains. In other scenarios such as in networking perspective, blockchain can be used to check which users accessed certain files on a network [9], [10]. In a traffic offence system, any police officer cannot undo the demerit points and fines being given to a driver thus it reduces the possibilities of having bribe.

The last characteristic which makes blockchain technology different from other system is the decentralised network. As mentioned before, transactions are distributed across network which forms in a decentralised network. Decentralised network helps to reduce monopolies or issues with intermediary thus removes unnecessary costs for centralised investment. It allows increasing the competition in the market by increasing pressure on involved parties to become more efficient in doing any transactions. In addition, involving parties allowed to transact without requirement for trust disrupts the current management styles of central authorities who facilitate trusts such as banks and lawyers. Transactions directly between peers can reduce the step of involving middle-men which further increasing market efficiency. With this characteristic, a traffic offence system requires less interference of other parties which are not involved directly with the system or act as intermediary.

A blockchain needs another layer to make a use case works properly. With smart contract in this layer, a blockchain can have the rules based on regulation so that the transaction stored follows the regulation. Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a pre-configured condition in a smart contract among involving parties is met then the parties involved in a contractual agreement can be automatically made transactions as per the contract in a transparent manner [11]. Smart contract makes the involvement of intermediary institution possible to be reduced. In 2015 Visa and DocuSign demonstrated smart contracts for leasing cars without the need to fill in forms. Smart contract in this PoW is applied based on the regulations where each offence has its own demerit points and fines, a driving license will get penalty after reaching 100 demerit points, and the penalties given are based on number of suspensions occurred. All of the contracts are automatically applied when police officer input an offence. It can detect the current state of a driving license and compare to the conditions of the contracts.

II. Blockchain Application Review

There is a number of blockchain system developed in the recent years. The first concept of blockchain system that was put in operation is the cryptocurrency [5]. Bitcoin is designed as an alternative way to perform independent transaction which traditionally involved governments, central authorities and banks. It is performed in form of electronic and peer-to-peer cash system.

Bitcoin was introduced in 2008. Since then, blockchain has started to have a new role from a mechanism to verify cryptocurrency to a broader field of commercial and economic applications. It has disruptive impact that is not limited to a specific industry [12] but rather enables the creation of a distributed, tamper-free, and transparent record of almost anything [13]. These factors are caused by its potential in reducing intermediary.

Another application related to Bitcoin is developed based on Bitcoin scripting language. It presented a reasonable protocol for transactional data where the commercial deal, the way data is delivered, and payment is performed, is essential. It is developed in such a way that if the buyer hasn't received the data then the seller is not able to redeem the payment and the buyer cannot receive the data if payment hasn't been made [14]. Another application which is inspired by Bitcoin is Cecoin. It follows the characteristics of Bitcoin such as immutable and public verifiable. Unlike Bitcoin, it utilised certificates to be treated as currencies and recorded on blockchain. The users can have access to a verification system. It verifies the validity of certificates based on smart contracts to ensure ownership consistency. It allows user to have multiple public-key certificates. Cecoin incorporates a modified algorithm based on Merkle Patricia tree which in later stage implemented as a distributed Certificate Library. It enables efficient retrieval and verification of certificates, and quick operations [15].

The application of blockchain is not always related to financial services but also Internet of Things (IoT). Hybrid-IoT is an application designed with a hybrid blockchain architecture for IoT. Then, the connection among the Proof of Work (PoW) sub-blockchains employs a BFT inter-connector framework, such as Polkadot or Cosmos. The PoW sub-blockchains formation, guided by a set of guidelines based on a set of dimensions, metrics and bounds [16]. Different application in IoT implemented and experimented a combination of bigdata and IoT technology to preserve renewable energy. Projects which are related to renewable energy are always get attention due to current environmental issues such as global warming. It introduces and implementation of blockchain technology for energy prosumer service model. This allows various energy sources to be connected to various users and producers. It also improves energy efficiency by analysing energy pattern of users. A transaction model that can collect, utilize, and process data more efficiently by combining the above technologies has also been presented [17].

In other domain such as industrial field, an application of blockchain technology related to the 4th Industrial Revolution (Industry 4.0) is presented with an example where blockchain is employed to facilitate machine-to-machine (M2M) interactions and launch a M2M electricity market in the context of the chemical industry. It involves one electricity consumer and two electricity producers performing transaction with each other in a blockchain environment. The research found out that this technology has significant under-researched potential to support and enhance the efficiency gains of the revolution and identifies areas for future research [18].

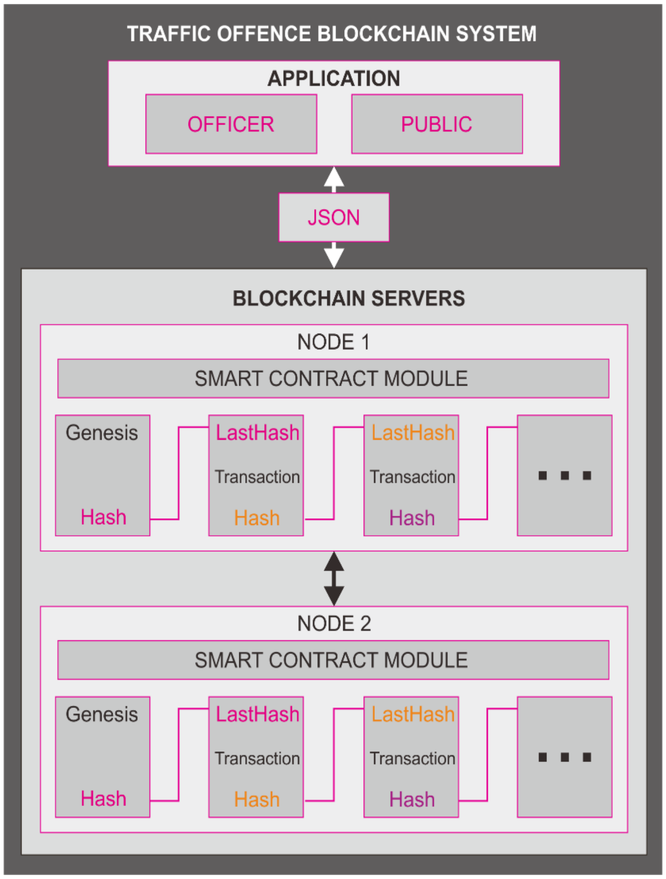


Fig. 1. Traffic Offence Blockchain Model.

Based on the reviews, it can be concluded that most of the blockchain implementations are related to financial and IoT. Although blockchain application is starting to be implemented in various fields [19], it hasn't reach governmental regulation field such as traffic offence system.

III. Traffic Offence Blockchain Model

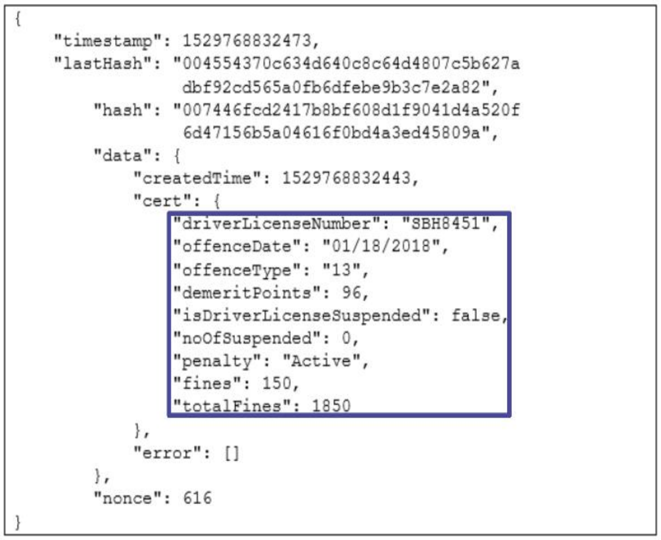
A model of traffic offence blockchain system is designed based on the requirements. As shown in Fig. 1, there are two main parts interact with each other by sending JSON objects namely Application layer and Blockchain Servers layer.

A. *Application Layer*

The first part is Application layer which acts as front-end interface to users such as police officer interface and public user interface. Both interfaces are connected to each other in which public users can retrieve the information or block that police officer has sent to blockchain servers.

B. *Blockchain Servers Layer*

For this PoW, two servers acting as nodes have been set up with Node 1 acts as the main server without removing the possibility to use Node 2 as the main server. Each node has the same layers inside with smart contract module as the first layer processing the transaction. It has been configured to match the regulations so that the transaction received is processed according to the configured conditions and allow the transaction proceeds to the blockchain layer. As its name suggests, it contains a chain of blocks which started with genesis block and followed by the transactions. A genesis block is a starting point of a blockchain which contains empty transaction and a pre-defined hash as agreed by involved parties. The hash will be used in the next block along with the transaction of the current block to create a hash of the current block. This hash will be used in the next block and the process repeated each time a transaction is received. In simple way, the hash of last block will link to the next block to make a chain. In each block contains transaction that has been processed by smart contract module. It contains its created time and a schema based on the input from police officer.



```
{
    "timestamp": 1529768832473,
    "lastHash": "004554370c634d640c8c64d4807c5b627a
                 dbf92cd565a0fb6dfebe9b3c7e2a82",
        "hash": "007446fcd2417b8bf608d1f9041d4a520f
                 6d47156b5a04616f0bd4a3ed45809a",
        "data": {
            "createdTime": 1529768832443,
            "cert": {
                "driverLicenseNumber": "SBH8451",
                "offenceDate": "01/18/2018",
                "offenceType": "13",
                "demeritPoints": 96,
                "isDriverLicenseSuspended": false,
                "noOfSuspended": 0,
                "penalty": "Active",
                "fines": 150,
                "totalFines": 1850
            },
            "error": []
        },
        "nonce": 616
}
```

Fig. 2. Transaction Schema in a Block.

C. *Transaction Schema*

A schema will be recorded in each block sent to a blockchain. The schema contains the details of a traffic offence. It will be based on inputs from traffic officer or any party who is involved in this system. The schema is designed based on requirement of a traffic offence system with added details to support smart contract implementation. An example of a block with the schema is shown in Fig. 2.

Transaction schema of the block is designed to match the real regulation rules which later will be used as input for smart contract. The details of the schema are as follows:

- Driver License Number: It shows the driver license number. It will act as identifier where the demerit points and other contract refer to.
- Date of Offence: It shows the occurrence date of the offence. It is stored in MM/DD/YYYY format.
- Offence Type: It contains selected offence type from 22 types as listed in Table 1.
- Demerit Points: It contains the sum of demerit points collected on each offence in a driving license.
- Fines: It contains total fines based on demerit points collected.
- Penalty: It shows the penalty given to the driver which refers to the third smart contract.
- Driver License Status: It may contain Active, Suspended or Revoked.

D. *Smart Contract Model*

Based on Malaysia regulation stated under Sections 35, 35A, 37 and 38, the 1987 Road Transportation Act and the Motor Vehicles (Demerit Points) Rules 1997, Demerit point is basically a way to reduce traffic offences and thus reduce road accidents. A smart contract model is developed based on the regulation. There are three contracts applied as Proof of Work such as:

- First contract: each traffic offence has its demerit points referring to the regulation and fines will be applied based on the demerit points as follows as shown in Table 1.
- Second contract: based on the accumulated demerit points, if a driver has exceeded 100 points, the driver license will be suspended and follows the penalty of the third contract.
- Third contract: Once a driver's demerit points racked up to 100 points or above, the first driving license suspension will be given. The first suspension is no longer than 6 months. If after the suspension, a driver makes another offence regardless of the demerit points, it will get a penalty of driving license suspension for no longer than 12 months. If another offence is made within 5 years after the second suspension, then the driving license will be revoked.

E. Decentralised Network Model

Node 1 and Node 2 are connected in such a way that transactions between them are synchronised. It serves a purpose to enhance the security where attackers who attack one of the servers and somehow modified the block will be detected by consensus system that compares the blockchain with another server. If the blockchain hash is not identical to other servers then the modified block will be replaced by the original one. Furthermore, it will act as a backup module for the blockchain since the blockchain is not stored in a database. In case of one of the servers is down then the other server still keep the blockchain. Due to the blockchain is only stored in the memory, it will be erased when the server is down and when it is back online, the blockchain is empty and start from genesis block again. Therefore, decentralised module is needed since it will automatically synchronise the blockchain to the empty server.

IV. Development

A blockchain application is developed based on the model explained before. The development is started by setting up two servers to fulfil blockchain concept of decentralisation. Each server acts as a node of blockchain decentralised network. Node 1 is Ubuntu 16.4 server located in US and Node 2 is CentOS 5.4 server located in Netherland. Both servers have been installed Node JS framework to run Javascript scripts on server side. The function of sending (POST) and retrieving data (GET) is handled by Express JS as Web API.

The application has three main parts, such as block generator, schema, and blockchain generator. In schema part, each of schema detail is declared based on the input. The data type of each of the inputs is validated before sent to block generator to ensure no data type error. Block generator has a function to generate a block or ledger based on the schema. It generates a block which contains block number, timestamp, hash from last block, hash of current block, the schema itself, and a nonce. A timestamp is attached to each block in order to keep track when the block is being generated. Before generating any block from a schema, block generator will create an empty block called as genesis block. As stated in the previous section, genesis block is needed to start a blockchain thus the first block generated will hash it as part of Hash from Last Block. The hashing method is using SHA-256 since it is a one-way encryption thus difficult to decrypt. As for Current Hash, it uses Last Hash, current schema, and timestamp to generate a hash. Since Current Hash is based on Last Hash, it makes blockchain immutable to any changes. A change to a specific block will need hash from previous block and repeated until the genesis block which is almost impossible to achieve. Nonce is a number showing the occurrence number of mining process to reach a matching hash. Every time a block is retrieved, it will be added to blockchain with additional condition from smart contract module.

All of three main parts are executed in a main file which requires parameters such as Peers' IP Address, HTTP Port, and Web Socket. It is required to connect among nodes so that each record can be updated on each node. In this development, each server has been set up with one HTTP Port and one Web Socket. After the connection is established, any application can point to either nodes to send a block and both nodes will be updated accordingly.

A. Smart Contract Implementation

The first contract filters the condition of each offence to define its demerit points and fines. According to Table 1, a condition can be written as shown in pseudocode below.

```
Contract 1
IF offenceType = 01 || 02 || 03 || 04 || 05
   THEN demeritPoints = 15, fines = 300
IF offenceType = 06 || 07a || 18b
   THEN demeritPoints = 10, fines = 200
IF offenceType = 07b || 08 || 09 || 10 || 11 || 12 || 13
   THEN demeritPoints = 8, fines = 150
IF offenceType = 07c
   THEN demeritPoints = 6, fines = 100
ELSE
   THEN demeritPoints = 5, fines = 80
```

The second contract is based on the first contract's demerit points. It will be executed if the total of demerit points reached 100. It will assign the variable of isDriverLicenseSuspended to be true and occurrence of suspension increased by 1 occurrence.

```
Contract 2
IF totalPoints >= 100
   THEN isDriverLicenseSuspended = true
   THEN noOfSuspended = +1
```

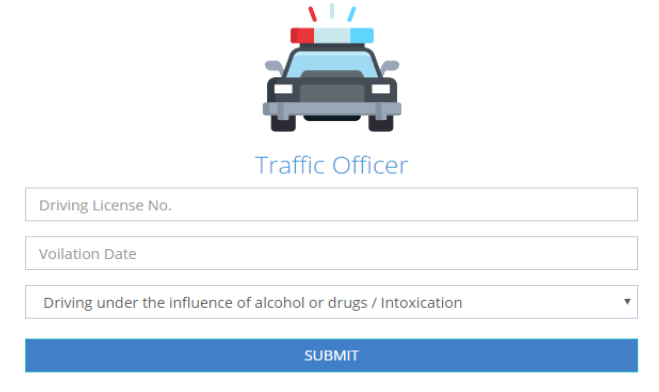
The third contract executed when second contract is fulfilled. Based on the number of suspensions, it will assign penalty to the driving license. When it reached 3 occurrences, the driving license will be revoked.

```
Contract 3
IF noOfSuspended = 1
   THEN penalty = Suspended for 6 months
IF noOfSuspended = 2
   THEN penalty = Suspended for 12 months
IF noOfSuspended = 3
   THEN penalty = Suspended for 6 months and License to be revoked
IF noOfSuspended > 3
   THEN penalty = Driver License revoked
```

B. Supporting User Interface

As shown in Fig. 1, the application layer contains an interface for police officer and public user. The interface is developed to show the input and output of the blockchain in readable form. The flow of registering a block is started by submitting offence details from Traffic Officer UI which contains Driver License Number, Offence Date, and Offence Type as shown in Fig. 3. As described in Fig. 1, the application layer sends data in JSON format to the server and retrieve the result in the same format.

The details will be processed in smart contract module to see if any conditions are met and then hashed and stored in blockchain. If the process is successful, the transaction will appear in the interface. Once an offence is registered as a block in blockchain, anyone can access it via Public interface as shown in Fig. 4. User can input the driving license number and check the status of it. An analytic dashboard is also provided to assist government to analyse the policies.



Traffic Officer

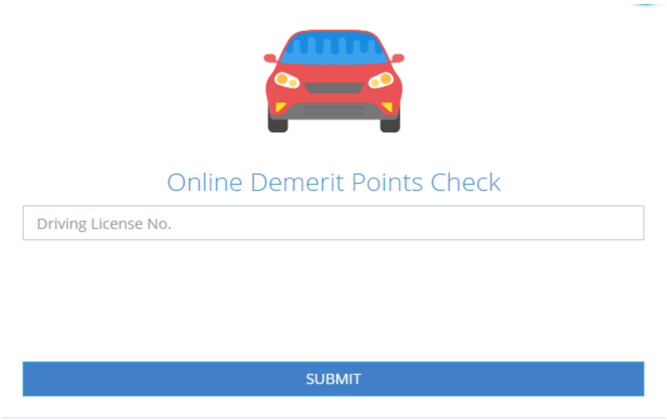
Driving License No.

Voilation Date

Driving under the influence of alcohol or drugs / Intoxication ▾

SUBMIT

Fig. 3. Traffic Officer User Interface.



Online Demerit Points Check

Driving License No.

SUBMIT

Fig. 4. Public User Interface.

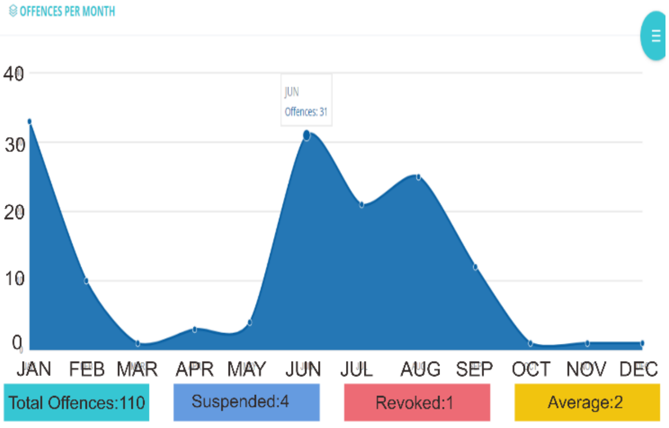


Fig. 5. Traffic Offences in a Year.

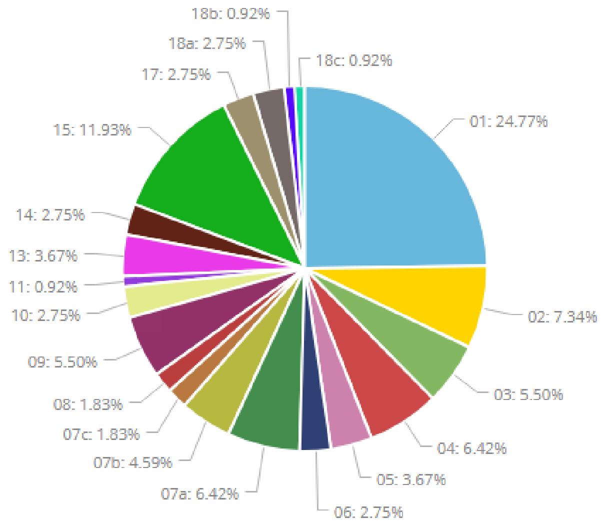


Fig. 6. Types of Offences Chart.

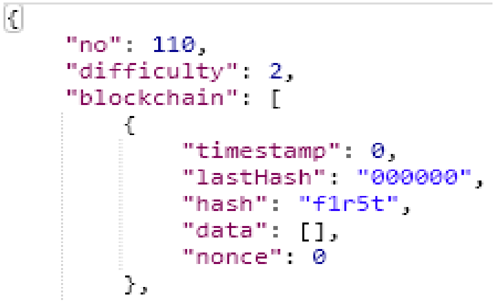
V. Evaluation

An evaluation is conducted using black-box approach to test the functionality of the system. This test has a purpose to check the rigidness of the smart contracts in filtering various conditions in transactions and to verify the creation of blocks in the blockchain. A set of instructions are given to a group of participants to ensure the variety of circumstances occurred on the blockchain.

A total of 110 blocks were received during the test. All of the blocks are properly recorded on the blockchain system proven by the charts shown in Fig. 5 and Fig. 6.

In Fig. 5, the chart provides offences on each month and few other statistics such as total offences, total license suspended, total license revoked, and average offences per month. The values are achieved from the test. It shows that the schema is stored properly as a block in blockchain and confirms the smart contracts are implemented properly with a total of 110 Offences, 4 License Suspended and 1 License Revoked. This test has shown that all smart contracts are executed. The chart shows total offences in January is 11, February is 14, March is 7, April is 4, May is 12, June is 11, July is 13, August is 6, September is 30, October is 1, November is 0, and December is 0. It can be concluded that there is a tendency of the users to pick the date close to the date when the test was conducted which is September.

The pie chart shown in Fig. 6 is provided to keep track on which offences have mostly occurred. It simply derives the Offence Type in the schema and sums it up. Similar to Fig. 5, the values are taken from the participants during test. It shows that most of the offences are Offence 01 which is "Driving under influence of alcohol / drugs" with 24.77%, Offence 15 which is "Using exhausted tire" with 11.93%, and Offence 02 which is "Driving dangerous/reckless" with 7.34%. Such statistics could assist the government to review the current policy and consider the next regulations to be composed.

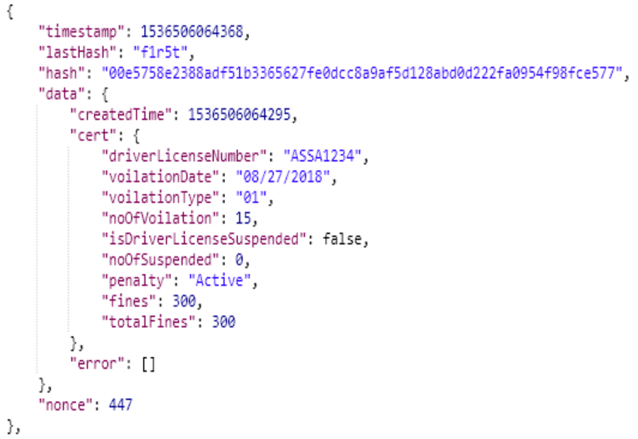


```
{
    "no": 110,
    "difficulty": 2,
    "blockchain": [
        {
            "timestamp": 0,
            "lastHash": "000000",
            "hash": "f1r5t",
            "data": [],
            "nonce": 0
        },
```

Fig. 7. JSON Output of Total Block on Both Servers.

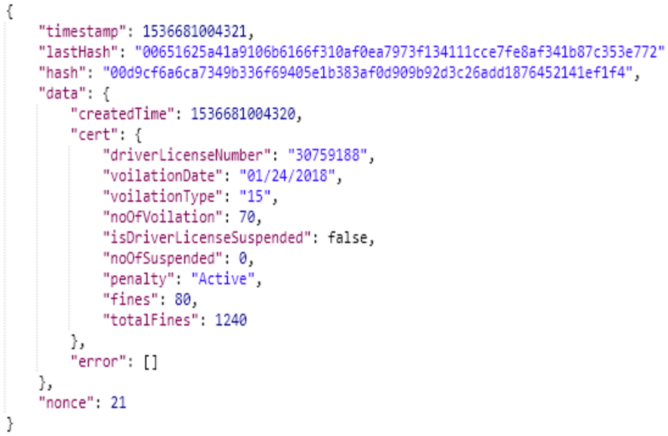
An evaluation is also conducted to check the decentralized model between Node 1 and Node 2. It checks the total blocks in the blockchain in each server as well as the first block after the genesis block and the last block in each server. It is to ensure the blockchain is synchronized between the servers.

Fig. 7 shows the total blocks in the blockchain i.e. 110 blocks. It is shown in JSON format as discussed in earlier section. It is retrieved from Postman application by sending GET request to Node 1 address which is https://myblockchain.asia:3001/blocks. The same output is retrieved from Node 2 address which is https://myblockchain.name:3001/blocks. It proves that all blocks are properly stored with the same number of blocks and thus the decentralized model is working well.



```
{
    "timestamp": 1536506064368,
    "lastHash": "f1r5t",
    "hash": "00e5758e2388adf51b3365627fe0dcc8a9af5d128abd0d222fa0954f98fce577",
    "data": {
        "createdTime": 1536506064295,
        "cert": {
            "driverLicenseNumber": "ASSA1234",
            "voilationDate": "08/27/2018",
            "voilationType": "01",
            "noOfVoilation": 15,
            "isDriverLicenseSuspended": false,
            "noOfSuspended": 0,
            "penalty": "Active",
            "fines": 300,
            "totalFines": 300
        },
        "error": []
    },
    "nonce": 447
},
```

Fig. 8. JSON Output of the First Block on Both Servers.



```
{
    "timestamp": 1536681004321,
    "lastHash": "00651625a41a9106b6166f310af0ea7973f134111cce7fe8af341b87c353e772"
    "hash": "00d9cf6a6ca7349b336f69405e1b383af0d909b92d3c26add1876452141ef1f4",
    "data": {
        "createdTime": 1536681004320,
        "cert": {
            "driverLicenseNumber": "30759188",
            "voilationDate": "01/24/2018",
            "voilationType": "15",
            "noOfVoilation": 70,
            "isDriverLicenseSuspended": false,
            "noOfSuspended": 0,
            "penalty": "Active",
            "fines": 80,
            "totalFines": 1240
        },
        "error": []
    },
    "nonce": 21
}
```

Fig. 9. JSON Output of the Last Block on Both Servers.

The next step is to look at the first block after genesis block whether Node1 and Node 2 produced identical first block. An output shown in Fig. 8 is retrieved by using the same request on each server. The first block contains the hash from genesis block which is "fir5t". It also contains its own hash which is "00e5758e2388adf51b3365627fe0dcc8a9af5d128abd0d222fa0 954f98fce577". The nonce of this block is 447 which is a unique number appear once in a blockchain. Node 1 and Node 2 produced identical JSON output for the first block. In conclusion, the decentralized model has shown a success on this step.

The last step is to check on the last block of the blockchain on both servers. So far, the total blocks and first block are identical thus the last block should have similar output. Fig. 9 shows that hash of the last block is "00d9cf6a6ca7349b336f69405e1b383af0d909b92d3c26add18 76452141ef1f4". The hash is identical on Node 1 and Node 2. It implies that the decentralized model has been implemented properly and worked as expected.

VI. Discussion

From the evaluation conducted, it can be seen that the results reflect the blockchain model are properly implemented. All inputs are successfully created as blocks which are stored in a blockchain. Demerit points and fines received from the inputs are matched with the real regulations as shown in Table 1. It executed Contract 1 based on the Offence Type inserted by the users. There is four Driver License Suspended from the inputs. It shows that Contract 2 is executed by four different Driver License since its total demerit points exceed 100 points. Contract 3 is automatically executed once a Driver License has executed Contract 2 and executed another Contract 1. Based on the inputs, only one Driver License execute Contract 3. In conclusion, all smart contracts are properly executed. The decentralized model is also proven to synchronize blocks created to all servers.

In real-world situation the smart contracts will be very helpful since it is only defined once, and it can filter any inputs since then. However, the smart contracts must be agreed over the involved parties to ensure minimal modification in the future. It reduces human errors in deciding how many demerit points are assigned in a particular offence. It also eases the process of record keeping with thousands of driver license registered and their respective demerit points, fines, and status recorded. With blockchain characteristic of immutable, once a smart contract is triggered and record the transaction as a block, then no one can modify it. It reduces the chances of misusing the regulation for negative purposes. For example, in normal system a database record can be easily modified in order to reduce the demerit points, reduce the fines, or even change the status of the driver license. As long as a person has an access to the database, it can be done. However, in blockchain even if a person has access to the server, he cannot do anything with the record for several reasons such as each of the block stored in a blockchain is secured with unique hash. A hash is unique and based on timestamp of the generated block therefore when a block is regenerated on purpose, the timestamp will be different and thus the hash will also be different. Another reason is the consensus method applied in decentralized network model. Any changes in a server will be verified first and compared to other servers before executed. Having blockchain technology in a traffic offence system is also helpful to prevent attack from inside and outside.

VII. Conclusion and Future Work

A blockchain Proof of Work with smart contract has been developed. The system shows that it is possible to implement and apply blockchain in a government policy such as traffic offence regulation. The system has successfully developed to fulfil blockchain characteristics of being distributed, immutable, trust-less, and decentralised. It also shows that the details of traffic offence can be converted into a block schema and later cryptographically secured using hash to secure the transaction. Although the overall system has been proven to work properly, there might be issues with the performance if the setup is changed with additional nodes. Being a blockchain system means that forking issues still exists when clients mining the data and found the identic nonce. Therefore, it is required to have a real-world performance test to this model before implemented in real policies.

Acknowledgment

This research work is sponsored by UTeM Zamalah Scheme from Universiti Teknikal Malaysia Melaka.

References

[1] C. Ramendran, “Offenders who chalk up 100 Kejara demerit points will have driving licence revoked,” The Sun, 2017. [Online]. Available: http://www.thesundaily.my/news/2219522. [Accessed: 06-Jul-2018].

[2] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, “Blockchain – the Gateway To Trust- Free Cryptographic Transactions,” Twenty-Fourth Eur. Conf. Inf. Syst., pp. 5–16, 2016.

[3] M. Risius and K. Spohrer, “A Blockchain Research Framework,” Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 385–409, 2017.

[4] B. Gipp, N. Meuschke, and A. Gernandt, “Decentralized Trusted Timestamping using the Crypto Currency Bitcoin,” pp. 1–6, 2015.

[5] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.

[6] B. Notheisen, J. B. Cholewa, and A. P. Shanmugam, “Trading Real-World Assets on Blockchain,” Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 425–440, 2017.

[7] T. Puschmann and R. Alt, “Sharing Economy,” Bus. Inf. Syst. Eng., vol. 58, no. 1, pp. 93–99, 2016.

[8] M. Nasser et al., “Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 1, 2018.

[9] M. F. Ali, N. Azman, and N. Harum, “A Novel Multiple Session Payment System,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 6, pp. 237–245, 2018.

[10] M. S. Talib, A. Hassan, B. Hussin, Z. A. Abas, Z. Saad, and Z. Sabah, “A Novel Stable Clustering Approach based on Gaussian Distribution and Relative Velocity in VANETs,” Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 4, pp. 216–220, 2018.

[11] D. Efanov and P. Roschin, “The all-pervasiveness of the blockchain technology,” Procedia Comput. Sci., vol. 123, pp. 116–121, 2018.

[12] D. Wörner, T. von Bomhard, Y.-P. Schreier, and D. Bilgeri, “The Bitcoin Ecosystem: Disruption Beyond Financial Services?,” in ECIS 2016 Proceedings, 2016.

[13] R. Böhme, N. Christin, B. Edelman, and T. Moore, “Bitcoin: Economics, Technology, and Governance,” J. Econ. Perspect., vol. 29, no. 2, pp. 213–238, 2015.

[14] S. Delgado-Segura, C. Pérez-Solà, G. Navarro-Arribas, and J. Herrera-Joancomartí, “A fair protocol for data trading based on Bitcoin transactions,” Futur. Gener. Comput. Syst., 2017.

[15] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, “Cecoin: A decentralized PKI mitigating MitM attacks,” Futur. Gener. Comput. Syst., 2017.

[16] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, “Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains,” pp. 1–10, 2018.

[17] J. Hwang et al., “Energy Prosumer Business Model Using Blockchain System to Ensure Transparency and Safety,” Energy Procedia, vol. 141, pp. 194–198, 2017.

[18] J. J. Sikorski, J. Haughton, and M. Kraft, “Blockchain technology in the chemical industry: Machine-to-machine electricity market,” Appl. Energy, vol. 195, pp. 234–246, 2017.

[19] F. Hawlitschek, B. Notheisen, and T. Teubner, “The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy,” Electron. Commer. Res. Appl., vol. 29, pp. 50–63, 2018.