S	
E1	
E2	
For Office Use Only	

Masters Project Final Report

(MCS)

2019

Project Title	**Vehicle Record/History Maintenance through Blockchain Technology**
Student Name	**Dhanusha Samarakkody**
Registration No. & Index No.	**2016MCS097 / 16440971**
Supervisor's Name	**Dr. Kasun de Zoysa**

For Office Use ONLY

Vehicle Record/History Maintenance through Blockchain Technology

A dissertation submitted for the Degree of Master of Computer Science

D.SAMARAKKODY

University of Colombo School of Computing

2019

Declaration

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student Name:

Registration Number:

Index Number:

_____

Signature: Date:

This is to certify that this thesis is based on the work of Mr. /Ms. ……..

under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name:

_____

Signature: Date:

Abstract

The used car market is in a demanding position in Sri Lanka. When selling a car, the seller typically knows significantly more about the vehicle rather than the buyer. This is a problem for the buyer as it opens them up to a potential fraud. To hedge against the risk of buying a 'bad' car, they tend to bargain for the price of the vehicle. Information exchanging between institutions such as RMV, Insurance, Leasing, Emission and Service Centers is also challenging as they maintain separate databases. This could lead to a huge collapse in the entire used car market. Market participants indicate a need of reliable, secure, and transparent historic operational vehicle data. This paper proposes TRUECARE: a novel, decentralized record maintenance system (dApp) which handles vehicle records by using the Blockchain technology. Leveraging the unique Blockchain properties, TRUECARE manages authentication, confidentiality, reliability and data sharing which are the crucial considerations when handling the records of vehicles. Ethereum is a major blockchain-based platform for smart contract. Smart contract is an appealing feature to facilitate, execute and enforce an agreement between untrusted parties without any involvement of a trusted third party. Smart contract is used to authenticate data providers and share data between them. The purpose of this paper is to expose a working prototype through which we analyze and discuss our approach and the potential for Blockchain in automotive industry.

Key words: Blockchain, Ethereum, Smart Contracts

Acknowledgement

First, I would like to thank my supervisor, Dr. Kasun De Zoysa, for encouraging me on this research. His vision and invaluable guidance have inspired me over the past year. His advice had a considerable impact on the way of conducting the research, presenting ideas, and evaluating the success. He taught me how to test and have condense in my ideas. I consider myself enormously lucky that I had the opportunity to work with you. Thank you.

In addition, I am grateful for the support and camaraderie of academic and management staff of University of Colombo School of Computing, Sri Lanka. And a special thank goes to my colleagues in my company for taking off my mind from company work when there is a deadline ahead. Thank you for tolerating my anxiety-riddled behavior on stressful deadlines, and for making me laugh on a regular basis.

Finally, I must express my very enormous gratitude to my wife and family for their unwavering support and continuous encouragement throughout the research process. This accomplishment would not have been possible without them.

Table of Contents

List of Figures

Chapter 1: Introduction

1.1 Background

This work has identified a blockchain based structure [1] that can apply to vehicle history report system. The report system is planned to build on this distributed ledger protocol originally associated with Ethereum [20].

Normally, blockchain uses public key cryptography to create an append-only, immutable, time stamped chain of content. Copies of the blockchain are distributed on every collaborating node within the network. The blockchain itself doesn't rely on a central, trusted authority. Rather, it is distributed to all nodes participating in the network. Because no centralized authority might verify the validity of the blockchain. So, it must be implemented a mechanism for reaching network consensus [1]. In Ethereum, a Proof of Work function is used to ensure network consensus. The Proof of Work algorithm used to secure the content from tampering depends on a trustless model, where individual nodes must compete to solve computationally expensive (but easily verifiable) puzzle before the next block of content can be appended to the chain. These worker nodes are referred to as miners, and the work required of miners to append blocks ensures that it is troublesome to rewrite history on the blockchain. This whole concept is used throughout the project.

Different Records regarding to a particular vehicle is collected from data providers' (RMV, Insurance Companies, Leasing Companies, Vehicle Service Stations, etc.) databases which are access granted through smart contracts. Consumers can view data publicly by entering the VIN of a vehicle in the web application provided. Even though the system is public, this approach provides many advantages over centralized system which is more complicated and not cost-effective. But the important factor is that the system should have some implementation to protect the content of smart contracts.

The objective of this project is to minimize the damage that could happen to the society by providing accurate and confident details about used vehicles as much as possible by reducing the risk associated with information which is being changed, faked, rewritten or manipulated (immutable). It is a right of every participant to know the accurate history of a vehicle which is to be sell. Knowing the full operational history of a vehicle will guarantee that the vehicle retains a certain level of value at the time of sale. The same cannot be ensured with a vehicle without any report.

The participants in the automotive industry, such as government, insurance companies, leasing companies, service stations, and departments of emission testing will be united into a single system for data exchange purposes.

1.2 Motivation

Shortcomings with used vehicles could be easily experienced or heard by anybody. Most of the time the buyers think that the amount of money they have spent is not compatible with the condition of the vehicle. This problem occurs as they cannot get accurate information. Currently there are certain vehicle records management systems but the accuracy of the information is questionable. They are using traditional databases with low security that can be easily break out which may lead to unreliable data. These all the difficulties and issues associated with the used car market, lead to this Blockchain application.

1.3 Statement of the problem

In Sri Lankan automotive industry, majority of customers are usually lean on purchasing used vehicles due to the financial states of citizens in the country. According to the statistics given by the Ministry of transport & Civil Aviation in Sri Lanka, the variance between number of new vehicle registration and number of transferences can be clearly identified. For an example, in the year of 2017, the number of new registration of Motor cars were 39,142 (Figure 1.3.1) and the number of transference of Motor cars were 130,027 (Figure 1.3.2). This clearly proves that buyers are impassioned to buy used vehicles.

Vehicle Population | **New Registration** | Transfering | Driving License | Gas Emission Test | Financial

Year	2012	2013	2014	2015	2016	2017
Motor Cars	31,546	28,380	38,780	105,628	45,172	39,142
Motor Tricycle	98,815	83,673	79,038	129,547	56,945	23,537
Motor Cycles	192,284	169,280	272,885	370,889	340,129	344,380
Buses	3,095	1,805	3,851	4,140	2,685	3,331
Dual purpose vehicles	37,397	24,603	20,799	39,456	26,887	16,742
Motor Lorries	12,266	5,872	5,121	6,602	7,229	11,432
Land Vehicles-Tractors	18,450	10,772	7,070	10,517	10,285	8,821
Land Vehicles-Trailers	3,442	2,266	2,012	2,128	3,996	4,228
Total	397,295	326,651	429,566	668,907	493,328	451,653

Figure 1.3.1 New Vehicle Registrations

Vehicle Population | New Registration | **Transfering** | Driving License | Gas Emission Test | Financial

Year	2012	2013	2014	2015	2016	2017
Lorries	37,328	40,992	44,731	40,207	47,098	56,749
Motor Cars	62,787	73,649	83,450	108,579	111,297	130,027
Commercial Vehicles	37,126	45,782	56,342	69,419	75,187	
Motor Tricycle	74,504	100,910	108,255	108,455	140,771	218,918
Motor Cycles	41,094	62,719	64,729	65,620	90,885	175,001
Buses	13,765	14,188	14,306	14,911	15,671	18,082
Land Vehicles	8,196	8,414	7,773	10,152	10,879	12079
Dual purpose Vehicles	-	-	-	-	-	97,345
Total	2,74,800	3,46,6654	3,79,586	4,17,343	491,788	708,201

Figure 1.3.2 Transferring Vehicles

But the problem is that whether the amount of money they are spending is compatible with the condition of the vehicle. Unfortunately, many frauds take place when a used vehicle is purchasing.

Normally, customers come along with a professional mechanic to check the condition of the vehicle. But there are some cases even a mechanic couldn't identify. For an example, the odometer readings cannot be trusted since anybody can change the values. Certain problems are associated with the history of accidents as well. And more importantly, it is not possible to identify how maintenance took place during the usage.

Sometimes, customer wants to know how many users utilized the vehicle before and in which areas they have driven the vehicles. Normally, customers do not like to buy vehicles which were driven in coastal areas or mountainous.

Buying a used vehicle would become a tragedy if customer get a stolen or misused vehicle.

The current situation is very complicated as mentioned above. Unfortunately, there is no any central single database for vehicles. Normally, Insurance companies, Leasing Companies, RMV or Emission Test Departments have their own commercial databases. But, they cannot solve this problem as their information is stored separately. And in the other hand, the accuracy of information cannot be ensured due to the security issues in these databases.

Usually, vehicle service stations do not maintain records regarding to the services that they have done. The reason behind this might be the cost associating with server machines.

By considering the above factors, it is cleared that no one has clear and overall information about used vehicles. Tracking the records (vehicle papers, service documents, emission test papers) with current facilities is impossible (no access for commercial databases for external persons), time and cost consuming or lack of trust. As a result, frauds in used vehicles pose a massive problem on customer and even for security concerns.

So, it is very important to have a confidential history report with relates to registration (RMV), maintenance (service, emission test, insurance, lease and etc.), accidents, and odometer readings. It is useful not only for buyers but also for the Leasing or Insurance companies to have a transparency with used vehicles to perform insurance or technical inspection tasks.

This concept can be demonstrated with the following example: A buyer has to make a choice between two identical vehicles. One with a full vehicle history report, and one without. In this scenario, the buyer is likely to choose the vehicle with the full vehicle report over the other even in cases that the report indicates past damage and/or repairs. This is due to the report providing an accurate reflection of the vehicle's history.

1.4 Aims and Objectives

The aim of this project is to design a decentralized, more secure, ease of access and reliable system to overcome from the disadvantages by having separate databases for each data provider parties. Unite participants in the automotive industry, such as manufacturers, insurance companies, dealers, service stations, and developers of navigation systems into a single ecosystem for data exchange purposes. Finally, Ensure the trust between parties (Sellers, Buyers, Leasing or Insurance Companies, etc.) by providing an open and transparent system and minimize the damage that could happen to the buyer.

Chapter 2: Background/Literature Review

Blockchain is generally celebrated for its respect to Bitcoin cryptocurrency. Bitcoin uses Blockchain technology in currency transactions. Satoshi Nakamoto introduced [1] a pure peer-to-peer electronic cash system which allowed online payments without having a trusted third party like financial institutions. The coins are made from digital signatures. It solves a part of the problem, but for preventing double spending or protecting from frauds, they decided that all transactions must be publicly announced. To know which transaction arrived first, the majority of nodes need to agree that it was first arrived. The solution they proposed begins with timestamp server [2]. To implement a distributed timestamp server, they used the concept, "proof-of-work". This is how the Blockchain technology has implemented. The steps to run the network with Blockchain as follows:

1) To all nodes, new transactions are broadcasted.
2) New transactions are collected by each node into a block.
3) Each node finds a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes. To complete transactions, miners' processing power is used and they are rewarded with Bitcoins as incentives.
5) If all transactions in the block are valid and not already spent, then only the nodes accept the block.
6) By creating the next block in the chain by using the hash of the accepted block as the previous hash, nodes express the acceptance of the block.

The amount of energy required to validate transactions in the proof-of-work is a major drawback in blockchain. Many people consider this as a "wasted energy" and feel it has a negative impact on the environment [5].

The success of the currency deployment depends on the anonymity which is a key property in blockchain. Anonymity in the bitcoin network is based on the fact that users able to create any number of undisclosed bitcoin addresses that will be used in their bitcoin transactions. This basic approach is a good starting point. But the underlying non-anonymous Internet infrastructure, together with the availability of all bitcoin transactions in the blockchain, has proven to be an anonymity threat.

In order to relieve the anonymity reduction of the bitcoin system that can be performed using the techniques described in [3] the use of mix services have been proposed. Bitcoin mixes are

services that allow a user to anonymize his/her bitcoins by mixing them with bitcoins of other users. Different proposals have been presented in this field showing that it is possible to design a mix service with a considerable level of security for the user.

However, Bitcoin cryptocurrency is not the only way that uses the Blockchain technology. Therefore, it is important to find the other applications developed by using the Blockchain technology. Identifying these applications can be help to understand the other directions and ways to use Blockchain.

Ethereum cryptocurrency is an important platform which is based for smart contracts [4]. Smart contracts are turing complete programs which are implemented in a decentralized network and control digital units of value. A common view of the global state is maintained by a peer-to-peer network of mutually disbelieving nodes and it executes code upon request. The blockchain stores the stated which is secured by a proof-of-work consensus mechanism which similar to that in Bitcoin. The core value proposition of Ethereum is suitable for executing complex business logic as it is a full-featured programming language. Decentralized applications without a trusted third party are appealing in areas like gambling, crowd funding, identity management and financial services. Smart contracts can be considered as a challenging research field that spread over areas as governance, programming languages, cryptography, consensus algorithms, finance, and law [6].

In a proof-of-stake model there will no longer be miners, but validators. There will no longer be cryptographic challenges but the difficult mathematical problems that miners must solve. Validators will be required to own ether and in order to validate a block they will be required to put their owned ether on the line to certify that a block is valid [5].

Another difference will be the method of reward. Instead of rewarding miners for creating blocks validators will earn a transaction fee for each transaction and smart contract they validate. This will be much more energy efficient and will put a focus on bandwidth rather than hash rate (number of calculations per second).

Soon after the companies, governments and consortiums started looking into the underlining technology of above mentioned cryptos and understood that “Blockchain is the real invention and not the Bitcoin”. With that a different type of blockchains were emerged such as,

1. Public Blockchain
2. Private Blockchain
3. Consortium or Federated Blockchain

There are some other complicated types also such as public-permissioned blockchain, private permissioned blockchain, etc.

The public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain network in the crypto market today.

The considerable amount of computational power which is required to support the distributed ledger is at a large scale. This is one of the disadvantages of public blockchain. To achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all are in sync. The privacy problems associated with transactions are considered as another drawback of public blockchain. Both of these drawbacks are considered as important factors in enterprise use of blockchain as described in [7], [8].

A secure and naturally decentralized framework is provided by Blockchain-based databases for transaction processing. Compared to other distributed databases, one of the major advantages of blockchain is the integration of data processing, security and consistency into an algorithmically enforced blockchain protocol, which eliminates the human factor from the equation. The institutions that operate financial ledgers or registries may be inclined to use permissioned blockchains due to legal and technical concerns as described in [9].

Permissioned blockchains could form the basis for blockchain innovations for services that operate ledgers or timestamped registries. Although permissioned chains do not require to use proof of work, this consensus protocol can still be utilized as an additional level of security and to increase auditability and attractiveness of chains for customers, especially if blockchain data is partially or completely public.

All the public and private sector healthcare providers to maintain electronic medical records (EMR) from 1st of January 2014 according to the American Recovery and Reinvestment Act, in order to keep their existing Medicare levels. To achieve that fundamental design changes needed to be happen focusing on availability and utilization of EMRs. Currently, healthcare providers are having centralized data stores systems for each foundation. However, the considerable amount of these systems does not have the capacity to share their health data [10].

Blockchain technology has the potential to address the interoperability challenges currently present in health IT systems and to be the technical standard that enables individuals, healthcare providers, healthcare entities and medical researchers to securely share electronic health data.

Bitcoin is based on open-source cryptographic protocols. It has proven as an extremely secured platform for cryptographic transactions. The platform provides transparency. Which means that anyone can access the blockchain and check balances and exchanges for any Bitcoin address. But the Bitcoin public blockchain is considered as unsuitable for a health blockchain due to the lack of data privacy and the absence of robust security. Further, the block size and the maximum number of transactions per second of the Blockchain standard, present scalability concerns for large-scale and widely used blockchain applications.

Private and consortium led blockchains would address the privacy, security and scalability concerns. However, these blockchains would pose different challenges as they run the risk of not being vendor neutral and do not use open standards.

Utilization of a proposed health blockchain: a private blockchain described in this paper [11] has the potential to interact with millions of individuals, healthcare providers, healthcare entities and medical researchers to share vast amounts of genetic, diet, lifestyle, environmental and health data with guaranteed security and privacy protection. Utilization of Ethereum's smart contracts to construct intelligent representation of existing medical records contains with record ownership, permissions and data integrity that are stored within individual nodes on the network. To easily navigate through the large amount of record representations, a system can structures smart contracts on the blockchain by implementing many types of contracts.

While the Blockchain is the foundation for cryptocurrencies like Bitcoin and Ethereum, the contribution of blockchain can make toward improving process efficiencies and saving money are fueling multiple use cases throughout the rest of the Financial Services industry [12]. Such as

1. Smart Contracts
2. Smart Assets
3. Clearing and Settlement
4. Payments
5. Digital Identity

Recently, Sampath Bank in Sri Lanka introduced a Blockchain Gifting App. It became the first bank in Sri Lanka to introduce a blockchain based solution [13].

When considering the application area of automobile industry which relates to this research, in Sri Lanka there is no any blockchain based system for retrieving the history of vehicles. Currently, Sri Lanka Motor Traffic Department has centralized database system which produce a vehicle information report focused on some basic details. Some of these details are for free of charge and some with a charge [14] (Figure 2.1).

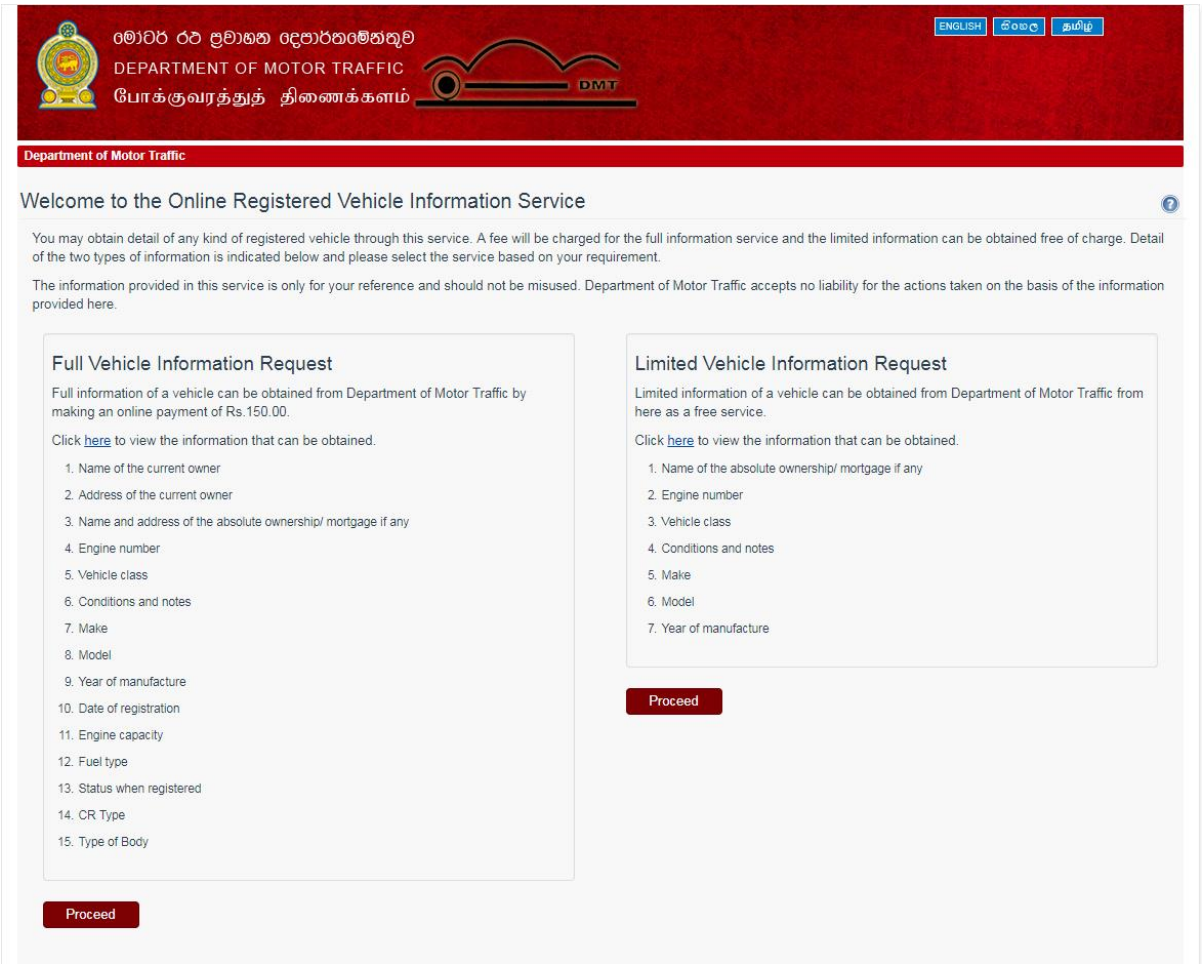


Figure 2.1 Motor Traffic Application

To proceed through the request made by a person, he/she required to log in using one of his/her existing accounts from the authentication providers they have given (Figure 2.2).

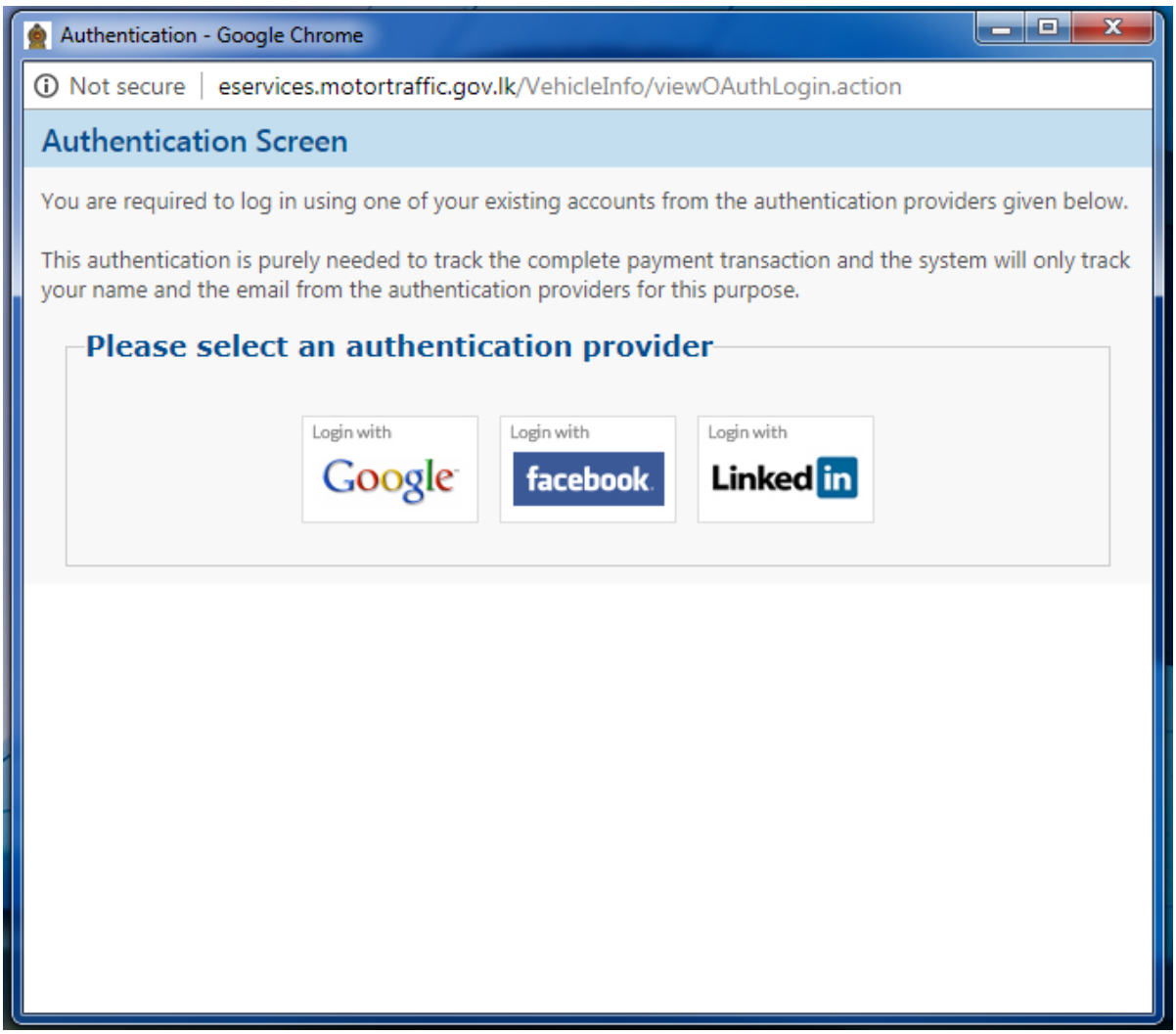


Figure 2.2 Motor Traffic Application Login

The ICT Agency of Sri Lanka (ICTA) and the Department of Motor Traffic (DMT) came together in launching a triple e-service. Under that, they also developed an android mobile app (Figure 2.3). The three e-services will provide information on the following: Details of the vehicle, last registration number of a given vehicular category and the period of validity and date of expiry of the vehicle revenue license.

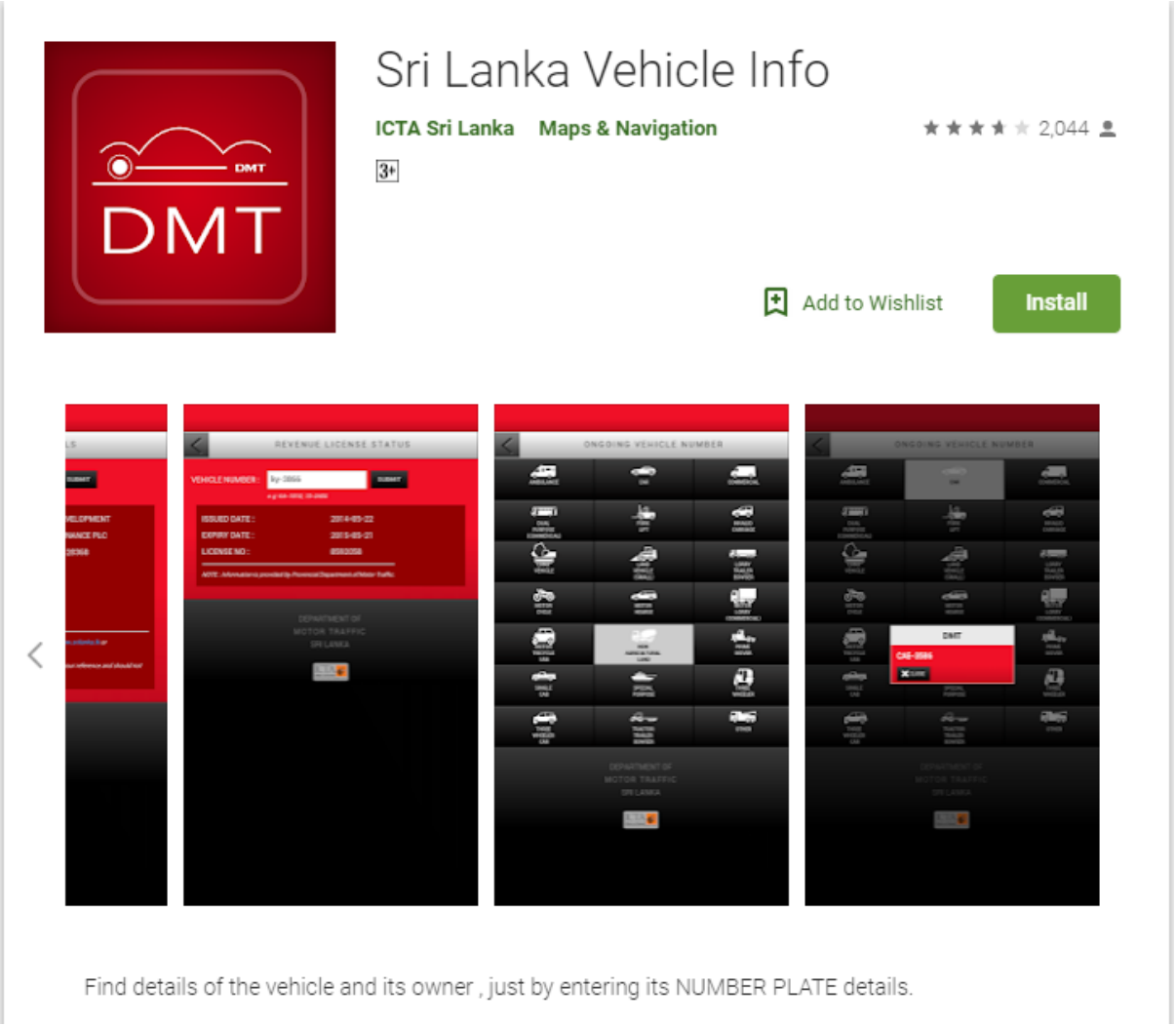


Figure 2.3 DMT Mobile Application

In Sri Lanka, there is a popular website named as 'ikman.lk' which is used by all most all of the vehicle buyers or sellers [15]. The website can be used by anyone who is having a valid email address and need to pay in order to upload advertisements about sales of a vehicle.

When buyer wants to search for a used vehicle for sale, he/she has the option to search it through the vehicle type, model, manufactured year, location and etc. Then it shows some basic information about the vehicle as shown in the Figure 3. The accuracy of this information cannot be guaranteed.

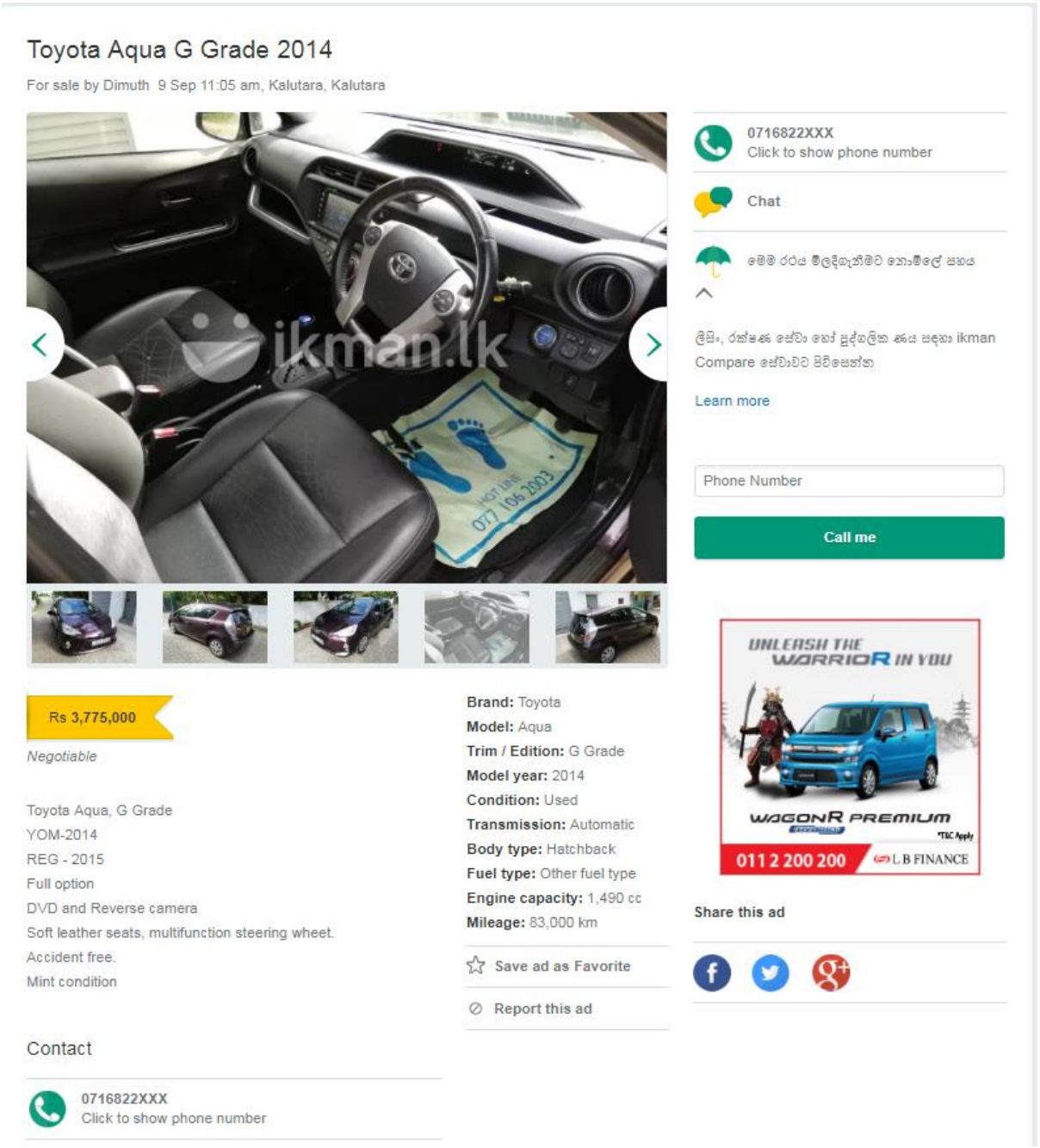


Figure 2.4 ikman.lk Web Application

There are few blockchain based vehicle history report applications around the world such as Uservice, carVertical, VINchain and Carblox [16] - [19].

VINChain, Carblox, carVertical are mainly focused on how to solve the problem of unbalanced information in the used car market by creating a decentralized, immutable, transparent, secure, and reliable vehicle lifecycle storehouse. But the main purpose of a platform like Uservice is to solve all the issues that the car owners face while using the car. Generally, Supplying and purchasing of spare parts for a user vehicle is one of the most important function in the Uservice

platform. When considering buying parts, there is a great exposure of purchasing a phony spare part, which is very difficult to distinguish from the genuine.

In storing and manipulating of information in above apps will be ensured by current decentralized technologies such as distributed file system (IPFS) and blockchain (Ethereum based).

Information about the vehicle is acquired in the databases of all data providers (manufacturers, insurance companies, service stations, banks and leasing companies, dealers, etc.) during the entire period of its use. All those records collected from data providers get hashed and added into Blockchain. Data providers hash their records and add it into Blockchain by themselves signed with their electronic digital signature (EDS). This mechanism allows excluding any side parties from the chain which makes the service and data trustworthy for the final consumer. The data itself is stored in service providers' databases but its hash in the Blockchain. The validity of the information provided can be checked by the hash code. Data hashing and adding it into the Blockchain makes it secure through several steps such as, the Blockchain receives the data hashed, the data hashed is signed with EDS, hashed again, compound into blocks. These blocks are signed with EDS and hashed.

Trust between the parties of the ecosystem will establish by the immutability and accessibility of information in the blockchain and confirm the authenticity of the information received from the registration. Smart contracts supported by Ethereum will be actively applied in these apps as a part of the functionality where decentralization allows for anonymity, security and authenticity of information.

Such a platform will consist of the following components:

1. WEB-application - Developed for user access to the functionality through a user-friendly web interface.
2. Data storage - All data received from data providers will be stored in a distributed file system and encrypted. Multiple backup functionality in a decentralization system will ensure the safety of data.
3. Blockchain - An internal payment system will be implemented based on blockchain (the token will be used as the means of payment). Due to smart contracts, the blockchain will also include information about a range of operations in platform (transactions, the transfer of ownership rights, and access to information). Another purpose of the blockchain is to store the digital fingerprint (hash) of data from the repository. This mechanism will confirm the accuracy of any information obtained from the platform.

4. API - Designed for the integration of third-party services, custom applications and telematics devices.
5. Client applications - To simplify the access to its functionality, multiplatform applications for different groups of its ecosystem members will be developed.

Each and every record of a particular vehicle is connected with the vehicle identification number (VIN) and placed in the blockchain system. This information is transparent and accessible to everyone with access to the system.

To maintain the accuracy of information, the blockchain technology and data hashing through the SHA-256 cryptographic algorithm (sha 2 family) is used. This guarantees reliability and security of data.

The mechanics of such system work as follows:

1. A request for data is received.
2. The entire chain is searched for relevant data.
3. Reports are created and provided in a structured form.
4. Members of the relevant registry receives a fee for providing Information.

The Buyer registers on a service provider's website or in the mobile app. By entering the VIN number of the vehicle, the buyer is allowed to check the vehicle's Blockchain-record availability if he/she is valid user.

Then service provider verifies the Buyer's request by checking the availability of data in all data-providers' databases and gives the Buyer a short report for free of charge.

This short report is a preview of a part of the information that is contained in the full report. If the buyer is satisfied with the abbreviated report, they can proceed and purchase the full report.

The decentralization makes the system even more secure. The data providers are united into a single system (nods) and store their up to date hash copies of each service provider.

In case of data lose it is possible to restore the data from any other system participant which is one of the advantages in decentralization. Because of that the final consumers will not suffer from such kind situations as it also guaranties 24/7 access to the system.

Each data provider will be able to get and add the information with the help of unique access certificate verified by the Project. In addition, there will be a data rating for each data provider. As a result, the provider will take responsibility for any information added. Each data provider

will be awarded with tokens depending on the rating. Tokens are used as internal currency. Each platform has created its own tokens for internal payments.

While studying these applications, it is possible to identify how the system is implemented practically.

Chapter 3: Methodology

3.1 Blockchain Background

This research is based on the discipline of Blockchain which is known as a decentralized, distributed and public digital ledger. Many people think of blockchain as the technology that powers the bitcoin. While this was its original purpose blockchain is capable of so much more. Despite the sound of the word, there's not just one blockchain. Blockchain is shorthand for a whole suite of distributed ledger technologies that can be programmed to record and track anything of value from financial transactions to medical records or even land titles.

Ethereum blockchain is used to create a de-centralized and distributed vehicle history report which is publicly available. But only certain service providers (RMV, Insurance Companies, Leasing Companies, and Vehicle Service Stations) have access to insert new data. These contributors are listed down using smart contracts. The Information adding is authenticated with a valid Ethereum account.

Each record of a vehicle represents a block. With combination of set of vehicle records, it creates the chain of blocks which is the Blockchain. Any changes to the information record in a particular block do not rewrite the original block. Instead, the change is stored in a new block. That means every change of ownership of a vehicle is represented by a new entry (block) in the ledger.

In blockchain, every member in the distributed network have a copy of every block. But that block is consisted of images, or any other large documents. So, replicating all vehicle records to every member in the network is not practical in storage perspective and it is wasting the network resources. To address the scalability problem, all the vehicle records added by the service providers is stored off from blockchain to a data repository (IPFS).

When a service provider (contributor) creates a vehicle record block with images, a digital signature is created by providing the authenticity for that information. Then, the information is sent to the data repository and hash value of the information is stored in the blockchain according to the rules with the use of the timestamp of the record. Every time an information is saved to the data repository, a pointer to that vehicle record is registered in the blockchain along with the vehicle identification number (VIN). Through this, it confirms the invariability of the information stored in the database of each service providers (contributors) even the service provider is attempting to do the changes.

In particular, these implementations place the records on the blockchain, requiring data providers to spend transaction fee (Tx Fee), termed as gas each time they insert, update or cancel a record. To do anything on the Ethereum platform (except retrieving stored data on blockchain and view on them), you need to pay for it, and the payment (or fee) is calculated in Ether (ETH) via an intermediary benchmark called gas limit and gas price.

Ether = Tx Fee = Gas Limit * Gas Price

Gas Limit is the amount of gas charging for completing a transaction. A gas limit of 21000 is considered acceptable for simple transfers and even for participating in token crowd sales. If you lower the gas limit apart from recommendation, your transaction is prone to fail, resulting in the loss of fees as well.

Gas Price is the cost of a single gas unit. It is usually calculated in gwei (1 Ether = 1000000000 gwei). It is set by miners and usually lies between 20 to 30 gwei, at the time of writing.

For a transaction with a gas limit of 21000 and gas price of 20 gwei, the total transaction fee will be 0.00042 Ether or $0.072 ($171.59 per Ether).

3.2 Smart Contract Structures

A smart contract is an executable code that runs on the blockchain to facilitate, execute and enforce the terms of an agreement. The main aim of a smart contract is to execute the terms of an agreement automatically, once the specified conditions are met. Ethereum is a public blockchain platform that can support advanced and customized smart contracts with the help of Turing-complete programming language. Ethereum platform can support withdrawal limits, loops, financial contracts and gambling markets.

The data save on Ethereum blockchain are not sensitive. But it should be able to protect parts of the dApp from intruders and snoopers through authentication and authorization. Instead of having a centralized database system, proposed a system that allows and disallows user access to pieces of data using smart contract on blockchain.

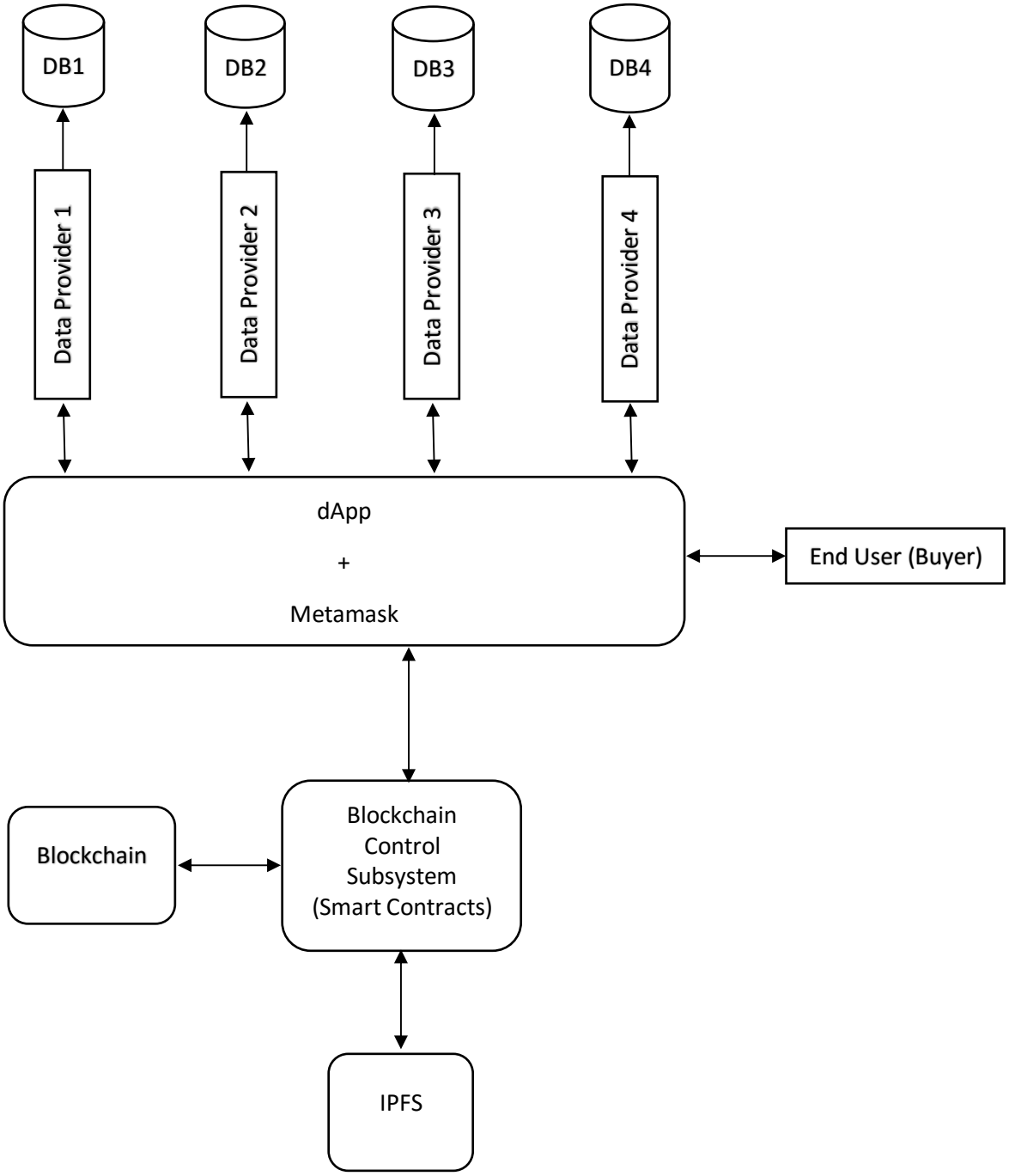
Utilized Ethereum account system (Metamask) for authentication and build an authorized system which uses the account address of the user. The account address that sends a transaction or a call is readily available inside the every function in Solidity, so that looks auspicious. However, it shows that the address is the only data about the user that is sent to the contract. Which makes it

needs to check the address against something in which the authorization has stored. This can be within the contract itself.

But it has to be checked with another contract, which would make it more beneficial. In that Access Control contract, user maps his/her details (name, address, registration no., role, etc.) to the account address and with that system checks whether the user has the required role and address to access the data. There are mainly 5 types of roles (rmv, insurance, leasing, emission and service). For each role, there is a separate smart contract to store data. To access that, user must have both authorized role and address. Then, system needs to figure out a way to make this work, due to the fact that the address of the contract (Access Control) that stores the details needs to be known in the contract that stores the data. To do so, at the deployment of smart contracts it passes the address of the Access Control contract to every other contract that stores data.

The same method is used when data exchange between separate roles (data providers) taken place by smart contracts which helps to maintain integrity and consistency of information which is circulated among data providers.

Chapter 4: Design



Chapter 5: Implementation

The web application (dApp) is designed for users to access the details of a vehicle through a convenient web interface. Through that interface any user who connect with Ethereum network can enter the VIN in given field and system will generate a report of details about vehicle and display it on web page.

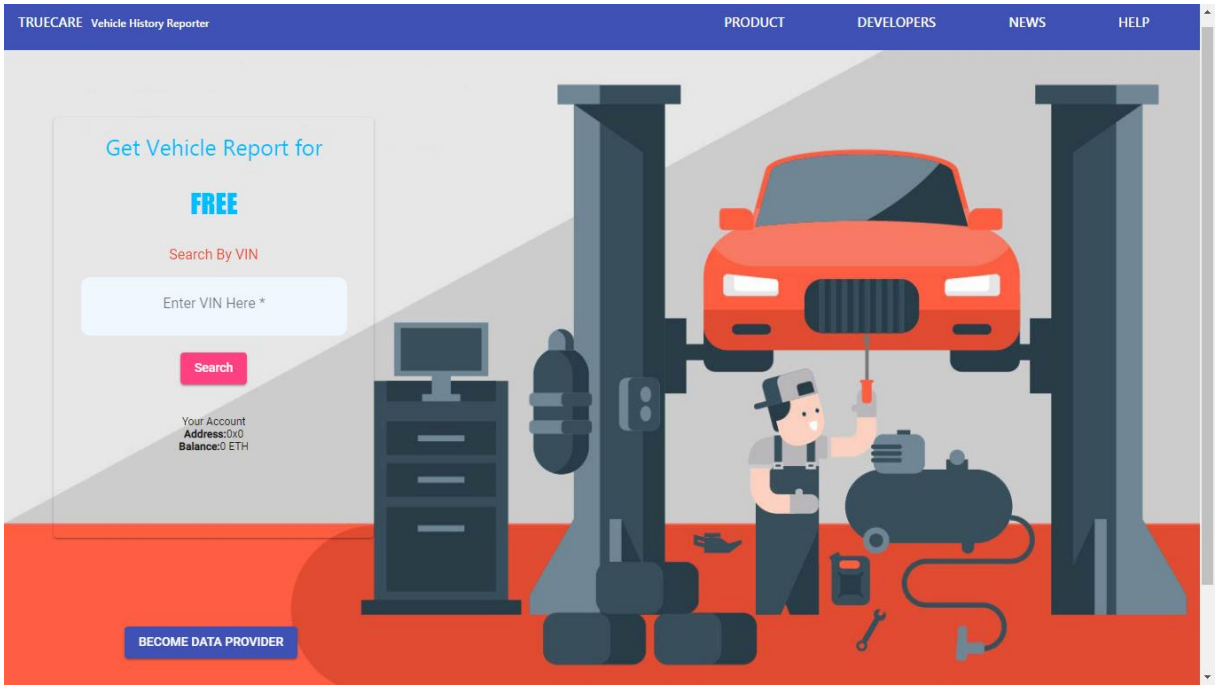


Figure 5.1 Home Page of TRUECARE

To become a data provider, the system has facilitated to register and submit their Ethereum account details (Figure 5.2). The system admin has ability to activate those accounts and by activating them grant access to the system (Figure 5.3). Data providers who are with valid accounts in the system (stored in smart contracts) have permission to insert or update data.

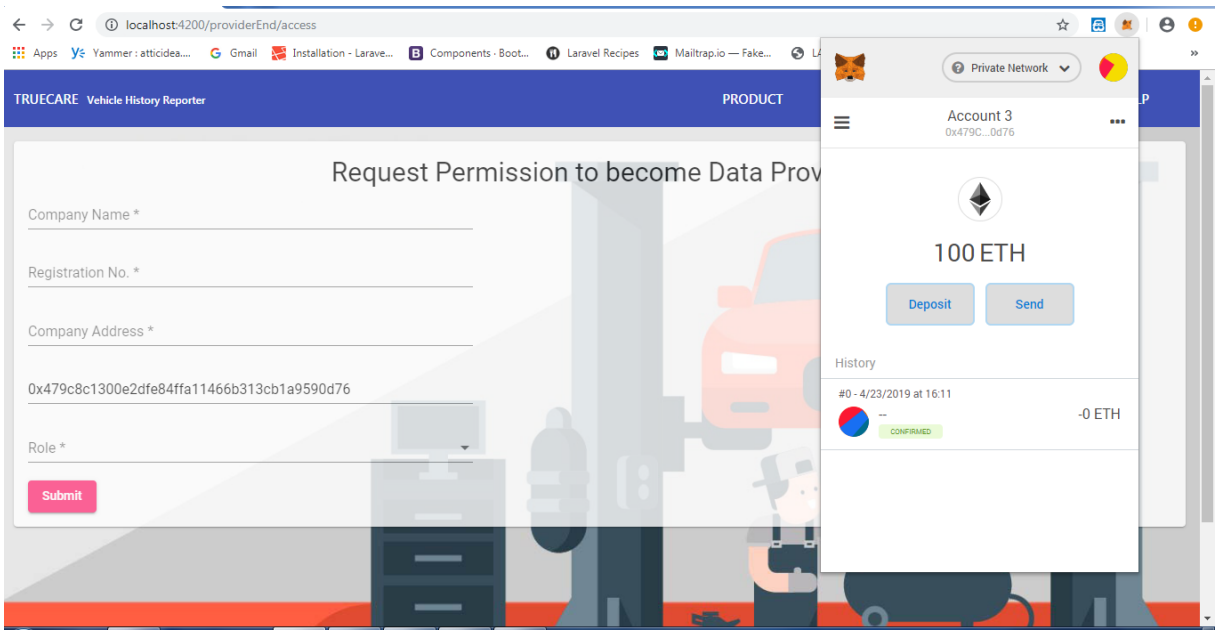


Figure 5.2 Registration of data providers

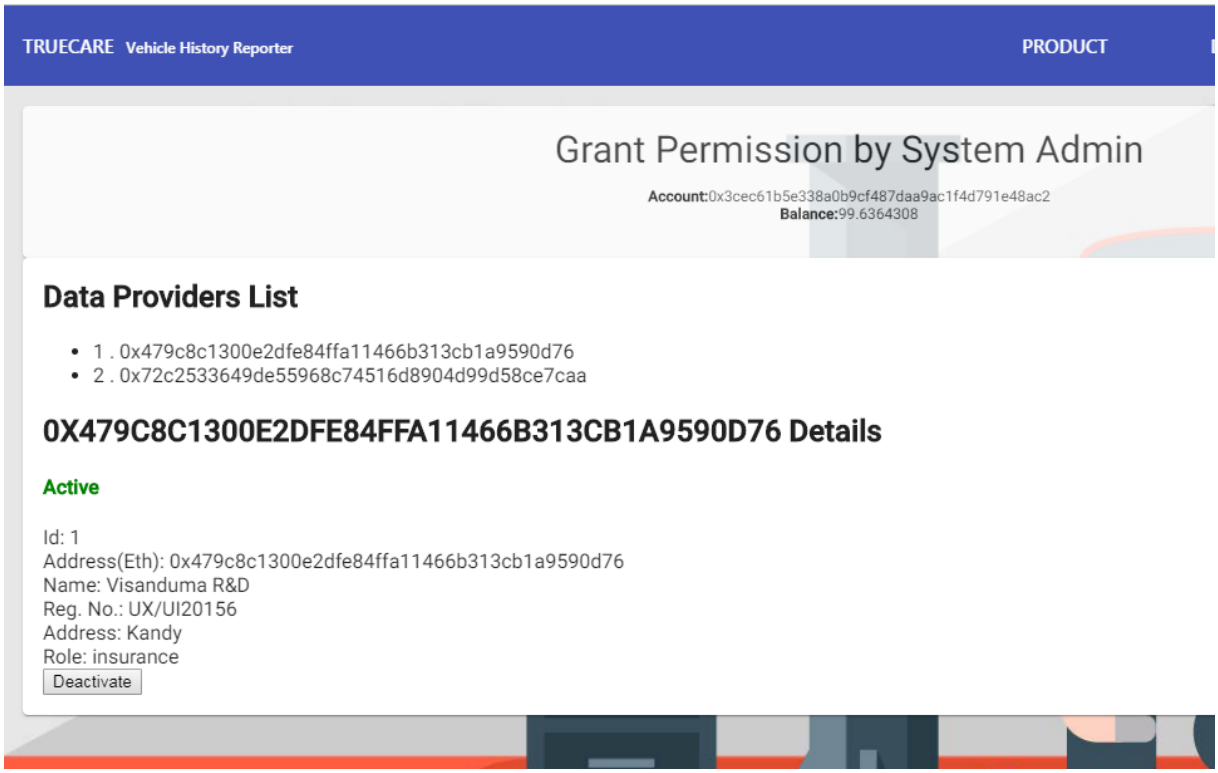


Figure 5.3 Admin dashboard to grant permission

A data provider who are registered with role of RMV (Motor Traffic Department) get the following web interface to add details.

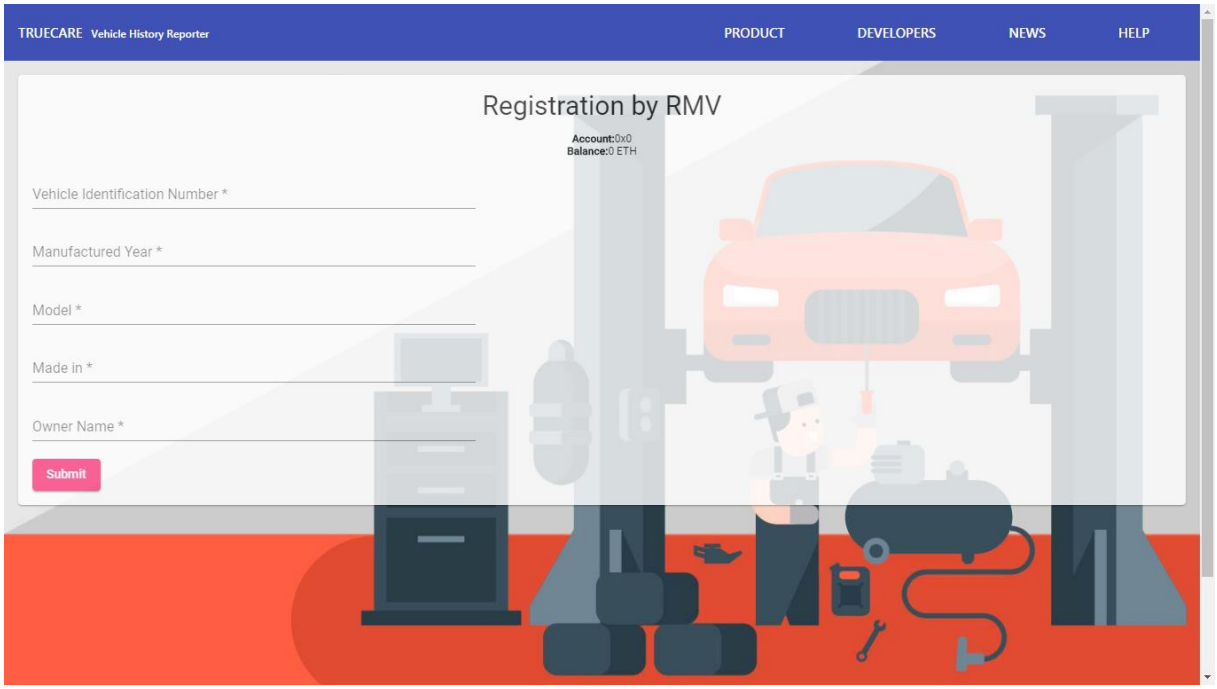


Figure 5.4 Sample of RMV web interface

In order to build dApp, needed to have few dependencies first.

5.1 NPM

The first dependency needed is Node Package Manager, or NPM, which comes with Node.js.

5.2 Framework

The Truffle Framework, which allowed to build decentralized applications on the Ethereum blockchain. It provides a suite of tools that allowed to write smart contracts with the Solidity programming language. It also enabled to test the smart contracts and deployed them to the blockchain. It also provided a place to develop our client-side application [21].

The following command line can be used to install Truffle with NPM

$ npm install –g truffle

5.3 Angular CLI

The client side of the application developed by using AngularJS. The purpose of Angular 6 is to create a great user experience as it runs in the browser, it is able to provide very reactive user experience. For that it needs to install the Angular CLI dependency using the NPM with following command line [22].

$ npm install –g @angular/cli

5.4 Ganache

The next dependency is Ganache, a local in-memory (virtual) Blockchain. It will give us 10 external accounts with addresses on local Ethereum Blockchain. Each account is preloaded with 100 fake ether.

5.5 Metamask

The next dependency is the Metamask extension for web browsers [23]. In order to use the Blockchain, consumers of dApp (nodes) must connect to it. It is important to install a special browser extension in order to use the Ethereum Blockchain. That's where Metamask comes in. With that, those nodes are able to connect to Ethereum blockchain with their personal account, and interact with smart contract.

5.6 IPFS API

The cost of storage on the Blockchain is extremely expensive. According to estimates [24] it costs $100 per GB of storage. If you are planned to store in Ethereum Blockchain it will cost $4,672,500. You can easily buy a 500GB hard drive for $100 in today's world. This leads to a bigger problem, when trying to store large quantities of data such as images, videos, audio and other datasets. The answer to this solution is cryptographic hashes**.** When hashing a file, it is possible to get a fixed length string that is unique to that particular file and its data. Rather than storing files, IPFS simply stores the hashes to files on series of nodes. These hashes can then be used to find the actual location of the file. A good analogy for this is inviting someone over to your house. Rather than physically moving your house to them, it have a tendency to provide them a pointer (address) to where we actually live and they come to us [25].

Chapter 6: Evaluation and Results

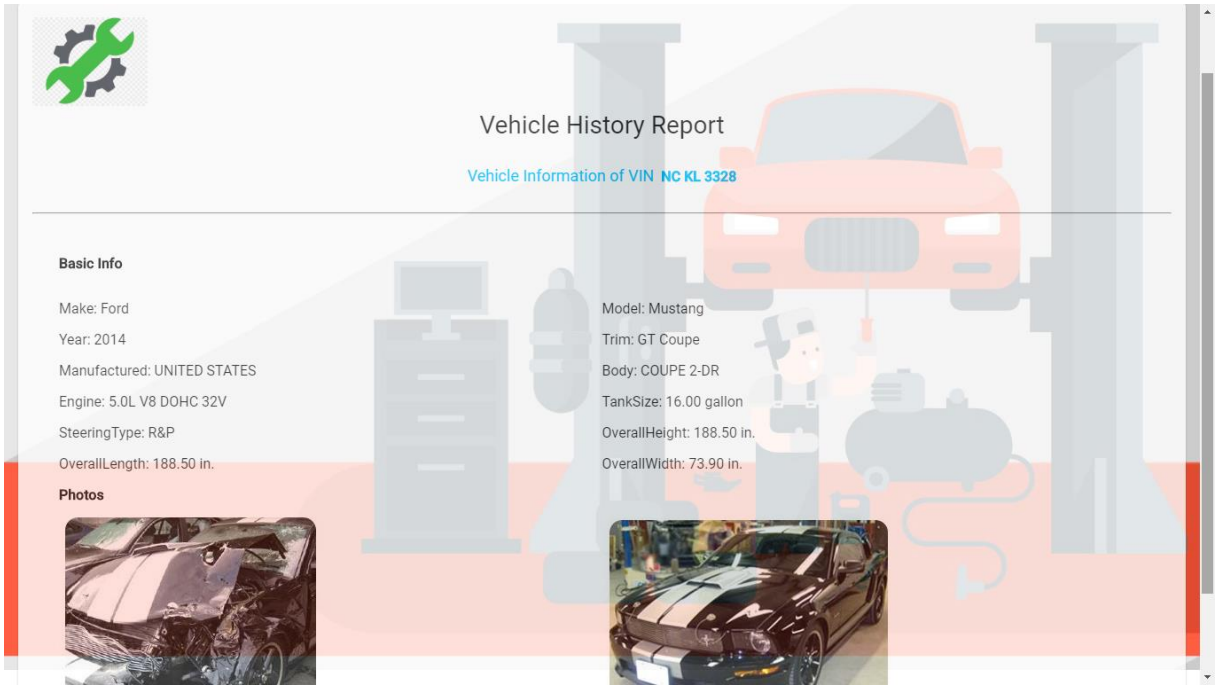


Figure 6.1 Sample Report

Application is tested with sample data entries regarding to each accessible data source. For an example the data fields associated with an insurance company may different from the data fields of a vehicle service center for a particular vehicle under the same vehicle identification number. Because of that different user interfaces will be provided by the application according to the needs of each service. By this, it is possible to identify the most relevant data fields which should add to the system for retrieving valuable data from the sources.

Finally, the buyer or consumer can view the added details, a report of a particular vehicle by submitting a vehicle identification number (VIN). That report contains all the information have on the Blockchain regarding that particular vehicle. The report will be providing an accurate reflection of a vehicle, which is sufficient enough to come up with the final decision.

Chapter 7: Conclusion and Future Work

The TRUECARE. Vehicle Record Maintenance System prototype provides a proof-of-concept system and demonstrates how principles of decentralization and Blockchain architectures could contribute to secure, interoperable vehicle record systems. Using Ethereum smart contracts it is possible to store content and orchestrate a content-access system, across separate storages owns by each data provider in Blockchain. Looking forward to continued work on the TRUECARE by demonstrating an innovative approach for integrating with data providers' existing systems through flexible API.

References

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online] Available at: https://bitcoin.org/bitcoin.pdf

[2] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," *In Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[3] Herrera-Joancomartí J. (2015) Research and Challenges on Bitcoin Anonymity. In: Garcia-Alfaro J. et al. (eds) Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. DPM 2014, QASA 2014, SETOP 2014. Lecture Notes in Computer Science, vol 8872. Springer, Cham

[4] Tikhomirov S. (2018) Ethereum: State of Knowledge and Research Perspectives. In: Imine A., Fernandez J., Marion JY., Logrippo L., Garcia-Alfaro J. (eds) Foundations and Practice of Security. FPS 2017. Lecture Notes in Computer Science, vol 10723. Springer, Cham

[5] Harm, J., Obregon, J. and Stubbendick, J. (n.d.). *Ethereum vs. Bitcoin*. [online] Available at:https://www.economist.com/sites/default/files/creighton_university_kraken_case_study.pdf

[6] Alharby, M. and Moorsel, A. (2017). A Systematic Mapping Study on Current Research Topics in Smart Contracts. *International Journal of Computer Science and Information Technology*, [online] 9(5), pp.151-164. Available at: https://airccj.org/CSCP/vol7/csit77211.pdf.

[7] Foundation, E. (2015). *On Public and Private Blockchains*. [online] Blog.ethereum.org. Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[8] Jayachandran, P. (2017). *The difference between public and private blockchain - Blockchain Unleashed: IBM Blockchain Blog*. [online] Blockchain Unleashed: IBM Blockchain Blog. Available at: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[9] Bitfury Group Limited (2015). *Part 1: Permissioned Blockchains*. Public versus Private Blockchains. [online] Available at: https://bitfury.com/content/downloads/public-vs-private-pt1-1

[10] Peterson, K., Deeduvanu, R., Kanjamala, P. And Boles, K. (n.d.). [online] Healthit.gov. Available at: https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf

[11] Ekblaw, A., Azaria, A., D. Halamka, J. and Lippman, A. (2016). *A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data*. [online] MIT Media Lab, Beth Israel Deaconess Medical Center: IEEE. Available at: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf

[12] Quotidien Finance Digitale, Crypto Finance Daily News. (n.d.). *The five major use cases for financial blockchains*. [online] Available at: https://www.finyear.com/The-five-major-use-cases-for-financial-blockchains_a35655.html

[13] Custodio, M. (2018). *Blockchain Gifting App Launched By Sri Lanka's Sampath Bank - BlockTribune*. [online] BlockTribune. Available at: https://blocktribune.com/blockchain-gifting-app-launched-by-sri-lankas-sampath-bank/

[14] Eservices.motortraffic.gov.lk. (n.d.). *Online Registered Vehicle Information Service - Department of Motor Traffic - Sri Lanka*. [online] Available at: http://eservices.motortraffic.gov.lk/VehicleInfo/home/

[15] ikman.lk. (n.d.). *New and used Vehicles for sale in Sri Lanka | Ikman*. [online] Available at: https://ikman.lk/en/ads/sri-lanka/vehicles

[16] Usrv.io. (n.d.). *USERVICE - Global Decentralized Blockchain Platform For Automotive Industry*. [online] Available at: https://usrv.io/en-US/whitepaper.pdf

[17] carVertical Reports. (2018). *carVertical Reports – Global Car VIN Decoder*. [online] Available at: https://www.carvertical.com/

[18] Vinchain.io. (2018). *VINchain DECENTRALIZED VEHICLE HISTORY*. [online] Available at: https://vinchain.io/files/VinChainWhitePaperEn.pdf

[19] Carblox.io. (2017). *Carblox - The World's First decentralized vehicle multi-platform on blockchain.* [online] Available at: https://carblox.io/doc/Carblox_Whitepaper.pdf

[20] Ethereum.org. (n.d.). *Ethereum Project*. [online] Available at: https://www.ethereum.org/

[21] Truffle Suite. (n.d.). *Truffle Suite | Documentation | Truffle | Overview*. [online] Available at: https://truffleframework.com/docs/truffle/overview.

[22] Angular.io. (n.d.). *Angular*. [online] Available at: https://angular.io/guide/quickstart

[23] Metamask.io. (n.d.). *MetaMask*. [online] Available at: https://metamask.io/

[24] Omaar, J. (2017). *Forever Isn't Free: The Cost of Storage on a Blockchain Database*. [online] Medium. Available at: https://medium.com/ipdb-blog/forever-isnt-free-the-cost-of-storage-on-a-blockchain-database-59003f63e01

[25] Health, C. (2018). *Learn to securely share files on the blockchain with IPFS!*. [online] Medium. Available at: https://medium.com/@mycoralhealth/learn-to-securely-share-files-on-the-blockchain-with-ipfs-219ee47df54c