Blockchain-based Forgery Resilient Vehicle Registration System

Leila BENAROUS1, Benamar KADRI2, Ahmed BOURIDANE3, Elhadj BENKHELIFA4,5

1 STIC Laboratory, University of Abou Bekr Belkaid, Tlemcen, Algeria.

2 STIC Laboratory, Faculty of Technology, University of Abou Bekr Belkaid, Tlemcen, Algeria.

3 Department of Computer and Information Sciences, Northumbria University, Newcastle, UK.

4 Cloud Computing and Applications Research Lab, School of Digital Technologies and Arts, Staffordshire University, UK

5 School of Engineering, Arts, Science and Technology, University of Suffolk, Suffolk, UK

Abstract—

Vehicle registration system is an essential process for recording the transfer of vehicles’ ownership. Most of existing systems are administratively centralized, semi-automated, and rely on a formal proof provision. While these systems were initially proposed to preserve the owner’s rights, prove their ownerships and legally record used motor-land transportation means. Unfortunately, these systems also allow the registration of illegally smuggled and stolen vehicles. This is mainly due to inefficient verification methods, long heterogeneous administrative procedures or to corrupt individuals at the motor registration departments. Regardless of the reasons, the fact that the system allows such cases hints on a faulty design. Current systems are centralized and do not perform a double checking until a report is made, which means that this occurs after the fact of registering the forged vehicle. Noting that these reports are not always fruitful, if the vehicle’s proofs were properly injected in the system. This paper proposes a system that is transparent where every vehicle registration is done under everyone’s watchful eyes. No denying, no alteration and no unauthorized injection may occur. The proposed system saves the owner’s information and the vehicle’s descriptions in transactions saved in a public blockchain where all the history of purchases regarding the subject vehicle may be tracked. The use of blockchain technology is motivated by its security, transparency and traceability as well as its immutability and scalability in terms of users. We have evaluated our proposed solution in terms of its security and resiliency to the injection of forged transactions by the elaboration of the attack tree. The results show our solution’s superiority when compared against current registration system.

Key-words— blockchain, vehicle registration systems, forgery-resilient systems, distributed systems.

1. Introduction

Vehicle registration systems are currently centralized and the department of the motor vehicle is the sole authority that is able to add/alter vehicle records. Although, individual users may read their own records either electronically or in printed format, they have no access to other users’ records. This is a security measure to ensure the confidentiality of records and prevents unauthorized individuals from altering them. However, this reduces the transparency and gives the chance to dishonest employers to abuse their authority and inject fake records to the system to register stolen and smuggled vehicles legally. This is difficult to detect especially if the vehicle is stolen from a county/country and registered in another. It becomes even harder as the records get older and the vehicle is purchased many times. When a vehicle is reported to be stolen to the police, it triggers an investigation to find it and identify the people involved. This operation is costly in terms of efforts made by police officers, it is time and money consuming; moreover, restoring the stolen vehicle may not be always possible. Since the systems are independent, in the majority of cases, the vehicle may even be registered legally in another county/country. Detecting such cases is difficult and sometimes impossible, because of the lack of cooperation with the investigation. Other possible reasons include delays in reporting the vehicle to the general motor department, absence of reports or lack of reports sharing between different departments, cities or countries. According to [1] the rate of recovered stolen vehicles in the US in 2017 is 59.1% from 773,139 reported theft cases. Increasing the rate of restoring vehicles depends on the fast reporting process, the broadcast of these reports which will help in reducing the legal registration of smuggled vehicles rates. For these purposes, Asset guard created a website to report stolen vehicles, send tips, or search a stolen vehicle. This website have helped in recovering 12776 vehicles [2]. It is noteworthy, that the legal registration of the stolen vehicles is a serious issue that highlights the faulty design of the currently used system that allows such cases to occur, without being detected.

The current system is paper-proof based. In what follows, we continue explaining its functionality basing on the procedures of vehicle registrations in New York state-USA [3]. We first resume the essential needed documents to register a vehicle which are: a filled vehicle registration application form, a proof of ownership, a proof of inspection and sale tax clearance, assurance card, identity proof and fees payment receipt.

The provided documents are stored in records at the department database system and archives. After the registration is done, the owner gets his/her vehicle registration certificate. If the vehicle is new or sold in another state, a new matriculation number is assigned to it as well. Noting that in case of a change in personal details (name and address), the user has to request a certificate update by providing the necessary proofs, filling update forms, and paying update fees. The same applies when the certificate expires, gets stolen or ruined, a renewal request is submitted accompanied with necessary documents and paid fees receipt [3].

Often each country and in many cases even each city of a county has its own vehicle registration system. These systems are often independent, which means that vehicle registration in a new county/country requires repeating the same administrative procedures. It also means that checking the vehicle state takes a longer time and follows some administrative protocols as well. This implies that the probability of forging records is higher. The vehicle registration system database is, usually, centrally managed in each county where only the vehicle registration department has access and thus it is privately kept. This ensures the confidentiality of the records, preserves the privacy of the users, and potentially, enhances the security against external attacks that aim to inject fake records. From a technical point of view, the current system suffers from protecting against the internal attacker’s fake record injection, moreover, these centralized systems suffer from the risk of a single point of failure. Besides to, the excessive administrative procedures and the high fees involved per each registration, renewal, or update as well as disparate systems between different counties which delays the verification of stolen vehicles records, not to forget that the system’s confidentiality prevents the forgery’s early detection. The current systems rely mainly on proof provision, paperwork, and reliability of individuals working in the vehicle registration department.

The emergence of blockchain technologies offer an alternative solution to vehicle registration systems with high levels of security, transparency, immutability, scalability, and design flexibility. The proposed blockchain solution in this paper is formed of three permissioned blockchains, for the customs, the state, and the manufacturer. The proposed systems records the vehicle’s purchase and registration history, which allows for the verification and the confirmation of the vehicle’s ownership and prevents the registration of forged or stolen vehicles. It also prevents the injection of fake ownership records and any illegitimate human manipulation of records. In the proposed blockchain-based system, the user provides identity proof to obtain certified keys, which are used to register in the blockchain. Upon a successful registration, the user may record the transactions regarding the exchange of a vehicle in the blockchain using the pair of certified keys. The seller and purchaser create and confirm the transaction (mutual agreement) and the authorized peers validate it and add it to the blockchain. No extra paper proofs are needed. Therefore, our proposed system is automated and publicly available.

In short, our proposal is a distributed secure system that is immutable, public and transparent. It eliminates the need to provide paper-proofs to register the vehicle transfer between individuals. The purchase and registration of the vehicle ownership transfer is done by the concerned parties (sellers and purchasers) themselves using the certified keys. the proofing and validations of these transactions are done by authorized peers under the watchful eyes of all the system peers. It requires only the verification of a valid chain of ownership to proof that the vehicle’s seller is its rightful owner and that the vehicle is being sold to the interested purchaser solely (no double simultaneous purchases to the same vehicle). Most importantly, the system is designed to prevent the legal registration of forged vehicle purchase, thus, it is forgery resilient.

The paper is organized as follows: Section 2 defines the blockchain technology, how it works, its types, applications, and implementations. Section 3 demonstrates the proposed solution. Section 4 analyses its security, illustrates its views and presents its advantages. Section 5 concludes the paper.

1. Blockchain

The blockchain technology gained enormous attention after it was introduced by Satoshi Nakamoto back in 2008 [4] when introducing the bitcoin. Although the two concepts are often related, we should not confuse them. A blockchain (the public ledger) is a distributed database of records of all transactions that have been executed. Each transaction is verified by the consensus of the majority of the participants in the system. Inserted transactions cannot be altered nor erased once added to the blockchain [5].An illustration of the blockchain types is found in Table 1. Blockchain is also considered as one of the decentralized forms of Cloud computing but with a fundamentally different governance [36, 37]

A blockchain transaction is an interaction between users to change the ownership of a physical or a digital asset [6]. The content of the transaction depends on the blockchain purpose and implementations but in general, it contains the sender’s address (or another relevant identifier), the sender’s public key, a digital signature, the transaction inputs, and outputs. The input of the transaction specifies the list of assets to be transferred and a reference to its origin (source). The output of the transaction specifies the amount of transferred asset, the identifier of the new owner(s), and the conditions that must be satisfied to spend (or transmit) this asset or value [7].

The users send candidates’ transactions to the blockchain via its software. These pending transactions are then propagated to the rest of the blockchain. They are added to the blockchain when a block containing it is successfully created and published. The block contains two sections, the header section contains the metadata of the block and the data section containing the valid transactions [8]. The blocks are chained together by the use of the hashes, each block contains a hash of the previous one forming a chain of blocks or the blockchain. If a block is altered or a new block is injected a different hash is extracted. Therefore, the block is rejected.

We mentioned before that the transactions are validated by the consensus of peers. In a matter of fact*,* the consensus process differs from one blockchain to another depending on the type and implementation. Some of the existing models are proof of work, proof of stake, round-robin, proof of authority, proof of elapsed time [9].

**Table 1: Blockchain types**

|  |  |  |  |
| --- | --- | --- | --- |
| **Blockchain** | **Public** | **Private** | **Consortium** [10] [11] |
| **Nodes** | Peers | Creator, peers | Creators, peers |
| **Validators** | All | Creator node | Selected nodes |
| **Permission** | Permission less | Permissioned | Permissioned |
| **Consensus** | PoW or PoS | Verification and insertion | Agreement protocol |

The Bitcoin [12], Ethereum [13], and Monero [14] are just a few of the many applications that use blockchain technology. Other applications include property registration such as: the residential rental system in [15] and land registration in [16]. The E-government (paperless) [17]. The health-care services [18]. For security purposes such as PKI [19], identity management [20], secure vehicle social networks [21] or mobile fingerprint verification and automatic log-in platform for the Internet of Things (IoT) in [22] and other IoT applications in [23] [24] [25] [26]. We cited a few examples of applications among the various existing. As the researchers and developers are directing their interest toward decentralized and distributed applications that replace the central databases. This interest leads to the appearance of new concepts such as the internet of blockchains and the blockchain of blockchains [27] [28] [29].

1. Proposed method

This section describes the proposed system based on the blockchain of blockchains vehicle registration architecture. To help the readers understand the strategy employed we first need to explain the possible cases of a vehicle purchase and how does it affect its registration. Then, we continue with the extraction of our system actors. Later, we specify and justify our chosen type of blockchain, followed by the general description of the system.

1. *Vehicle purchase and system actor’s extraction*

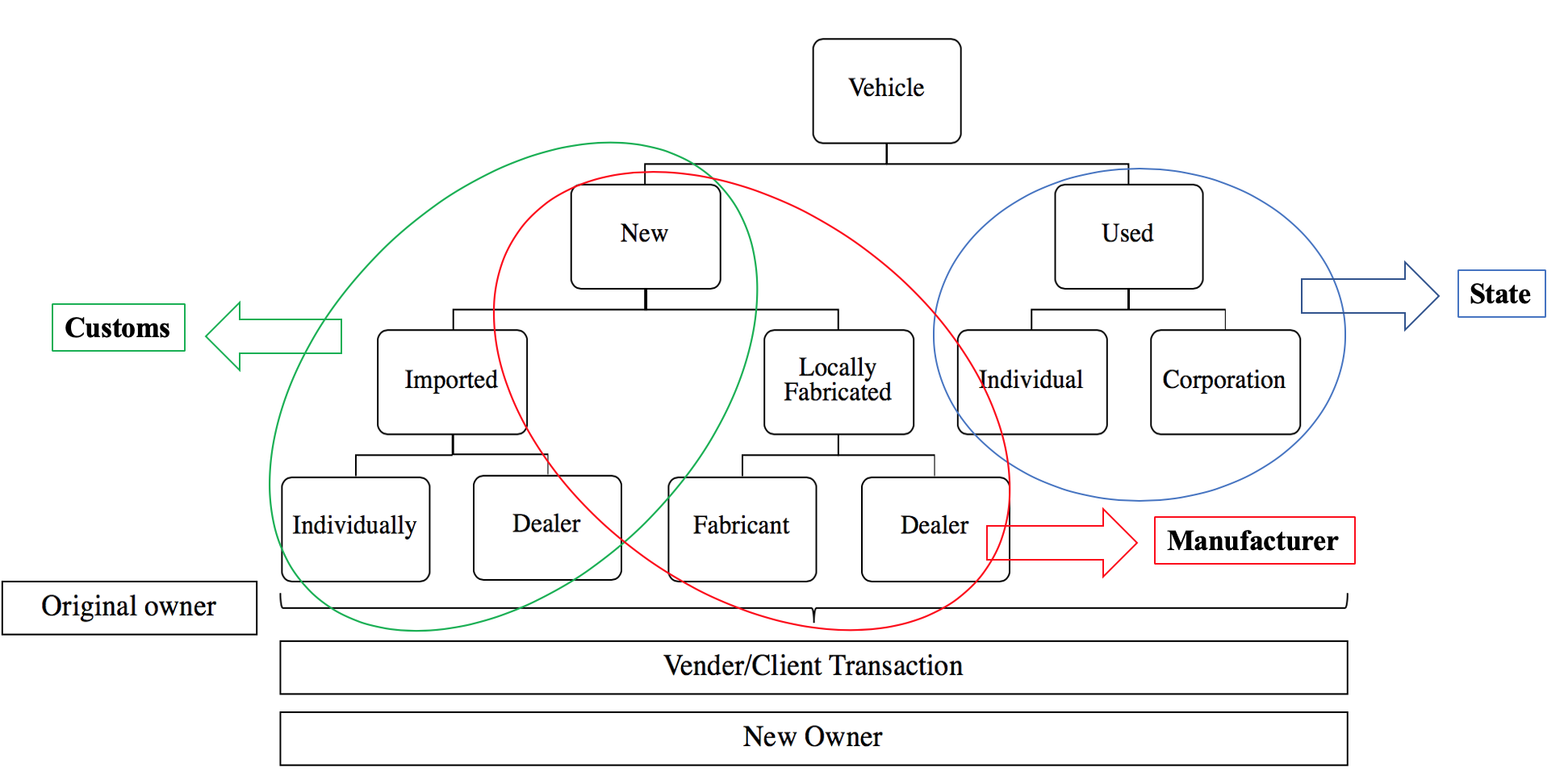
The purchase of a brand-new vehicle is done either from the manufacturer of the vehicle (local or imported) or from a dealer of new vehicles. As for the second hand (used) vehicles, they can be either purchased from individuals or corporations as illustrated in Figure 1. From a technical point of view, this means that the vehicle purchase records are stored by three authorities:

* if the vehicle is second hand, then this mean that it is already registered by the state general motor department (GMD)
* if the vehicle is brand-new then it is already recorded on the manufacturer system, and,
* if it is imported, then it must have been registered by the customs upon entering the country.

Therefore, apart from the end-users purchasing the vehicle, the customs, the state representatives, and the manufacturers are the main actors of our system. Another principal actor is the certifying authority (CA) which is needed to generate certified keys for the end-users to use in registering the blockchain system. We explain briefly the roles of these actors:

* ***Manufacturers*:** manufacturers record their fabricated vehicles in the manufacturer blockchain (BC).
* ***Certifying authority (conventional PKI):*** it links the public key used in the blockchain to its user. The certificate proofs the ownership of the public key and links it to the real user with valid and correct information such as name, date of birth, address, and other data (identity proof are needed for the public key to be generated). If the network node is not a physical user but an organization, the certificate would contain other identifying information.
* ***Customs:*** maintains in its blockchain the imported vehicles.
* ***State vehicle registration authority:*** each county has a set of registered vehicles saved in the state blockchain.
* ***End-users:*** they are the purchasers and the sellers of the vehicle.

Noting that regardless of the node’s type: individual user, organization, manufacturer, customs, or state. They are represented by a public key in the blockchain.



**Figure 1:** Vehicle purchase scenarios and Actors extraction for the Blockchain system.

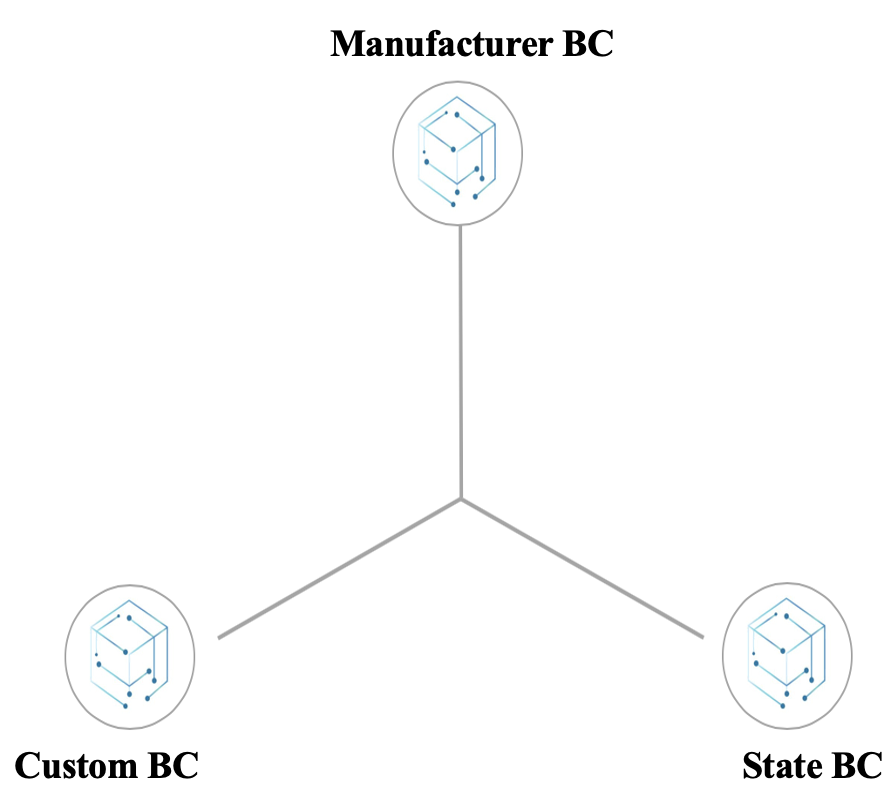
1. *Choice of Blockchain*

We designed the vehicle registration system over blockchains because of their security and their effectiveness in preventing data alterations. As we clarified earlier, this technology ensures the transparency and immutability which are the two characteristics we are earnest to add to the vehicle registration system. While the blockchain technology has various implementations and types depending on the different use cases, our system is designed as a blockchain of permissioned blockchains maintained by the three main actors, which are the state, the customs and the manufacturers. We considered this scheme after analyzing the system’s actors and functionalities, besides the study of the different purchase scenarios. Thus, unlike digital currencies, it cannot be created, mined or awarded by the system peers. On the contrary, every transaction records an exchange of a real vehicle represented by its unique VIN. Therefore, an extra control is fundamentally needed to prevent the block injection and creation of fake records of non-existing vehicles in the blockchain. In addition, to ensure the transparency and availability, the users are allowed to read the content of the blockchain and to download it. To balance the load and render the system flexible, the users may initiate and confirm transactions. This emulates the mutual agreement between the purchaser and seller to record the exchange of the vehicle on the blockchain. This mutual agreement helps the authorized peers (validators) to validate the transactions and add it to a block. Noting that the block creation and validation are exclusive tasks for the authorized peers. Also, although the blockchains are permissioned, they are not independent. In a matter of fact, they are connected forming the blockchain of blockchains concept. The authorized peers representing the main actors are connected together through secure channels where they exchange the blocks to be validated and chain them to the corresponding blockchain upon validation. The system is illustrated in Figure 2.

1. *System Description*

The vehicle can be purchased in many ways. Consecutively, the registration process depends on the purchase case. In this section, we first describe the proposed system, then, explain how does the registration of a vehicle happens for each purchase scenario.

Since, our system is a blockchain of permissioned blockchains each blockchain is maintained by an authority that selects a set of validator nodes. The blockchains are all connected together (see Figure 2). The authority and its preselected set of validators have the write-rights, while the rest of the nodes have the read-rights only. The blockchain of blockchains has a set of coordinators and validators that would check the validity of each field in the transaction and would publish the valid blocks. Moreover, to prevent the abuse of power and the record injection possibility, every block is initially signed by the generating authority then is signed by one of the maintainers of the other two blockchains of the network. In other words, each block is signed by three peers representing the maintainers of each blockchain. In that way, the false record injection may not occur. Also, because everything is public under the watchful eyes of all the network peers, transparency and immutability are ensured.

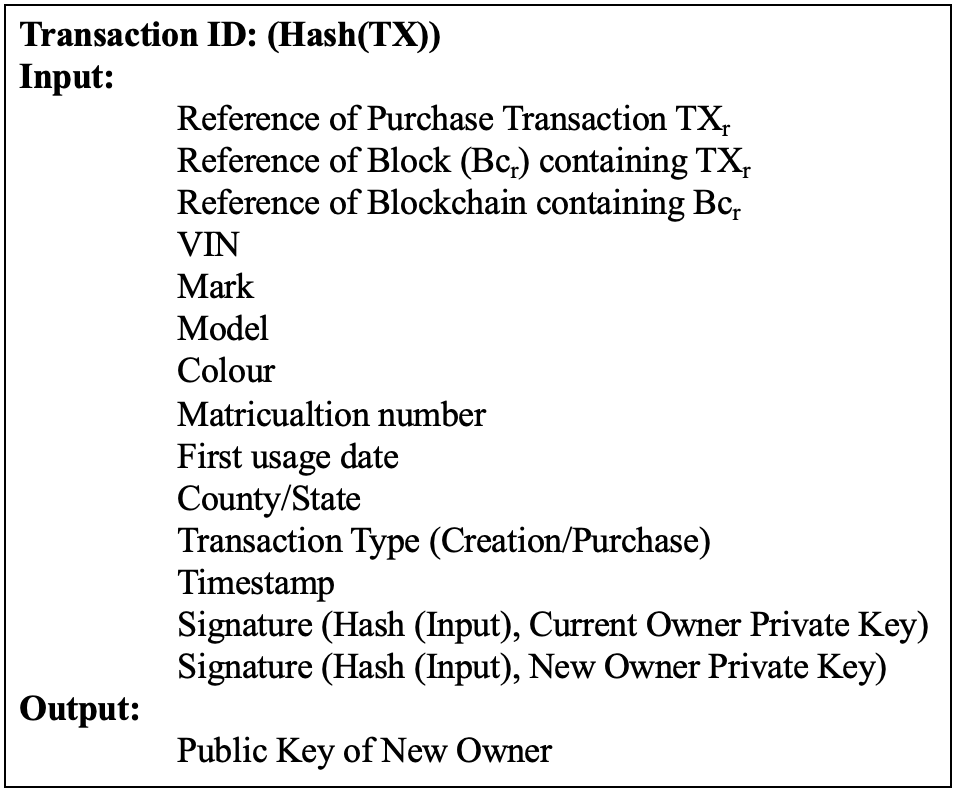


**Figure 2:** Blockchain of Blockchains Vehicle Registration System (BC-VRS)

Before we illustrate the vehicle registration in our proposed framework (***BC-VRS***), we ought to first clarify the following cases:

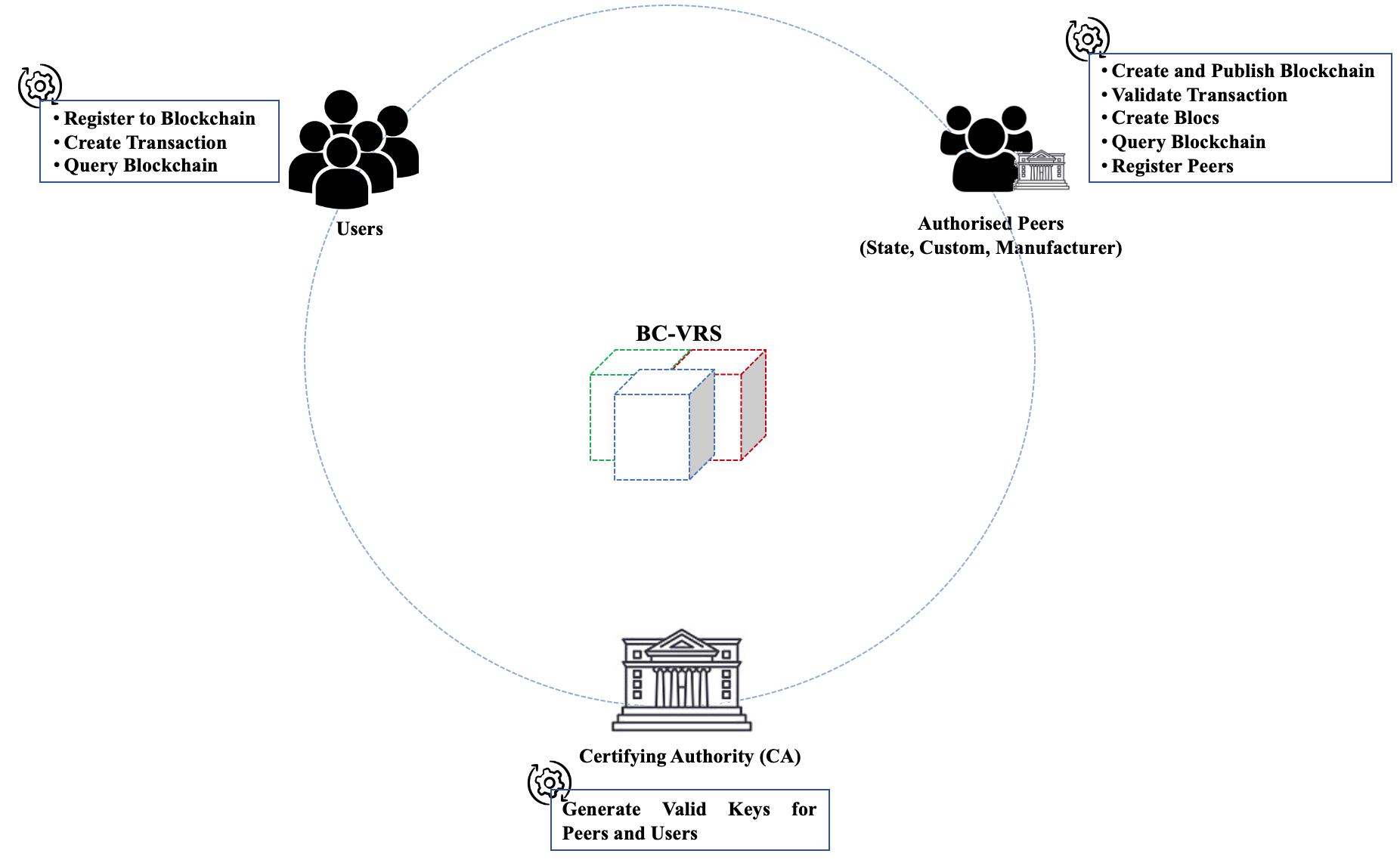
* The vehicle may be purchased from the manufacturer if it is brand new, in this case, the purchase transaction registered in the state blockchain must refer to the vehicle transaction in the manufacturer blockchain.
* The vehicle may also be imported, in that case, the purchase transaction in the state blockchain refers to the custom blockchain recording imported vehicles, which in its turn refers to the manufacturer transaction if it is a new vehicle or the original country state BC if it is used one.
* The vehicle may be bought from individuals or corporations if it is a used one, where the registration transaction of purchase refers to the proof of ownership transaction (original purchase transaction) in the state blockchain.
* The registration to the blockchain framework is done using the certified pair of public/ private keys. Therefore, it is fundamental that each user registers him/herself to the certifying authority providing identity proofs to obtain the certified keys prior to their usage in the blockchain. Also, it is essential for the user to back up and safe-guard his/her private keys, as the owner of this key may register selling and purchasing operation of the vehicle into the blockchain. In other words, the owner of the key is the owner of the vehicle it is registered with it. In case the key is destroyed or stolen, it must be promptly reported to the certifying authority to be revoked and prevent its misusage.
* The vehicle is identified by its unique VIN (Vehicle Identifier Number) in our framework.

Taking the above-cases into considerations, we proposed one unified type of transaction for the three permissioned blockchains forming our framework. The transaction is composed of three parts, the first is its address or ID which is its hash value, the second part is the input of the transaction and the third part is its output. The input of the transaction specifies the vehicle’s characteristics and origins (source), it also specifies the transaction type (creation or purchase). The output part specifies the new owner of the vehicle. The structure of the vehicle registration transaction is illustrated in Figure 3. Noting that the transaction fields match the fields required by the current vehicle registration systems.



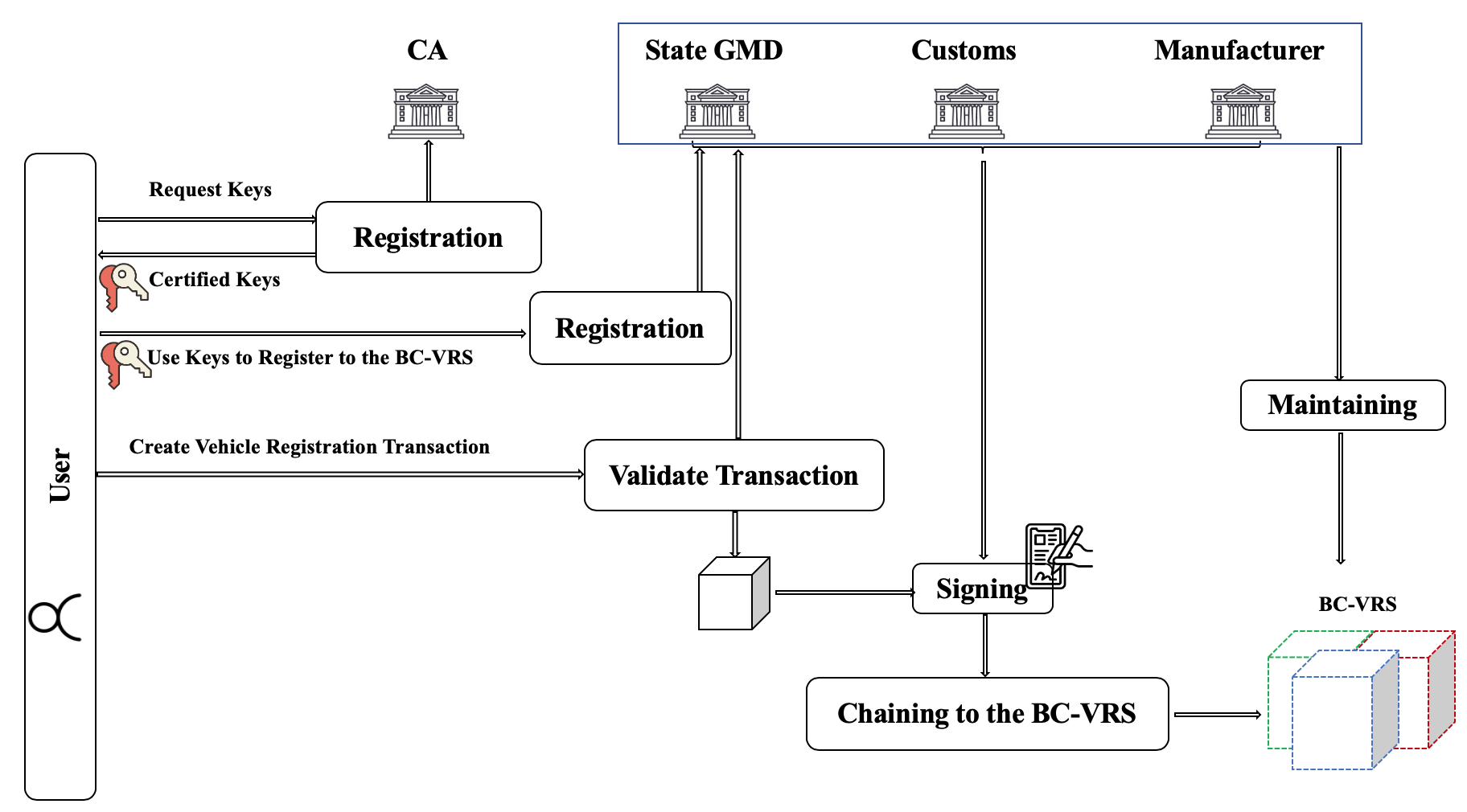
**Figure 3:** Vehicle registration transaction in the state BC

Figure 4 illustrates the interacting peers with the blockchain-based vehicle registration system (BC-VRS) along with the processes executed by each peer. The authorized peers are the maintainers of the blockchain, the only nodes allowed to validate the transactions, create blocks, and register users. The end-users may create/confirm transactions and query the blockchain: search, download, and read the blockchain content. The certifying authority (CA) generates certified keys for all the network peers (authorized nodes and end-users).



**Figure 4**: Processes Executed by each node with the blockchain vehicle registration system BC-VRS

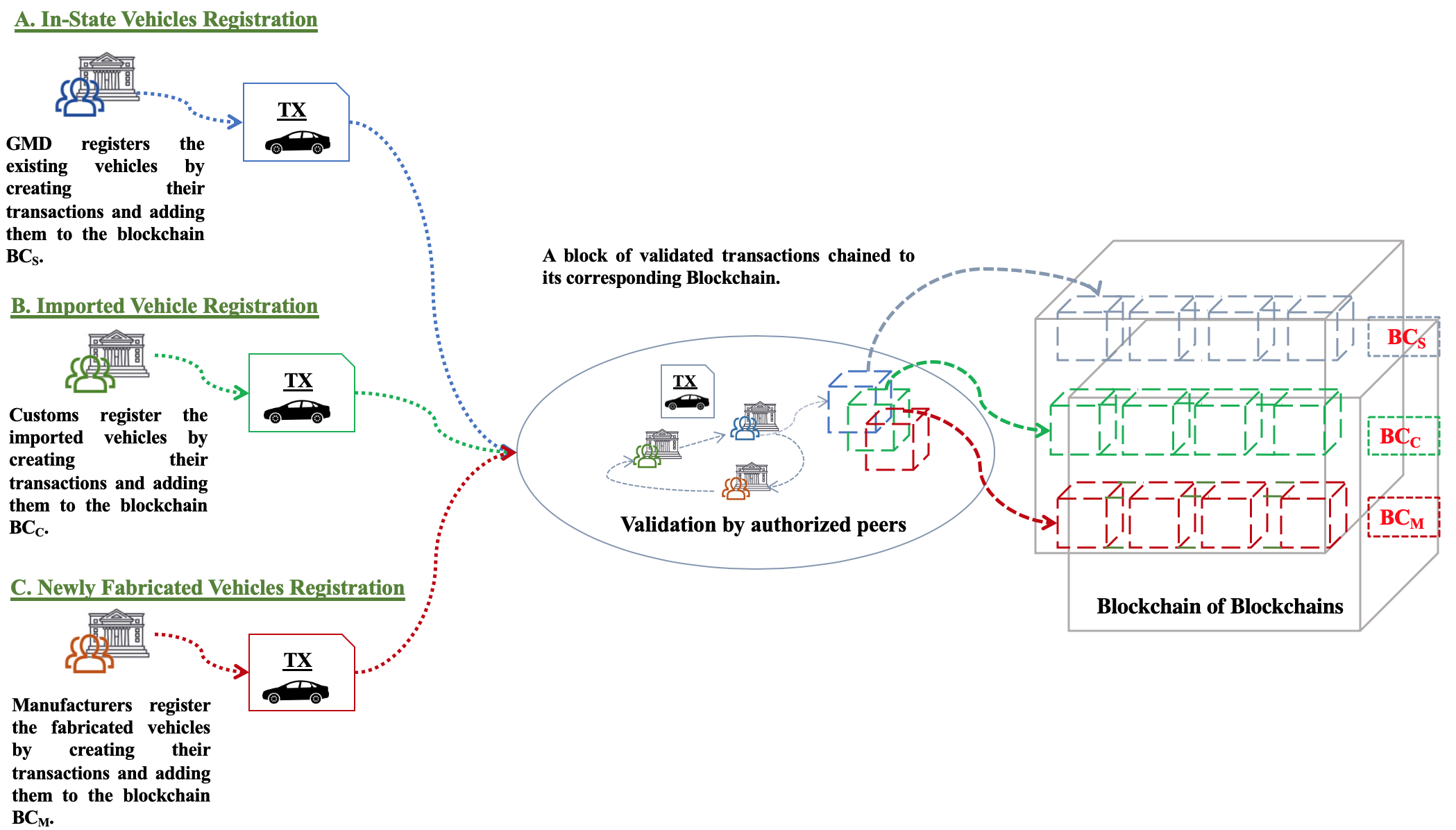
Since the blockchain is permissioned, only permitted nodes may validate the transactions, as well as, create, validate and chain the blocks. These nodes are representative of the states, the customs and the manufacturers. The vehicle owners may initiate the creation of the registration transactions. However, these transactions are in pending status until they are validated by the authorized peers. Noting that the block containing the valid transactions ought to be signed by the representatives of the three composing blockchains as illustrated with Figure 5. To use our system, the user must first register to the CA to obtain a pair of certified keys which will be used to subscribe to the blockchain system. To register the purchase of a vehicle, the user creates a transaction that will be validated by the state-authorized peer and inserted in a block. The block is signed by the representative of the three authorized peers (state, customs, manufacturer) and chained to the corresponding blockchain of our system (State Blockchain). The validated block is published to the network peers as well.



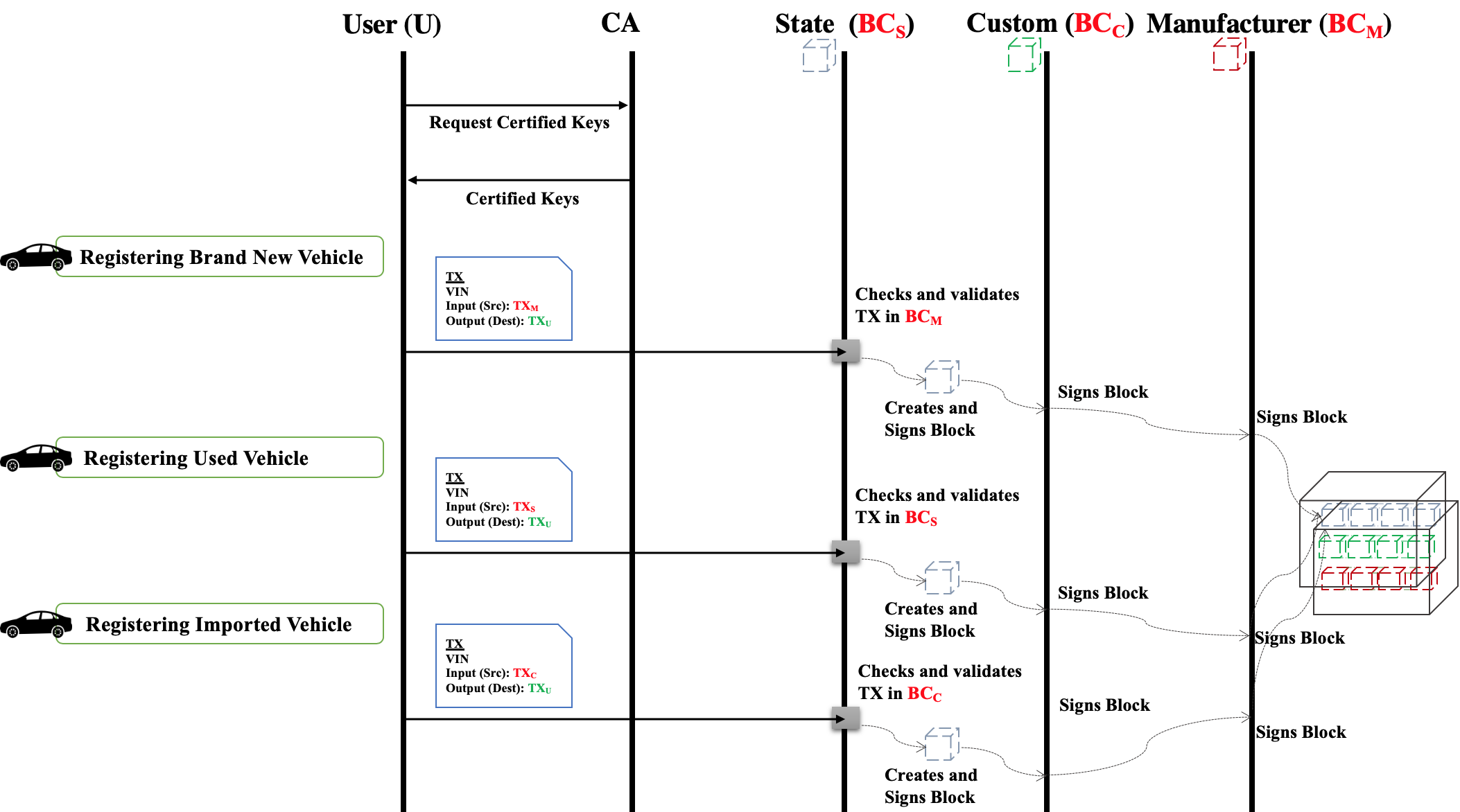
**Figure 5**: Description of the vehicle registration in our system.

Figure 6 explains the genesis block creation in each blockchain where the manufactured, imported and used vehicles are registered. The state blockchain genesis blocks contain all the currently registered vehicles. It is initiated by the general motor department. The users present their certified keys to the registration department to create transactions recording ownership of the user to the subject vehicle. The custom blockchain contains initially all the imported vehicles, while the manufacturer’s blockchain contains all the fabricated vehicles. Noting that the manufacturers and customs create the registration transaction of imported and fabricated vehicles stating themselves as the new owners in the transaction output. The three blockchains are continuously updated whenever a new vehicle is fabricated, imported, or purchased. The registration of the future vehicle purchases transactions refers to the created transaction existing on the genesis blocks of the blockchains and in general to a past existing transaction. The referral to a source transaction is done by referring to its containing blockchain, then block. i.e. the source transaction is identified by the triplet (Blockchain ID, Block ID, Transaction ID).

Figure 7 highlights the different purchase scenarios using our framework. We distinguished the three possible cases. The first is the purchase of the brand-new vehicle from the manufacturer, in that case, the purchase transaction refers to the source transaction in the manufacturer blockchain. The second is the purchase of used vehicles where the source transaction is registered in the state blockchain. The third is the purchase of imported vehicles where the purchase transaction refers to the custom blockchain.

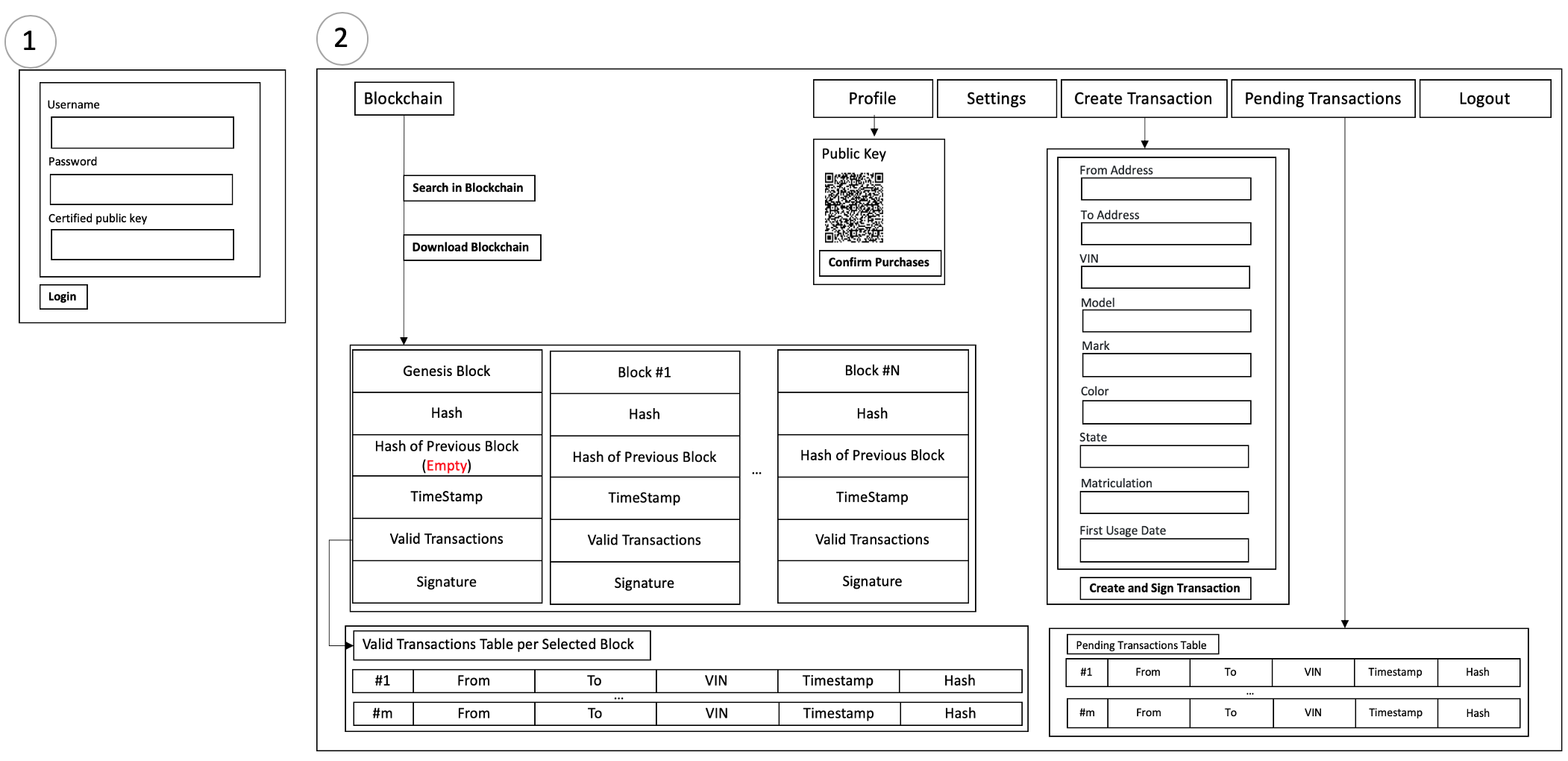


**Figure 6**: Creation of genesis blocks containing registered vehicles.



**Figure 7:** Different cases of vehicle registration using our Proposed framework.

To better illustrate the system’s functionality, Figure 8 depicts the system’s template views, which is the interface the user will be interacting with while using our system. The user may view the blockchain content, its blocks and valid transactions. S/He may search in the blockchain using the vehicle’s VIN and may also download the blockchain. The user may confirm transactions if s/he is a purchaser and create transactions if s/he is a buyer of a vehicle. s/he may also view the pending transactions. To facilitates the exchange of keys we saved them as Qcodes. Noting that the creation of transaction and their confirmation is only possible for logged in users. The authorized peers have extra functions in their views such as the transaction validation, block signature and subscription of users.



**Figure 8**: Template of our system's view

Our solution is based on the transactions’ creation and validation processes. While the transaction creation process is initiated by the user selling the vehicle, the purchaser ought to confirm by signing the transaction. Therefore, our system is based on the execution of the three Algorithms 1, 2 and 3. Before we explain our Algorithms, Table 2 explains what each notation means

**Table 2**: Notations

|  |  |
| --- | --- |
| **!** | Negation operation, |
| ***&&*** | AND operator. |
| BC-VRS | Blockchain of registered vehicles |
| Blc | A block containing valid transaction |
| BLOCK-SIZE | The predefined size of the block in terms of number of valid transactions within it. |
| ChainBloc(blc, BC-VRS) | Sign the block and chain it to the blockchain. |
| ConfirmTX(VIN, PKv-p, Pkv-o) | Confirms the purchase transaction, the purchaser signs the transaction to confirm that s/he is the intended buyer and that the transaction is authentic and that s/he agrees to be part of it. |
| CreateBloc(TX) | Creates a block containing the valid transaction if no pending block exist. If a block exists then add transaction to the pending block. |
| CreateTX(VIN, PKv-p, Pkv-o) | Creates a transaction as illustrated in figure 3. |
| *Double-spending(BC-VRS, VIN)* | Checks if the vehicle VIN is found or not in two Inputs of transactions simultaneously. |
| *IsOwner(BC-VRS, VIN, PKv-o)* | Checks if the vehicle VIN is owned by the user having PKv-o. This is done by checking the input section signature of the vehicle source transaction using the owner’s public key. Also, that the user is still the owner of this vehicle (did not sell it before making the current transaction) |
| IsValid(PK) | Checks if the Public Key PK certificate is valid (fresh and non-revoked) |
| PKv-o | Public Key of the vehicle owner |
| Pkv-o | Private Key of the vehicle owner |
| PKv-p | Public Key of the purchaser |
| TXp | The pending transaction of the vehicle |
| TXv-src | The source transaction of the vehicle |
| ValidHash(TX) | Checks if the Hash of a signature is correct. |
| ValidSIG(TX, PK) | Checks if the digital signature is correct. |
| VIN | Vehicle Identification Number |

Algorithm 1 explains the process executed by the owner of the vehicle to initiate the registration of the purchase transaction. Before initiating this transaction, the purchaser interested to buy the vehicle sends his/her public key to the owner. The unconfirmed transaction is sent to the purchaser so as s/he checks the transaction’s content as explained in Algorithm 2 and validates it by signing it.

|  |
| --- |
| **Algorithm 1:** Transaction Creation |
| ***Begin***  ***If*** (IsValid(*PKv-p*)  CreateTX(VIN, PKv-p, Pkv-o)  ***endIf***  **End.** |

Algorithm 2 explains the process executed by the purchaser to confirm the purchase transaction of the vehicle. The purchaser needs to check that the vehicle is not being acquired by another user simultaneously and that the current owner is the real owner of the vehicle. Once the verification is done, the purchaser (new owner) of the vehicle signs the transaction to confirm the purchase, this confirmation allows the authorized peer to know that the purchaser is aware and agrees to the transaction content. The created transaction is in a pending state until the authorized peers validates it by adding it to a block.

|  |
| --- |
| **Algorithm 2:** Transaction Verification and Confirmation |
| ***Begin***  ***If*** (!double-spending(BC-VRS, VIN) **&&** IsOwner(BC-VRS, VIN, PKv-o))  ConfirmTX(VIN, PKv-p, Pkv-o)  ***endIf***  **End.** |

The transaction validation process executed by the authorized peers is explained in Algorithm 3. An authorized peer checks that both the purchaser and the seller are using valid keys, that no double-spending occurs, that the owner is who s/he claims to be, that the purchaser agrees to the transaction (valid signature) and that the transaction is not tampered with. Once these tests are satisfied, the transaction is validated by inserting it into a block which will be chained to the blockchain. The created block is signed by three representative peers of the three composing blockchains to prevent the alteration and injection of any fraudulent transaction.

|  |
| --- |
| **Algorithm 3:** Transaction Validation by Authorized Peers |
| ***Begin***  ***If*** (IsValid(*PKv-o*) **&&** IsValid(*PKv-p*) **&&**  !double-spending(BC-VRS, VIN) **&&**  IsOwner(BC-VRS, VIN, PKv-o) **&&**  ValidHash(TXp) **&&** ValidSIG(TXV-src,PKv-o) **&&**  ValidSIG(TXp,PKv-p) **&&** ValidSIG(TXp,PKv-o))    Blck=CreateBlock (TXp)  ***If*** (Blck.size()=BLOCK-SIZE)  ChainBlock(Blck, BC-VRS)  ***endIf***  **End.** |

1. Analysis
2. *Security Analysis*

Our proposed solution offers more security and transparency. It is achieved by the publicity of ledgers. Every transaction may be verified by any node at any time. Every addition of a block is under the supervision of all users which may have downloaded a recent version of the blockchain. The forgery of transactions to register a vehicle is no longer possible unless all of the block validators and network peers are bribed forced to accept these transactions.

To evaluate the security of our proposal against currently used one, we have developed an attack tree for each system. In Figure 9 we illustrate the attack tree of the current vehicle registration system while Figure 10 presents the attack tree for our proposal. The purpose of this comparative analysis is not only to prove that our system works better, but also to allow the reader to observe and understand better how each system works and what are the vulnerabilities of each system that may be exploited by the attacker to achieve his/her aims. Besides the possibility to execute each attack against both systems. To do so, we calculated the probability of success for these attacks and the probability of achieving our highlighted aim which is to register a forged vehicle successfully without being detected using each system. To do the calculation, we have used the standard grade chart in Table 3 [30] [31]. We calculated the probabilities of occurrence (PO) demonstrated in Tables 4 and 5 using formula (1) [30] [31]. The probability of achieving the final objective is calculated from down to top (leaf to root) where the OR operation is translated by (+) and the AND is replaced by (\*).

**Table 3:** Standard Grade Chart [30]

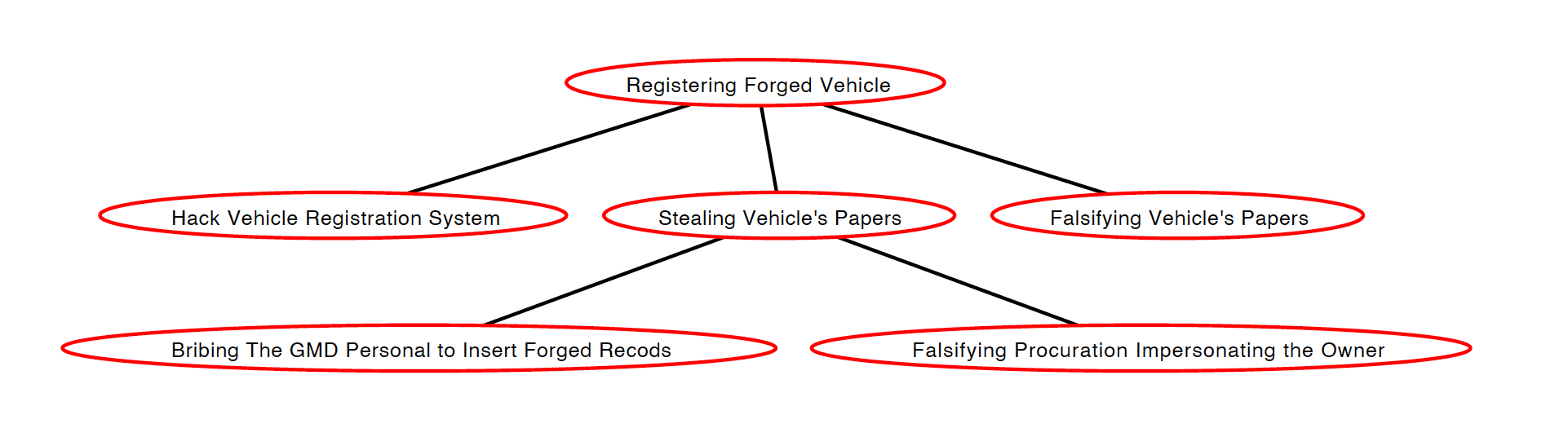
|  |  |  |  |
| --- | --- | --- | --- |
| **Grade** | **Attack Cost (Cst)** | **Technical Execution Difficulty (Exed)** | **Detection Difficulty**  **(Detectd)** |
| 5 | Quite Costly | Quite Difficult | Quite Difficult |
| 4 | Costly | Difficult | Difficult |
| 3 | Moderate Cost | Mediate | Mediate |
| 2 | Cheap | Simple | Simple |
| 1 | Quite Cheap | Quite Simple | Quite Simple |

*………(1)*

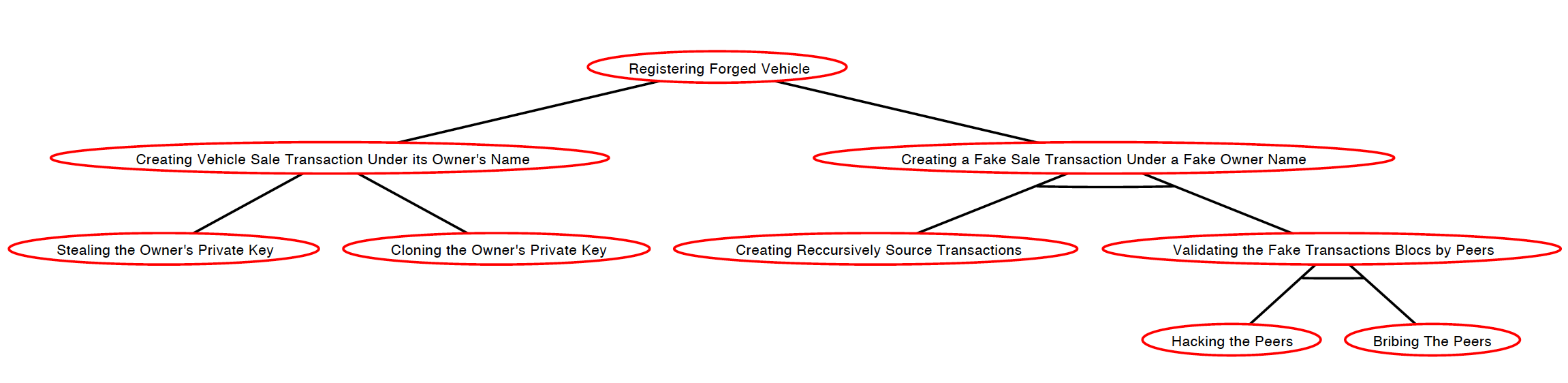
*Where U* is the utility function and is the parameter’s weight. W equals to 1/3 like in [30] [31].

The utility function is calculated like in [30] [31] as illustrated with (formula 2).

*where Cf=0.2 ……… (2)*



**Figure 9:** Attack Tree for Registering forged Vehicles using Current System.



**Figure 10**: Attack Tree for Registering forged Vehicles using Our Proposed Framework.

**Table 4**: Probability of Occurrence of Attacks Against Current System

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Current System*** | ***Execution Difficulty*** | ***Detection Difficulty*** | ***Attack Cost*** | ***Probability of Occurrence*** |
| Hack Vehicle Registration System | 5 | 4 | 3 | 0.05 |
| Bribing the GMD Personal to Insert Forged records | 3 | 3 | 3 | 0.06 |
| Falsifying Procuration Impersonating the Owner | 4 | 3 | 4 | 0.05 |
| Falsifying Vehicle's Papers | 4 | 3 | 4 | 0.05 |
| **Registering Forged Vehicle** |  | | | **0.23** |

**Table 5:** Probability of Occurrence of Attacks Against Our Proposed Framework

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Our Proposed Framework*** | ***Execution Difficulty*** | ***Detection Difficulty*** | ***Attack Cost*** | ***Probability of Occurrence*** |
| Hacking the Peers | 5 | 1 | 5 | 0.09 |
| Bribing the Peers | 5 | 1 | 5 | 0.09 |
| Creating recursively source transaction | 5 | 1 | 5 | 0.09 |
| Stealing the owner's private key | 4 | 4 | 3 | 0.05 |
| Cloning the owner's private key | 5 | 5 | 3 | 0.04 |
| **Registering Forged Vehicle** |  | | | **0.10** |

The probability of registering forged vehicles using the current system is 23% and using our framework is reduced to 10%. Therefore, our framework is more secure to forgery. It resolves also the backup issue. It ensures transparency and immutability as well.

1. *Complexity Analysis*

The main key functions of our proposed system are the transaction creation, confirmation and validation (Algorithm 1-3). Therefore, the performance analysis of our proposal depends on the performance of these algorithms which is known as the complexity analysis. We study the complexity of our algorithms by calculating the computational cost, which is translated by the time cost of each algorithm to be executed, we also calculate the storage cost which is the amount of space of memory used by our algorithms. To calculate the costs of the algorithms we need to evaluate the cost of each composing instruction and sub-function. Table 6 contains the time and space costs of the sub-functions and instructions used in Algorithm 1, 2 and 3. Table 7 illustrates the time and space cost of both Algorithms. Before we continue with the cost study, we first explain the notation used, let ***n*** be the number of valid transactions created between the purchase transaction timestamp of a subject vehicle and the sale transaction timestamp (time of current transaction); ***k*** is the number of valid transactions among ***n*** containing the vehicle subject in their input, ***k=*0** if the owner of the vehicle is the initiator of the transaction, and else case ***0***<***k***<<***n***; ***m*** is the number of pending transactions; ***l*** is the number of transactions per block. **CostV-SG** is the time cost for the verification of a signature; **CostSrch** is the cost of search operation which is the comparison operation between the searched value and the current value. **CostSIG** is the time cost of the signing process. **CostTx** is the cost of creating the transaction. **CostK** is the cost of verifying the validity of a key; **CostH** is the cost of Hash verification and **Costhash** is the cost of hashing operation, **Cost*B*** is the cost of adding transaction to block. **B** is the block size in bytes and **T** is the transactions size in bytes as well. The time costs depend on the hardware technology tested in, therefore, instead of giving empirical values which may vary from device to another, we choose to give more stable, hardware independent, generalized cost evaluation in Tables 6 and 7.

**Table 6: Cost of key instructions used in Algorithm 1, 2 and 3**

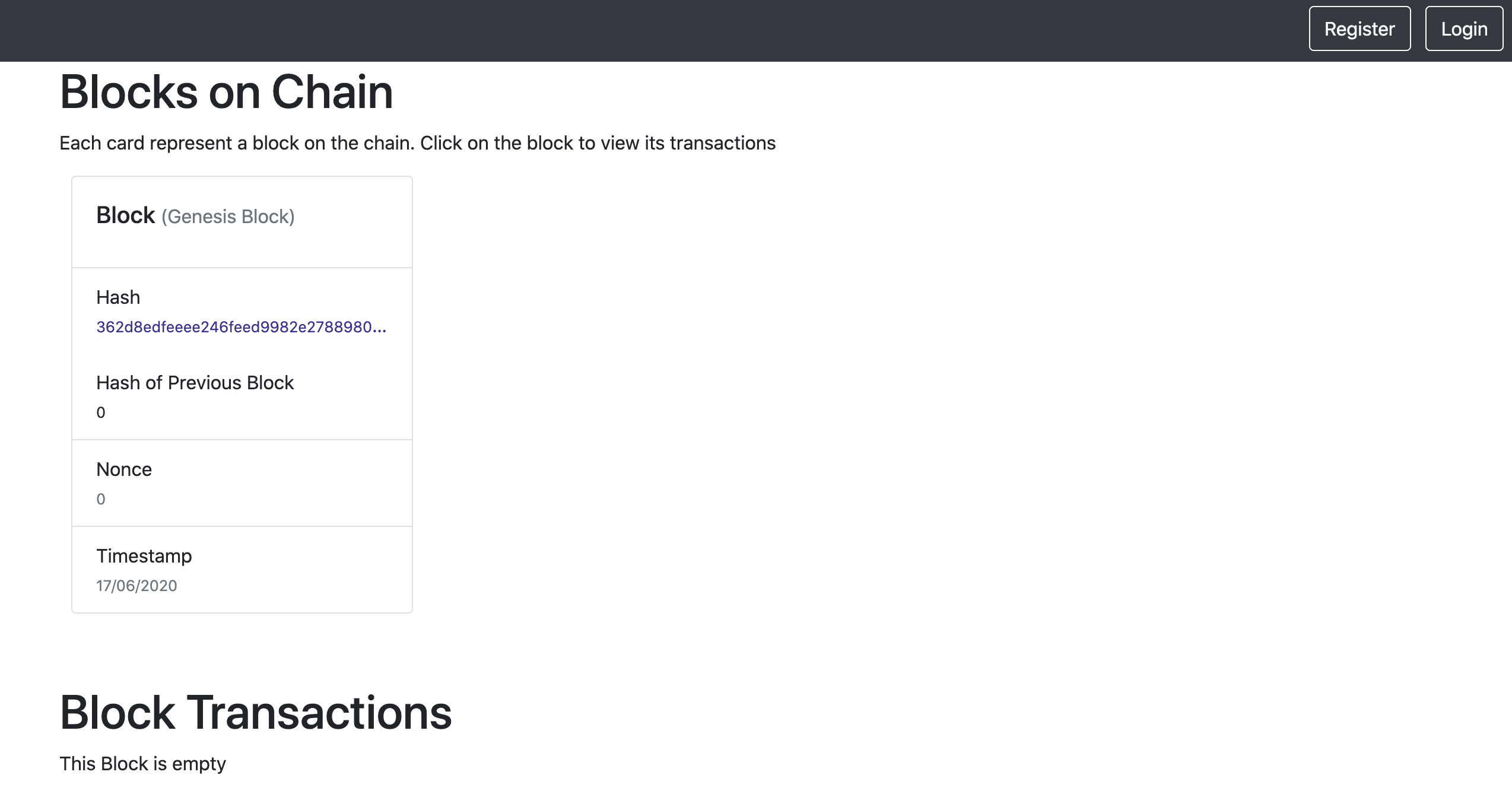
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Instruction*** | ***Double-Spending*** | ***IsOwner*** | ***createTX*** | ***ConfirmTx*** | ***IsValid*** | ***ValidHash*** | ***ValidSIG*** | ***CreateBlock*** | ***ChainBlock*** |
| ***Time cost*** | m **\*CostSrch** | **CostV-SG** +n\* **CostSrch** | **CostTx** | **CostSIG** | **CostK** | **CostH** | **CostV-SG** | ***l*\* Cost*B+***  **3\*CostSIG** | **CostH** |
| ***Space Cost*** | m \*T | n\*T | T | T | T | T | T | B | 2\*B |

**Table 7: Time and Space Cost for Algorithm 1, 2 and 3**

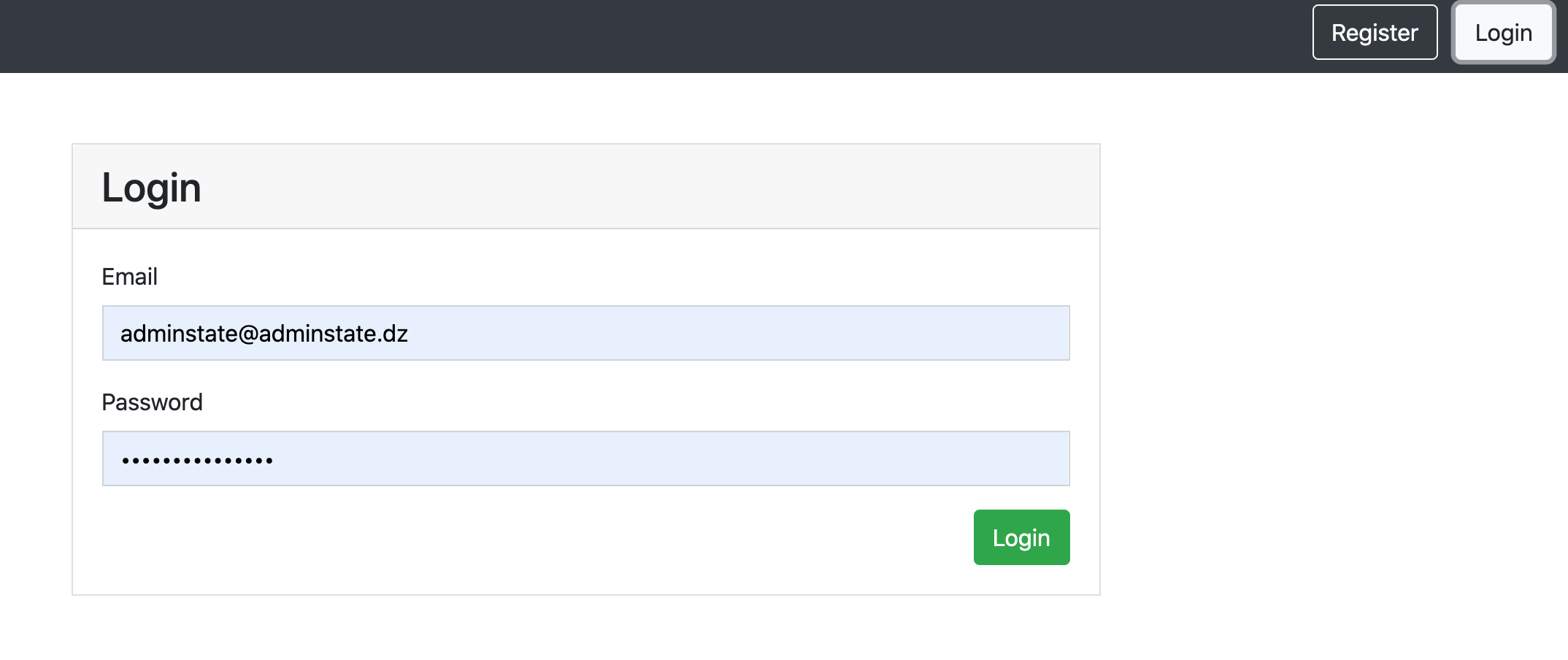
|  |  |  |  |
| --- | --- | --- | --- |
| ***Cost Analysis*** | ***Algorithm 1*** | ***Algorithm 2*** | ***Algorithm 3*** |
| ***Time Cost*** | **CostK+ CostTx** | (n+m) **\*CostSrch+ CostV-SG + CostSIG** | 2\* **CostK+**(n+m) **\*CostSrch+2\* CostH +4\* CostV-SG+ *l*\* Cost*B+*3\*CostSIG** |
| ***Space Cost*** | T | (n+m+1) \*T | (2+ (n+m+1)/*l*)\* B |

1. *Implementation*

Before we implement our solution, we searched for available open source implementations from which we aimed to understand the core of this technology. The available implementations used different validation and consensus processes; each has its own implementation language. Most of the implementations were for crypto currencies which relied on public permission-less blockchains with proof-of-work consensus model, Bitcoin is one of these famous implementations. Ethereum [13], Multichain [32], Openchain [33] and Hyperledger [34] on the other hand allowed the implementation of private blockchains (permissioned). The review of authors in [35] explains the different technologies and implementations, as well as the pros and cons of each solution. Taking this in consideration and the particularity of our solution which is that it is a blockchain of permissioned blockchains and that it saves physical assets. We decided to implement our solution from scratch using JavaScript. We started by building the back-end which is the blockchain, blocks and transactions, the validation process and their dependencies explained in Algorithms 1 and 2. Then, we build the front-end using Angular. In the current version of the application which is under-testing phase, the keys are generated upon the subscription of the user and are not certified. Also, the users subscribe directly by themselves and not by the authorized peers. However, the validation is done by the authorized peers. We alleviated the subscription of the users and eliminated the certifying of the keys because this is just a test version. In real world use, we must add the certifying authority to generate the keys and must require the subscription to be done by the authorized peers at the general department. We used the Qcode to facilitate the exchange of public keys between the seller and purchaser when creating the purchase transaction. The current version of the application follows the template presented earlier in Figure 8. The current version is under-test and its improvement is in progress. Figures 11-17 illustrates some views of our system. Noting that the filled example are not real and are for testing purposed only.



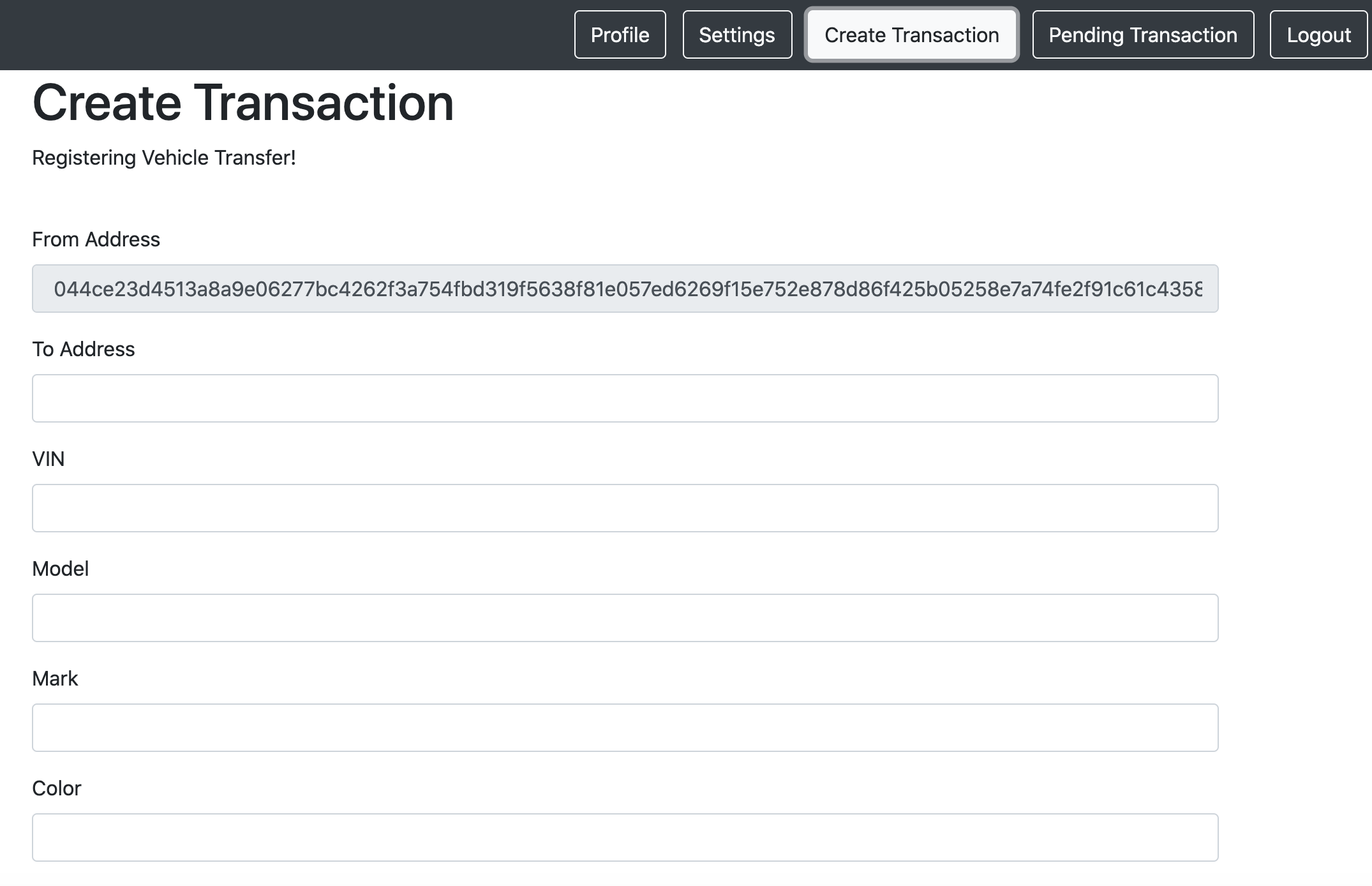
**Figure 11:** Home Page of our Vehicle Registration System



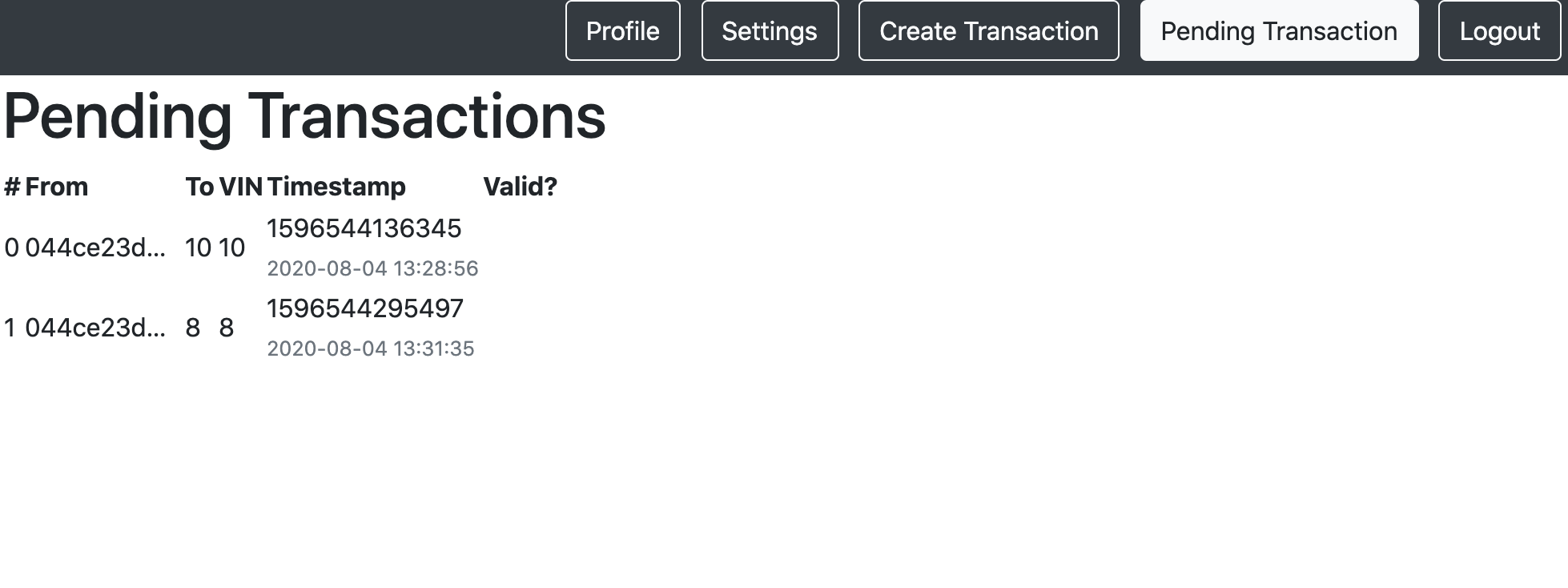
**Figure 12**: Login Page of our Vehicle Registration System



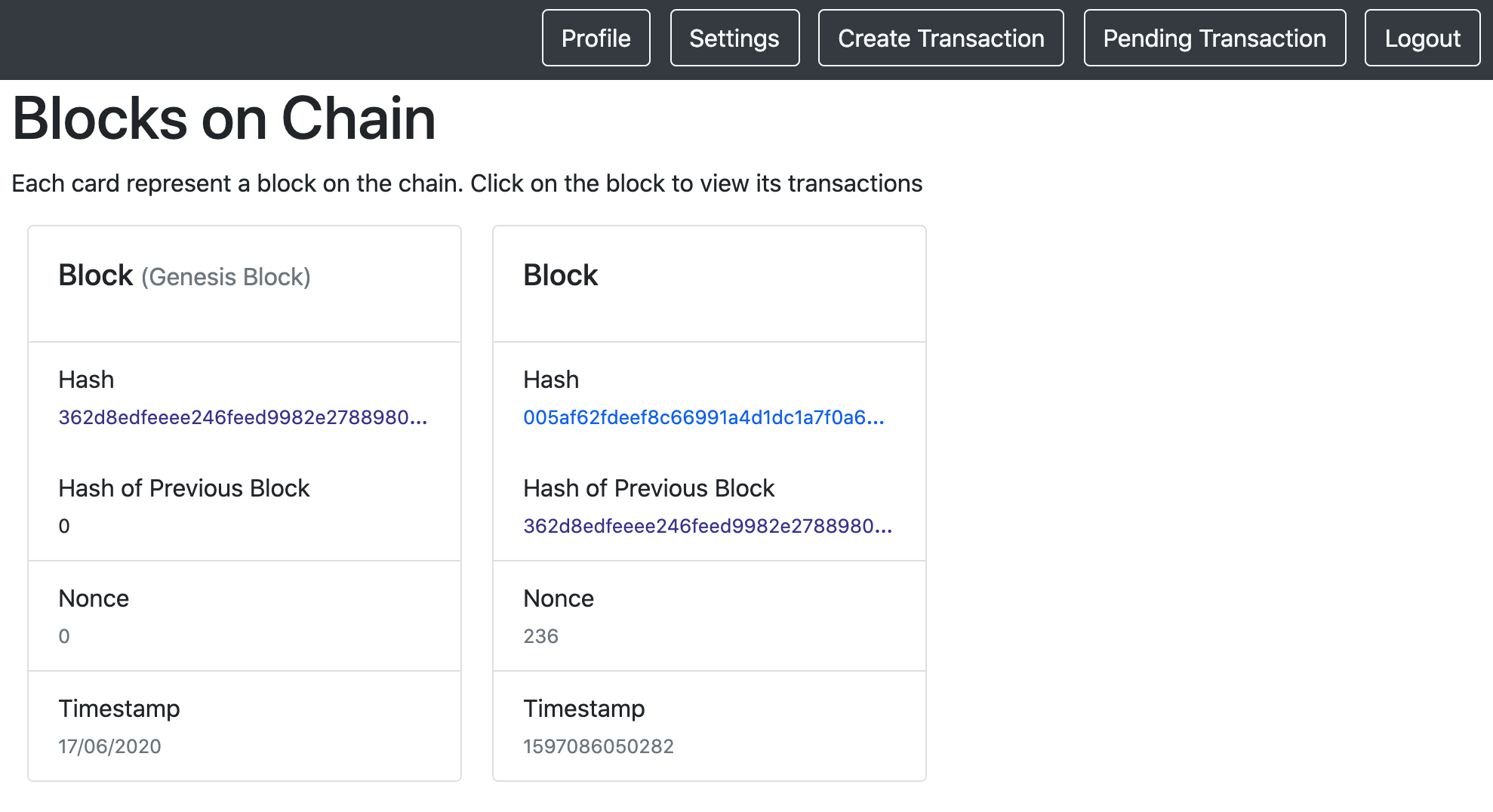
**Figure 13**: A user Profile in our Vehicle Registration System



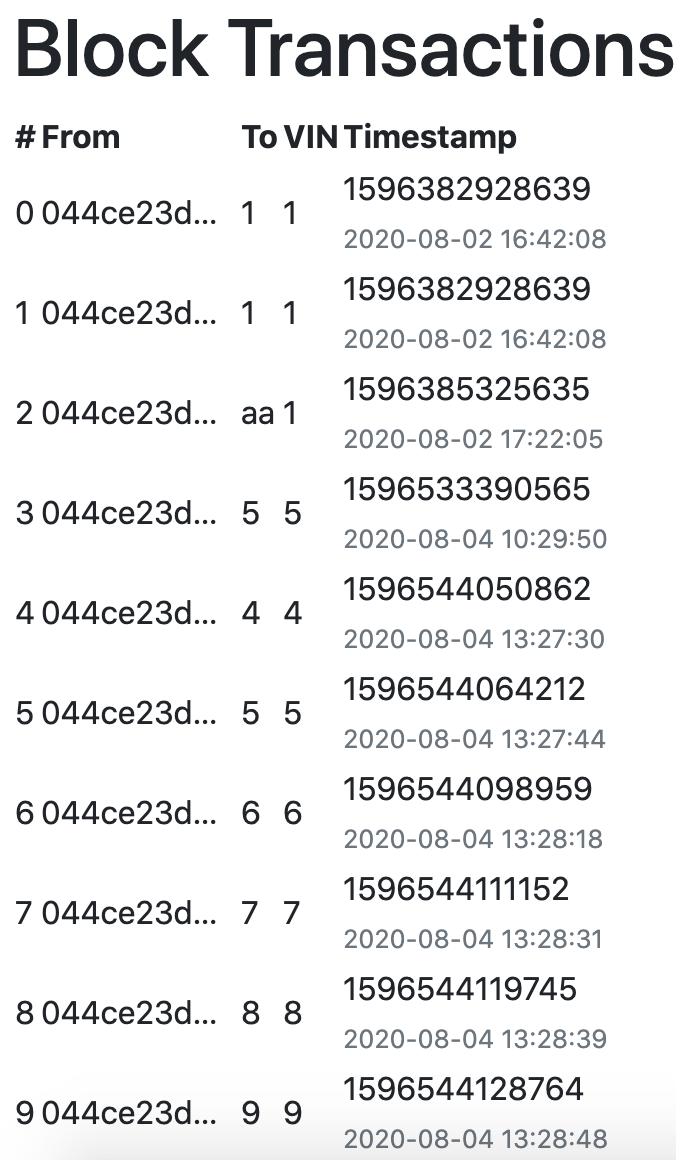
**Figure 14:** Part of the Transaction creation page in our Vehicle Registration System



**Figure 15**: The Pending Transaction Table



**Figure 16:** Example of validated Blocks in our Vehicle Registration System



**Figure 17**: Illustrations of valid transactions inserted in valid block

1. *Advantages*

The blockchain-based vehicle registration system is designed to resolve the issues found in the current system. It offers more flexibility as the vehicle purchase will be done online from anywhere and registered successfully in the blockchain. Two users may exchange their vehicles and register this operation from road thanks to the internet and the blockchain technology build over it. The solution has various other benefits, we state the following:

* ***Public***: the blockchain is publicly available, it is visible to the network peers, it can be downloaded and updated at any time. This facilitates the research and verification of transactions.
* ***The availability:*** the blockchain exists in every node of the network. Thus, the system does not suffer the single point of failure, on the contrary, the peer’s copies can serve as extra backups when needed.
* ***The Non-alteration***: the blockchain is stored in all nodes of the network. Thus, it is observed by everyone and no one can alter it knowing that this action can be detected. Also, because the many backup copies exist, it can be restored to the correct state at any time. More importantly only the authorized peers are able to create transactions and blocks and only them are able to validate these transactions and blocks.
* ***Security***: the blockchain technology relies on the use of hashing algorithms and public key signing and verification approaches, from which it gets its security characteristics.
* ***Resiliency to fraud***: if someone steals a vehicle and tries to sell it legally, s/he has to provide a valid transaction already existing in the blockchain proving that s/he purchased this vehicle and is currently its owner. If s/he fails to pinpoint the purchase transaction, the buyer cannot sign the transaction to confirm the purchase from his/her side. In the case where the thief does pinpoint a fake transaction s/he can immediately be exposed if the buyer cannot use the provided public key to read the hash in the non-validated transaction. i.e. when verifying the signature of the pinpointed transaction.
* ***Avoids the double spend problem***: the blockchain which is public prevents the case of double spending because a vehicle cannot figure in two inputs at the same time. The user cannot sell his/her vehicle to two users simultaneously because the buyer can detect that when validating the transaction and so does the authority that maintains the blockchain.

1. Conclusion

This paper presents a blockchain-based vehicle registration that is resilient to forgery and prevents inserting records of stolen vehicles to be legally reused. The solution is more secure, distributed and public. It takes its advantages from the blockchain technology. Besides, it gets us a few steps closer toward paperless e-government. In our system, the vehicle is registered by the use of a pair of public and private keys. The private key is essential, its holder is the only one that may sell the vehicle and register this operation. Therefore, it should be kept secure. Every transaction is done by the use of this private key. To analyze the security of our solution and its resiliency to forgery and fake transaction injection we elaborated the attack tree and calculated the probability of occurrence which is less than 10% in overall. This low probability further proves that our solution is secure and out-bests the existing system.

# References

[1] "Recovery rate of stolen property in the United States in 2017, by type," Statista, 2017. [Online]. Available: https://www.statista.com/statistics/252444/recovery-rate-of-stolen-property-in-the-us-by-type/. [Accessed 13 11 2018].

[2] "Stolen Car," Asset Guard LLC, 2020. [Online]. Available: www.stolencar.com. [Accessed 13 June 2020].

[3] "Registering/Titling a Vehicle in New York State," Departement of Motor Vehicle (dmv.ny.org), New York State, 2018.

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

[5] Crosby M, Nachiappan PP, Verma S, Kalyanaraman V. "BlockChain Technology Beyond Bitcoin," Sutardja Center for Entrepreneurship & Technology Technical Report, university of Berkeley, October 16, 2015.

[6] Drescher D, Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

[7] Yaga D, Mell P, Roby N and Scarfone K, "NISTIR 8202 Blockchain Technology Overview," National Institute of Standards and Technology, US department of Commerce, October 2018.

[8] Wattenhofer R, The Science of the Blockchain, 2016.

[9] Seang S and Torre D. "Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies," 2018.

[10] Zheng Z, Xie S, Dai H, Chen X, Wang H. " An overview of blockchain technology: Architecture, consensus, and future trends.," in Big Data (BigData Congress), 2017 IEEE International Congress , 2017.

[11] Schmid P. "The Blockchain: What Is It? And Why Is It Important to Risk Management and Insurance?," RIMS, 2017.

[12] "bitcoin," [Online]. Available: https://www.bitcoin.com/. [Accessed 14 11 2018].

[13] Buterin V, "Ethereum White Paper, a next generation smart contract & decentralized application platform".

[14] Alonso KM and koe, "Zero to Monero: First Edition," monero, 2018.

[15] Karamitsos I, Papadaki M and Al Barghuthi NB, "Design of the Blockchain Smart Contract: A Use Case for Real Estate," Journal of Information Security, vol. 9, no. 3, p. 177, 2018.

[16] Salmeling M and Fransson C. "The land registry in the Blockchain—Testbed," A development project with Lantmäteriet, Landshypotek Bank, SBAB, Telia company, ChromaWay and Kairos Future, Sweden, 2017.

[17] Hou H. "The application of blockchain technology in E-government in China.," in Computer Communication and Networks (ICCCN), 2017 26th International Conference on. IEEE, 2017. p. 1-4.

[18] Hegadekatti V. and Hegadekatti K. " Blockchain applications in medical sciences.," international journal of scientific research, vol. 7, no. 4, 2018.

[19] Yakubov A, Shbair W, Wallbom A, Sanda D. "A Blockchain-Based PKI Management Framework," in The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS, Tapei, Tawain, 2018.

[20] Reed D, Sporny M, Longley D,  Allen C, Grant R, Sabadello M."Decentralized Identifiers (DIDs) v0.9," 02 04 2018. [Online]. Available: https://w3c-ccg.github.io/did-spec/#overview. [Accessed 07 04 2018].

[21] Yahiatene Y, Rachedi A,  Riahala MA, Menacer DE, Nait‐Abdesselam F. A blockchain‐based framework to secure vehicular social networks. Trans Emerging Tel Tech. 2019; 30:e3650.

[22] Huh JH, SEO K. "Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing," The Journal of Supercomputing, pp. 1-17, 2018.

[23] Pohrmen FH, Das RK, Saha G. Blockchain‐based security aspects in heterogeneous Internet‐of‐Things networks: A survey. Trans Emerging Tel Tech. 2019; 30:e3741.

[24] Singh SK, Rathore S, Park JH. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Generation Computer Systems. 2020. 110, 721-743.

[25] Tseng L, Yao X, Otoum S, Aloqaily M, & Jararweh Y. Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. Cluster Computing, 2020, 23(3), 2151-2165.

[26] Tseng L, Wong L, Otoum S, Aloqaily M, & Othman JB. Blockchain for managing heterogeneous internet of things: A perspective architecture. IEEE Network, 2020, 34(1), 16-23.

[27] "Cosmos," 14 08 2018. [Online]. Available: https://cosmos.network/docs/. [Accessed 14 11 2018].

[28] "OneLedger," [Online]. Available: https://oneledger.io/en/. [Accessed 14 11 2018].

[29] Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KKR. A systematic literature review of blockchain cyber security. Digital Communications and Networks. 2020. 6(2), 147-156.

[30] Ren D, Du S, Zhu H. A novel attack tree-based risk assessment approach for location privacy preservation in the VANETs. In: Communications (ICC), 2011 IEEE International Conference on. IEEE, 2011. P. 1-5.

[31] Benarous L, Kadri B, Bouridane A. Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Networks. Arabian Journal for Science and Engineering. 2020. 45, 6033–6049

[32] "Multichain Open Source Blockchain," [Online]. Available: https://www.multichain.com/. [Accessed 12 08 2020].

[33] "Blockchain technology for the enterprise," [Online]. Available: https://www.openchain.org/. [Accessed 12 08 2020].

[34] "Hyperledger," [Online]. Available: https://www.hyperledger.org/. [Accessed 12 08 2020].

[35] Knirsch F, Unterweger A, Engel D. Implementing a blockchain from scratch: why, how, and what we learned. EURASIP J. on Info. Security. 2019, 2.

[36] Al-Ruithe M, Benkhelifa E, Hameed K. Key dimensions for cloud data governance. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). P. 379-386

[37] Al-Ruithe M, Benkhelifa E, Hameed K. Data governance taxonomy: Cloud versus non-cloud. Journal of Sustainability. 2018. 10, 1.