Implementation of the Blockchain in the Optimization of the Security of Transport Documents (Driver's License and Vehicules Registration Cards)

Georges Bell Bitjoka[1], Pierre Bilong[2], Moses Macaire Nnanga Edoa[2]

[1]Department of Telecommunications, National Advanced School of Engineering, University of Yaounde I, Yaounde, Cameroon

[2]Department of Computer Science, Faculty of Sciencies, University of Yaounde I, Yaounde, Cameroon

Email address:

georges@bellbitjoka.com (G. B. Bitjoka), alphaomegbp@gmail.com (P. Bilong), nnangamacaire@gmail.com (M. M. N. Edoa)

[*]Corresponding author

To cite this article:

Abstract: Data security has become very important nowadays, especially with the increase of data from the big data, forcing each sector to review its security system. The security of driving license and the vehicle registration is always attributed to an authority. This authority can be public or private. In Cameroon, in the transport sector, the security of the driving license and the vehicle registration document is attributed to two private authorities. Presprint Pl for the driving license and High Tech Telesoft for the vehicle registration card. Their objective is to prove the authenticity, availability and confidentiality of the holder of the driving license or car registration card. But until now, the security of these transport documents has encountered certains problems such as the fact that some individuals possess false driver's licenses or false vehicle registration cards. Sometimes with the complicity of certain system managers, the time taken by an applicant to obtain his driver's license or vehicle registration card, the management of the data to be secured by a single authority. Faced with this situation, in order to ensure that only qualified persons who have received appropriate driver training and hold a authentic driving license can be authorized to drive vehicles. The security of the system will be optimized through the use of blockchain technology, in allowing transparency in data management and without a central authority.

Keywords: Blockchain, Optimized, Security, Driver's License, Car Registration, Vehicle Registration Card

1. Introduction

Among the influential sectors of the Cameroonian economy we have in good place the transport sector. Indeed, by its geography and its position, transport which development began since the colonial era plays an important role in the national and sub regional scale. It ensures the circulation of goods and people for administrative management and development of the territory, promotes transit from or to the two Cameroon landlocked neighbors, Tchad and the Central African Republic, and allows exchanges between the CEEAC and DEDEAO areas. However, the ratio of the number of killed compared to the number of vehicles is extremely high: a vehicle in Cameroon kills on average 123.8 times more than in developed countries, with a significantly higher comparative factor, when it comes to carry out comparisons with countries such as Japan (229.7), Germany (187.2) or France (144.2) [1]. The type of transport vehicle causing the most deaths in Cameroon is the motorcycle vehicle. By way of illustration, according to the Ministry of Transport, in Cameroon, 41% of those killed by traffic accidents are users of motorcycle taxis. In 2006 alone, just over 600 cases of motorcycle taxis were registered, including 150 deaths, or 25% of those injured [2]. At international scale, the World Health Organization (WHO) estimates that road accidents will be the fifth leading cause of death by 2030, with increasing disparity between rates in developed and developing countries, and the UN has given a decade by 2020 to stabilize and then reduce the number of road deaths [3].

In an effort to reduce the death rate from road traffic crashes, all the different factors leading to road fatalities need to be studied. According to the WHO, the main factors causing accidents are human error, speed, driving while intoxicated or under the influence of psychoactive substances, distracted driving, dangerous vehicles, no application of the driving code [4]. All of the factors listed below can be generalized to the validity of a person to be able to drive a vehicle and the authorization to drive by the competent authorities. According to the procedure of transport authorities in Cameroon, a person is valid and authorized to drive only if he has in his possession a set of documents concerning him and the vehicle he is driving. This guarantees the training of the person in driving but also in the driving code and the good condition of the vehicle through technical visits. Our work will focus on one of the most important parts, namely the driver's license. It is an essential part in transportation for any driver. It makes it possible to guarantee the validity of the person able to drive and to identify him. In the transport sector, the demand for driving licenses and vehicle registration certificates is increasing day by day. Despite all the measures, the presence of false driver's licenses and vehicle registration documents continues to increase. The presence of false driving licenses and vehicle registration documents is favored by certain factors such as: corruption of certain officials, data processing errors, which require the unique presence of a single person to manage the data, the centralization of data management by sometimes faulty systems.

In view of this, we are led to ask the question of how can we secure the process of obtaining a driving license in order to reduce the number of disabled and unlicensed drivers. This in order to improve traffic on our roads by first preserving human lives and finally property. To achieve this, it will be a question of providing transparency in the management of transport data by optimizing the security of the process of obtaining a driving license and vehicle registration through blockchain technology.

2. Key Concepts

2.1. The Blockchain

2.1.1. The Definition

A Blockchain is an open source, decentralized, disintermediated, secure, inviolable, forgery-proof, and data storage and transmission technology based on P2P exchanges. By extension, it constitutes a decentralized, reliable, inviolable public database (or not in the case of private and consortium Blockchains) and without a central control entity. Once the information and exchanges have been entered in a Blockchain, they can not be modified and are stored there permanently. It can be compared to an anonymous ledger. There is no "entrance fee". Anyone can consult all the exchanges and transactions recorded on a blockchain since the first block created. Users are identified by an "account number" making it impossible to identify them. Asymmetric key encryption solves cryptographic problems for block validation. Its distributed nature also provides security since all blocks are replicated on all nodes of the network [5].

2.1.2. Transaction

Transactions between network users are grouped together in a data structure called a block. The blocks are ordered and hierarchically arranged in one and only chain. Each block points to the last valid previous block. This chain is distributed and replicated to all nodes in the network. Each new transaction and/or Smart Contract, pending, is grouped in a new block. To add this block in the Blockchain, it must be validated. This validation is carried out through specific nodes of the network called miners. The role of these nodes is to answer a complex crypto mathematical puzzle. Each answer found is specific to one and only one block, thus preventing its reuse for the validation of a new block. Once the block is validated by a miner and approved by the other nodes in the network, it is time-stamped and added to the top of the block chain (last valid block created) and all nodes in the network add it to their copies of the chain. There are many valid solutions for a given block. It is sufficient to find at least one of them for validated the block through the consensus process [5].

2.1.3. The Consensus

Consensus refers to the mechanism of guarantee that a transaction is not fraudulent and is valid. The only way to create a global validation within the network is to obtain a vote. The assumption is that malicious users will always be fewer in number than honest users. It is therefore important for the security of the network that there are mechanisms or rules that are recognized, shared and validated by all, which make it possible to validate a transaction before that it is added to the chain.

2.1.4. The Characteristics of Blockchain

Decentralization: Instead of relying on a single trusted entity, trust is spread across multiple or all participants, depending on the agreed-upon consensus algorithm [8]. This does not only mean that multiple copies of a data item are stored on all nodes, but also that the integrity of the data is governed by many decentralized parties.

Immutability: Once data is committed to the blockchain and a sufficient number of participants have agreed on this state, the information is stored permanently and immutably. Changing the information contained in a particular block would require to also changing all the following blocks up to the last block, which is considered to be infeasible [9].

Scalability: The block rate, comprised of the throughput and propagation time of information, depends on the consensus algorithm and the number of participants. This can be a limiting factor for applications that require high throughput [8]. Since all nodes hold a copy of the blockchain, scalability issues also arise in terms of the total amount of data that can be stored. Furthermore, in order to check the integrity of the blockchain, a new node needs to download a copy and validate the integrity of the entire chain. Note that more recent proposals for BFT-based consensus algorithms

improved on this, e.g., [10].

Secure: Decentralized hosting also makes blockchain a secure technology: it makes it almost impossible to delete all copies of documents, which exist on a multitude of servers around the world. The blockchain has great resistance, because all the data is copied to the different servers. This makes it resistant to cyber-attacks or state control. Indeed, if it is possible to attack one or more computers, it is more complicated to attack the blocks of information copied in all the computers connected to the network. This provides the blockchain with a high level of security. The blockchain is therefore considered unassailable and inviolable. However, this also makes it difficult to adjust.

Transparent: There is no "right of entry". Anyone can consult all the exchanges and transactions recorded on a blockchain, from the first block created. Once a document is registered on the blockchain, this is enough to prove that the latter exists at time T and that it has not been modified. The blockchain is qualified as transparent because everyone can download it in its entirety and check its honesty at any time. All blockchain users can thus view current and past transactions.

2.1.5. The Types of Blockchain

Blockchain technologies can be roughly divided into three types:

i. The Public Blockchain

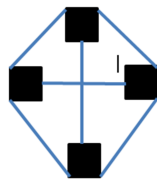Open and accessible to all, anyone can join. Carry out or verify transactions.

Figure 1. *Public Blockchain.*

ii. The Private Blockchain
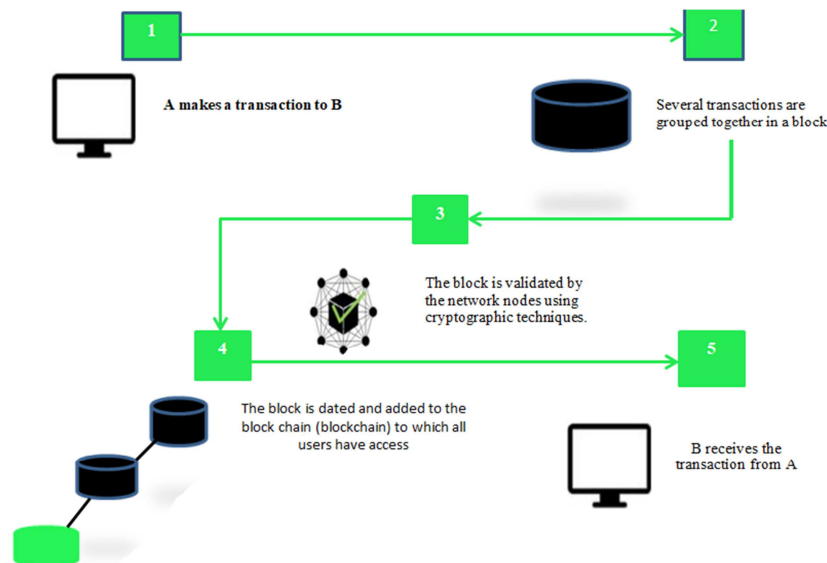
Is not open to the public, but is accessible by invitation only and all participating members know and trust each other.
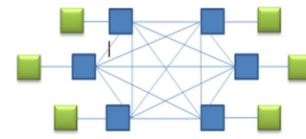

Figure 2. *Private Blockchain.*

iii. The Consortium Blockchain

This is a hybrid blockchain: some nodes can be public, while others remain private for sensitive actions. It is therefore a blockchain with accesses managed by a part of the actors, which is suitable for the following contexts.
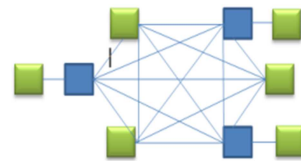

Figure 3. *Consortium Blockchain.*

2.1.6. The Types of Blockchain

According to figure 5 below, the main working processes of blockchain are as follows:

Step1: A network node initiates the transaction

Step 2: The transaction is broadcast throughout the p2p network and inserted in a block awaiting validation.

Step 3: The network of nodes (miners) validates the transaction using hashing algorithms such as: Proof of work (PoW), proof of stake (PoS), or PBFT (Practical Byzantine Fault Tolerance).

Step 4: Once the block is validated, it is added to the block string

Step 5: Finally the transaction will be completed successfully.

This can be represented in the following way:

A makes a transaction to B

Several transactions are grouped together in a block

The block is validated by the network nodes using cryptographic techniques.

The block is dated and added to the block chain (blockchain) to which all users have access

B receives the transaction from A

Figure 4. *Fonctioning of Blockchain.*

2.2. Driver's License

2.2.1. Definition

A driving license is an administrative right of movement giving permission to drive one or more vehicles such as cars, motorcycles, mopeds, trucks or buses on a public road in a given geographical area, usually a country.

2.2.2. Types of Driver's Licenses

i. Category A

AM: A moped with a speed limit of 45 km/h by construction with a cylinder capacity of less than 50 cm^3 (internal combustion engine) or a maximum power of 4 kW (other engines) or a light quadricycle with a maximum power of 4 kW. In this category we find small carts. For this class, it is not permitted to take a passenger, except in the case of a cart with two seats and a driver with an AM licence who is at least 18 years of age, although this licence is available from the age of 16. This permit can be taken either on a moped or in a cart, and success the in this class allows you to drive any vehicle in the AM class.

A1: Light motorcycle (with or without sidecar) with a maximum power of 11 kW (15 hp), which does not exceed 125 cm^3 of cylinder capacity, and whose power/weight ratio does not exceed 0.1 kW/kg; a motor tricycle with a maximum power of 15 kW.

A2: Motorcycle (with or without sidecar), with a power not exceeding 35 kW and with a power/weight ratio not exceeding 0,2 kW/kg; a motor tricycle with a maximum power of 15 kW [6].

ii. Category B

Vehicles with a maximum authorized mass (MMA) less than or equal to 3.5 tonnes, a B licence is sufficient to carry a maximum of 8 people, not including the driver, a total of 9 people in the same vehicle [6].

iii. Category G

Category G is only valid on national territory. A category G driving licence is required for drivers of agricultural vehicles, as well as for vehicles registered as agricultural equipment, motor cultivators or harvesters. This licence is required for all persons born after 1 October 1982. This category does not exist in its form E, the GE licence does not exist [6].

iv. Category Heavy Duty

Categories C and D, are heavyweight categories. You will therefore need a medical certificate in order to obtain a permit in these categories.

C1: Vehicles with a MAM greater than 3.5 tonnes and less than or equal to 7.5 tonnes. These vehicles are also designed and constructed for the carriage of not more than 8 passengers in addition to the driver. Vehicles in this category may be coupled to a trailer with a MAM of 750 kg or less.

C: Vehicles with a MMA greater than 7.5 tonnes. These vehicles are also designed and built to carry a maximum of 8 passengers in addition to the driver. Vehicles in this category may be coupled to a trailer with a MAM of 750 kg or less.

D1: Vehicles used for the carriage of passengers having not more than 16 seats in addition to the driver's seat and measuring up to 8 metres in length. Vehicles in this category may be coupled to a trailer with a gross vehicle mass (GVM) not exceeding 750 kg.

D: Vehicles used for the carriage of passengers having more than 8 seats in addition to the driver's seat or carrying more than 8 persons excluding the driver. Vehicles in this category may be coupled to a trailer with a gross vehicle mass (GVM) not exceeding 750 kg. [6]

v. Category E

The E permit authorizes the driving of category B, C or D vehicles coupled to a trailer. There are therefore three E permits: the BE permit, the CE permit and the DE permit [7].
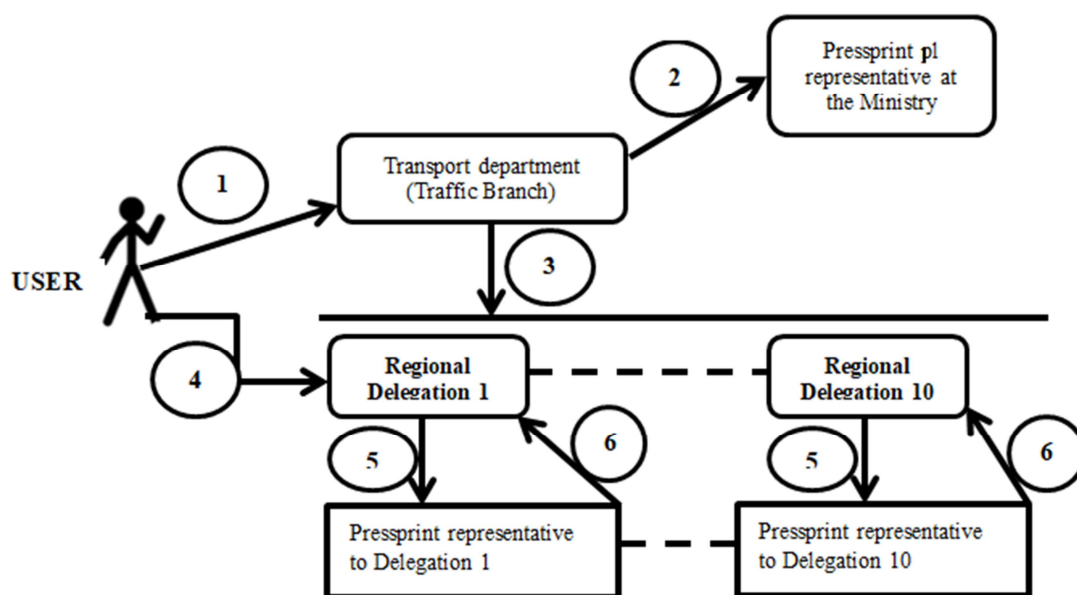

Figure 5. Driver's license creation process.

2.3. Driver's License Creation Process

In this case we have two parties involved in the management of the driver's license: The Traffic Branch at the Department level or the Driver's Licence Application Recovery Unit. The pressprint pl representative in charge of creating and securing the driver's licence and the signature of the Director of Road Transport or the Minister of Transport are stored in the pressprint pl server.

The user applies for the driver's licence from the Ministry of Transport;

The information received from the user by the road traffic branch after verification of its completeness is forwarded to the pressprint representative for the creation and securing of the driver's licence;

The Ministry of Transport shall send lists of all those admitted to the driving licence competitions to each pressprint representative located in each regional delegation;

The user applies for the driving licence from a regional delegation;

The unit in charge of receiving driving licence applications at the regional delegation level forwards the information received to the pressprint representative for the creation and securing of the driving licence;

After the driver's licence has been created and secured, the pressprint representative returns the driver's licences to the unit in charge of receiving applications in order to issue them to the applicants.

2.4. Some Techniques to Defraud a Driver's Licence

Dishonest people use every possible means to achieve their goals. Thus in the creation and issuing of driving licences to people who do not deserve a driving licence, we can note some methods:

2.4.1. Production of Driving Licences Using Specialized Computer Software

From a genuine driving licence, obtained either by theft of the owner's driving licence, or by assault of the owner or by the consent of the legitimate owner, an identical copy of the real driving licence is reproduced just with some modifications according to the personal data of the applicant.

2.4.2. Obtaining a Driver's Licence Through the System Without Fulfilling the Required Conditions

Issuing a driver's licence to a person who does not deserve it with the help of people working in the system, either by inserting unauthorized data into the database or by using identity theft.

2.4.3. System with Security Flaws and Therefore Exposed to Attacks

Knowing that any system can be vulnerable, it is possible for fraudsters with computer knowledge to find ways to access the system's database and modify the information.

2.5. Registration Certificate

2.5.1. Definition

The registration certificate is a document that evidences the authorisation to drive a registered motor vehicle and enables it to be identified. The registration certificate is a police document. It can in no way be considered as a civil status document or a title deed.

2.5.2. Operating Principle

The subdirectorate for road transport at the level of the ministerial department or the unit for collecting applications for vehicle registration certificates at the departmental level. The High Tech Telesoft representative in charge of creating and securing the car registration document and the signature of the regional delegate or the minister of transport are stored in the High Tech Telesoft server.

In order to be allowed to circulate on the public highway in Cameroon, any motor vehicle, semi-trailer or trailer whose maximum permissible laden weight exceeds 500KG must be license plate. Several factors are taken into account when assigning vehicle registration numbers.

Civil Mass-Produced Motor Vehicles

The number is composed of: Two (2) letters designating the province where the owner of the vehicle is domiciled, a group of four (4) digits constituting the sequence number in the series, A group of letters indicating the licence plate series in which the vehicle is registered. Example: LT 4568 A the 4568th vehicle licensed plate in the coastal province in the A-series.

Table 1. Regions and their code.

Code	Region
EN	Far North
NO	North
AD	Adamaoua
ES	East
NO	North West
OU	West
SU	South
SO	South West
LT	Littoral
CE	Center

Coupled vehicles (trailers and semi-trailers), mechanical equipment,

Agricultural or road tractors

The number is composed of: Two (2) letters designating the province where the owner of the vehicle is domiciled, A group of two (2) letters indicating the type of rolling stock: RE for trailer, SR for semi-trailer, SE for construction machinery and agricultural tractors, TR for road tractor, A group of four (4) digits constituting the sequence number in the series, A group of letters indicating the series in which the vehicle is licensed plate.

Example: LT SR 9652 A the 9652e semi-trailer licence plate in the coastal province in Series A.

State-Owned Motor Vehicles

The number is composed of: Two (2) letters designating the party concerned, CA for Administrative Corps, NA for National Assembly, A group of four (4) digits constituting the sequence number in the series, a group of letters indicating the series in which the vehicle is licensed plate.

Coupled vehicles (trailers and semi-trailers), mechanical machines, agricultural or road tractors, motorcycles and others belonging to the state obey this rule. The region code is replaced by CA. Example: AN 9652 E.

Motor vehicles belonging to members of the diplomatic and consular corps and to the administrative staff of a diplomatic mission, or of an international organization.

The number is composed of: A group of letters, CMD for the Chief of Diplomatic Mission, CPC for head of consular post, CD for Diplomatic Corps, CC for Consular Corps, and PA for Administrative Staff.

A group of numbers indicating the code of the diplomatic mission or international organization in the Department of External Relations. The codes assigned to diplomatic missions range from 02 to 99. The codes assigned to international organizations range from 102 to 199. The group of two (2) letters RC for Republic of Cameroon. A group of digits at the end indicating the vehicle serial number. Example: PA 02 RC 521.

Vehicles Belonging To Technical Assistance Staff.

The number is dialed: IT code for Temporary Registration, Of a group of five (5) digits constituting the sequence number, From the group of two (2) letters RC for Republic of Cameroon. Example: IT 21052 RC [16].

2.6. Registration Car Creation Process

The process of creating and obtaining a vehicle registration document is based on a licence plate application submitted to the competent services of the Ministry of Transport or to a regional delegation of its choice. After verifying the information provided by the user, this information is transmitted to the department for creating and securing the vehicle registration document, which is managed by the Hight Tech Telesoft representative located at the Ministry of Transport and in each regional delegation. The schematic representation of the process of creating and securing the vehicle registration document is as shown in figure 5, where

we will just replace pressprint pl by Hight Tech Telesoft.

2.7. Some Technicals Frauds of Registration Certificate

2.7.1. Imitation and Usurpation of Signature on Vehicle Registration Documents

In fact, all you have to do is fill in the certificate of declaration of transfer of a vehicle in place of the owner, forge the signature on the declaration and on the vehicle registration document, and that's it, because no one will check its authenticity. The assignment may be made by means of this false declaration of assignment with impunity, without the consent of the owner.

2.7.2. Fraudulent Alteration of Administrative Document

Often, the personal information contained on a vehicle registration document is fraudulently altered to serve a wide variety of purposes: vehicle theft, licence plate registration of stolen vehicles, export and/or sale of stolen vehicles, etc. Individuals involved in this type of criminal activity need genuine vehicle registration cards, on which to change certain data regarding the owner, vehicle, serial number or other information. That is why the theft of vehicle registration documents is so common in today's society.

2.7.3. Expertise of False Administrative Documents

A final possible check, which is very common among victims of this type of usurpation, is the technical expertise of the vehicle registration document and the false declaration of transfer of the vehicle, because a real handwriting and a real signature can be transferred to the form by technical means, by digital photomontage. In this case, there will be the real writing and signatures of the seller on the declaration of transfer of the vehicle and on the vehicle registration document, but following a fraudulent process: documentary fraud.

2.8. Analysis of the Security of the Driving Licenceand Registration Certificate in Cameroon

The security of the driving licence with this system in Cameroon has some weaknesses that are summarized in the table below:

Table 2. Analysis of the security of the driving licenceand registration certificate in Cameroon.

	problems	solutions proposed by the current system	weaknesses
Driver's Licence	The application form of getting a driver's licence is still handwritten.	Generation of a computerised driving licence containing all the information of the person concerned	the handwritten form poses a problem of reliability of the information the form may get lost, or the information may be changed
	Assigning and managing certain key information to a single person.	In case of loss or disclosure of information the person responsible will be severed according to the law.	In spite of the sanctions provided for by the system, the problem of data integrity will arise because there is no guarantee that the input information will be what is expected at the output.
	Office fire	Restores information when renewing or declaring a lost driving licence.	If there is a fire at the driver's licence office, the unit in charge of creating the licence will use the copies when the persons concerned come to renew or report the loss of the document. This does not always guarantee the reliability of the solution, because if the user had a false document, we will then issue a genuine driving licence.

	problems	solutions proposed by the current system	weaknesses
Registration CAR	Centralization and management of the data to be secured by a single entity	The company presprint has strengthened security measures with the addition of elements such as the generation of the QR code which uses cryptographic methods to encrypt codes, OVI ink and the use of a distributed database connected to a central server located at the base of the company presprint pl.	Knowing that any system can have flaws so there is no guarantee that the data will not be altered. The time it takes to obtain a driver's licence is considerable because of the management of the data by a single entity.
	The application form of getting a registration car is still handwritten.	The application form for the vehicle registration document and filling in the information online	
	Assigning and managing certain key information to a single person.	In case of loss or disclosure of information the person responsible will be severed according to the law.	In spite of the sanctions provided for by the system, the problem of data integrity will arise because there is no guarantee that the input information will be what is expected at the output.
	Centralization and management of the data to be secured by a single entity	The High Tech Telesoft company has reinforced security measures with the introduction of an online car registration application and the use of a distributed database connected to a central server located at the base of the High Tech Telesoft company.	Knowing that any system can have flaws so there is no guarantee that the data will not be altered. The time it takes to obtain a driver's licence is considerable because of the management of the data by a single entity.

3. Method of Securing of the Driver's License and Registration Certificate

3.1. Framework to Improve Security of Driving Licence with Corda

In the case of the driving licence we have two types of actors: those who can write and read in the distributed register and those who can only read in the register. Our system will therefore have a part reserved (private) to a category of people with the possibility to manage the driving licences thus constituting the nodes of the network. And another part of the system will just allow checking the authenticity of the (public) driver's license. For this purpose a consortium blockchain will be favorable to set up our system. With this consortium blockchain approach all stakeholders will be allowed to read the ledger. But only the user's information, the verification whether the user has been admitted to the driving licence competition and the type (category) of driving licence will be recorded during the creation of the driving licence. Corda is an example ofconsortium blockchain.

3.2. Presentation of the Corda Framework

Corda has been open source software since 2016. The design of Corda has ben-efitted from the collaboration of a global and diverse alliance of organisationsrepresenting many industries, and regulatory engagement has been a key ele-ment of this design processc. The requirements of the financial industry formedthe original basis of Corda's design but field experience have demonstrated thatCorda has broad applicability, well beyond banking [13].

The motivating problem, which Corda seeks to solve, is the problem of man-aging contracts and other agreements between any combinations of firm's andindividuals, especially when those parties trust each other enough to trade butnot enough to have their counterparty maintain all the records [13].

Corda isdesigned to allow information and assets gained through usage of one CorDapp to be used in a different context with different counterparties in a differentCorDapp. This stands in contrast with other enterprise-focussed blockchainplatforms, which are designed to be deployed as isolated instances for eachsupported application [13].

3.3. The Caracteristics of Corda

Corda is a DLT (Distributed Ledger Technologies) specifically designed to meet the needs of financial companies. Its specialization allows it to have a simpler architecture than other distributed registry technologies, such as Hyperledger Fabric, which is relatively complex. Despite this specialization, Corda's framework makes it entirely possible to create a DLT for any use case, even outside of finance. Its use may nevertheless be less suitable than other more complete DLT frameworks [14]. The Corda approach is quite different from a consortium blockchain such as Hyperledger Fabric, Ethereum or Quorum, where information is shared with everyone by default. Indeed, with the Corda platform, information is not visible to everyone, but is sent from point to point. This makes it possible to manage inter-company flows. Corda, like the various consortium blockchains, does not involve any incentive unlike public blockchains such as BTC or ETH - and therefore no exchange of cryptomoney, no decentralized monetary system. Transparency is not total as in a classic blockchain. Corda is rather a kind of secure messaging, to make it (very very) simple [15].

3.4. Presentation of the Corda Framework

Corda is coded with a modern programming language that is little used by the community, the Kotlin language, which runs with the Java virtual machine. On Corda, smart contracts can be written in Kotlin or Java. The framework contains 3 essential components.

Corda Node: A corda node is the node of an organization. Each of them can carry several Cordapp, the applications incorporating Corda's smart contracts. CorDapps (Corda

Distributed Applications) are distributed applications that run on the Corda platform. The goal of a CorDapp is to allow nodes to reach agreement on updates to the ledger. They achieve this goal by defining flows that Corda node owners can invoke over RPC.

Network Map: It allows the different organisations in the network to discover each other. Implemented as an HTTP service, it can be located behind a CDN and is cached by each of the nodes in the network.

Notary: This is the service that allows for consensus on double spending in the network.

Non-Validating: It ensures that there is no double spending of an asset in the same Corda network and must sign these spending transactions. It simply verifies that a statement has not already been consumed; it therefore respects the confidentiality of the transaction in question. He is the most frequently used notary.

Validating: It checks if the smart-contract checks referenced in the transaction are correct. It does not respect confidentiality in transactions if it is not used with SGX type enclaves (currently being implemented). [11]
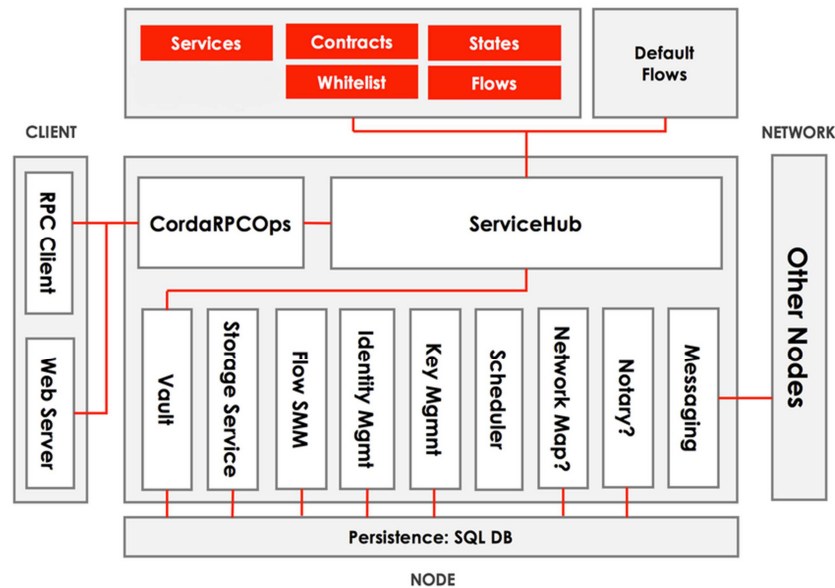
This can be represented in the following way:

Figure 6. The node's internal architecture [12].

The core elements of the architecture are:

A persistence layer for storing data: The persistence layer has two parts: The vault, where the node stores any relevant current and historic states; the storage service, where it stores transactions, attachments and flow checkpoints.

A network interface for interacting with other nodes: All communication with other nodes on the network is handled by the node itself, as part of running a flow. The node's owner does not interact with other network nodes directly.

An RPC interface for interacting with the node's owner: The node's owner interacts with the node via remote procedure calls (RPC).

A service hub for allowing the node's flows to call upon the node's other services: Internally, the node has access to a rich set of services that are used during flow execution to coordinate ledger updates. The key services provided are: Information on other nodes on the network and the services they offer, Access to the contents of the vault and the storage service, Access to, and generation of, the node's public-private keypairs, Information about the node itself, The current time, as tracked by the node.

3.5. Corda's Consensus

Corda's consensus is based on the one hand on the

validation of the transaction by the signatory and on the other hand on its uniqueness. The validation of the transaction is ensured by its participants: they must sign the transaction and pass the smart-contract checks. It is also necessary to check that all transactions that led to the received transaction are validated: for example, if we receive cash, we want to verify that it was issued by a central bank during the first transaction. The validation of its uniqueness is done with the help of the Notary: it is he who will ensure the finality of a transaction. For example, he will certify that the cash we receive has not been sent at the same time to another organization. In this fraud attempt, one of the two receiving organizations will not be able to use it, because it will already be consumed. Notaries do not need to see the content of the transactions, so confidentiality is maintained. It is possible for the same Corda network to have several notaries. It is also possible, as with Fabric, to abstract a Notary in a cluster, with a RAFT consensus or with a Byzantine fault tolerant consensus (here, BFT SMaRt). These two consensus are functional in Corda.

3.6. Transaction Flows

The workflows automate the approval process for general ledger updates. Communication between nodes takes place

only within these flows, and is point-to-point. Integrated workflows are provided to automate common tasks.

A flow is a sequence of steps that tells a node how to achieve a specific ledger update, such as issuing an asset or settling a trade.
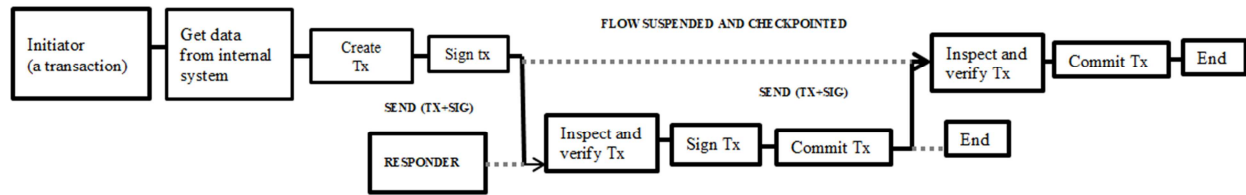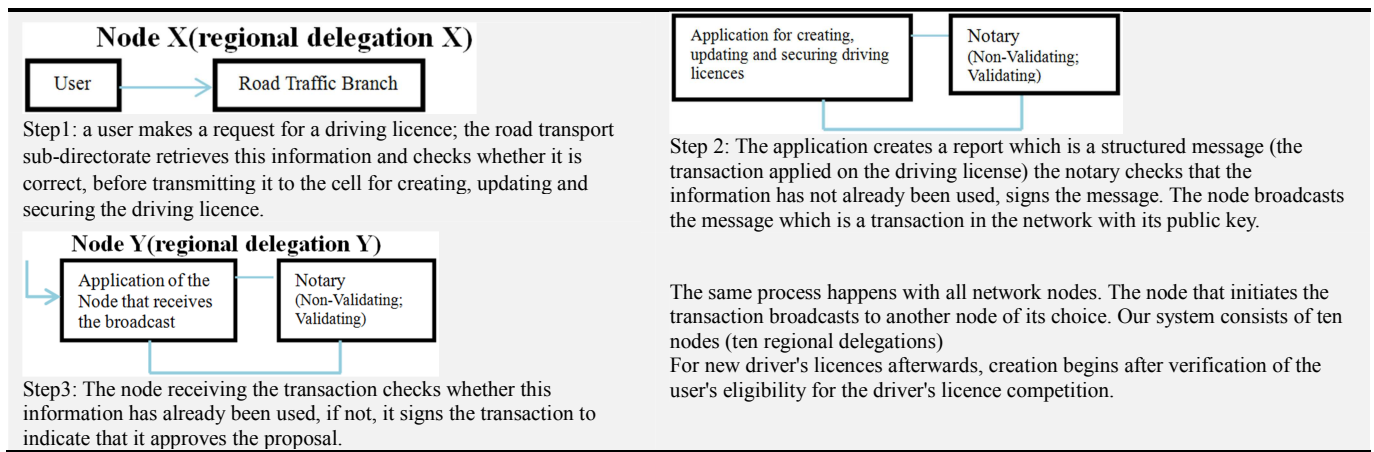
This can be represented in the following way:

Figure 7. *Transaction flows.*

3.7. Case Study: Driver's Licence in Cameroon

To implement, we will need the following structures for a start: Ministry of Transport: for the registration driver's licence, and updates (Change of category (type of driving licence), conversion du permis de conduire, licence renewal, loss of licence declaration).

Table 3. *Transaction with two nodes of organizations.*

3.8. Scalability

Scalability of block chains and block chain inspired systems has been a constant topic of discussion since Nakamoto first proposed the technology in 2008. Corda provides much better scalability than other competing systems, via a varietyof choices and tradeoffs that affect and ensure scalability. Scalability can be measured in many different dimensions, extending even to factors like how manyapps the ecosystem can handle. The primary techniques used to scale better than classical systems are as follows: partial visibility, multiple notaries, Parallel processing, Chain snipping, Signatures of validity, JIT compilation [17].

4. Result and Discussion

4.1. Discussion

4.1.1. The Strengths of This Work
We can cite:

Decentralization of the operation of the system and of its database in each node of the blockchain network;

No modification of the data once it has been recorded in the database;

Total obligation for all those who want the driver's license to follow the normal road for obtaining it;

The half time to get the driver's licence and registration car is reduced;

Traceability and transparency during the audit;

Creating a driver's license for someone who has not been admitted to the driver's licence competition becomes difficult because all nodes in the network have the results;

The Corda Framework is suitable for all use cases not only for financial transactions;

Decrease in traffic accidents due to the non-training of drivers in a driving school.

4.1.2. The Weaknesses of This Work
We can cite:

A mechanism for the identification of permits on the road.

Not all nodes in the network receive the automatically initiated transaction as in other frameworks because the node that creates the transaction must broadcast it with all other nodes.

4.2. Result

Table 4. The results of implementation of Corda.

	problems	solutions proposed by the current system	weaknesses	Strengths: Corda's solutions
Licence	The application formof getting a driver's licence is still handwritten.	Generation of a computerised driving licence containing all the information of the person concerned	the handwritten form poses a problem of reliability of the information the form may get lost, or the information may be changed	By using blockchain technology the information will be present and unforgeable as long as the bockchain exists.
	Assigning and managing certain key information to a single person.	In case of loss or disclosure of information the person responsible will be severed according to the law.	In spite of the sanctions provided for by the system, the problem of data integrity will arise because there is no guarantee that the input information will be what is expected at the output.	Responsibility, management and retention of information will be equal with all nodes in the network facilitating the audit.
	Office fire Disappearance of the driver's licence and file.	Restores information when renewing or declaring a lost driving licence. Restore the driver's licence register with the help of users with authentic licences.	If there is a fire at the driver's licence office, the unit in charge of creating the licence will use the copies when the persons concerned come to renew or report the loss of the document. This does not always guarantee the reliability of the solution, because if the user had a false document, we will then issue a genuine driving licence. The person in charge of restoring driving licences uses his intuition and all the technical means at his disposal.	The blockchain is like a large distributed register which is copied in several places, if we lose in one place, we end up in another. It's impossible to lose the driver's licence, because of its distributed nature.
	Centralization and management of the data to be secured by a single entity	The company presprint has strengthened security measures with the addition of elements such as the generation of the QR code which uses cryptographic methods to encrypt codes, OVI ink and the use of a distributed database connected to a central server located at the base of the company pressprint pl.	Knowing that any system can have flaws so there is no guarantee that the data will not be altered. The time it takes to obtain a driver's licence is considerable because of the management of the data by a single entity.	As the blockchain is distributed it is almost impossible to fake it because you have to go through all the nodes of the network and all the blocks. Knowing that after a very short time another block is added to the chain
Registration CAR	The application formof getting a registration caris still handwritten.	The application form for the vehicle registration document and filling in the information online	A single entity is responsible for receiving requests	From any node of the network you can receive a query
	Assigning and managing certain key information to a single person.	In case of loss or disclosure of information the person responsible will be severed according to the law.	In spite of the sanctions provided for by the system, the problem of data integrity will arise because there is no guarantee that the input information will be what is expected at the output.	Responsibility, management and retention of information will be equal with all nodes in the network facilitating the audit
	Centralization and management of the data to be secured by a single entity	The High Tech Telesoft company has reinforced security measures with the introduction of an online car registration application and the use of a distributed database connected to a central server located at the base of the High Tech Telesoft company.	Knowing that any system can have flaws so there is no guarantee that the data will not be altered. The time it takes to obtain a driver's licence is considerable because of the management of the data by a single entity.	As the blockchain is distributed it is almost impossible to fake it because you have to go through all the nodes of the network and all the blocks. Knowing that after a very short time another block is added to the chain
	Sale of fake car registration documents	identify the Perpetrators of this criminal. act and to bring them to justice.	The sale of fake registration car.	It is impossible for one to find false registration car, indeed one of the characteristics of the blockchain is its security.

5. Conclusion and Perspectives

In this work, we presented a solution to the problem of securing the car registration and driving licence. This solution consisted in setting up a consortium blockchain based on the corda framework which uses consensus algorithms such as Raft or Byzantine fault tolerance, and also allows to manage the scalability of the network and data storage. We also presented the functioning of security of the current system of the driving licence and the car registration from the request to the obtaining of the document which are managed by two instances Pressprint Pl for the driving licence and Hight Tech Telesoft for the car registration, which have their representative in each regional delegation and at the Ministry of Transport of Cameroon. In terms of

perspective it will be interesting to look at the international level and the realization of an application allowing easy access to the users of the system.

References

[1] Department of Transport, Urban Development and ICT; Cameroon, Note on the transport sector; AFRICAN DEVELOPMENT FOUND; 2015; www.afdb.org; https://www.afdb.org/fileadmin/uploads/afdb/Documents/Publications/AfDB_-_Cameroun_-_Note_sur_le_secteur_des_transports.pdf.

[2] Guy Rostand DJIEPMO NDJOUKYA; The challenges of road safety in urban areas in Cameroon: the case of motorcycle taxis in Yaounde; Master in Transport Economics and Trade Logistics 2008; University of Yaounde; Cameroon; https://www.memoireonline.com/02/10/3152/Les-defis-de-la-securite-routiere-en-milieux-urbain-au-Cameroun-le-cas-des-motos-taxis-a-Yaoun.html.

[3] Global road safety status report; 2018; World Health Organization; https://www.who.int/violence_injury_prevention/road_safety_status/2018/French-Summary-GSRRS2018.pdf?ua=1.

[4] Road accidents; 7 December 2018; World Health Organization; https://www.who.int/fr/news-room/fact-sheets/detail/road-traffic-injuries.

[5] Christophe Dorothe; When the Blockchain revolutionizes the sharing economy; 20 October 2017; https://www.lesechos.fr/idees-debats/cercle/quand-la-blockchain-revolutionne-leconomie-de-partage-1011765.

[6] Driver's License; Wikipedia Free Encyclopedy; Last modification on 6 June 2020; https://fr.wikipedia.org/wiki/Permis_de_conduire.

[7] Ministry of Interior of Republic of France; The Differents Driver's Licenses; Road Safety, Living Together; https://www.securite-routiere.gouv.fr/les-differents-permis-de-conduire.

[8] XAVIER; Mining: Proof Of Work (POW), cryptocurrency calculation engine; 13 July 2018; https://www.canardcoincoin.com/proof-of-work-pow-crypto-monnaies/.

[9] Godefroy Galas; Analysis and comparison of consensus mechanisms in the blockchain; 14 May 2018; https://medium.com/@godefroy.galas/analyse-et-comparaison-des-m%C3%A9canismes-de-consensus-dans-la-blockchain-f91aee511ea3.

[10] What is the Proof of Work in tne Blockchain? 29 August 2018; Business AM; https://fr.businessam.be/quest-ce-que-la-preuve-de-travail-dans-la-blockchain/.

[11] Loup Theron; Consortium Blockchain: Corda or Fabric ?; 19/07/2018; https://blog.octo.com/blockchain-de-consortium-corda-ou-fabric-1-2/.

[12] Nodes; Corda Documentation; 2020; https://docs.corda.net/docs/corda-os/4.4/key-concepts-node.html.

[13] Richard Gendal Brown; The Corda Platform: An Introduction. May, 2018; https://www.r3.com/wp-content/uploads/2019/06/corda-platform-whitepaper.pdf.

[14] Floriane Bobée. Corda the open source blockchain for business; https://bitconseil.fr/corda-r3-caracteristiques-permissioned-blockchain-dlt/.

[15] Joy Boswell; Blockchain: Focus on the particularities of Corda; 20/12/2018; https://blog.octo.com/blockchain-lapproche-corda-fait-sens/.

[16] Immatriculation des véhicules civils de transport routier au Cameroun. http://www.logistiqueconseil.org.

[17] Mike Hearn, Richard Gendal Brown. Corda: A distributed Ledger. August 20, 2019 https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf.