ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 3, 251-259 (2019)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Proposal of Ledger Technology to Apply to a Public Organization in Ecuador

Segundo Moisés Toapanta Toapanta*[,1], Adrian Alberto Chávez Monteverde [1], Javier Gonzalo Ortiz Rojas[1], Luis Enrique Mafla Gallegos [2]

[1]*Departament of Engineering Systems, Universidad Politécnica Salesiana (UPS), Guayaquil, Ecuador*

[2]*Faculty of Engineering Systems, Escuela Politécnica Nacional del Ecuador (EPN), Quito, Ecuador*

ARTICLE INFO

Article history:
Received:02 April, 2019
Accepted:19 June, 2019
Online: 30 June, 2019

Keywords:
Public Organization
Ecuador
Blockchain
Ledger Technology
Algorithm
Database
Distributed System

ABSTRACT

Ledger technology has now changed financial systems around the world, applying this technology to the improvement of the public sector, mainly to the debt collection system, we improve the speed of payment and its immediate registration, we make use of the advantages of Ledger technology with respect to reliability, security and speed. The objective is to propose how we apply Ledger technology within a public organization, considering the improvement of this, without diminishing its efficiency, security and current productivity. We use a deductive method to analyze the information obtained from the scientific articles reviewed. The results of our research are reflected in an algorithm that shows the operation and application of Ledger technology. It was concluded that the strengths of the algorithm, together with the good distribution and application of Ledger technologies solve problems regarding efficiency, safety and savings.

1. Introduction

Today, the public sector is seen as an ineffective, ineffective service, and citizens need better performance from the public sector. The public service in Ecuador many years ago needs a very profound change that is effective and demonstrable in the services offered to citizens, because of this reason we can find solutions in various technological fields, we focus on a solution offered by Ledger technology applied to a public organization.

Technology advances day by day to immeasurable levels from which we can obtain benefits, some countries have begun to implement Ledger technology in their systems of collection of debts, goods, etc. In the countries where Ledger technology is implemented, the results have become positive in every field in which it was applied, showing results that can be used as an example to achieve objectives in Ledger technology applications.

Today the public organizations that manage the debts with the citizenry are collected through banks and other private financial institutions that provide their service and that has a high degree of security and reliability that offers to the citizens, but for the transaction to take place an intermediary in the collection of the debt, which is the private sector, because of this it takes away the speed of the payment process and the reflection thereof between the citizen and the private financial entity and this in turn with the public entity, which generates an additional cost that is paid by the citizen [1].

If the current system is robust, safe and effective, why should Ledger technology be deployed to a public organization? The current way to pay a debt to a public entity is through private sector entities which has a cost that is charged by the private sector intermediary and paid by the citizen this generates in an increase in the cost of transaction in total and should also be added the protection to our information, the private sector have possession of this, can make use of it or at worst have leaks or thefts of our private information.

Ledger technology helps us reduce costs by paying for transactions, which is a saving for the average citizen, and save budget for hardware needed by the public sector to have the current collection system run between a public organization and a private organization, which gives us robustness [2], in the case of the application of the Ledger technology gives us an advantage that the payment is made directly and anonymously with the participation of the citizen and the public organization, without offering our personal and bank information to a private entity, which gives us security and efficiency [3].

* Segundo Moisés Toapanta Toapanta, Email: stoapanta@ups.edu.ec

https://dx.doi.org/10.25046/aj040333

An important advantage is the saving of money, both by the citizen who saved the cost by performing the transaction through the private sector, also the public institution will save on hardware, because the processing cost was shared by all participating nodes within the network, this way less hardware was needed for the network to work also decreases costs in different areas: hardware cost, electrical power, personnel capable of handling specialized hardware [3].

If the benefits are higher, then why is the study and implementation not applied? Because the change that is taking place could generate conflicts for the citizen, by explaining all the functions and advantages that a Ledger technology would have in applying it, the beneficiaries can resist the change, so it would be a problem because people do not want to participate in the application of the Ledger technology, another problem is the change of certain functions in the public organization, leaving aside some traditional actors but, In the same way, new participants enter the collection system. For this reason, it is necessary to create a new definition of the responsibilities of the infrastructure and of the participants in the provision of collection services.

The articles reviewed for this research are:

Centralized solution to securely transfer payment information electronically to banks from multiple enterprise resource planning (ERP) systems [1]: The model is basically composed of ERP business resources planning applications, this model offers security, effectiveness and cost savings of up to 75% without geographical restrictions. The main users are large business units that frequently carry out banking or financial transactions such as payment to local or foreign suppliers, payroll, etc., thus having a relationship with our system due to the collection and payment of debts, which instead of being a bank, it will be a public organization, from which we obtain an implementation already applied to financial systems, in this way we will be able to obtain results according to the exposed thing guaranteeing in our systems equal or superior results.

Lightweight and Manageable Digital Evidence Preservation System on Bitcoin [2]: We found a structure for the preservation of light digital evidence that has the characteristics of privacy-anonymity, audit-transparency, function-scalability and light-operation, such characteristics that we will apply in our system, obtaining information from studies conducted using bitcoin systems (cryptocurrency) which helps our system to use virtual money and its characteristics by applying them in the correct way guaranteeing results.

Towards dependable, scalable, and pervasive distributed ledgers with blockchains [3]: We find the distributed general ledger technology (DLT), its structure, classification and applications in three generations: 1.0 (cryptocurrency), 2.0 (Apps) and 3.0 (omnipresent applications). It presents all aspects of the blokchain, showing how the block chain systems are balanced, from which we have learned and used the study done to the blockchain, which allows us to apply it in the best way to our system, having the knowledge offered by blockchain.

Redecentralizing the Web with Distributed Ledgers [4]: Presents that the contracts or accounting books distributed represent a service of reliability, responsibility and security in transactions without the need for centralized validation authorities, projecting the web as a true decentralized autonomous system, which helps us to understand the benefits offered by the application of daily books and at the same time be able to offer the advantages of the same to our implementation.

CoC: Secure Supply Chain Management System Based on Public Ledger [5]: CoC (supply chain on blockchain) is a supply chain management system that provides a security mechanism to circumvent any access that is not registered as authorized to the general ledger database, since the general ledger generally lacks security, we will use this method of building blocks within our system to be able to make use of the advantages of it, This way applying a more level of security to our locks that handles the default Ledger technologies.

PQChain: Strategic design decisions for distributed ledger technologies against future threats [6]: The importance of a well-structured strategy for an appropriate chain of blocks is highlighted, when instances are created means that a large number of participants must be dealt with and it is the trust in the centralized authorities that determines the security guarantees provided by the cryptography, in this way we have created and structured good chains of blocks to be able to manage within the network, in this way we ensure the security of each block received and sent by the network for the benefit of the application within the public organization.

Distributed Ledger [7]: It demonstrates a systematic description of the most remarkable principles of the DL field, because there is currently no structural approach and definition of DL, from which we can learn clear concepts that help us to apply Ledger technologies to our system, which we take advantage of so that knowing the fundamentals we can succeed in implementation.

Security of Distributed Ledger Solutions Based on Blockchain Technologies [8]: Provides information on the security aspects of blockchain technology, identifies the most relevant security threats and challenges for technology development, with these studies we will be able to apply them to provide the necessary security to be able to apply the blockchain, through this study we will be able to understand and apply the security that we will have to offer to our entire system for a successful application.

Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph [9]: Develops a new model in the field of distributed accounting technology, it is compared with tools like Ethereum, Bitcoin and Nano, with the blockchain being the two most important paradigms for distributed systems. In order to achieve the reduction in the size of the ledger and the effectiveness of the transactions that are generated, we obtain the comparison with the blockchain, In this way we can know advantages and disadvantages compared to the blockchain and by this comparison we can obtain better results in the application of Ledger technologies.

Blockchain-based Proof of Delivery of Physical Assets with Single and Multiple Transporters [10]:. It presents a solution for the Proof of Delivery (PoD) of the physical assets negotiated based on the blockchain. They use the aspects of the chain of blocks Ethereum so that payments are automated and generate records that can identify fakes, all this in order to gain reliability and present transparency, we can find a relationship in the handling of money to be able to carry out transactions within ledger technologies, using electronic money (cryptocurrencies) and in turn understand the benefits that it guarantees with the use of cryptocurrencies which we take advantage of in our application.

A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain [11]: It proposes to reduce the storage space required by the blockchain to store all transactions, using a coded network (NC) and distributed storage (DS): NC-DS, which proposes to use the NC-DS encodingDS achieves in a reduction of our data storage to use for the backing of all monetary transactions within the analyzed system in this way reducing cost compared to the current systems.

Distributed ledger technology for decentralization of manufacturing processes [12]: The use of distributed general ledger (DLT) is studied to innovate industrial cyber physical systems, establish limits of the DLT comfort zone, measurable performance and high impact indicators (KPI), allowing us to apply these innovations to our public systems and thus apply them in the best way to obtain the best possible results according to the needs.

The method used was deductive research to proceed to analyse the information of the articles under study and to obtain the steps for the development of the algorithm.

The result obtained in this phase is a prototype of an algorithm in which flow diagramming techniques were used.

The objective is to analyze the application of Ledger technology in a public organization, to determine the positive impacts it has on the improvement of its operation.

2. Materials and methods

Within the Ledger technology we find the blockchain (block chain), which is a digital journal, in which are recorded all the transactions that have been made grouped in blocks that are linked linearly between them, that is, the first block is linked to the second block, the second block to the third block and thus successively. Ledger technology ensures that every transaction made is valid and unalterable. In this way we will see each block as if it were a page of a virtually infinite accounting book, but in this case the transaction can neither be erased nor repeated because each transaction has a unique fingerprint, with this we guarantee that all transactions are immutable.

It uses a distributed system that will integrate the nodes and the main system which includes all the information necessary for the recording of transactions and equally security rules and encryptions in this way will be controlled by the public organization to ensure that transactions are more secure and robust [4].

The blockchain can be private and public, this is responsible for defining how is the management of the distributed network, if in the case it is a public blockchain, all the participants within the distributed network have the same level of authority and level of access to the information allowing all the nodes to have the same hierarchical level within the network and at the same time all these nodes have full access to the information that exists within the network, this is a disadvantage for the reason that the nodes considered citizens are not can have information from other nodes as it would leak information within the network, instead it is a private blockchain, the main node that is the public organization has higher authority than the other participants or nodes and this is responsible for establishing rules and conditions to participate in the network and in addition to controlling and verifying the information already processed by all the nodes, a final information and already processed, since only this main node has access to the final information, it guaranteed more security and anonymity to the system [4].

For example, rules and conditions were established for entering or performing transactions within the network, the citizen who enters as a node to the system must be over 18 years old to be able to enter the network, the citizen's digital portfolio must have sufficient funds to be able to carry out a transaction, must have active debts to be able to make a payment, must have a PC with internet connection and offer it to be a node within the system in order to be able to enter the network, etc., any node that does not comply with one of the rules must not be accepted or removed from the distributed system and any transaction that does not comply with the conditions must be rejected, both restrictions serve to maintain the safety and efficiency of the network.

The security offered by the blockchain along with a CoC (supply chain on blockchain) encryption, which was in charge of encrypting the transactions within the distributed system, has a greater degree of security than the blockchain offers us, which worked as follows: information is encrypted by encryption algorithms offered by the blockchain technology along with CoC encryption and an additional measure of security is that the transaction is replicated to each node within the network and each node verified this encryption, if all the nodes accepted the validity of the encryption. the encryption is proceeded to complete the transactions that were sent to each node, without this acceptance the transaction is not made, this additional security measure increased the security when making the transactions, with these benefits offered by the Ledger technology, it became a very safe and robust system, for which it is useful and very considerable when taking into account for the implementation [5].

When applying CoC encryption to our network, we must take into account the advantages and disadvantages generated by the use of this type of encryption, the advantages that we consider greater, the encryption is greater, offering more security to each transaction, the latency of the network will decrease considerably unlike the basic use of the blockchain, a storage scheme that relieves the data overload that the blockchain will have, each participating node keeps a copy of the chain which allows having a less load within the network when validating the encryptions , the participating entities do not need to trust each other due to the behavior of the encryption, allows only registered users to the network to write in the transaction blocks, allows to establish entry and operation protocols for the participants in this way, allows adjusting the network in a better way to the operating conditions.

Now we must consider the disadvantages, in this way we will know the disadvantages and improvements for our network, being a centralized network and the CoC works better with decentralized networks should be implemented with some adjustments to maintain the expected functionality, since a copy of the chain in all the nodes and being a centralized network this causes a double expense and the network suffers delays at the time of encryption, it can be difficult to achieve a consensus on the nodes committed to our network at the moment of building the chains; it needs that the set of nodes within the network is complete, all the participants must maintain a history of transactions which in the long run generates histories of very large sizes that can affect the functioning of the participants.

Figure 1 contains a prototype general outline of a distributed system for a public organization and its members (nodes), which allows us to show the structure of the distributed system that allows us to obtain an optimization of the resources of the network and thus obtain an appropriate performance by applying Ledger technologies [6].

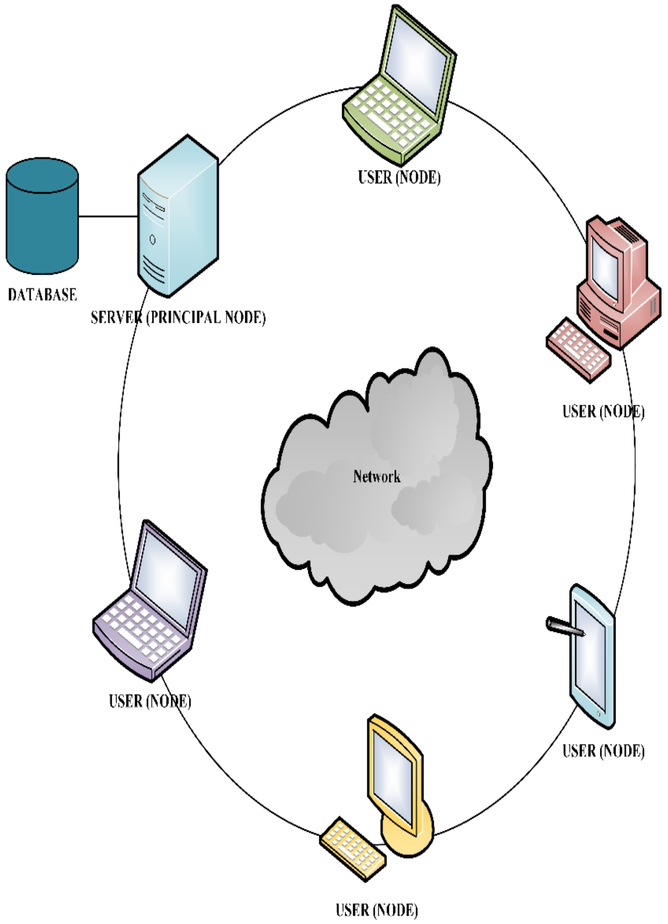

Figure 1: General outline prototype of the distributed system.

A private blockchain was established for this case, where the highest authority within the network will be the public organization, which will determine the rules and conditions of use for all its nodes (citizens) and also verifies the hash of each transaction, is the only one in charge of verifying this information, it does it to each of the transactions, in this way it can detect intruders with false validations [7], instead the nodes can only verify the encryption hash of the previous node, it is not necessary to verify the encryption of other nodes, thus saving node resources.

Such technologies need to maintain the highest level of security both inside and outside the network, in order to ensure a moral integrity that all transactions made have not been modified by administrators of the main node belonging to the public organization, Private Ledgers can have many owners. When a successful transaction is completed and the journal is registered, the ledger is checked to maintain its integrity through a consensus process. This is carried out by a different public organization, which will perform a role of trusted agent, this process helps to ensure the integrity of all transactions that are performed, thus avoiding alterations made within the public organization for malicious purposes or for common errors committed by main node administrators.

In Figure 2 we show how a block is treated by a node, is encrypted, each block has a previous hash of the last block which contains the last hash, a time stamp that tells us how long it takes to find the correct encryption for each block, if this time is exceeded the transaction is cancelled, a nonce that is a random number that allows us to verify that the old hash cannot be used again by for example repeated attacks carried out by intruders and finally the way in which the hash of each block of a transaction.

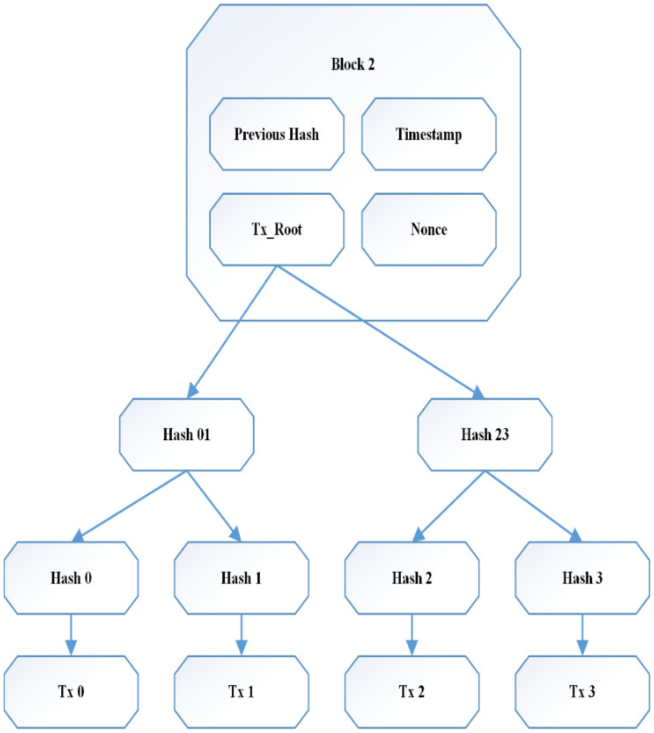

Figure 2: Encryption of each hash transaction in each block

As shown in figure 2 we will use a type of algorithm to generate the hash, the one that offers greater advantage for the blockchain is SHA-256 due to its balance between security and complexity at the moment of generating the keys, for the moment of creating the SHA-256 type key, it will be possible to identify if the transaction has been modified in the trip to its destination, for which the transaction would be rejected when detecting that the hash has changed. By the time the hash has been generated with its algorithm, it will be distributed through the network using the dispersion method, which is commissioned by a search function to find the position of the hash needed, due to this implementation access to keys is almost direct and in a short time, because you would only need one or two memory attempts to achieve your goal by avoiding collisions within the network when distributing hash keys, the search time for each key is independent of how many keys exist within the network.

Applying this set of cryptography to the network we achieve security and robustness, but we must consider the performance of the network due to these applications, we can reduce collisions by not applying this set of cryptographic functions. When the described cryptography is not applied to the network, we will find two main problems that will affect the network seriously, generating two keys pointing to the same index will not be able to store the information creating collision problems that will cause the network to have delays when sending information from node to node, another problem that we found is the agglomeration that occurs at the time the structure causes that commonly used keys tend to fall very close to each other and can fall consecutively, this degrades the network because it accumulated the keys making the cost of processing and time to solve it significantly large in the search. We solve this by applying detailed methods, due to the method of dispersion the search accelerates the desired hash thus avoiding the collision with little use of memory and process achieving a network more robust in security and more efficient when making secure transactions and the crowding will not affect the network due to the search in a few attempts and times.

To develop the system within a distributed scope, it was necessary that the money that is used within the digital portfolios within the virtual net (bitcoin), in this way was guaranteed security and anonymity for each citizen, since no other node will be able to know where the payment comes from or where the payment goes only the main node being the control within the network, it knew at the end of the transaction, who made the payment and to which debt it was addressed.

In order to demonstrate the functioning of the network and all its participants and the functions they performed, the order of operation of the network shall be followed:

The network must have a minimum of 5 active nodes, that is to say that it is not carrying out any activity and that it is waiting for a request, it must be stated with this minimum amount due to the required transactions, that all transactions sent by the nodes will always be divided into 5 tasks that will be solved by the active nodes in this way an order is maintained within the network and an overload of the network or the disutilization of resources is avoided, if there are more than 5 active nodes and they are waiting for requests, these nodes will work as a backup in the event that a node may fail or may no longer be available at the time of the transaction, in this way we ensure that the network is always complete in order to be able to resolve the request. And if there are no nodes available, the transaction will be put on hold until we have the minimum acceptable to resolve the transaction.

2.1. The transaction was generated

A virtual journal was responsible for recording all transactions that have been made within the network, this method was used to record all monetary transactions that were made within the network. The transaction was generated by a node (citizen) and is encrypted under the rules and CoC encryption, which was sent to the administrator node (server of the public entity) of the distributed network, which was in charge of verifying all the rules and conditions are fulfilled.

The transaction was sent to other node that worked as blocks within the chain to solve the complete transaction, different small jobs are assigned to the participating nodes, to be able to resolve the transaction as: resolve that the transaction was made with satisfaction, another node took care that the citizen's monetary balance was reduced from the value paid and another node of the public entity's monetary balance was increased from the value paid by the citizen, another node gathered the information that will be shown once it was confirmed or the transaction was denied, another node was responsible for verifying the encryption of the virtual currencies (bitcoin) is correct, due to this the processing load of the whole transaction was divided into the different nodes belonging to the network, which expedited the workloads and helped the centralized systems of public entities have less transaction burdens, so only the public server was in charge of registering the transactions once they were completed and informing the citizen through their information systems (web page) [8].

2.2. The movements of the network were verified

A user of the blockchain network made a transaction, the transaction was divided into several tasks: verifying the legality of the transaction, decreasing the monetary balance, increasing the monetary balance, recording in the digital journal, these tasks were performed by a different node within of the network, through Ledger technology, the tasks were performed anonymously and distributed throughout the network, in this way each transaction is isolated from the knowledge that the owner of the node [9] can have, without knowing the information that contains the transaction, it was possible to include anonymity to the transactions and the user (citizen), in comparison with a transaction made with a private institution, which earns a commission for carrying out the transaction and which has access to private information generated by the public institution, due to the transaction will run the risk of a leak of information that exists on behalf of the public institution.

The movements that exist in the network are verified both node to node that information is sent by encryption that contains the hash of the past node for a verification that the sent information has not been manipulated or changed, just as the main node is in charge of verifying that the entire block transaction has been successfully completed and at the same time controlling the encryption of each of the blocks, in this way the transaction has not been modified by any intruder external to the network, since its hash will not be recorded within the network, it is assumed that the transaction has been manipulated [10].

2.3. Effectiveness of the transaction

When all the transactions have been resolved by the nodes of the network, and the encryption keys of all the nodes have been verified by the main node, it can be assumed that the transaction has been completed and the main node which is the public institution was in charge of registering the complete transaction, in a centralized database in which no node has access to be able to protect the information of all the participating nodes since there will only be private connection between the main node and the database, with the help of an NC-DRDS framework is responsible for coding all the incoming information of the transactions resolved by the nodes, this decreases the load both in the network and in the database, by sending the compressed data in small blocks, in which the framework is responsible for compressing them in their minimum allowed equivalence and at the same time when it is necessary to decompress it for the use of information [11].

The transaction information once completed, and stored in the database, the web server used this information to replicate it on the public institution's website for the user's use, as for example to be able to see reflected the debt but already once the payment transaction was carried out, in your digital portfolio you can see the decrease in your monetary balance by performing the payment transaction or proof of payment of the debt by means of a certificate issued by the public organization in order to be able to support the physical payment [12].

3. Results

The research demonstrated a model that allowed the public organization to implement Ledger technology more effectively, because of the benefits of Ledger technology can offer to an infrastructure of a public organization.

Figure 3 will show the algorithm that served as a guide for the total resolution process of a user's transaction with a public institution:

Start: The citizen required to make the request for a transaction to make the payment to a public organization, becoming a node of the network.

Data entry: All data necessary to perform the transaction was requested, data will belong to the citizen and public organization, such as digital portfolio, node data, debt list, which are treated only by the main node to ensure data integrity.

Encrypting the transaction: The participating node as the public organization is in charge of encrypting the information they are going to send to the network with CoC encryption, both nodes when encrypting the information ensure that the message cannot be manipulated either by other nodes of the same network or external agents of the same, guaranteeing security to the information of both parties.

Verification of the encryption: The public organization that is the main node receives the information necessary to carry out the transaction and be sent to the network and is in charge of verifying that the encryption of the information that has passed through the network is correct and not has been manipulated and changed, this way we add a more level of security.

Validation of rules and encryption: The main node that is the public organization was in charge of validating that the node requesting the transaction complies with the rules that the server has established, which is greater than 18 years, who has money in his account, who has outstanding debt and to verify the encryption of the node, otherwise if he does not comply with the rule or the encryption is not correct the request is rejected waiting for another request from another node.

Transaction accepted and divided: The transaction was accepted fulfilling all the requirements of the server, a node takes care that the transaction is divided into small processes that were resolved by the other nodes within the network.

Transactions sent to nodes: When the transaction is divided, it is sent to each node of the network, which each will have a different encryption, where each node verifies its own encryption and the transmitting node, avoiding manipulation of information in the course of the network.

Decrease balance: One node took care to resolve this process of diminishing the balance of the digital portfolio of the node that the payment transaction requires.

Increase balance sheet: One node was responsible for resolving this process of increasing the balance of the digital portfolio of the public organization by collecting the debt of the transaction.

Collect information: A node was in charge of gathering the information of the citizen and the debt to be able to show this information at the time of completion.

Verify encryption: A node was in charge of verifying the encryption that the transaction needs once completed, in order to send it to the main node.

Distribute information: A node is in charge of gathering the necessary and public information for the server to publish in its media (web page).

Validation of transactions and their encryptions: validates that all processes ordered to each node have been resolved and that the encryption of all nodes are correct otherwise the transaction is cancelled completely.

Sending to main node: Each node sent to the server that does the main node function, all information already processed.

Gathering information: The main node is responsible for attaching all the information I receive and use to give you.

Database: All information collected by the server was recorded and sent to be stored in the database of the public organization.

Display public information: We proceeded to display information that may be public for the node that requested the transaction by means of media such as web pages of the public organization.

End: Completes the transaction and is expected by another node that requires the resolution of another.

Now, in Figure 3 we describe the algorithm that helped us solve the established needs.

Figure 3 shows us by means of a flow diagram how the system works, but it is not exempt from problems or faults, which are solved by establishing operating conditions within the network, One of the most important problems is when a node has its designated transaction and is no longer available for the network,

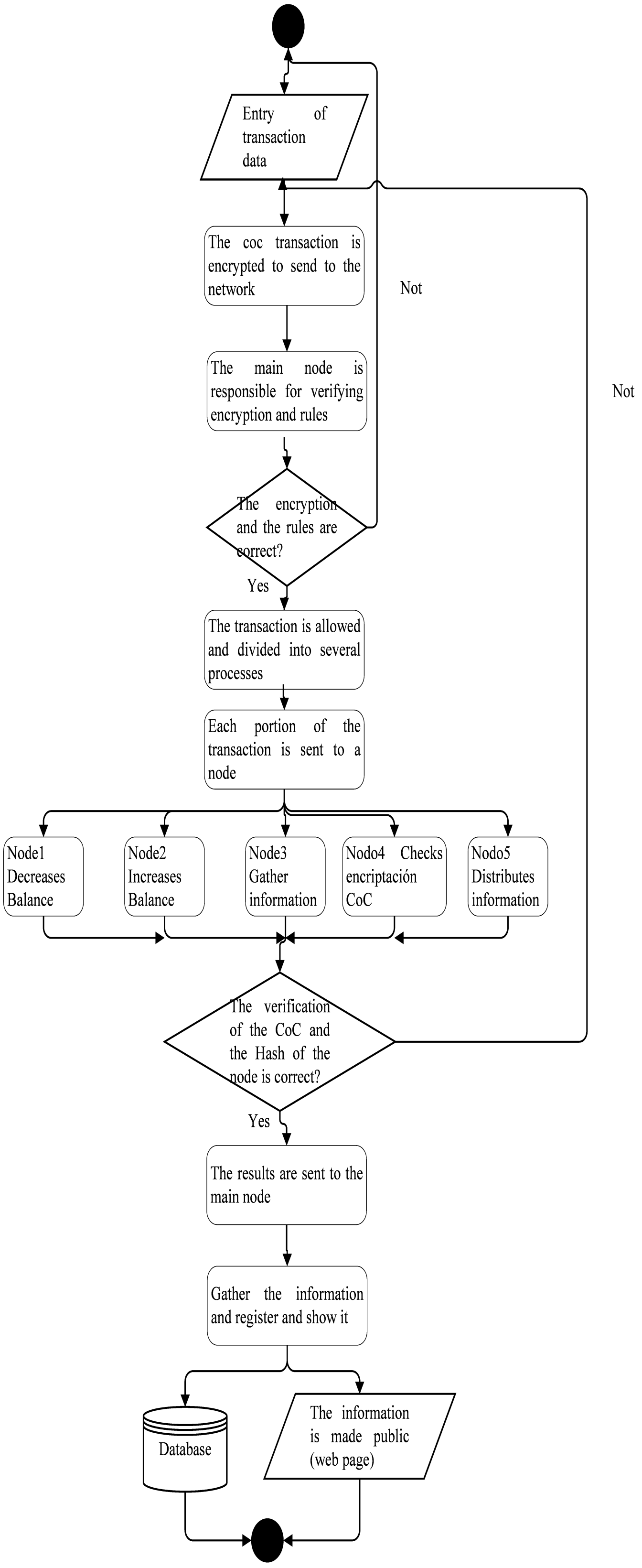
Entry of transaction data
The coc transaction is encrypted to send to the network
Not
The main node is responsible for verifying encryption and rules
Not
The encryption and the rules are correct?
Yes
The transaction is allowed and divided into several processes
Each portion of the transaction is sent to a node
Node1 Decreases Balance
Node2 Increases Balance
Node3 Gather information
Nodo4 Checks encriptación CoC
Nodo5 Distributes information
The verification of the CoC and the Hash of the node is correct?
Yes
The results are sent to the main node
Gather the information and register and show it
Database
The information is made public (web page)

Figure 3: Prototype of the system operating algorithm.

for this a node that is available within the network and is waiting for a transaction, will replace the node that is no longer available, in this way we ensure that the network is always complete to resolve a transaction, although due to this substitution the network will suffer a small delay in operation due to the replacement of nodes, but in this way we ensure its operation and compliance.

In Figure 4 we show a simplified form of the main steps of resolving a distributed transaction.

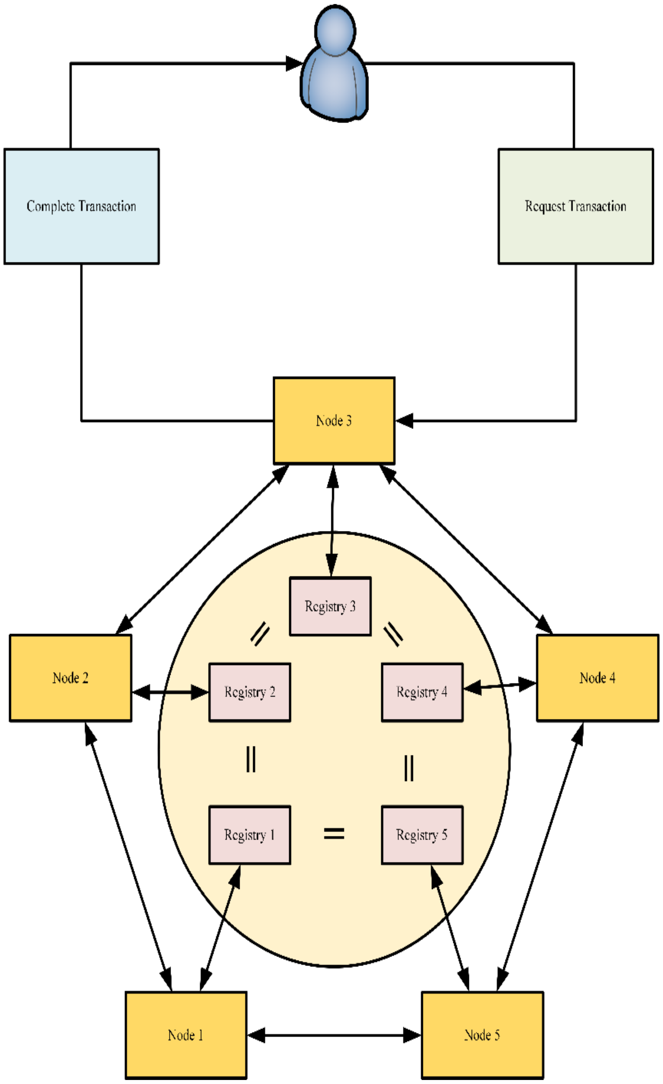

Figure 4: Resolution scheme within the distributed

A user requires the resolution of a payment transaction, the node belonging to the user sends this request to a main node, requesting its processing. Once the application is received, it is sent to the network and other nodes verify the identity of the applicant and certify the transaction in a way as the consensus mechanism declares, confirming that the applicant has the necessary credentials to perform the transaction. Each node oversees resolving each part of the transaction, sending the information resolved by each node to the main server of the public organization, which handles it and shows it to the citizen who made the request.

This scheme ensures a distributed system according to the Ledger technologies, in this way guaranteeing security, efficiency to the whole network and its operation, thus achieving objectives necessary for the success of the implementation.

For the encryption of the messages that are sent in each node, basic encryption offered by the Ledger technology is used, which we will proceed to explain in equation 1 along with its mathematical sustenance:

$$A = g^a \bmod p \tag{1}$$

A random prime number is established which will be p, and a generator g of prime values smaller than p, where the node chooses a number at random smaller than p and is recorded in a, with this proceeds to the calculation of A and sent to the node with which it communicates.

$$B = g^b \bmod p \tag{2}$$

In equation 2 the node does the same work as the node with which it communicates, establishes a prime number, uses a G generator and is calculated in the same way as B and is sent to the node with which it communicates.

$$K = A^b \bmod p = B^a \bmod p \tag{3}$$

In equation 3, it states that the value of K must be equal in both nodes to know that the encryption of both nodes is correct, for which both nodes use the result sent by the other one, This way each node can get its value of K.

At the time a request is sent, the issuer is in charge of searching for the public key that has the receiver's encryption, at this time it encrypts its request with the receiver's key, and when the message reaches the receiver, is in charge of deciphering it using its own hidden key.

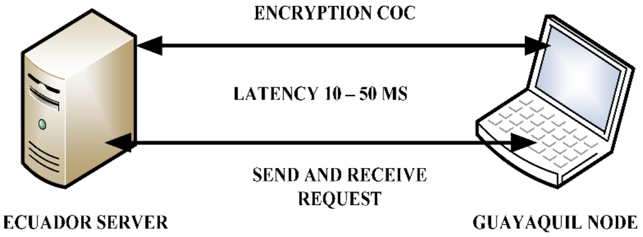

Figure 5: Operation of a node and impact on the network.

As we can see in Figure 5 the performance of a node with the server affecting the network, the main server sends the first message with CoC encryption, which will have a latency of 20 to 30 milliseconds, in order to meet these objectives it must be have a minimum standard for the network, the main one that the network has a bandwidth of 1 megabyte and that the node and server comply with distance limits, in this case by the guidelines generated by the main node, they are within the same country that governs the Public Organization. Once the server and the node have sent and received the encryption, the server sends the request and the node resolves it, for this transaction the latency is affected by the increased information traffic, handling the minimum standard of 1 megabyte of bandwidth, latency can vary between 20 to 50 milliseconds, the difference between the two interactions that have the server and the node, for encryption when using the search method ensures that the network sends less information through the network affecting the latency in the network, decreasing it, on the other hand for the interaction of resolving the request, the latency is increased in the network, because the complete transaction is processed, affecting the latency.

4. Discussion

According to the results of this research of our model we will obtain that the implementation of the blockchain together with a distributed network and centralized systems manage to guarantee benefits such as safety, speed, efficiency, effectiveness, reduction of costs and anonymity between the citizen and his environment except for the public organization that needs such knowledge for the operation of the collection model.

Our algorithm along with the encryption that the network has proposes a more efficient way than the current one in order to carry out the transaction following the standards of the blockchain achieving the proposed objectives.

5. Future Work or Conclusion

The blockchain model has benefits that provide viable features to this model applied to the environment under study, but there are improvements in information encryption and block chain management, we have chosen the methods proposed by the obtained results, but there are improvements with different methods of encryption and system design.

The algorithm generated along with the developed scheme, offer security advantages and are efficient, but for better security and avoid failures within the running model, the public entity (higher authority within the system) must apply very strict rules and maintain control, which will set a higher level of security that will help make the model more robust and safer.

Acknowledgment

The authors thank the Salesian Polytechnic University of Ecuador, the research group of the Guayaquil Headquarters "Information Technology, Security and Information for a Globalized World" (CSITGW) created in accordance with resolution 142-06-2017-07-19 and the Secretariat of Higher Education Science, Technology and Innovation (Senescyt).

References

[1] M. Kohli and E. Suarez, "Centralized solution to securely transfer payment information electronically to banks from multiple enterprise resource planning (ERP) systems," Proc. - 2016 15th Int. Conf. Inf. Technol. ICIT 2016, pp. 275–282, 2017.

[2] M. Wang, Q. Wu, B. Qin, Q. Wang, J. Liu, and Z. Guan, "Lightweight and Manageable Digital Evidence Preservation System on Bitcoin," J. Comput. Sci. Technol., vol. 33, no. 3, pp. 568–586, 2018.

[3] K. Zhang and H. A. Jacobsen, "Towards dependable, scalable, and pervasive distributed ledgers with blockchains," Proc. - Int. Conf. Distrib. Comput. Syst., vol. 2018–July, pp. 1337–1346, 2018.

[4] L. D. Ibáñez, E. Simperl, F. Gandon, and H. Story, "Redecentralizing the web with distributed ledgers," IEEE Intell. Syst., vol. 32, no. 1, pp. 92–95, 2017.

[5] L. Xu, L. Chen, Z. Gao, Y. Lu, and W. Shi, "CoC: Secure Supply Chain Management System Based on Public Ledger," 2017 26th Int. Conf. Comput. Commun. Networks, pp. 1–6, 2017.

[6] R. El Bansarkhani, M. Geihs, and J. Buchmann, "PQChain: Strategic design decisions for distributed ledger technologies against future threats," IEEE Secur. Priv., vol. 16, no. 4, pp. 57–65, 2018.

[7] D. Burkhardt, M. Werling, and H. Lasi, "Distributed Ledger," 2018 IEEE Int. Conf. Eng. Technol. Innov., pp. 1–9, 2018.

[8] M. R. Ogiela and M. Majcher, "Security of Distributed Ledger Solutions Based on Blockchain Technologies," no. c, pp. 1089–1095, 2018.

[9] F. M. Benčić and I. P. Žarko, "Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph," Proc. - Int. Conf. Distrib. Comput. Syst., vol. 2018–July, pp. 1569–1570, 2018.

[10] H. R. Hasan and K. Salah, “Blockchain-based Proof of Delivery of Physical Assets with Single and Multiple Transporters,” IEEE Access, vol. PP, no. 8, pp. 1–1, 2018.

[11] M. Dai, S. Zhang, H. Wang, and S. Jin, “A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain,” IEEE Access, vol. 6, pp. 22970–22975, 2018.

[12] M. Isaja and J. Soldatos, “Distributed ledger technology for decentralization of manufacturing processes,” Proc. - 2018 IEEE Ind. Cyber-Physical Syst. ICPS 2018, pp. 696–701, 2018.