A Hyperledger Model for the Deployment of Smart Contracts in a Public Organization in Ecuador

*Segundo Moisés Toapanta Toapanta
Department of Computer Science
Universidad Politécnica Salesiana(UPS)
Guayaquil, Ecuador
stoapanta@ups.edu.ec

Javier Alfredo Espinoza Carpio
Department of Computer Science
Universidad Politécnica Salesiana(UPS)
Guayaquil, Ecuador
jespinozac1@est.ups.edu.ec

Luis Enrique Mafla Gallegos
Faculty of Engineering Systems
Escuela Politécnica Nacional (EPN)
Quito, Ecuador
enrique.mafla@epn.edu.ec

Ma. Rocio Maciel Arellano
Department of Information Systems
CUCEA- University of Guadalajara
Guadalajara, México
ma.maciel@academicos.udg.mx

***Abstract*—Were analyzed the deployment of a Smart Contract in a Public Organization in Ecuador, also were analyzed a current problem in the Ecuador´s Public Sector, like is the inefficient handling of resources. The objective of this research is to define a model Hyperledger based Blockchain solution. For this research the method selected to this analysis was the method deductive. As results we have a simplified model Hyperledger of the implementation of a Smart Contract, A mathematical model to prove the efficiency of the using Smart Contracts in the processes of hiring in the organizations publics and a Prototype of a generic algorithm for the deployment of a Smart Contract by means of based Blockchain solution. After the analysis it was concluded that the implementation of Smart Contracts both in the Ecuadorians sector public and in any other is a benefit to the organizations.**

Keywords—Blockchain, Hyperledger, Smart Contract, Public Organization

I. INTRODUCTION

The Public Organizations in Ecuador are not currently characterized by the implementation of recent technology due to the high costs that it represents, and due to the difficulty of the implementation. In the country, contracts are handled in a traditional way, being these physical documents in which the contracting parties agree to fulfill one or more obligations and for this the support of a third parties enforcing said legal document is required, the third represents a cost for the contracting parties. Another advantage of the implementation of this technology is that the third parties aren't longer necessary for transactions to be valid, significantly reducing the costs of the bureaucracy or third parties.

The idea of this implementation is avoid the needing of this third party to certify the validity of the contract having a system that meets this function, for it we will use some benefits of Blockchain based technology[2], which will help to fully comply with this assignment.

What would be the impact by the implementation of this technology in an Ecuadorian public's organization? The impact depends on the field in which the company operates; the impact of a service provider company implementing Smart Contracts that will be used for service contracts would not be the same as an organization that implements the Smart Contracts for hiring the employees.

In either case; the implementation brings us important benefits as the case of the service provider company when using Smart Contracts, there would be a record of what was agreed with the contracting parties in the information base of the Blockchain, which could be revised all the time by both parties.

In this research, the authors analyze the results of the implementation of Smart Contracts in a public company in Ecuador through various tools. In the case of the organization that hires employees through Smart Contracts, is similar, since the information stipulated in the contract will also be available and secure in the nodes of a network[3], these being replicated in each node of the network, thus ensuring the availability and continuity of the information.

The objective of this research is to define a model Hyperledger based Blockchain solution.

But is it feasible to implement Smart Contracts in this Sector? The answer is affirmative because the organizations in the Ecuador at the time of agreeing on a contract does in the traditional way in which both parties involved need a third to have that agreement valid, generally a Bank, supporting institution or a third party that accredits said contract.

The importance of implementing Blockchain technology for the use of Smart Contracts in the IoT (internet of things) for a better use or efficient management of time-consuming workflows is highlighted [1]. A smart contract allows with the integration of Blockchain, to perform a self-executing real-time task with a low cost[2]. The new mechanism to manage contracts, based on Blockchain, allows to prevent an attacker from monopolizing resources and in this way keeps the contract information safe[3]. The performance of the Blockchain platform is important in any business application[4]. A decentralized way of storing private data in an immutable way is used that provides us with new approaches to solve common problems in centralized systems[5]. Transactional privacy, information transparency and data immutability are some of the characteristics of the Blockchain[6]. Hyperledger is an open source platform that allows to execute smart contracts in a nodular architecture[7]. Cybersecurity is a very important issue when signing a contract, which is handled very efficiently thanks to the advantages that smart contracts offer us through the Blockchain[8]. It is possible to manage assets safely thanks to the nodular architecture in the Blockchain[9]. The problem of mutual trust between the nodes of the network is solved by means of an algorithm that is the core of the Blockchain[10].

978-1-7281-9466-0/20/$31.00 ©2020 IEEE

Smart contracts have a wide range of applications in both the public and private sectors[11]. The information of a public organization can be managed efficiently and securely through a Blockchain[12]. In the administrative processes of a public organization, cyberattacks should be considered as a threat, which is reduced by implementing a nodular structure in an immutable network such as Blockchain[13]. In electoral processes in a country, the technology offered by The Blockchain gives us the confidence that the electoral information will be reliable and immutable, which guarantees a successful electoral process[14]. There are several components used in the Hyperledger platforms for the implementation of smart contracts through Blockchain, such as endorsers, confirmators and validators[15]. Blockchain has numerous applications in the internet of things such as in health, business, housing [16]. The results of the Blockchain implementation are analyzed [17]. Several processes such as those of insurance companies can be successfully implemented with Blockchain technology [18].

The deductive method was selected and used to perform the analysis of the referenced articles. It's concluded that the implementation of the Smart Contracts in the Ecuadorians sector public is a benefit to the organizations for the offer of robustness, reliability, availability, immutability and security in ours contracts.

II. MATERIALS AND METHODS

A. Materials

The authors determined to achieve automation of the contracting process in public organizations the implementation of Smart Contracts is necessary, under a Hyperledger model. The main actors are the parties involved, which will sign a digital contract in which they must be agree on the contractual details, the conditions of breach of the contract, the responsibility for the breach of the contract and the external verification data sources[4].

The authors proposes the use of a process of creating a Smart Contract to ensure reliability, when a new block is created by means of an algorithm and added to a previous block is needed to solve a computationally complicated puzzle, named a work-test puzzle, the puzzle is resolved competitively to the participants[5].

In this research, the authors proposes the use of Smart Contracts as a solution to the inefficient way in which contracts are currently carried out in public organizations in Ecuador.

The authors suggested a based Blockchain solution that allows reliable networks, because the parties can make transactions even if they don´t know each other. The absence of the reliable intermediary means a quicker reconciliation between the parties that carry out transactions[6], which in turn allows us to benefit in reduction of bureaucratic costs.

Blockchain through Bitcoin has created Smart Contracts in which; the parties that agree are governed by rules of the contract, and once these rules are fulfilled, the agreed upon is carried out [7]. An example would be that two parties sign a contract in which they have an idea that needs to raise a little amount of economic funds to be able to execute, but there is a deadline. The Smart Contract stipulates that if the stipulated amount is not collected until the deadline, the money is returned to the investors and the idea is not carried out.

Steps used in the flow for the realization of a Smart Contract:

- Agreement and creation of a contract between the contracting parties.
- Development of a Smart Contract, the two or more contracting parties are the protagonists, who can be two or more, it is worth mentioning that once the Smart Contract is created, and the contract can't be changed or modified by some of the parties. The Blockchain structure is defined.

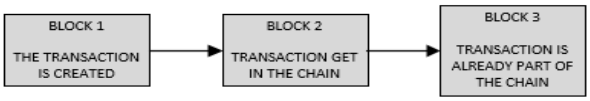

Fig. 1. Transaction created in the structure inside a Blockchain.

In Fig. 1, we can see the states through which our transaction passes, or in this case Smart Contract, following the flow in a very similar way as Bitcoin does.

- Hyperledger solution based in Blockchain allows us to implement this in the determined sector, which gives us the main benefit of not needing an intermediary to make our contracts, allowing us to optimize important public sector resources.
- The information of our Smart Contract is decentralized, immutable and transparent.

Implementing a Blockchain for Smart Contracts also will help us to better manage the supply chain of the resources of a Public Organization, contracts can include what is assets, supplies, money among others that are going to be destined or used by third parties and that are assigned through contracts, in this case Smart Contracts that can automatically assign said resources depending on how we define the rules in the contract[8].

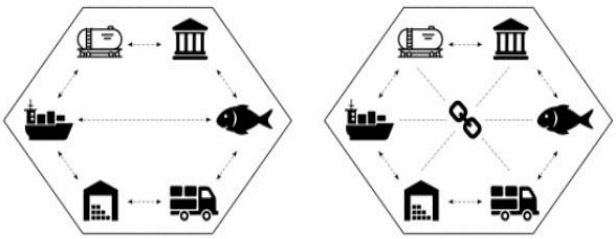

Fig. 2. Traditional SCM (left) is compared to supply chain management based on Blockchain (right).

In the figure 2 we can see a traditional Supply Chain Management distributed, in which there is no a central entity. An SCM fueled by blockchain keeps a distributed ledger, the actors can update and understand the current status of the SCM.

Rights Management. This mechanism includes a new consensus: It is a method that uses a credibility score and creates a hybrid blockchain through this method and test game alternately. This helps prevent an attacker monopolizing the resources[9]. Blockchain is being praised as a technological solution that allows to innovate the way in which the society make the basics activities, this reputation is in particular attributable to its properties of allowing entities that distrust

each other to exchange financial value and interact without relying on a trusted extra[10].

We can define a smart contract like a computer software that consists of a set of rules or politics, are based in the chain of blocks. With the increase of the chain of blocks, Technology in the last ten years, it is demonstrated that it has many fields or areas of application[11]. The deployment of the based Blockchain solution and the Smart Contract gives flexibility to develop and design as well as to implement some of the problems in the society at a lower cost of resources like time and without third party implications as it is traditionally[12]. While there isn't a standard unique in the Blockchain field today, all ongoing efforts involve some combination of transaction, database, encryption, virtualization, consensus and other distributed system technologies[13]. In the administration most production deployments, are also now operational, the emergence of smart devices that are online in the global network and can be accessed and controlled remotely by computer networks[14], it has increased the expectations of new improves[15].

TABLE 1. PURPOSE OF THE PROCESS

Type of Process	Purpose of the Process	Contracting stage
Special regime	Hiring the printing service necessary for the development of activities of unemployment survey Underemployment ENEMDU 2018	Contract Execution
Special regime	Hiring of the national air tickets service, necessary for the development of the activities corresponding to projects currents of INEC	Contract Execution
Special regime	Hiring of the national air tickets service, necessary for the development of the activities of the PAC INEC	Contract Execution
Special regime	Hiring of mobile data service for data boards and Mobile Internet per person	Contract Execution
Special regime	Hiring the cell phone service for the lord executive Director of INEC	Contract Execution

Table 1: Some examples of the Annual Contracting Plan (PAC) as of January 15 (Art. 22 of the Organic Law of the National System of Public Procurement), according to INEC 2018.

We can see in the Table 1 the types of contracts implemented in a public organization, can be perfectly created in Smart Contracts, obtaining in this way the benefits that the implementation of this technology entails in public sector organizations.

B. Methods

1) Analysis for the creation of a Smart Contract

- A website that accepts Bitcoin is used will allow to us to create a Smart Contract
- A public key, is generated and that will serve to give authenticity to our process.
- User creates first transaction and is assigned a value, active etc.
- The hash of the first transaction that is related to the contract is sent.
- The unsigned transaction is sent to the user and it's ciphered.
- The user verifies the information before signing or accepting the contract.
- The stipulations in the contract are met.

Once our Smart Contract is created, we have what is our transaction that can represent digital assets or money. We can assure that our transaction is reliable and is safe since it is replicated for each single nodes of the network. To carry out the Hyperledger model in Smart Contracts, the authors has analyzed the information compiled about Blockchain.

The structure in a Blockchain is similar to a block, which consists of multiple transactions, is connected to a previous block in the form like a chain. Smart Contracts are a set of procedure rules of Scenario-Response and logic. In other words, they are reliable and decentralized shared codes that were implemented in Blockchain.

III. RESULTS

The authors proposed as results of our experiment:

- A simplified model Hyperledger of the implementation of a Smart Contract.
- Prototype of a generic algorithm for the deployment of a Smart Contract by means of blockchain technology.
- A mathematical model to prove the efficiency of using Smart Contracts in the processes of hiring in the organizations publics.

1) A simplified model Hyperledger of the implementation of a Smart Contract

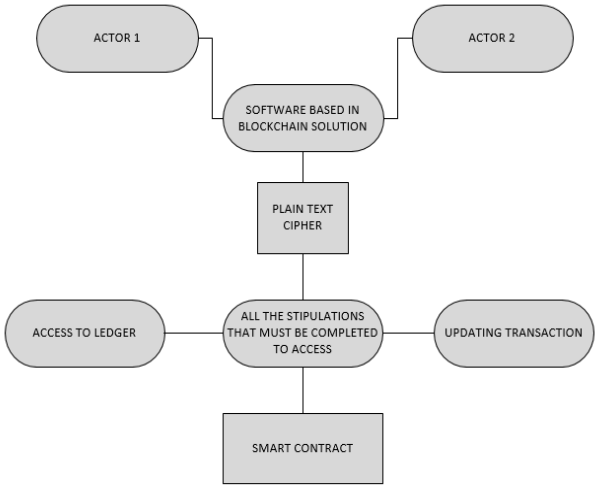

Fig. 3. Model for the realization of a Smart Contract.

In the Fig. 3 we can see we obtains a Smart Contract created without the intervention any intermediary, but with all the reliability and confidence that Blockchain solution based technology provides us.

Mathematical model from the Fig. 3.

$$Ec = \frac{\sqrt{C(na-1)+(na)}}{t*Cpr}*100 \quad (1)$$

The authors proposed a formula based on the Fig. 3, where is calculated the saving resources obtained from the model of the implementation of a Smart Contract; where *C* is the variable of contract, *na* is the amount of actors or parties in the process of hiring in an Organization Public, *t* is the time average in days of the transaction and *Cpr* is the amount of parties (1).

Example: When *C* is 1, *na* is 3, *t* is 10 and *Cpr* is 5 the result is 1.90%; when *C* is 2, *na* is 5, *t* is 14 and *Cpr* is 8 the result is 5.14% of saving resources.

2) Prototype of a generic algorithm for the deployment of a Smart Contract by means of Blockchain technology

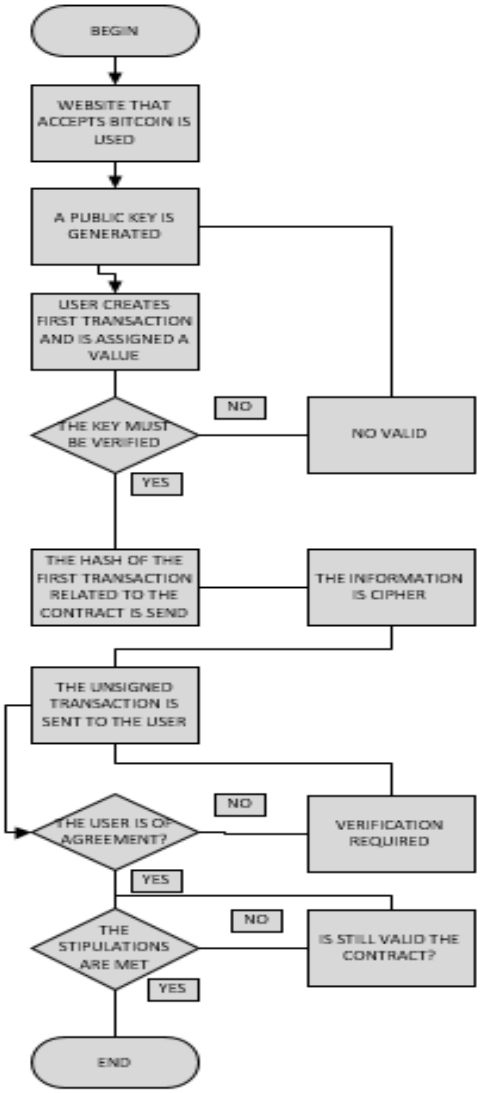

Fig. 4. Prototype of a generic algorithm for the deployment of a Smart Contract by means of Blockchain technology.

In figure 4 we can see that the algorithm follows the flow of creating a transaction in a smart contract, in which a verification is made if the users agree with the provisions of the contract, and then a second verification is carried out in which if the information was previously validated by means of the generated key, the flow continues and the Smart Contract is created.

Mathematical model from the Fig. 4.

$$Ed = \frac{ni+1}{\sqrt{ntc*ntr}+nc}*100 \quad (2)$$

The authors proposed a formula to calculate the additional information based on the algorithm from the Fig. 4, where *ni* is the amount of parties involved in the process of hiring, *ntc* is the amount of transactions in the process of hiring in an Organization Public, *ntr* is the amount of validations to the process and *nc* is the amount of contracts. When *ni* is 2, *ntc* is 1, *ntr* is 3 and *nc* is 2 the result is 8.04%; of additional information generated.

The authors used a website that accepts Bitcoin, a public key is generated, user creates first transaction and is assigned a value, active, etc., the hash of the first transaction that is related to the contract is sent, the unsigned transaction is sent to the user, the user agrees, depending on this, it is determined if the contract has to be re-verified by the issuer, the stipulations of the contract are complied with and it remains in force until its fulfillment.

Through the steps carried out in the algorithm, we can also verify that the contract information is kept safe, only the interested parties participate.

The Advantages of implementing a Smart Contract

- As the main advantage we have the optimization of resources by not needing an intermediary to grant validity to our contract.
- Have always updated our information about contracts.
- A very good security based on the Blockchain technology.

3) A mathematical model to prove the efficiency of the using Smart Contracts in the processes of hiring in the organizations publics.

As the authors has mentioned in the solution proposed to the inefficient way in that the organizations publics in Ecuador hiring, one of the principal reasons is the avoidable costs that represent the third parties, so we have the equation to evaluate the improvements that the implementation of Smart Contracts offers.

$$E = \frac{(Ra*100)/Ptc}{Er/10}(100) \quad (3)$$

In the equation where Ra is the currently cost with the Smart Contract implemented and the Er is the expect result without the Smart Contract or the traditional cost with third parties. The result achieved is 60% less in comparison with the expected result without the implementation of Smart

Contract, and PTC would be the number of participants (only two) in the transaction(3).

IV. DISCUSSION

According to the results obtained, through the methods proposed by the authors we can see that the process of creating a Smart Contract was performed in a very simple and practical way compared to the traditional way in which contracts are currently carried out in Ecuador, and we got the benefits of implementing smart contracts in a company.

In the research process, it was identified that an important consideration that must be taken for the implementation of Smart Contract is the business model of the public organization, due it was found that the efficiency of Smart Contracts can vary depending the business model. The implementation of smart contracts in a public organization is an open topic for discussion, since depending on the business model of the organization, it will be more convenient or not to use this solution Blockchain based.

For each case depending of the type of contract to be executed, it is necessary to carry out an analysis in relation to the subject, in certain cases there is sensitive information handled by public organizations that are generally not in the public domain, for security reasons. In this work the characteristics of implementing Smart Contracts were exposed. The flowchart of the experiment is subject to changes or modifications according to the business model of our organization, and remember that a public organization can be dedicated to providing services and products, Smart Contracts can handle perfectly.

V. FUTURE WORK AND CONCLUSIONS

The encryption of information through Smart Contracts, the immutability of the Blockchain and the no longer having the need to have a third party to hiring in the public sector has an important role for the public organizations for the optimization of the handled resources.

It is advisable that when carrying out this implementation in a public organization, the issue of cost be analyzed, which can be a significant investment but will provide significant benefits, as we saw in the research.

A topic of future research is suggested to be the implementation of Hyperledger specifically in the public medical system, several types of contracts are handled which it would be interesting to investigate.

The authors have concluded that:

- The implementation of Smart Contracts in the Ecuadorians sector public and in any other is a benefit to the organizations due the solution Blockchain based used for the creation of the contract, due to the offer of robustness, reliability, availability, immutability in ours contracts.
- The transparency of the information handled in public contracts is a very important point which is guaranteed with the use of Smart Contracts due the contract is always available to the parties involved.
- The Smart Contracts offers us the same level of security that Bitcoin offers, so we can be sure that the information cannot be altered, preserving its veracity and validity any time.

A point to mention is that a potential problem that the implementation of this technology could present is the confidentiality of certain information of the state or of the organizations that have a confidential nature, due the information of the contracts in a decentralized network it is open to people to consult the information of the contracts, having as a solution to this problem the implementation of private Blockchains, which would be subject of future study.

ACKNOWLEDGMENT

The authors would like to thank to Universidad Politécnica Salesiana from Ecuador, to the research group of the Guayaquil Headquarters “Computing, Security and Information Technology for a Globalized World” (CSITGW) created in accord to resolution 14206-2017-07-19 and Senescyt (Secretaría de Educación Superior Ciencia, Tecnología e Innovación).

REFERENCES

[1] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," 2016.

[2] B. K. Mohanta, S. S. Panda and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," IEEE, 2018.

[3] C. Mohan, "Blockchains and Databases: A New Era in Distributed Computing," IEEE, 2018.

[4] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," IEEE, 2018.

[5] K. Wust and A. Gervais, "Do you Need a Blockchain?," 2018.

[6] Y. Hao, Y. Li, X. Dong, L. Fang and P. Chen, "Performance Analysis of Consensus Algorithm in Private Blockchain," 2018.

[7] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain contract: Securing a Blockchain applied to smart contracts," IEEE, 2016.

[8] H. Sukhwani, N. Wang, K. S. Trivedi and A. Rindos, "Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network)," IEEE, 2018.

[9] P. Yuan, X. Xiong, L. Lei and K. Zheng, "Design and Implementation on Hyperledger-based Emission Trading System," IEEE, 2018.

[10] C. DeCusatis, M. Zimmermann and A. Sager, "Identity-based network security for commercial Blockchain services," IEEE, 2018.

[11] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin and F. Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," IEEE, 2018.

[12] S. Toapanta, F. De La Rosa, E. Fernandez, F. Trivino and L. Gallegos, "Prototype to optimize the management of information security used by internal users in a public organization of Ecuador," in *CITS 2019 - Proceeding of the 2019 International Conference on Computer, Information and Telecommunication Systems*, 2019.

[13] S. Toapanta, I. Ochoa, R. Sanchez and L. Mafla, "Impact on administrative processes by cyberattacks in a public organization of Ecuador," in *Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2019*, 2019.

[14] S. Toapanta, J. Piguave and L. Gallegos, Analysis of Adequate Bandwidths to Guarantee an Electoral Process in Ecuador, vol. 165, 2020, pp. 255-265.

[15] P. Thakkar, S. Nathan and B. Vishwanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," IEEE, 2018.

[16] A. Stanciu, "Blockchain Based Distributed Control System for Edge Computing," IEEE, 2017.

[17] L. S. Sankar, M. Sindhu and M. Sethumadhavan, "Survey of consensus protocols on Blockchain applications," 2017.

[18] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay and K. Y. Lam, "A Blockchain Framework for Insurance Processes," IEEE, 2018.