

A Blockchain Approach to Mitigate Information Security in a Public Organization for Ecuador

Moisés Toapanta¹, José Mero², Dario Huilcapi³, Máximo Tandazo⁴, Antonio Orizaga⁵, Enrique Mafla⁶

^{1,2,3,4}Computer Science Department, Universidad Politécnica Salesiana – Sede Guayaquil, Chambers 227 and 5 of Junio, Guayaquil, Ecuador – stoapanta@ups.edu.ec, jmeroa@est.ups.edu.ec, dhuilcapi@ups.edu.ec, mtandazo@ups.edu.ec.

⁵Informations Systems Department CUCEA, Universidad de Guadalajara, Periférico Norte No 799, Nucleo Universitario, Los Belenes, C.P. 45100, Zapopan, Jalisco, México – jose.orizaga@academicos.udg.mx

⁶Faculty in Engineering Systems, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito, Ecuador. Enrique.mafla@epn.edu.ec

Abstract. It was analysed in a general way and the security problem of the public organizations of Ecuador was determined. The objective is to generate a prototype in a blockchain diagram, based on an algorithm using flowchart techniques to provide robustness against failures, third-party attacks and mitigate information vulnerabilities. The deductive and exploratory research method was used in order to analyse the information available in the medium and scientific articles. Resulted an algorithm developed through flow diagram techniques to improve the processing of information in a public organization in Ecuador from the use of the Blockchain technology and the use of the SHA 256 algorithm. It was concluded that access to the data to a generic public organization of Ecuador will have an alternative to improve the security of the information with the implementation of the blockchain.

1. Introduction

The public Organizations of Ecuador and several countries of the world have problems of integrity in the security of the information; to solve this problem, one of the alternatives is the implementation of safety rules based on blockchain technology[1].

The blockchain is a technology that originated from bitcoin, providing robustness against faults and attacks, as well as functions for the origin of data[2].

The blockchain provides a unique data storage between pairs of replicated transactions and enables new forms of distributed software architectures, where an agreement can be established on how to share decentralized and transactional data in a large network of third party participants[3].

Why is it necessary to identify the operation and perform the analysis of blockchain technology as an alternative to mitigate the security of information of a Public Organization of Ecuador?

The objective is to generate a prototype in a blockchain diagram, based on an algorithm using flowchart techniques to provide robustness against failures, third-party attacks and mitigate information vulnerabilities.

The articles related to the subject analyzed are:



Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT[1]; Integrating blockchain for data sharing and collaboration in mobile healthcare applications[2]; Evaluating Suitability of Applying Blockchain[3]; The use of authentication technology blockchain platform for the marine industry[4]; An Overview of the Emerging Technology: Blockchain[5]; Blockchain Based E-Voting Recording System Design[6]; Blockchain Application in Food Supply Information Security[7]; The applicability of blockchain in the Internet of Things[8]; Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G[9]; A Blockchain Framework for Insurance Processes[10]; Decentralization Transaction Method Based on Blockchain Technology[11]; A comprehensive integration of national identity with blockchain technology[12]; Checking laws of the blockchain with property-based testing[13]; A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain[14]; Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks[15].

The method used in this research is deductive and exploratory with the purpose of analyzing the information available in the medium and scientific articles.

It is concluded that access to data to a generic public organization in Ecuador will have an alternative to improve information security with the implementation of the blockchain in their systems of security.

2. Material and Methods

2.1 Materials

The information of the published articles was used to analyze the situation of a generic Company of the Public sector of Ecuador in terms of information security.

In this phase, all the articles that have to do with the investigation were analyzed. The basic structure of the blockchain technology shown in Fig. 1 was analyzed.

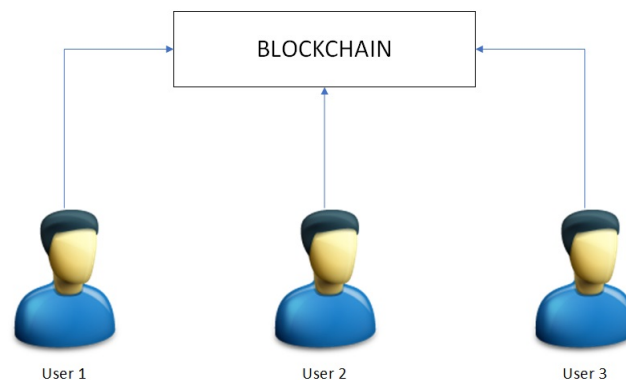


Fig. 1. Basic structure of the blockchain

The requirements of the blockchain technology are defined, establish procedures for the protection of access, protect the information of modifications or eliminations of third parties[4].

Some of the characteristics of Blockchain: Immutable, it means that it is really difficult to alter; irreversible, that what has already been done cannot be undone; distributed system means that a copy of the ledger is present with all its members; without centralized authority, it does not depend on a central server to master and, therefore a peer-to-peer system; elasticity, this characteristic shows that it is not prone to any kind of attack of consideration[5].

Blockchain is a public and distributed database in which all transactions are registered that work through a distributed network of computers, that is, it does not require any central authority or third parties to act as intermediaries[6]; it works just like a ledger but in this case the notes are public and decentralized.

Blockchain is formed by a block chain designed exclusively to avoid its alteration once the data has been published. There are several information security algorithms, but for the present work, those detailed in Table 1 were considered.

Table 1. Types of hashing algorithms

| Hash Algorithms | Description |
|-----------------|---|
| MD5 | (Message Digest Algorithm 5) Creating digital signatures |
| SHA-1 | (Secure Hash Algorithm) |
| RSA | (Rivest, Shamir, Adleman) encryption key |
| SHA 256 | Secure Hash Algorithm 256 |

The authors propose a solution for integrity and non-repudiation using blockchain technology that provides everyone with decentralized trust; the blockchain that can be described as a public book that is impossible to alter. Each user or node has exactly the same ledger as all other users or nodes in the network[7]; This ensures consistency to users.

This transfer does not require a centralized intermediary to identify and certify the information, but it is distributed in multiple independent nodes that register and validate it without the need for trust between them; once entered, the information cannot be deleted, only new records can be added, and will not be legitimized unless most of them agree to execute[8].

The Hash SHA256 of the encrypted resource. Although we cannot obtain the information directly through the transaction, the integrity and authenticity of the encrypted information can be verified by the Hash value[9].

SHA-256 is used in the creation of public keys or addresses and in Bitcoin mining. Mining or mining is the term used to refer to adding blocks to the chain of blocks in Bitcoin. Therefore, the responsibility of the miner is to deal with the accepted transactions and add them to the blockchain public ledger. In Bitcoin, a work test function is used to guarantee the consensus of the network.

The blockchain processing involves the following steps according to Fig. 2 and the reference[10]:

1. The blockchain, as its name suggests, is a chain of blocks. Each of these blocks contains the encoded information of a transaction in the network.
2. Each block of the chain carries the package of transactions and two codes, one that indicates which is the block that precedes it (except the source block, of course), and another for the block that follows it, that is, they are interlinked or chained so they are called hash codes or pointers.
3. The process of validating the information. In the process of mining or checking, when there are two blocks that point to the same previous block, it simply wins the first one to be decrypted by most of the nodes, that is, that most points in the network must agree to validate information.

Therefore, although blockchain generates multiple block chains, the longest chain of blocks will always be legitimized.

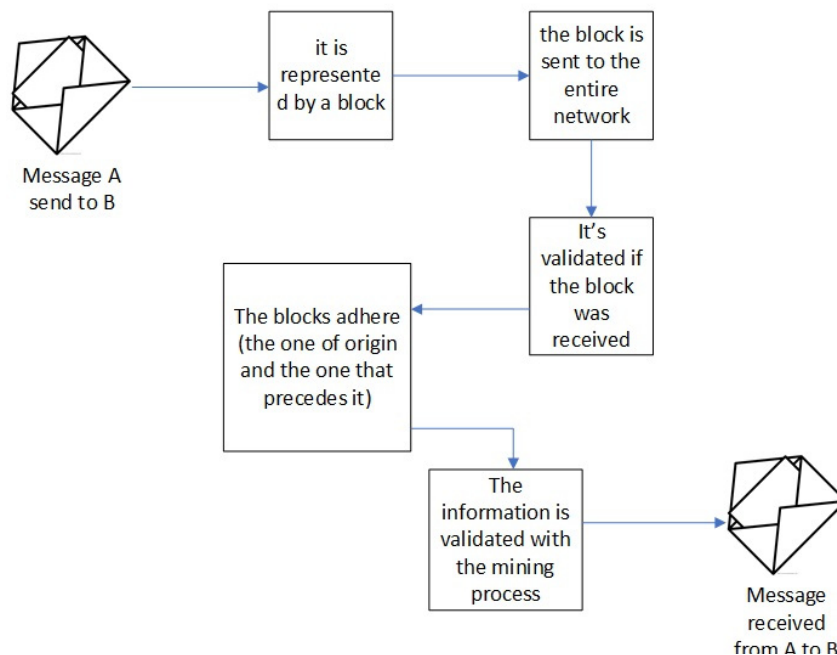


Fig2. Blockchain working process

The authors propose an architecture where security is granted through the blockchain technology, which are data integrity and the robustness of the against errors and malicious attacks; according to the analysis, the algorithm to be used is the SHA 256[11].

The algorithm SHA 256 performs the encryption of the information sent or requested by the users. A prototype is proposed where it shows that the integrity of the data and privacy is guaranteed; using the SHA 256 encryption algorithm and the blockchain technology to each data upload or download transaction.

2.2 Methods

For this research, the deductive method was applied to determine the correct use of Blockchain technology in a generic public organization in Ecuador.

1. In the first phase, a general structure of the blockchain was analyzed.
2. In the second phase the specific process that makes it blockchain was analyzed.
3. In the third phase, the different types of most relevant hash algorithms were analyzed.
4. In the fourth phase it was determined to choose the algorithm SHA 256 for encryption for the creation of public keys or addresses.

3. Results

From the analysis performed, an algorithm was obtained using flow diagram techniques for the treatment that can be offered to the public organization of Ecuador using the Blockchain technology and the use of the SHA 256 algorithm.

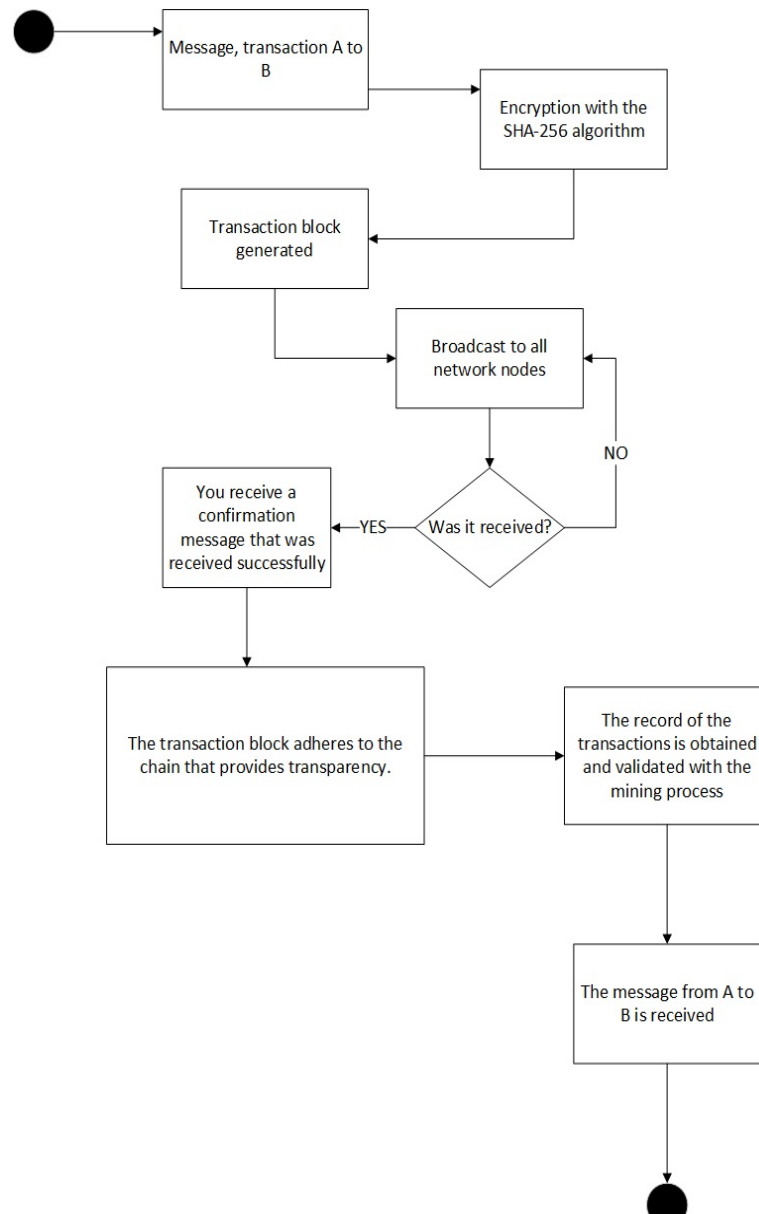


Fig. 3. Blockchain operating process (Algorithm)

The steps that were used in the prototype can be seen in Fig. 3:

1. **Start:** The main activities were loaded into the memory so that the information system can create the processing objects.
2. **Message or Transaction:** Once the system was started, the necessary data that the process requires was entered, after which you can send or make any transaction.
3. **Encryption of data:** It is done through the SHA-256 algorithm.
4. **Broadcast:** The message or transaction is sent to all the nodes in the network.
5. It is asked if the package was received or not in all the nodes of the network, if not, it is sent again to all the nodes of the network if the next step is continued.
6. **Confirmation:** A message is received that was received successfully from all the nodes in the network.

7. **Transaction block or message:** The transaction block adheres to the chain created by the blockchain that will provide transparency and reliability of the data[12].

8. **Mining process:** Here you get the record created by the blockchain process where all the transactions are generated and validated by the mining process that takes place when two blocks point to the one where the first one wins to be decrypted[13].

9. **End:** The process was completed successfully. And the resources were free for a subsequent execution.

The proposed flow chart will help to ensure several failures either by employees, third parties or people who want to harm the organization. This diagram will guarantee the integrity of the data and mitigate the security of the information.

4. Discussion

The results obtained in the research were the authors' criteria on the security of information in systems that determine integrity and security as a priority.

In the research the prototype of an algorithm was obtained using flowchart techniques on the use of the blockchain as an alternative to mitigate the security of the information in a generic public organization of the Ecuador.

The prototype raised, can be taken as a reference for other companies apart from the Public Company of Ecuador.

It was concluded that the Blockchain technology can efficiently assure the information that is shown to the user, because when combining peer-to-peer technology a new form of digital exchange is created so that unexpected changes of the information do not occur[14][15].

5. Future Work and Conclusions

In order to determine the vulnerabilities and risks of the information, the evaluation of each process and systems available to the generic public organizations of Ecuador must be done prior to the implementation of the blockchain as an alternative to get better the security of the information.

From the research carried out, the following can be concluded:

1. The access to the data to a generic public organization of Ecuador will have an alternative to improve the security of the information with the implementation of the blockchain in their systems the security.
2. Blockchain becomes a fundamental rule to provide security, robustness against failures and attacks from third parties.
3. That the integrity of the information in the generic public organizations of the Ecuadorian state have a higher priority over confidentiality and authenticity.

Acknowledgment

The authors thank CUCEA of Universidad de Guadalajara, Jalisco, México, Program IT PhD Information Technologies, Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters "Computing, Security and Information Technology for a Globalized World" (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaria de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References

- [1] O. Novo, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," IEEE Internet Things J., vol. 5, no. 2, pp. 1184–1195, 2018.
- [2] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC, vol. 2017-October, pp. 1–5, 2018.
- [3] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, "Evaluating Suitability of Applying Blockchain," Proc. IEEE Int. Conf. Eng. Complex Comput. Syst. ICECCS, vol. 2017-November, pp. 158–

- 161, 2018.
- [4] D. G. Mamunts, V. E. Marley, L. S. Kulakov, E. M. Pastushok, and A. V. Makshanov, "The use of authentication technology blockchain platform for the marine industry," 2018 IEEE Conf. Russ. Young Res. Electr. Electron. Eng., pp. 69–72, 2018.
 - [5] R. Chatterjee and R. Chatterjee, "An Overview of the Emerging Technology: Blockchain," 2017 3rd Int. Conf. Comput. Intell. Networks, pp. 126–127, 2017.
 - [6] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl., pp. 1–6, 2017.
 - [7] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain Application in Food Supply Information Security," pp. 1357–1361, 2017.
 - [8] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the Internet of Things," 2018 10th Int. Conf. Commun. Syst. Networks, pp. 561–564, 2018.
 - [9] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, 2018.
 - [10] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K.-Y. Lam, "A Blockchain Framework for Insurance Processes," 2018 9th IFIP Int. Conf. New Technol. Mobil. Secur., pp. 1–4, 2018.
 - [11] Q. Liu and K. Li, "Decentration Transaction Method Based on Blockchain Technology," 2018 Int. Conf. Intell. Transp. Big Data Smart City, pp. 416–419, 2018.
 - [12] K. Mudliar and H. Parekh, "A comprehensive integration of national identity with blockchain technology," 2018 Int. Conf. Commun. Inf. Comput. Technol., pp. 1–6, 2018.
 - [13] A. Chepurnoy and M. Rathee, "Checking laws of the blockchain with property-based testing," 2018 Int. Work. Blockchain Oriented Softw. Eng., pp. 40–47, 2018.
 - [14] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," 2017 3rd IEEE Int. Conf. Comput. Commun., pp. 1180–1184, 2017.
 - [15] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks," IEEE Trans. Smart Grid, vol. 3053, no. c, pp. 1–12, 2018.