Model for the elaboration of Smart Contracts using the Cardano network

Walter Orozco
Email: worozco@upse.edu.ec; wa.orozco@alumnos.urjc.es
ORCID code: https://orcid.org/ 0000-0002-8224-1152
Affiliation: Universidad Península de Santa Elena, Ecuador; Universidad Rey Juan Carlos, Spain

Jaime Orozco
Email: jorozco@upse.edu.ec
ORCID code: https://orcid.org/ 0000-0002-6929-1411
Affiliation: Universidad Península de Santa Elena, Ecuador

Julio Orrala Moreira
Email: julio.orralamoreira@upse.edu.ec
ORCID code: https://orcid.org/0000-0002-0904-0979
Affiliation: Universidad Península de Santa Elena, Ecuador

Mercedes Villarroel
Email: mercedesj.villarroel@educacion.gob.ec
ORCID code: https://orcid.org/0000-0001-8373-5747
Affiliation: Unidad Educativa Salinas (24H00272)

Abstract

Technology plays a preponderant role in many areas of daily business. Organizations invest and use technology as a basic tool in every process. In the business environment, contractual activities are formalized by employing a contract. The elaboration of a contract requires two entities involved and a validating entity, where it is specifically and objectively stated how it will be carried out. The objective of this article was to propose a model for the elaboration of Smart Contracts using the Cardano network, as well as to analyze the main characteristics of Latin American scientific production regarding the study of Smart Contracts. Among the main findings is that of the Latin American countries. Brazil was the nation that achieved the highest number of publication records carried out in high-impact journals indexed in the Scopus database during the period 2017-2021, with a total of 97 documents. It is expected that, through the development of this research, the design of models for the development of Smart Contracts will be achieved to optimize such processes within the organization.

Keywords: Smart Contracts, Cardano Network.

DOI Number: 10.14704/nq.2022.20.13.NQ88316 Neuro Quantology 2022; 20(13):2548-2554

1. Introduction

All contractual relationships are carried out with confidence in the fulfillment of this; it is a priority to deal adequately with the terms of a contract, eliminating the asymmetric factors of the information that may arise, the breach of one of the parties to the contract brings with it the loss of confidence, customer or credibility and increased conditions for the development of future contracts. In addition, technological advances have become indispensable for business, improving certain processes and reducing the time required to obtain results.

Blockchain technology brought with it, among other benefits, the possibility of making smart contracts; this help fulfill the terms stated in the contracts without intermediaries, granting another method of payments to foreign clients. The "Smart Legal Contract" is a new form of contracting in the Ecuadorian commercial code.

Smart legal Contracts are a legal figure with high growth potential that marks great expectations in

its application, as they are a safe and effective means of contracting capable of being executed thanks automatically to Blockchain technology; when the fulfillment of a condition is verified, this quality cannot be ignored as no other known mechanism in Law has managed to provide legal certainty to the parties in the way that a smart legal contract does [2].

It has been corroborated that the execution of smart contracts responds to objective criteria, i.e., a consequence can only be triggered if the verifiable fact involves a material valuation; this statement is given thanks to the Boolean logic by which smart contracts work; on the contrary, circumstances that are subject to interpretation cannot be verified, so their application is technically limited, despite this, there are several areas in which a smart contract can be perfectly applied and thus take advantage of its full potential [2].

The use of platforms that make contracts more simple is the idea that people who practice or study law should be doing or projecting and specializing in programming to make electronic legal contracts in order to create a new branch of study and thus improve every day the worldwide acceptance of smart contracts to improve what we know as the internet of things [3].

The self-executability is one of the essential elements at the time of the use or consent of these contracts since it can be used as a tool to fulfill requirements without the need for someone to intercede to enforce the parties, only with the simple fact that both parties belong or are within the blockchain, this is executed alone if the selling party does not comply with the agreed automatically the money negotiated within the blockchain [3].

In this context, signing a contract can become a problem if the parties are not present, either synchronously or asynchronously. Therefore, the goal is to have a methodology or tool that allows the creation of an intelligent contract supported by the Cardano Network technology and guarantees compliance without the obligatory presence of the actors for the respective signature. This activity is very beneficial for businesses where time and costs are key factors and agility in operations is required; shipping companies are an example.

2. General Objective

To propose a model for the elaboration of Smart Contracts using the Cardano network, as well as to analyze the main characteristics in the Latin American scientific production regarding the study of Smart Contracts.

3. Methodology

The construction of smart contracts requires a proper way of working; fulfilling the established phases allows a formal document for the transaction to be fulfilled. The following scheme shows the 4 phases to be fulfilled:

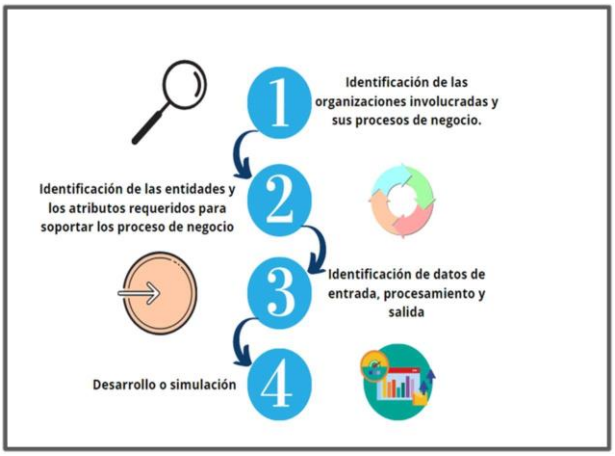

Figure 1. Methodological design

Source: Own elaboration.

✓ Identification of the organizations involved and their business processes

The first step is to determine which organizations are involved in the project; for this, people can consult the history of customers who have accessed the services and, in the case of other companies or organizations, consider their origin. Some countries have policies regarding this type of contract or linkage and their currency of exchange. Business processes are the basic element; to identify them, it is possible to check if there is already documentation of these processes, which can be automated in the organizations involved [7].

Related data is stored in the blockchain; the storage capacity of a block can be a limitation, which is why determining the importance of the data to be included should be a priority. To help decide what information should be stored, the

following questions should be answered the attribute of interest to more than one organization involved in the system; if so, does the attribute require the non-repudiation property; is it of interest to the organizations involved to obtain information about the transactions that have modified the attribute; is it of interest to the organizations involved to obtain information about the transactions that have modified the attribute; and if so, does the attribute require the non-repudiation property. If yes to the above questions, it is very likely that the evaluated data should be stored on the blockchain [7].

✓ **Identification of the entities and attributes required to support the business processes.**

With the attributes identified to be stored in the blockchain, it is necessary to define the different operations or actions that are required to be performed on the attributes to fulfill the objective of the business process. To perform such a task, it is necessary to ask the following question: does this activity modify the attributes stored in the chain? If the answer to this question is yes, then the activity should be implemented through a smart contract [7].

✓ **Identification of input, processing and output data.**

In general, companies manage five steps to provide services, where each one contributes to the fulfillment of an established contract, divided as follows:

Tickets:

- Request for services through any communication method: The customer communicates with the company through its web portal, mail, etc. Where he/she specifies the service he/she wishes to acquire.
- Payment method: It must be specified from the beginning if it is credit or cash and if they are from the same bank or to which bank the transaction should be made. Processing:
- Payment validation: We wait until the payment has been made and confirmed with the respective financial institution.
- Invoicing: The invoice for the services to be provided is made, and the net costs of the company do not include the additional values of commissions by the banking entities. Outputs:
- Report: It details the activities carried out by the company, where the fulfillment of the services is written and delivered to the captain or person in charge of each vessel.
- Service: The activity detailed in the services provided by the company is carried out, complying with established deadlines and dates.

✓ **Development or Simulation**

Once the previous steps have been completed and taken to support the information flow diagram that reflects the order to be followed to generate the contract, it is possible to code or capture the processes through Haskell or Blockly, using the Marlowe tool. With this tool, it is possible to simulate a direct interaction with the blockchain, and thus be able to specify the "Smart Contracts." In addition, the tool allows a testing and validation process before putting it into production. Using a development model is the right way to achieve a stable solution and minimize errors. The development time will depend on the type of contract, its complexity and the factors involved; therefore, it is necessary to have an adequate level of specificity and objectivity.

4.1 Bibliometric review

Bibliometric review on the variable *smart contracts* to know the current state of the literature published in high-impact journals indexed in the Scopus database during 2017-2021 by Latin American institutions.

4.1.1 Data collection for the bibliometric review.

Quantitative analysis of the information provided by Scopus under a bibliometric approach on the scientific production related to the study of smart contracts is carried out.

The search is performed through the tool provided by Scopus and the parameters referenced in Figure 2 are established.

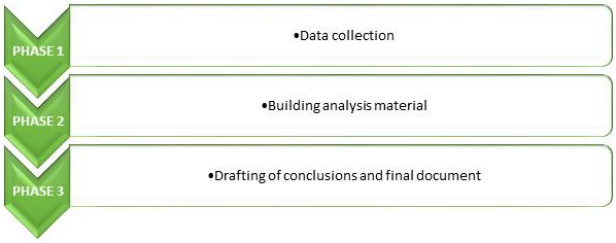

Figure 2. Phases of data collection.

Source: Own elaboration

4.1.1.1 Phase 1: Data collection

The data collection was carried out through the Scopus web page search tool, through which a total of 162 publications were identified. For this purpose, search filters were established consisting of:

- ✓ Published papers whose study variables are related to the study of Smart Contracts.
- ✓ Limited to Latin American countries.
- ✓ Without distinction of area of knowledge.
- ✓ Without distinction of type of publication.

4.1.1.2 Phase 2: Construction of analysis material

The information identified in the previous phase is organized. The classification will be made through graphs and figures based on data provided by Scopus.

- ✓ Word Co-occurrence.
- ✓ Year of publication
- ✓ Country of origin of the publication.
- ✓

4.1.1.3 Phase 3: Drafting conclusions and final document

After the analysis carried out in the previous phase, the study drafts the conclusions and preparing the final document.

4. Results

The Smart Contracts design methodology applied to Cardano's network demonstrates a significant reduction in the time to draw up and formalize the contract and the time to pay for the services to the beneficiary of the contract. Costs are reduced when using the Cardano Blockchain. When using wallets belonging to this network, there is no fee for transferring to another digital wallet; otherwise, a bank transfer to foreign financial institutions has additional charges according to the legislation of the country where the transactions are carried out.

Table 1. Comparison between contract characteristics.

Variable	Smart Contract	Traditional contract
Weather	Defined before starting	Varies according to execution
Cost	No commissions	Transaction fee

Source: Own elaboration

The table above compares two basic characteristics of contracts: time and cost. While the cost in a smart contract may be present, it will depend on the network used for transactions.

4.1 Bibliometric analysis

The main characteristics of the volume of scientific production related to the topic proposed by this article are presented below. A total of 162 studies related to the analysis of Smart Contracts were identified.

4.1.1 Keyword co-occurrence

Figure 3 shows the co-occurrence of keywords within the publications identified in the Scopus database.

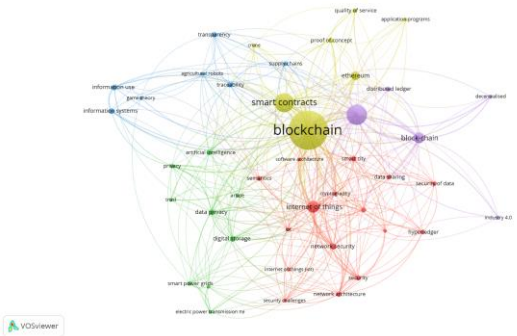

Figure 3. Word co-occurrence

Source: Own elaboration (2022); based on data provided by Scopus.

Blockchain was the keyword used most frequently within the scientific production identified through the Scopus search parameters established above; this variable is a new technology based on hashing, which is at the base of the platforms for cryptocurrency trading and the execution of smart contracts, in fact, Smart Contracts was the variable that showed the highest correlation in the implementation of research projects associated with the study of the proposal for the development of this type of contracts in Latin American organizations. Internet of Things, Private Data, Artificial Intelligence, Network Security, were other variables that represented the intention within the implementation of methodologies for the generation of new knowledge, thus confirming the relevance of the analyzed articles with the objective set for this document.

4.1.2 Distribution of scientific production by year of publication.

Figure 4 shows the scientific production distributed according to the year of publication, considering the period from 2017 to 2021.

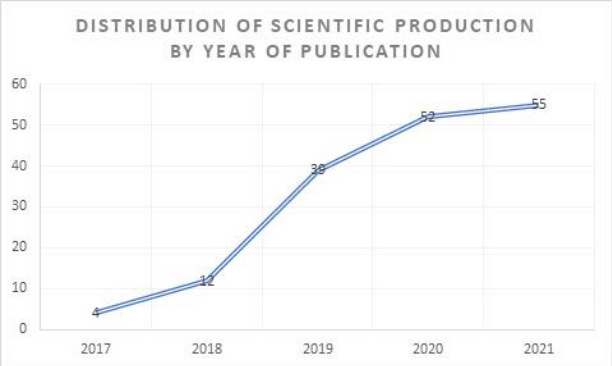

Figure 4. Distribution of scientific production by year of publication.

Source: Own elaboration (2022); based on data provided by Scopus.

The volume of scientific production concerning the study of Smart Contracts has been characterized by significant annual growth, as shown in the figure above. It went from 4 documents registered in 2017 to 55 publications in 2021, which means that the research referring to the said variable is directly proportional to the technological advances of globalization that have proposed the automation of each process inherent to the organization. Additionally, it is possible to infer from the fact that the last two years, i.e., 2020 and 2021, have been the ones with the highest volume reported in Scopus, that the emergence of the pandemic called Covid-19, which generated a high degree of uncertainty in all social and economic sectors globally, forced to virtualize a large number of processes inside and outside the companies. Hence, the celebration of Smart Contracts took great strength in implementing strategies based on technologies to provide continuity to the activities of each company.

4.1.3 Distribution of scientific production by country of origin.

Figure 5 shows how scientific production is distributed according to the nationality of the institutions with which the authors are affiliated.

Figure 5. Distribution of scientific production by country of origin.

Source: Own elaboration (2022); based on data provided by Scopus.

Brazil was the Latin American country with the highest number of scientific production registered in Scopus, with 97 documents published in high-impact journals indexed in the Scopus database from 2017-2021, followed by Mexico with 23 documents and Ecuador with 16. At this point, it is worth noting that the production of scientific publications, when classified by country of origin, presents a special feature and that is the collaboration between authors with different affiliations to both public and private institutions, and these institutions can be from the same country or of different nationalities so that the production of an article

with co-authorship of different authors from different countries of origin allows each of the countries to add up as a unit in the overall publications. This is best explained in Figure 6, which shows collaborative workflow from different countries.

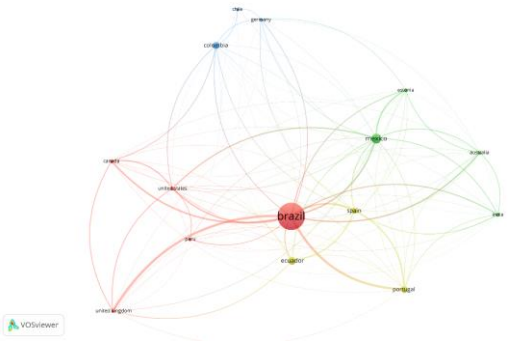

Figure 6. Co-citations between countries.

Source: Own elaboration (2022); based on data provided by Scopus.

Brazil, Peru, Canada, the United Kingdom and the United States represent the main countries with the greatest international co-authorship in scientific production. Colombia, on the other hand, is close to the works written by Chilean and German authors. In addition, researchers affiliated with Mexican institutions present joint research with authors from India and Australia.

5. Conclusions

As a topic requiring knowledge regarding cryptocurrencies, the general public is unfamiliar with this term or the use of this technology that emerged in the last decade. Therefore, this technology is currently limited to a certain group of users interested in cryptocurrencies and currency exchange platforms.

In order to access this type of contract, internet access and a digital wallet are required, as well as financial knowledge in cryptocurrencies, which in sectors without internet access is difficult, a serious example is the manufacturing companies of construction materials, which are far from cities and sometimes in areas without internet access, or their network connection has a high latency.

As these are smart contracts, they are immutable, which means that the contract must be well-specified and well-thought-out in order to avoid any inconvenience during its execution. If there is any problem during the contract's execution, it is impossible to modify values such as time lapses or refunds.

On the other hand, it is expected to encourage research on the study of Smart Contracts, supported by new technologies that arise within the same globalization and technological trends at the organizational level, which could facilitate the generation of new knowledge and support to new companies seeking the optimization of their processes through the virtualization of specific aspects within their functional areas.

References

[1] R. Sarmiento Lotero, «TEORÍA DE LOS CONTRATOS: UN ENFOQUE ECONÓMICO,» Cuadernos Latinoamericanos de Administración, vol. 1, pp. 11-24.

[2] D. G. Villafuerte Guerrero, «El Smart Contract como nueva forma de contratación en el código de comercio Ecuatoriano.,» 2020. [En línea]. Available: http://repositorio.puce.edu.ec/bitstream/handle/22000/18563/TESIS%20Gabriela%20Villafuerte%20Guerrero.pdf?sequence=1&isAllowed=y.

[3] A. Carvajal Guerreo y Y. H. Suarez Lobo, «Posibles usos de los contratos inteligentes en una blockhain para el comercio de bienes y servicios.,» Visión Internacional (Cúcuta), vol. 4, nº 1, pp. 27-40, 2021.

[4] H. L. Avila Baray, Introducción a la Metodología de la investigación., CD. Cuauhtemoc, Chihuahua, México.: Edición Electrónica, 2006.

[5] IBM, «What is blockchain technology?,» IBM, [En línea]. Available: https://www.ibm.com/topics/what-is-blockchain.

[6] Bit2me Academy, «Smart Contracts: ¿Qué son , cómo funcionan y qué aportan?,» Bit2me, 2022. [En línea]. Available: https://academy.bit2me.com/que-son-los-smart-contracts/.

[7] C. Omar Solís, E. Pérez Cortés y H. Cervantes Maceda, «Hacia una metodología para el diseño de contratos inteligentes,» ReCIBE, Revista electrónica de computación, Informática, Biomédica y Electrónica, vol. 8, nº 1, 2019.

[8] González REA, Mora JFM, Olvera GAA. La legislación ecuatoriana y los derechos humanos desde su perspectiva. Universidad y Sociedad [Internet]. 2022 [cited 2022 Oct 7];14(S3):498–503. Available from: https://rus.ucf.edu.cu/index.php/rus/article/view/2979

[9] Real Academia Española, «Criptomoneda,» Real Academia Española, [En línea]. Available: https://dle.rae.es/criptomoneda?m=form.

[10] Mora JFM, González REA, Arvelo PMM. La Constitución Ecuatoriana y los principios democráticos. Universidad y Sociedad [Internet]. 2022 [cited 2022 Oct 7];14(S3):487–97. Available from: https://rus.ucf.edu.cu/index.php/rus/article/view/2978

[11] I. B. Ferre, «Criptomoneda,» Economipedia, 25 septiembre 2017. [En línea]. Available:

https://economipedia.com/definiciones/criptomoneda.html.