ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 2, 762-768 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Analysis of the Blockchain for Adoption in Electronic Commerce Management in Ecuador

Segundo Moisés Toapanta Toapanta*[,1], Daniela Monserrate Moreira Gamboa[1], Luis Enrique Mafla Gallegos[2]

[1]*Department of Computer Science, Universidad Politécnica Salesiana (UPS), Guayaquil, Ecuador*

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

ARTICLE INFO

Article history:
Received: 09 December, 2019
Accepted: 10 April, 2020
Online: 24 April, 2020

Keywords:
Blockchain
E-commerce
Transactions
Security information
Cryptographic techniques

ABSTRACT

The document describes the advancement of technology in commercial negotiations and functionality for various electronic transactions in Ecuador, with the aim of analyzing the blockchain and its adoption in managing e-commerce. The quantitative approach with a deductive and descriptive method has been used to identify the benefits in transactional activities and data security, both customers and businesses. The results indicated that it is effective use of cryptography, the algorithm EDCSA, together with the SHA algorithm to maintain greater security efforts. It was concluded that the use of these algorithms are effective for transactions of buying and selling and financial aspects, but it needs to maintain a permanent control and simulation processes to avoid flaws in procedures.

1. Introduction

The main problem of e-commerce in the country, is related to security transactions via the web, as ill-intentioned people, dabble systems, therefore, to improve business.

System implementation encrypted block databases to people who want to affect users or businesses use access keys and other mixed systems, may obtain better results, the answer to this is the use of the blockchain, which it consists of several blocks, where each block includes information specific addresses [1].

Also, the information security is one of the main characteristics to be achieved within organizations worldwide [2]. The object is to analyze the blockchain for adoption in managing e-commerce in Ecuador.

How to apply the blockchain management in e-commerce in Ecuador?

Commercial activities in medium and large companies are experiencing a revolution, involving the technological sphere and this requires the application of the blockchain, using cryptographic secure, especially the algorithm EDCSA, where the chain applied blocks decentralized systems for distribution networks, whose properties allow transparency information.

Deductive and descriptive approach is used to analyze the information of reference articles and quantitative approach is applied, in order to present the result.

The results indicate that effective use of cryptography, the algorithm ECDSA, together with the SHA algorithm maintain greater security in trade negotiations.

It is concluded that the use of these algorithms are effective for transactions of buying and selling and financial aspects, but it needs to maintain a permanent control and simulation processes to avoid failures in future procedures.

2. Materials and Methods

2.1 Materials

They have been revised valuable resources that have allowed recognize the benefits of applying the technology blockchain in e-commerce. We have considered different bibliographic resources such as scientific articles and information regarding outstanding commercial activities carried out in the local context.

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

https://dx.doi.org/10.25046/aj050295

In Ecuador each year increase users who use payment methods online, but there are doubts security and protection of data and information, since people rely on the Internet for all types of transactions, whether banking, product purchases on -line, national or international, among other procedures. This maelstrom involves people of all ages and in all social contexts. Data were recorded and presented by means of figures, tables, formulas and algorithms were also used. It is undeniable that when technology is mentioned, is looking for ways to innovate in the market in terms of safety, as given in the use of blockchain [3].

2.2 Methods

To carry out this study the deductive and descriptive method is used to analyze the data and quantitative approach is applied, in order to present the result, point's transverse, business and user views were also considered, as well as security, transactional processes and functionality of the blockchain.

2.2.1 The use of enterprise-level blockchain

The blockchain technology is being applied in different contexts, with important benefits, including those business, for which several aspects are analyzed:

- The use of mobile applications for web transactions
- Advantages and disadvantages of electronic commerce
- Solving problems of e-commerce through blockchain
- Blockchain implement successful national companies
- User benefits
- Cryptographic techniques, to provide security

In centralized models required a physical or electronic location on a network that allows transactions with securities centralized in one place, on the other hand, trade decentralized implementation of securities is facilitated since there is no single centralized server.

Industry 4.0 (I4.0) several emerging technologies, Internet of Things (IoT), artificial intelligence (AI), and cloud computing development is commonly known as the fourth revolution incorporating industry, including cyber physical systems open, secure and intelligent [4]. In addition, Tanwar adds Virtual Reality (VR) and Augmented Reality (AR), which have revolutionized engineering, and manufacturing industries including automotive, computer, electronics, defense and aerospace [5].

Thus, the introduction of disruptive technologies in any sector brings with it many challenges and complexities [6].

Figure 1 shows the process that electronic commerce has in recent years and the reception it has, translating into an increase in transactions where its application becomes relevant in the Ecuadorian electronic medium.

The figure shows the process with e-commerce in recent years and the welcome they have, resulting in an increase in transactions is observed.

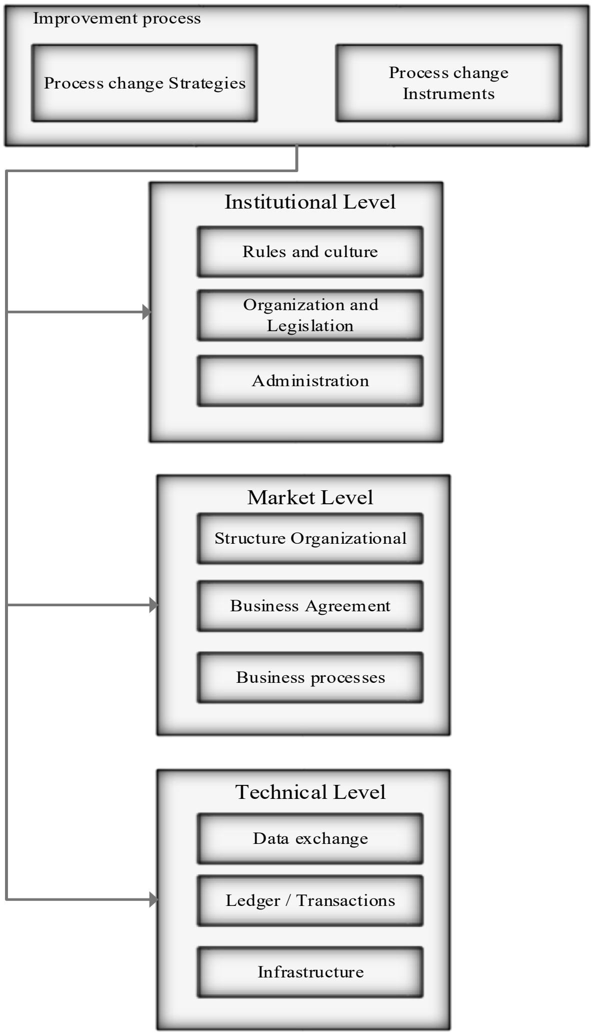

Figure 1: Analysis of the electronic commerce process.

2.2.2 Increased transactions

It is valuable to recognize the advantages of the use of technology blockchain:

a) There are more people make purchases and payments services online

b) The safety of this medium has increased

c) The online procedures are more agile

d) Are observed more transactions in financial areas, health, among others

About blockchain of technology, Khan states that it has brought a lot of attention with prominent applications in finance, health and the management system supply chain [7].

2.2.3 The decentralized model

In this system are presented, typically, nodes or miners collectively grouped validated and batch transaction blocks and then add these blocks to a chronological chain [8].

The development of new information technologies has allowed the world to move to the Industry 4.0, allowing establishing new collaborative environments based on large-scale decentralized systems.

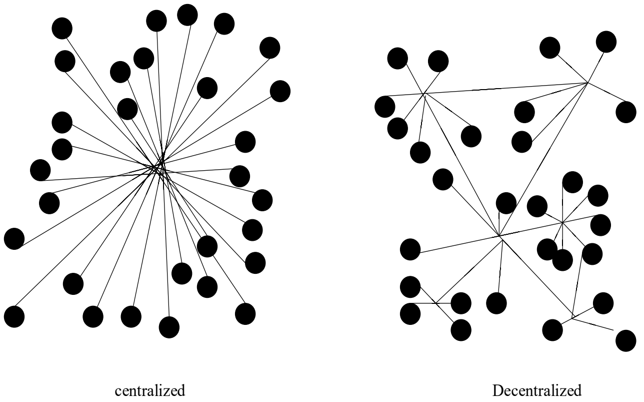

Figure 2: Centralized and decentralized model.

The figure 2 shows that the decentralized model sends information to all points, helping to decongest the means to send information and reduce the amount of work.

The decentralization of blockchain attribute facilitates the distribution of the same information across the network because no node can control the transaction [9].

Table 1: Advantages and disadvantages of the decentralized model.

DECENTRALIZED MODEL	
ADVANTAGES	**DISADVANTAGES**
It allows decision making is a way more efficient because no requires authorization from a central axis.	A poorly executed process can cause serious problems.
He did not receive commands from a single central authority or authorization of this, the decision-making process is accelerated.	If there isn´t good communication between all points, it may be an unnecessary copy of tasks.
In the same increasing interaction channels also it increases accountability.	Lack of proper training can cause failure.

Table 1 an analysis of the strengths and limitations of the model is presented.

This information is stored not only on one site, but also on other computers at the same time, and this prevents a hacker can attack directly to the system.

The recent emergence of blockchain technology has been announced as the next revolution that will transform the shape and size of organizations and how business transactions are conducted [10].

The chain block is the next step in the evolution of the internet along with step resulting from technological advances in storage management and data encryption contribute the economy [11].

2.2.4 Blockchain applied to electronic commerce

Applying blockchain is based on a set of problems presented by electronic commerce, in turn, born distrust the use of personal information.

The main problems emerged:

- Lack of confidence in payment systems
- Data security breaches
- Lack of control in the management of the supply chain
- Deficiencies in inventory and distribution systems

Blockchain implementation has the potential to solve problems with greater security and transparency through the implementation of smart payments and contracts.

This technology, in e-commerce, offers maintain a competitive market as well as reducing transaction costs through decentralized platforms. Today we live in a networked society [12] and use of mobile applications are taking more and more ground in the country and with them a number of benefits for the protection of personal data information through blockchain also promises secure transactions for users. Through the use of a cryptographic algorithm is able to demonstrate the operation and application of technology in e-commerce.

For a better analysis of e-commerce in the country has been divided into categories, as noted:

A. A store level.

E-commerce is a gateway for many companies in Ecuador, as there are countless online stores where you can find a variety of products, they especially target young people, but it requires:

- Reliability with respect to the delivery of data and personal information, credit cards, etc.
- Warranty, because nobody is exempt from buying a product that can be damaged in a short time
- Destination, the product may not reach its destination, because creating a possible fraud

Businesses and governments can use the chain blocks to make your work more efficient and reliable.

Table 2: Advantages and disadvantages of electronic commerce

Electronic commerce	*ADVANTAGE*	*DISADVANTAGES*
BUSINESS	Create new forms of marketing and sales.	Hackers.
	Reach many more users through advertising on social networks.	Problems sending the product to your destination.
	Variety of products in one place.	Do not ship the product on time.

	Catalog price list.	Web platform failures that cause waste of time and money.
USERS	Find products at good price.	No proximity between the seller and the buyer if the buyer does not agree with what has been received (product complaint).
	Offers	Display capability of the product (product quality) is lost.
	Delivery of the product to the comfort of home.	Ghost scam business.

The table 2 poses advantages and disadvantages for both the users make a purchase online, and companies that provide this service.

Blockchain is the new way of managing processes and sensitive information by much faster and reliable functional use of encryption where transactions would [13].

To the perform It online purchases using credit cards or other transaction is made by an application, what It facilitates users to transfer money on time without having to go to any institution financial or commercial.

B. At company level, the blockchain technology can lead to the emergence of new business models, which previously were not viable.

In different industries, food industry, textile, among others, are implementing systems for buying and selling online, but there are also problems with hackers, affecting markets or ill-intentioned people create fake companies.

The food industry also benefit con complex systems supply and the large number of products enter the market, your intermediaries often play key roles in reducing transaction costs and expanding the possibilities of transaction [14].

On the other hand, Blockchain promotes the demobilization of goods by offering deeper information for consumers [15].

2.2.5 Cryptography

Blockchain technology to make it functional requires use Cryptography, it born from the need to have a safe, private and understandable communication between two sides, this has led to increased security options online, which is in high demand in different parts of the world. Cryptographic considered two approaches, private cryptography or symmetric key, which establishes a key agreement between authorized users. It also has asymmetric public key cryptography in which a user has access only and only the user can decrypt the message.

This research was based on public key algorithms focused on solving issues of confidentiality, authenticity, integrity, unchanged.

To treat problems you can run two types of algorithms, which are of low complexity (easy), also called Polynomial Complexity and a second call difficult or not polynomial complexity. For this research we chose the difficult complexity without key is decrypted using Elliptic Curve Discrete Logarithm (PLDE).

With the PLDE is found the result where n ∈ N, since P, QE (K) with $Q = nP$.

In addition, several algorithms using elliptic curves, including the Diffie -Hellman is used for the key exchange. Also, the Gamal algorithm used for sending encrypted messages, finally, Elliptic Curve Digital Signature Algorithm (ECDSA), which is based on the digital signature, being based in which this study option [13].

2.2.6 ECDSA algorithm

Elliptic Curve Digital Signature Algorithm (ECDSA) is a algorithm that makes use of operations on points of elliptic curves instead of exponentiation algorithm key short this creates a high level of security, being more complex so it is difficult to break.

Function footprint h must have certain characteristics that must be met for safety.

1. Existence of a message m, which should be quick and easy, is calculated h (m)
2. With digital h0 footprint, very difficult characteristics (no existence in polynomial time algorithm) for calculating x0 so that h (x0) = ho. He is also known as resistance to find a pre image.
3. Calculate x0 h (x0) = h0, where it is impossible to find x1, such that h (x0) = h (x1). He is also known as resistance to find a second pre-image.
4. Considered impossible to calculate x0 and x1, x0 x1 with such that h (x0) = h (x1). He is also known as Crashworthiness.≠
5. The public key is the principal to decrypt the signature, thus ensuring data security.
   For further understanding of the algorithm ECDSA the following occurs:
   Where a uses $E(K)$ and a base point $P \in E(K)$. To calculate $Q = kP$ so that xQ differs from 0. Then is calculated $k^{-1} \bmod n$ Y hm $= h(m)$ and then $s = k^{-1}(hm + nAxQ)(\bmod n)$. With the condition if S = 0 $(\bmod n)$ is chosen k again and proceeds to do all the calculations again, otherwise it (xQ, S). To send the signature is inserted into the message (m) this is encrypted and sent to B. For signature verification proceeds to decrypt the file to get the message m and signature xQ, S.
6. For calculating $h(m) = hm$: (1)

   $$V = hmS^{-1}P + xQS^{-1}RA \quad (2)$$

   Where: $xQ = Xv(\bmod n)$ (3)

   The signature is accepted, if otherwise is rejected.
7. The following formula was used for verification:

$$\begin{gathered} V = hmS^{-1}P + xQS^{-1}RA = (hm(hm+nAxQ)^{-1k})P) + \\ (xQ(hm+nAxQ)^{-1}knA)P = ((hm+nAxQ)(hm+nAxQ)^{-1k})P = kP = Q \end{gathered} \tag{4}$$

Once the trace function (electronic signature)is in a document file, message, text, etc.), encryption is performed, which is attached to the document, which becomes a signed and encrypted document, which will be sent designated by the network to the recipient, who in turn passes the verification stage decrypting the message clearly and signature [16].

2.2.7 Algorithm SHA.

Secure Hash Algorithm (SHA) is an algorithm used to transform a lot of information in a single secure cryptographic chain. SHA is used to secure public addresses starting from a ECDSA key. The characteristic of blockchain storage technology involves distributed database [17].

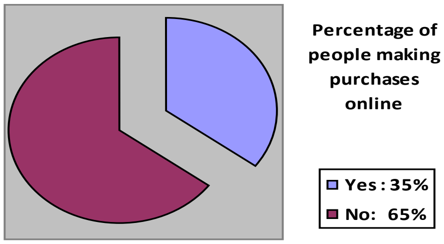

Figure 3: Percentage of people who make purchases on the Internet in recent years.

In Figure 3, Ecuador observed in 65% of the population does not make purchases on the Internet, while the other 35% of the population itself, according to the SEO of Quito, but will increase over the years.

3. Results

The use of the blockchain is massing in the world, having a significant weight in financial activities.

To be effective the use is required of cryptography, for which the use of the algorithm EDCSA suggested.

3.1 Process EDCSA signature algorithm.

By using a public key

Where:

d = it is the private key.

P = base point.

Q = public key.

The private key "d" can be an integer value to the random number in this case is used between 1 and n-1, where n is a prime number. The public key is Q that is obtained by multiplying the private key "d" base point "P".

The public key is obtained from the following equation.

$$Q = dP \tag{5}$$

Signing process:

1. Select a random number (k).

2. Select a base point (P).

3. Calculate kP

Where:

x1, y1 = are integers.

the following equation is obtained:

$$kP = (x1, y1) \tag{6}$$

For signing the message (m) are the numbers r and s, represented in the following equation (7).

4. Calculating r.

If r = 0, return to step 1.

$$r = x1 \bmod n \tag{7}$$

5. Calculate S.

If S = 0, return to step 1.

H (m) is the hash of the message to be signed, calculated with the algorithm SHA-1. The equation is as follows:

$$k - 1(H(m) + dr) \bmod n \tag{8}$$

Purchases and sales online transactional processes require valid, as evidenced in Figure 5.

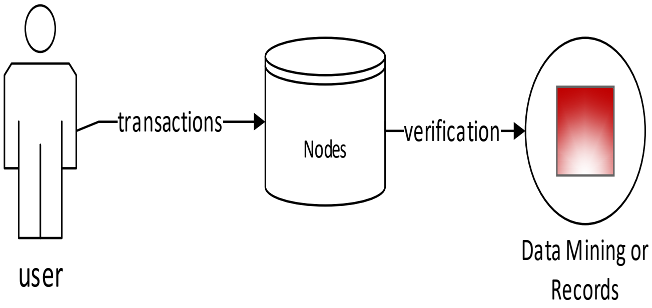

Figure 4: Model of transaction processing and validation.

Figure 4 evidences a transaction, requesting verification of data. To work more safely is important la private key with a random number on which you can perform mathematical calculations.

Further, signature algorithm ECDSA, It contains:

Verification:

R and s are checked within the range [1, n-1].

1. Calculate w:

$$s - 1 \bmod n \tag{9}$$

2. Calculate u1:

$$H(m)w \bmod n \tag{10}$$

3. Calculate u2:

$$r - w \bmod n \tag{11}$$

Get u1 and u2 to perform the following equation:

$$u1P + u2Q = (x0, y0) \tag{12}$$

The signature verifies if and only if v = r

$$v = x0 \bmod n \tag{13}$$

For the result of the firm, check the proof where r and s are first within the range [1, n-1] by v. If v = r mean r (process), v (verification) are well-executed.

$$A = \frac{n!}{(n-1)!} = x \tag{14}$$

Also, application of equation (14) based on transactions made by the blockchain. Where the variable "A" starts the transaction process and the verification takes place in the node to be validated or not accordingly you can determine whether or not the transaction was conducted successfully "B". Where:

A: it is the uninitialized variable.

N: it is passing through a process node.

!: node N validated.

x: it is the result of non-validated transaction.

B: is the result of the validated transaction.

If node A is invalid, the calculation is done by adding the value of -1, which means that the transaction process has been invalidated.

$$A = \frac{n}{(n+1)} = B \tag{15}$$

Otherwise, the process of equation (15) is validated node n (n + 1) is reflected, resulting in B, a successful transaction.

Once transmitted, given the approval of the transaction, where the information block can be added to the rest of the chain as a successful registration and transparent. A successful transaction with B, ends the transaction.

To demonstrate how a transaction using chain block is performed is shown the diagram below where, flowchart shows how the block chain works, where A seeks to make a transaction to B via an electronic medium. This transaction is shown on the network as an information block, then this block of information is transmitted to all points of the entire network.

All transactions to go from point A to point B, pass through the safety chain, where the process requires authentications or comparative keys that can only be validated by the authorized person, this process is linked from the transmitter block to the receiver block.

In Figure 5 shows how a transaction can be performed from A to B using the validation of the equation (14) and equation (15).

The blockchain has helped to raise the security level transactional processes from different companies and this can be considered different algorithms.

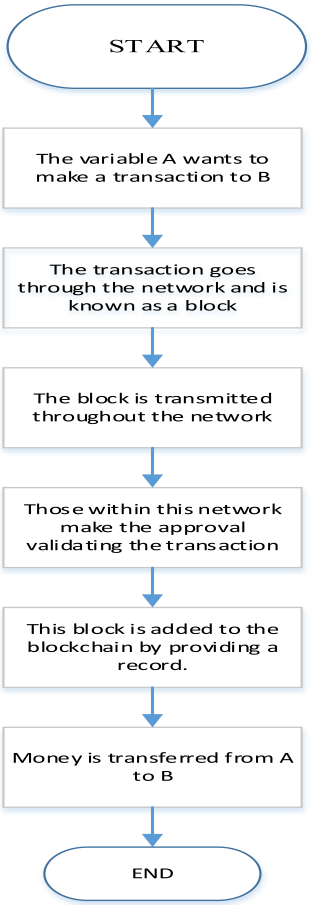
START
The variable A wants to make a transaction to B
The transaction goes through the network and is known as a block
The block is transmitted throughout the network
Those within this network make the approval validating the transaction
This block is added to the blockchain by providing a record.
Money is transferred from A to B
END

Figure 5: Analysis Diagram blockchain process.

4. Discussion

A literature review focused on studies are in blockchain benefits of technology in business transactions of large companies, because their technology infrastructure is higher and cause a competitive advantage over companies with less capital.

The application of the chain blocks and security processes in e-commerce in Ecuador, can ensure effective, easy accessibility, greater acceptance of the market, but it requires superb manageability, better preparation of staff and management commitment high.

It is important that the country has policies that allow trade practices to exercise more smoothly and safety that benefits companies, workers and society in general.

But despite having a security system with the implementation of chain blocks in e-commerce, companies need to have several requirements to be effective:

- Security politics
- Detection system vulnerabilities that may arise in the system.
- Develop a contingency plan in case of breach in security measures.

Also, companies shall carry out the respective case study simulation and testing platform for observing management support and thus get better results.

5. Conclusions

Application of Blockchain technology in e-commerce for small businesses. Blockchain technology adoption in the financial and banking system.

Using blockchain allowed in increased electronic commerce in the world and himself in Ecuador, as companies are taking steps to adopt technologies, applying security measures to provide greater comfort and effectiveness in public and private transactions. Using EDCSA algorithm is effective for business transactions, by using the public key and chain blocks. Despite its effectiveness, should be performed simulations to identify the best options eligible companies, because some systems become ineffective in the course of time.

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 the resolution 142-06-2017-07-19 and the Secretariat of Higher Education Science, Technology and Innovation (Senescyt).

References

[1] S. Singh, «Factores de éxito críticos de blockchain para una cadena de suministro sostenible,» web of science, vol. 152, nº 104505, p. 11, 2019.

[2] S. M. Toapanta Toapanta, A. J. Bravo Jácome y M. G. Tandazo Espinoza, «An Immutable Algorithm Approach to Improve the Information Security of a Process for a Public,» Astes, vol. 4, nº 3, p. 6, 2019.

[3] E. Ganne, «¿Pueden las cadenas de bloques revolucionar el comercio internacional,» 2018. [En línea].

[4] Liu, X. L., Wang, W. M., Guo, H., Barenji, A. V., Li, Z., & Huang, G. Q. (2020). Industrial blockchain based framework for product lifecycle management in industry 4.0. Robotics and Computer-Integrated Manufacturing, 63, 101897.

[5] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.

[6] Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. International Journal of Information Management, 50, 302-309.

[7] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems, 105, 13-26.

[8] A. Islam, M. Mäntymäki y M. Turunen, «¿Por qué se dividen las cadenas de bloques? Una perspectiva de actor-red sobre las divisiones de Bitcoin,» Scopus - Technological Forecasting & Social Change, vol. 148, p. 10, 2019.

[9] A. Zhang, «Arquitectura del sistema para la transparencia basada en blockchain de la sostenibilidad social de la cadena de suministro,» Scopus, vol. 63, nº 101896, p. 9, 2019.

[10] K. Behnkea, M. Janssen, «Condiciones límite para la trazabilidad en las cadenas de suministro de alimentos utilizando la tecnología blockchain,» Scopus, nº 0268-4012, p. 10, 2019.

[11] Achargui, A. A., & Zaouia, A. (2016). Traditional, Web-based or Internet-enabled ERP systems adoption for SMEs in Developing Countries. In 2016 5th International Conference on Multimedia Computing and Systems (ICMCS) (pp. 676-680). IEEE.

[12] Kanamori, S., Nojima, R., Sato, H., Tabata, N., Kawaguchi, K., Suwa, H., & Iwai, A. (2016). (pp. 418-422). IEEE.

[13] Nosouhi, M. R., Yu, S., Zhou, W., Grobler, M., & Keshtiar, H. (2020). Blockchain for secure location verification. Journal of Parallel and Distributed Computing, 136, 40-51.

[14] Y. Chen, C. Bellavitis, «Blockchain disruption and decentralized finance: The rise of decentralized business models,» Scopus, vol. 13, p. 8, 2019.

[15] Allen, D. W., Berg, & Markey-Towler, B. (2019). Blockchain and Supply Chains: V-form Organisations, Value Redistributions, De-commoditisation and Quality Proxies. The Journal of the British Blockchain Association, 2(1), 1-8.

[16] Castagna H., Publicaciones Matemáticas del Uruguay. Volumen 17, Julio 2019, Páginas 293–297 ISSN 0797-1443.

[17] Lukmanova, O., Volkova, E., Zabolotnyi, A., & Gorelik, A. (2019, January). Blockchain Technology for Public Utilities. In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 1790-1793). IEEE.