ISSN 1870-4069

Information Reliability in Estimate Process: A Novel Blockchain Model

Inés Borunda, Iván Pérez, Erwin Martínez, Alberto Ochoa Zezzatti

Universidad Autónoma de Ciudad Juárez,
Mexico

{al187052, emartine, ivan.perez,
alberto.ochoa}@uacj.mx

Abstract. This study is based on the implementation of the Blockchain in the process of the "recuse for quote" process that feeds the system of estimates for the quotation of new products, or changes to existing ones, used by automotive companies These companies develop close working and business relationships with their suppliers, that's why is extremely valuable to have accurate information, since it depends on it to make strategic decisions to improve the quality, reduce costs and minimize delivery times. The proposed data network model (blockchain) manages the exchange of information between the different departments involved in an estimated procedure, so that all parties can synchronize the reliable information, avoiding using modified information, which creates confidence in the decisions making. Decision-making with inaccurate information implies the loss of trust and competitiveness with suppliers and customers. The implementation the blockchain helps to detect any type of manipulation or alteration in the information in a timely manner and improve the integrity of the infrastructure in the information security.

Keywords: Blockchain, information security, estimated procedure and decision making.

1 Introduction

One of the problems faced by manufacturing companies is to have the reliability of their information systems, since this, they feed the system to be able to provide an estimated quote for new products. Considering that the estimates require certainty in the unit costs of production, the value of direct labor, the components in the list of materials and the indirect charges that may occur soon. This implies that the estimated costs must indicate what it can cost to produce a new product, providing the analysis tools necessary for decision making. However, it is not uncommon to find discrepancies between the information provided by the suppliers and the information in the estimate systems.

This risk has been previously identified [1] who points out that because the information is asymmetric the problem of fraud can occur between the subjects of the company. Therefore, the supervision and restriction corresponding to the security systems is required to guarantee the reliability of the data, through the different departments involved in the request for quote process. Prioritizing policies according to management guidelines, in order to guarantee the reliability of information and assertiveness in decision making, the risk of generating estimates with inaccurate information can result in the loss of business, credibility as a company and sustainability, in the future.

Therefore, it is proposed to apply blockchain to this key process in manufacturing organizations. By 2020, it is estimated that 60% of the leading manufacturers will depend on digital platforms, which will be responsible for supporting the functions that are responsible for 30% of their revenues. By 2021, the range of new technologies will be integrated into the manufacturing sector, with 20% of the leading manufacturers depending on some combination of artificial intelligence, internet of things; cognitive systems and blockchain [2].

That is why achieving transparency requires accurate and secure data collection in the storage of these, a difficult task that is currently entrusted to third parties through centralized information repositories [3].

Therefore, it is extremely important to consider that sectors such as: health, insurance, government and supply chain management are likely to be transformed by the *blockchain* [4, 5] discussed the value of the *blockchain* application in the smart contract. [6] proposed *blockchain* applications to influence laws and regulations. [7] built the data of the shared security network system.

However, *blockchain* has not been detected in the handling of customer-supplier information regarding the "*recuse for quotes*" used to quote estimates. This model provides the security tools based on cryptography using mathematical formulas incorporated in the hash function that allows the information received to not be modified by any department. It is worth mentioning that each department involved in the "recuse for quote" process can add information regarding their position, without modifying the information of the other departments.

2 Theoretical Framework

2.1 BlockChain

Blockchain technology is relatively recent, so it is frequently related to bitcoin. However, the *blockchain* and bitcoin are different. Because the information in the *blockchain* is encrypted through mathematical formulas, as well as non-symmetric encryption algorithms that guarantee the security of data in the transaction and technology of economic models, obtaining the principle of cryptography, reconciling the parties involved without the need for an intermediary third party [8]. What makes *bitcoin* a successful application in the *blockchain*. In essence, the *blockchain* is a database distributed, decentralized, secure and reliable similar to an account book (distributed accounting), which records all transactions digitally permanently with the ease of being able to achieve its trajectory [9].

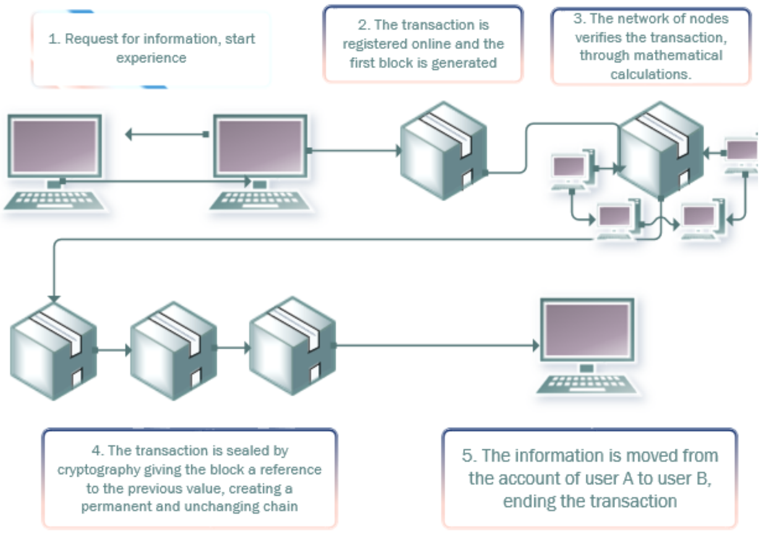
1. Request for information, start experience
2. The transaction is registered online and the first block is generated
3. The network of nodes verifies the transaction, through mathematical calculations.
4. The transaction is sealed by cryptography giving the block a reference to the previous value, creating a permanent and unchanging chain
5. The information is moved from the account of user A to user B, ending the transaction

Fig. 1. Information transfer by using blockchain.

When the transaction is sent from A to B, as you can see on Fig. 1, a private key is granted to A and B "the receiver" is decrypted with the sender's public key [10] giving the opportunity that the individual can prove his property in anonymity [11].

In this way, the information is certain that it will not be lost unless all nodes are destroyed or more than 51% of the nodes of the entire network are compromised. Same, that elaborates a unique and unrepeatable hash in each block that must coincide with the hash of the previous block thus guaranteeing the reliability of the transferred information.

The loss of any node does not affect the operation of the entire system, due to its distribution design. Being the collective participation a decisive factor that guarantees transparency, to ensure the correctness and security of the transaction, reassuring that human intervention has no effect on the system.

Since the accounts remain synchronized in real time, and data that has been validated and registered cannot be manipulated [12]. It should be mentioned that the node must be certified to join the consensus process [13].

2.2 Hash

Involving the hash function that transforms an input of arbitrary size into an output of fixed length of n bits, being unidirectional the hash cannot be altered. Therefore, with this technology we can solve the problem of fraud among the personnel working in the company by providing an information base so that the analysis in the decision-making process is more precise for each part of the process [14]. Which leads to a decision making in an assertive, timely and correct manner. Corroborating the benefits incorporated by using the hash algorithm and cryptography in data transfer.

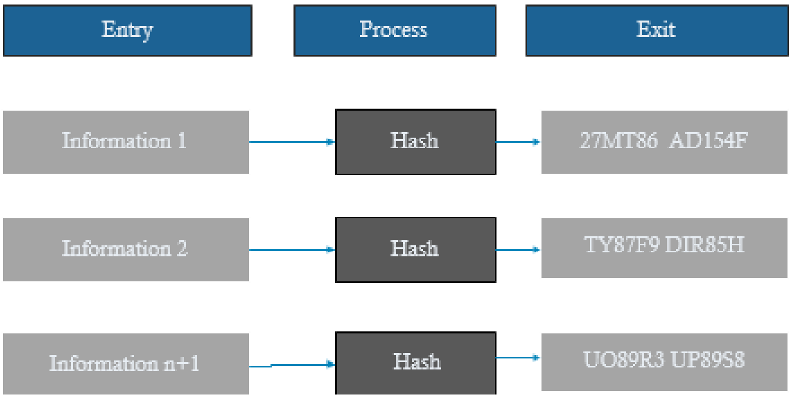

Fig. 2. Hash Function.

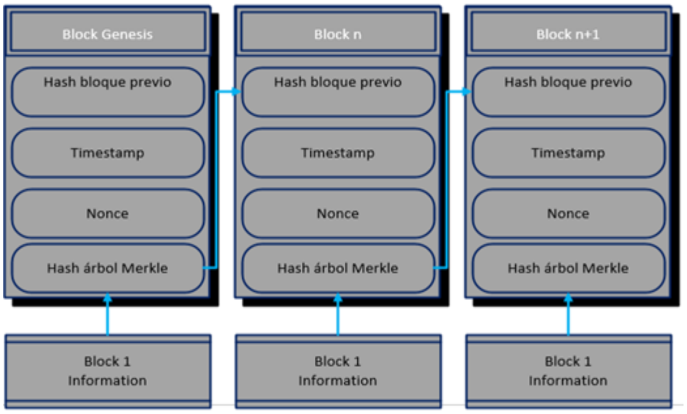

Fig. 3. Blockchain block structure.

The first block is known as the genesis block; it is shown in Figure 2. A block consists of a header and a body [15]. The body of the block contains the list of transactions [16]. The block header contains several fields, mainly the Block Version that indicates the set of rules that must be followed for validation, a hash of the previous block header, a timestamp, one hash root of the Merkle tree represents the hash value of all transactions in the block [17] as we can see in Figure 2.

The nonce is a 32-bit field that increases until the equation is solved [18]. In addition to be a distributed master book, blockchain is also defined by three key concepts: consensus, smart contract and cryptography [19]. When making a transaction, smart contracts are invoked to execute the term of a contract / procedure on each node in the network [20].

In blockchain, the block structure is made up of block header and block body, andthe hash values of the business data are gradually divided into pairs and form the Merkle tree structure.

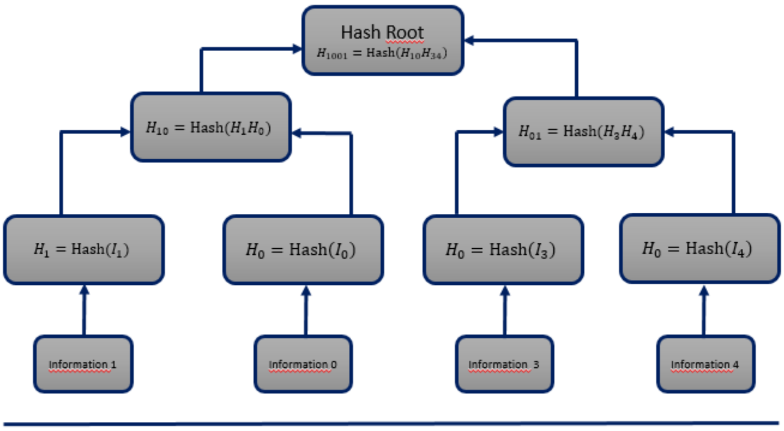
Hash Root
$H_{1001} = \mathrm{Hash}(H_{10}H_{34})$
$H_{10} = \mathrm{Hash}(H_1H_0)$
$H_{01} = \mathrm{Hash}(H_3H_4)$
$H_1 = \mathrm{Hash}(I_1)$
$H_0 = \mathrm{Hash}(I_0)$
$H_0 = \mathrm{Hash}(I_3)$
$H_0 = \mathrm{Hash}(I_4)$
Information 1
Information 0
Information 3
Information 4

Fig. 4. Merkle Hash Tree.

The leaf nodes are the initial hash values of the business data, and the body of the Merkle tree is stored in the body of the block, and the root of the tree is stored in the header of the block. Commercial data is a mapping relationship built with the leaf nodes of the Merkle Tree, and commercial data can be stored in the body of the block [21].

In a centralized system, the administrator could be bribed, and the entire system could be subject to manipulation and falsification of information [22]. With the structure of the blockchain this risk is avoided.

3 Proposal of the Model

For a large production company, the endogenous risk of its supply chain can be divided into two parts: the credit risk caused by the asymmetry of information between the companies within the supply chain and the risk caused by incomplete information [23]. Therefore, the main objective of the model is to create certainty in the information that reaches the company and is transmitted by the different departments involved in the process of "recuse for quote". Being an improvement plan for assertive decision making based on transparency in information, and offering managers relevant information for decision making and providing information to third parties about the value of the company or organization.

Figure 5 shows the interaction of departments A, B and C, where A sends information to B, B cannot modify it, but can add new information and transfer it to C, where in turn C can add information, but not modify the previous one, since it is protected by the Hash cryptology.

Creating a reliable ecosystem between suppliers and their customers [24]. This is achieved through a policy that focuses on the transparency of the chain to ensure the traceability of the product, where accurate data collection and secure storage of them is required. Suppliers and the company must be synchronized by the use of the Etherium

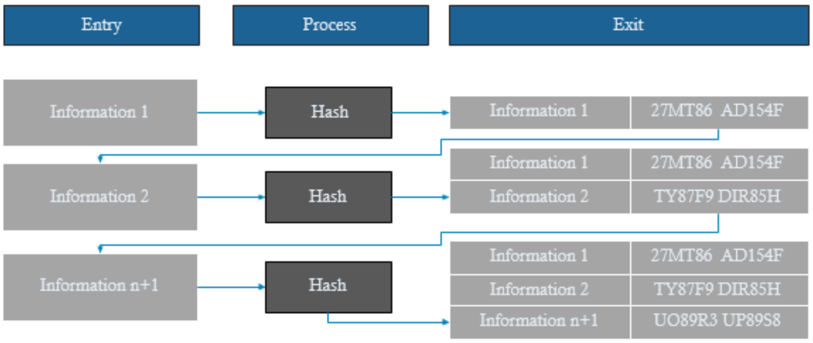

Fig. 5. Incorporation of several processes in the information network chain, using blockchain.

system, in which it will be used to transfer the information to the different departments involved.

3.1 Model Description

a) When accessing the information to the system, the provider protects its information through a hash, which will be kept during the reception of each department, so that no department can modify the information received.

b) The private key is protected by a cryptographic coprocessor.

c) The departments involved that require access to the information and add new content, will be able to do so since this is where the innovation arises to the model, because with the previous model the information cannot suffer any alteration in its trajectory.

d) Data is collected and transferred by each department involved in the estimation process, where they will be safe and reliable before being stored in an immutable and decentralized database.

e) In the transition between blocks, the next block will copy the previous one having the previous information content blocked, however, you can add new block information, quickly generating virtual data according to the recovery requirements and with the content of the last block as input .

f) The blocks are chained to each other by the immediately preceding block. In this way, any modification that was intended to be introduced at some point in the chain would affect the hash and only the hash of the last block would have to be verified to detect where the anomaly happened.

g) The hash is created by mathematical formulas, which make it unrepeatable.

h) Each block may have the information of the previous block without the right to write about the part of the information, however, it will have its own space to add information from its department, which will go to the next block, where the process is repeated , until culminating, providing a system of authentication and storage of information.

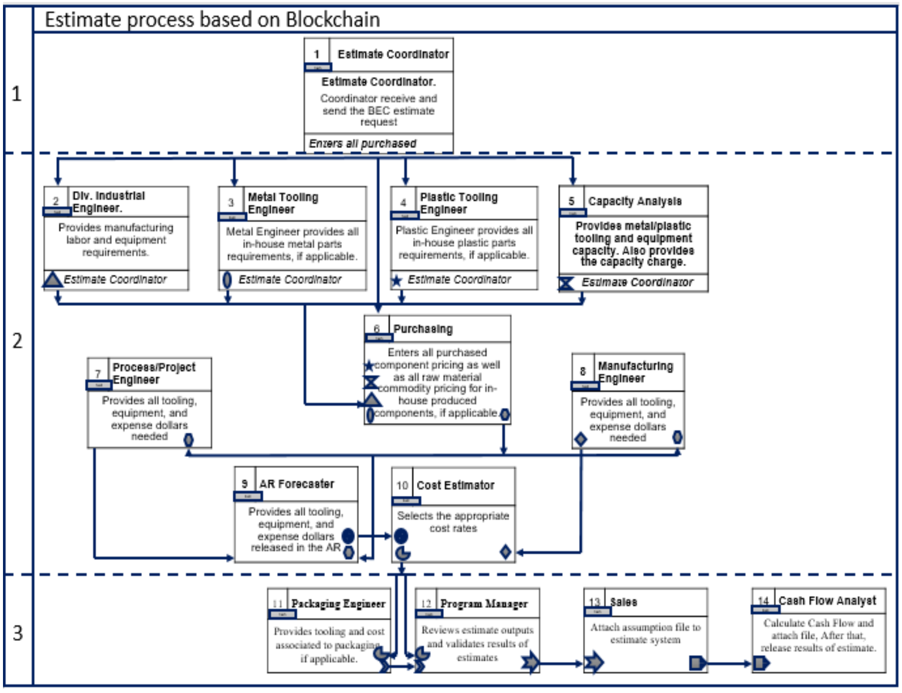
Estimate process based on Blockchain
1
2
3
1 Estimate Coordinator
Estimate Coordinator.
Coordinator receive and send the BEC estimate request
Enters all purchased
2 Div. Industrial Engineer.
Provides manufacturing labor and equipment requirements.
Estimate Coordinator
3 Metal Tooling Engineer
Metal Engineer provides all in-house metal parts requirements, if applicable.
Estimate Coordinator
4 Plastic Tooling Engineer
Plastic Engineer provides all in-house plastic parts requirements, if applicable.
Estimate Coordinator
5 Capacity Analysis
Provides metal/plastic tooling and equipment capacity. Also provides the capacity charge.
Estimate Coordinator
6 Purchasing
Enters all purchased component pricing as well as all raw material commodity pricing for in-house produced components, if applicable.
7 Process/Project Engineer
Provides all tooling, equipment, and expense dollars needed
8 Manufacturing Engineer
Provides all tooling, equipment, and expense dollars needed
9 AR Forecaster
Provides all tooling, equipment, and expense dollars released in the AR
10 Cost Estimator
Selects the appropriate cost rates
11 Packaging Engineer
Provides tooling and cost associated to packaging if applicable.
12 Program Manager
Reviews estimate outputs and validates results of estimates
13 Sales
Attach assumption file to estimate system
14 Cash Flow Analyst
Calculate Cash Flow and attach file, After that, release results of estimate.

Fig. 6. Estimate process based on Blockchain.

i) What guarantees the construction of the information storage mechanism is to improve the storage efficiency and privacy protection of this. The large chain of information network of the company based on blockchain depends on a private industrial network and the Internet, as well as the staff of the different departments affiliated with the blockchain network with prior authorization, avoiding interference to the users system that are not relevant by reducing the risk of malicious users falsifying information in the system together.

Applying the model in the manufacturing industry we can appreciate the structure presented in Figure 6, which shows the relationship that exists between the different departments involved in the estimation process.

As we can see, companies are structured by different specialized departments, which are involved in the transfer and use of information. Its objectives are to optimize its production processes, increase sales and achieve profitable and sustainable growth.

As Figure 6 shows, the initial information reaches a different department, and can be altered by them. The image shows how hash cryptography is implemented since the information reaches the company, along the way, the information can be easily tracked through the code and verifies where the modification was made.

The difficulty can be changed by increasing or reducing the number of zeros in front of the hash of the block header on which the hash function is then applied. An additional figure is shown from each department, which represents the cryptograph, where each hash must match the next block. With which the correlation of businesses of different

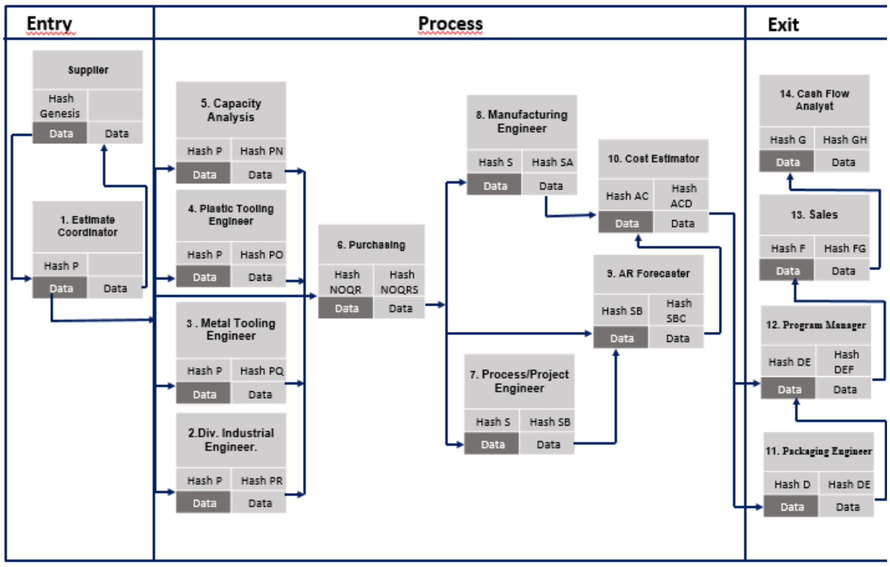

Fig. 7. Model for the Estimate process based on Blockchain.

subjects in ascending and descending sense can be detected constructing their relations of interaction of information.

Demarcating the fellows that do not have commercial interaction relationships or any connection, so that they cannot understand the information of other fellows, whose relationship of information interaction of a section [23].

4 Simulation Methodology

A centralized management system represents a threat to data integrity, availability and resilience, because the system is subject to corruption, fraud and manipulation [25]. Therefore, the distributed information technology Blockchain can help maintain transparency and reliability in the information flows in the different departments, generating a reliable system, under the following work scheme where the data received is unalterable. Due any modification in a specific block will invalidate all subsequent blocks [26].

Considering that the communication between the front end and the blockchain is done through the HTTP server on the representative state transfer (REST) API, using JSON to encode and decode requests and responses [27]. The model proposed in Figure 7 is shown, which is composed of different departments involved in an estimation process. In the first instance, department 1 asks the suppliers for the information, which is not encrypted by hash, since the suppliers must generate the information.

Once such information returns to department 1, it will be encrypted by hash P, which will be transferred to departments 2, 3, 4, 5 and 6, where the new hash will be the union of some digits of the previous plus the new remaining for 2PR, 3PQ, 4PO and 5PN who

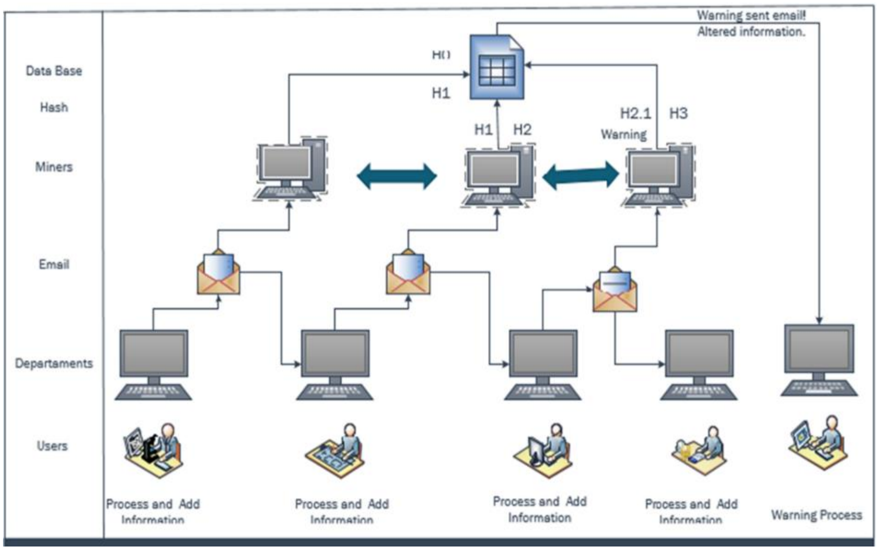

Fig. 8. Model for the Estimate process based on Blockchain.

cannot modify the information received in "P", but having enabled the part of the system that corresponds to add their data, "R", "Q", "O" and "N ”Respectively, they will also send their encrypted information, in addition to the encrypted information that they had previously received, in this case to department 6 who has the hash S, to which“ N, O, Q, R ”is added. Department 6 transfers the “S” to departments 7, 8 and 9, which generate their own hash to encrypt their information and send it so on until the information is transmitted by all the departments involved.

The model allows establishing a virtual security environment with the incorporation of the different departments, through a set of mathematical equations that guarantee the integrity of the information in the decision-making process in the company or a specific area of it.

The promise he makes us implies a future in which no one has absolute power in the network, and no one can lie about past or present events [28], providing full certainty in decision making.

The proposal of the model focuses on the use of Ethereum, as a blockchain-based encryption model, however this has a limited capacity in handling a large amount of data, which would generate the need to investigate about the BigchainDB for manipulation of large amounts of information in less time.

The evaluation of Hyperledger's legation that has a better performance. Within the investigation it was also found that terms of security attack, Ethereum and Parity are vulnerable exposing the system to double spending attack [29]. However, Ethereum is still considered the most advantageous in terms of scalability, reliability and maturity of the system, which allows a large number of participants [30].

5 Conclusions and Future Research

Having this clear how vulnerable the manufacturing sector is to fraud, the implementation of *blockchain* technology would generate an immutable tamper-proof record for the departments involved. Being the objective of these functions to be able to detect if a message has been modified or not, to verify the integrity of the message. Blockchain reduces fraud, errors and delays identified in the supply chain ecosystem, increases trust between the customer and the provider in data management, *blockchain* was integrated, to ensure availability, accuracy and accessibility of data for all the chain, improving business decisions and providing insight into all system vulnerabilities [29].

This leads to an efficient implementation of the consensus protocol to improve the growth of the economy, ensuring the correct functioning of the *blockchain* and avoiding any malfunction of the *blockchain* architecture [31]. Having a correct manipulation of the use due to the information, through the different departments will contribute reliability of this. It is worth mentioning that a disadvantage in that *blockchain* has a weight restriction in the information and transfer of it.

However, to avoid the low performance of the *blockchain*, dual storage architecture can be implemented to handle a large amount of data. The communication protocol based on data rate, communication range, energy consumption, and cost should also be considered.

6 Future Resarch

The implementation of the *blockchain*-based computer security model is a long process of adaptation, modification and awareness of the different departments and therefore personal in charge of what requires a culture of collaboration. Modifying the organizational culture based on previously established processes, generates a huge challenge in the industry, and more if some processes have been flawed over the years. Therefore, it is essential to have the participation of both management levels and key personnel of the different departments.

What makes this project an opportunity for improvement, ensuring reliable information for assertive decision-making based on achieving the company's objectives. The next process is to test the model regarding the veracity, speed and performance of the system using blockchain in the company, simulating the processes see the Figure 8 to evaluate the model.

References

1. Fu, Y., Zhu, J.: Big production enterprise supply chain endogenous risk management based on blockchain. IEEE Access, 7, pp. 15310–15319 (2019)
2. Mire, S.: Blockchain for manufacturing (2018)

3. Abeyratne, S., Monfared, R.: Blockchain ready manufacturing supply chain using distributed ledger. International Journal of Research in Engineering and Technology (2016)
4. Kshetri, N.: Blockchain’s roles in meeting key supply chain management objectives. International Journal of Information Management (2018)
5. Meijer, D., Carlo, R.W.: The UK and blockchain technology: A balanced approach. Journal Payments Strategy Systems, 9 (2016)
6. Yang, D., Pan, Z.D.: The blockchain bring finance and law optimization. China Finance (2016)
7. Wang, J., Lingchao, G., Aiqiang, D., Shaoyong, G., Hui, Ch., Xin, W.: Block chain based data security sharing network architecture research. Journal of Computer Research and Development (2016)
8. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2016)
9. Daming, L., Zhiming, C., Lianbing, D., Xiang, Y., Harry, H.: Wang information security model of block chain based on intrusion sensing in the IoT environment. Cluster Computing, 22(Z1), pp. 1−18 (2018)
10. Ping, Z., Yu, D., Bin, L.: White paper on China's blockchain technology and application development. (2016)
11. Zheng, Z., Xie, S., Dai, H., Wang, H.: Blockchain challenges and opportunities: A survey. Researchgate (2016)
12. Yonggui Zhu, Jianming Zhu: Big production enterprise supply chain endogenous risk management based on blockchain. IEEE Access, 7, pp. 15310-15319 (2019)
13. Azzia, R., Kilany, R., Chamouna, M.S.: The power of a blockchain-based supply chain. Computers & Industrial Engineering, 135, pp. 582−592 (2019)
14. Pierro, M.: What is the blockchain? Computing in science and engineering (2017)
15. Zheng, Z., Xie, S., Dai, H., Wang, H.: Blockchain challenges and opportunities: A survey. Researchgate (2016)
16. Gupta, M.: Blockchain for dummies. 2nd IBM limited edition. IBM (2018)
17. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access (2016)
18. Yonggui, Z.: Jianming big production enterprise supply chain endogenous risk management based on blockchain. (2019)
19. T. Anh, D., Ji, W., Gang, C., Rui, L., Beng-Chin, O., Kian-Lee, T.: Blockbench: A framework for analyzing private blockchains. In: Proceedings of the ACM international conference on management of data (2017)
20. Yonggui Fu, Jianming Zhu: Big production enterprise supply chain endogenous risk management based on blockchain. IEEE Access, 7 (2019)
21. Bocek, T., Stiller, B.: Smart contracts-blockchains in the wings. Digital marketplaces unleashed, pp. 169–184, Springer (2018)
22. Moreno, J., Serrano, M.A., Fernández-Medina, E.: Main issues in big data security. Future Internet, 8(3), pp. 44 (2016)
23. Pincheira, C., Salek-Ali, M., Vecchio, M., M., Giaffreda, R.: Blockchain-based traceability in agri-food supply chain management: A practical implementation. In: IoT vertical and Topical Summit on Agriculture-Tuscany (2018)
24. Sankar, L.S., Sindhu, M., Sethumadhavan, M.: Survey of consensus protocols on blockchain applications. In: Advanced Computing and Communication Systems (2017)