Blockchain-based architecture for the control of logistics activities: Pharmaceutical utilities case study

YERAY MEZQUITA*, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

ROBERTO CASADO-VARA, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

ALFONSO GONZÁLEZ BRIONES, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

JAVIER PRIETO, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain.*

JUAN M. CORCHADO, *BISITE Digital Innovation Hub, University of Salamanca, Edificio Multiusos I+D+i, 37007 Salamanca, Spain, Department of Electronics, Information and Communication, Faculty of Engineering, Osaka Institute of Technology, 535-8585 Osaka, Japan, Universiti Malaysia Kelantan, Kelantan, Malaysia.*

Abstract

Logistics services involve a wide range of transport operations between distributors and clients. Currently, the large number of intermediaries are a challenge for this sector, as it makes all the processes more complicated. To face that problem, we propose a system that uses smart contracts to remove intermediaries and speed up logistics activities. Our new model combines smart contracts and a multi-agent system in a single platform to improve the current logistics system by increasing organization, security and getting rid of several human intermediaries to automate its processes, making distribution times significantly faster. Also, with this kind of approach, it is possible to apply penalties to parties that do not comply with the terms of using this platform.

Keywords: Blockchain, smart contract, multi-agent system, logistical utilities.

1 Introduction

Logistics is concerned with transporting products between parties. It is currently an important area for companies. However, the problem of this sector is that its scale may lead to delays and defaults in the delivery of goods as well as other issues. In addition, large distributors need a large volume of

*E-mail: yeraymm@usal.es

Vol. 29, No. 6,
Advance Access published 8 September 2020 https://doi.org/10.1093/jigpal/jzaa039

workers to meet the high demand of stores. All this may contribute to big delays in order processing and increases the possibility of losing some of them [31]. In an attempt to solve this problem, companies have automated all their processes, contributing to a significant increase in the number of businesses and distributors in the logistics sector.

However, an increase in the amount of digitized data and the expansion of Internet companies means that the risk of attacks on their databases is also greater. Hackers may intend to modify, steal or delete data [16, 34].

We suggest an alternative way of solving this problem. The case study conducted in this work, a pharmaceutical utilities platform, considers two different scenarios [33]. Firstly, we provide security to the data of the companies involved in the logistics sector by including blockchain. Secondly, multi-agent systems will be used to manage the organization's problem [32]. It has been proven that multi-agent systems provide efficient solutions to a huge variety of problems [54]. These include, but are not limited to, the use of agents for image classification [18], decentralized network control [39], real-time problems [11], distributed model predictive control [12, 24] and Internet of things (IoT) applications [15, 25].

In this paper, we propose a new model that makes use of blockchain technology, smart contracts and a multi-agent system to protect the data of the logistics sector [50] while speeding up logistic activities. In addition, the multi-agent system is capable of coordinating all the logistic services [14], improving the efficiency of the logistics sector.

The proposed model is capable of protecting the data generated within the platform from being tampered thanks to the use of a blockchain. Also, with the use of smart contracts to control the operation of the platform, it is possible to remove intermediaries [19, 43].

The challenges in logistics parameters, such as delays in delivery, loss of documentation, unknown source of products, errors, etc., can be minimized and even avoided by blockchain implementation. With the security mechanisms granted by the use of blockchain technology, it is possible to create a framework for trusted communications between the actors of the platform. Thanks to that, it is much more difficult to make cyber-attacks such as phishing and man in the middle [28, 29].

On the other hand, the multi-agent system uses smart contracts to control and validates the workflow of the platform, while the blockchain network is in charge of storing the transactions carried out by the agents [22]. Although there is a lot of discussion on the use of blockchain in logistical services, there have not been many platforms that would implement and evaluate it in real use case scenarios [51]. In addition, this type of systems have not been propagated sufficiently because the companies that could benefit from them, lack information and therefore do not invest enough money in the implementation of such solutions [27].

Our approach is a functional prototype which has been evaluated empirically. Furthermore, it has been proven that it resists third-party attacks, such us phishing and man in the middle. In the case study, the payments between stakeholders have been automated, which makes this logistic model more efficient than a traditional one.

This paper starts by providing a background in Section 2 of what is blockchain technology and how it works. In Section 3, the designed model is proposed and described, while in Section 4 it has been done an analysis of how this platform carries out a normal workflow and its associated monetary costs, while its advantages are evaluated in line with the conventional model. Finally, a conclusion is provided in Section 5.

2 Background

A blockchain is a distributed data structure that is replicated and shared among the members of a network [9]. It was introduced with Bitcoin [40] to create a distributed ledger that would enable the automation of transactions while solving the double-spending problem [44].

To ensure the authenticity of the stored transactions, it is first necessary to ensure the integrity of the nodes of the network that support the blockchain by implementing a consensus algorithm [13]. With this algorithm, the nodes of the network are able to agree on the information they must keep stored and who will be the next one that adds a new block of data.

There is an increasing number of consensus algorithms with their own variations. The most widespread algorithms are the ones that work best, this is why they, or some of their variations, are used by the vast majority of blockchain networks [38].

In the two most popular blockchain networks, Bitcoin and Ethereum, the consensus algorithm [26, 56] used is called proof of work (PoW). The basis of this protocol is that the node that wants to add a new block of data to the blockchain, called miner, must follow a series of steps in order to complete the task successfully and obtain the reward [40]:

1. Gather the transactions that the miner is interested in storing in the blockchain.
2. Create a Merkle tree with the hashes of the transactions in the leaves. In order to create the root of the tree, the transactions are being hashed by pairs, creating the inner elements of the tree. Those elements are hashed by pairs again, to create another layer of inner elements, repeating this process until there is no more than one element in the most inner layer of the tree [3].
3. Create the new block with the following fields in the block header [41]:
   - Version: the number of the version used to create this header. It is used to track software/protocol upgrades.
   - Previous block hash: a reference to the previous block of the blockchain. The hash of the block is used to get its identifier [5, 16, 47].
   - Merkle tree root: the Merkle tree root obtained in the previous step.
   - Timestamp: the approximate creation time of this block (seconds from Unix epoc).
   - Difficulty target: the difficulty level used to create this block in the PoW algorithm.
   - Nonce: it is a number that the miner inserts in order to make the hash of the block, once all the fields are filled, it falls within the upper limit established by the difficulty target of the algorithm.
4. Using a trial-and-error method, the miner searches for a nonce that meets the requirements of adding the new block.
5. Once the nonce is found, the mined block is broadcasted to the network in order to be validated.

Thanks to this mechanism, blockchain's ledger of logged transactions becomes immutable [52]. To attack this mechanism, an entity or organization needs to have more than the 51% of the network hash rate power, something pretty difficult to acquire in the case of blockhains like Bitcoin or Ethereum [1, 21].

The link established by the blocks forms the blockchain [4, 10]. Sometimes, a part of the network has received different legal blocks than the other part due to concurrence issues, creating different blockchains, called forks [7, 42]. When this situation happens, it is the consensus mechanism used by the network the one that says which one of the forked blockchains will be accepted by the entire network, discarding the other one [46].

Another key feature of the systems that make use of blockchain technology is that the communications between the entities and the blockchain are encrypted point to point. This is achieved by the

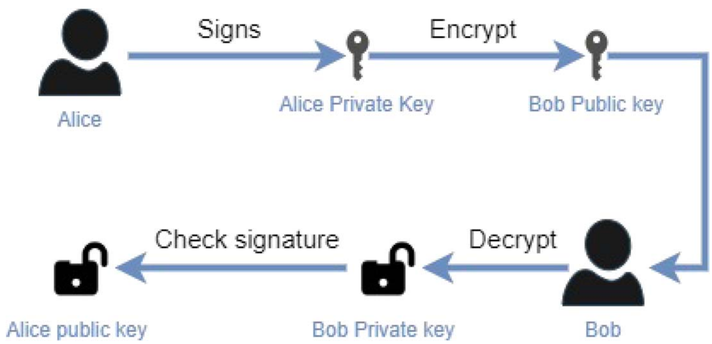

FIGURE 1. Graph of a typical public-key-based mechanism in communications.

use of public-key cryptography mechanism [53]. The basic operation of this mechanism consists of using one key pair per entity, one key is public and can be known by everyone, while the other one is private and is kept for the entity alone [36].

As shown in Figure 1, the public key is used normally by other entities to cipher a message that is supposed to be read only by the owner of that key [35]. Then the owner deciphers it with their private key. Also, the private key is used to sign the messages sent by the owner, while its public key is used to verify its signature by the receivers. So, when an entity wants to use the blockchain to make a transaction, it signs the message with its private key to let the network know it wants to make a transaction, while helping the nodes to verify that message comes from him.

With the implementation of blockchain technology in this platform, smart contracts are included to make transactions between different entities faster and more effective use. Nick Szabo introduced this concept in 1994 and defined a smart contract as 'a computerized transaction protocol that executes the terms of a contract' [48]. Szabo suggested that the clauses of contracts could be transferred to code, thus reducing the need for intermediaries in transactions between parties. In the blockchain context, a smart contract is a script that is stored on a blockchain [49].

Smart contracts have a unique address in a blockchain (i.e. they are in a block with a hash that identifies it). We can trigger a smart contract in a transaction by indicating its address on the blockchain. It is executed independently and automatically in a prescribed manner on every node in the network, according to the data contained in the triggered transaction [38].

A multi-agent system is a computerized system composed of multiple intelligent agents that interact with each other. Multi-agent systems are used to solve complex problems and achieve very good results [24]. Multi-agent systems are used in a wide range of applications. Gazafroudi *et al.* [25] presented a multi-agent system for the intelligent use of electricity in a smart home and thus, an increase in its energy efficiency.

The application of a multi-agent system to logistics is not a new idea; in [30], a multi-agent system is proposed to provide a solution to the logistical problem. In addition, another successful application of multi-agent systems is the problem of distributed computing [6], as well as the distributed model predictive control in the chemical industry [24].

From a range of systems that integrate blockchain and multi-agent systems, the work of [2] is worthy of mention. This work proposes the use of both technologies to increase security and privacy in decentralized energy networks. In [55], authors proposed a model that employs agents and blockchain for a ride-sharing system.

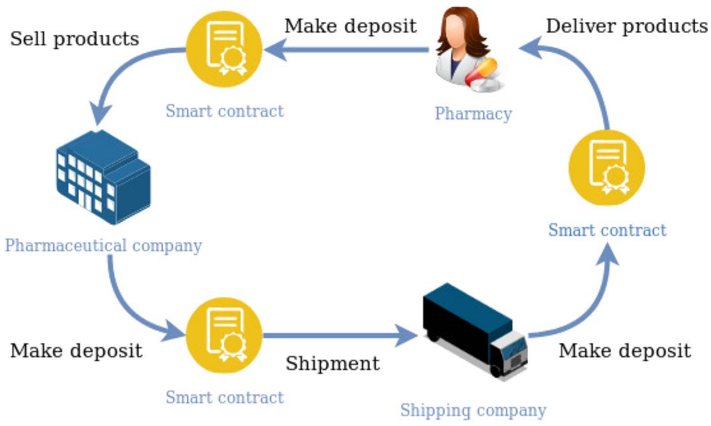

FIGURE 2. Graph based on smart contract for pharmaceutical logistics sector.

In addition, there are other applications of blockchain and multi-agent systems, like [20], in which the authors proposed an innovative blockchain model for IoT platforms. In [37], a blockchain-based multi-agent system is proposed; it simulates the tracking of agri-food assets in an agri-food supply chain. Smart contracts and sealed devices have been used to make sure that the data stored in the blockchain can be trusted.

However, after looking at the state of the art, we believe that the current blockchain and multi-agent system models have some shortcomings. We propose a new model that leverages smart contracts and multi-agent systems, making use of audit systems that will help trust the data created in the blockchain in a similar way as in [37] but adapted to this use case.

In this model, the network of Ethereum is also used as the mechanism to control the workflow of the platform through the smart contracts deployed in it. Thanks to the use of the smart contracts and the blockchain in the communications layer as well as in the storage layer, the management efficiency of the logistics system increases, automating the workflow and removing the failure and time delays caused by humans. This paper describes a case study which verified the proposed model, it focused specifically on logistics transport in the pharmaceutical sector.

3 Methodology

This paper presents a new model which consists of the following elements: a public blockchain network that is used as a service and all transactions and smart contracts are stored in it, like in [37]; smart contracts that will manage commercial transactions between the different parties; and a multi-agent system that enables the execution of all of these operations. In this section, we describe how our model works.

The parties involved in a business operation have smart devices which monitor the status of each operation. The case study was conducted in the pharmaceutical sector; Figure 2 shows process members: the client (pharmacies), the producer (pharmaceutical companies) and the shipping companies.

In this use case, the clients have sensors that monitor the number of drugs stored in the pharmacy, the type of drugs sold and the amount of money stored. Regarding the pharmaceutical companies, they have sensors in charge of knowing the available stock and current production levels. Finally, transportation companies have sensors on each of their transport vehicles to monitor the position of the cargo. All these elements make up the wireless sensor network (WSN) that monitors operations in the pharmaceutical sector.

Within the WSN that monitors the operations carried out in this use case, there are smart devices that are responsible for creating the transactions with the monitored data. Those transactions are sent to the blockchain network by the smart devices. In the blockchain, along with the data generated, it also stored the smart contracts that control the workflow of the platform.

A multi-agent system controls the whole process. The architecture of the multi-agent system consists of the following layers (see Figure 3):

1. Client layer: this layer consists of three different types of agents that manage pharmacies. These include the data management agent that keep updated the stock of the pharmacy and the agent that is responsible for placing orders and that which verifies the delivery of the purchased products, changing its state in the blockchain through smart contracts.
2. The source layer contains the following agents: two agents receive orders from pharmacists and another agent places orders with the transport company in order to take the goods to the pharmacies. Another agent's task is the control of stock and production levels. Finally, there is an agent responsible for verifying whether smart contract conditions are fulfilled.
3. Shipping layer has the following agents: an agent that manages the incoming orders, another agent that manages the fleet of vehicles and, finally, an agent that verifies smart contracts.
4. Workflow management layer is composed of two agents, a workflow management agent and a smart contract control agent this agent. This layer is in charge of creating smart contracts, keeping the money while making transactions and applying penalties in case of non-compliance with the smart contracts.

Thus, one of the agents included in each of the 4 layers verifies that the smart contract terms are abided to. For instance, when the workflow of a smart contract smart contract is initiated between a pharmacy and a pharmaceutical company for the purchase of medicine, both have to agree on a set of terms. The pharmacy pays for the drugs, but money is kept in the blockchain by a control entity, in this case the agent that verifies the smart contract. When the pharmacy receives the drugs it ordered, this agent confirms that the conditions of the smart contract have been fulfilled and automatically pays the pharmacist the agreed sum of money.

4 Results

Once the multi-agent system has been designed, the number of times the platform interacts with the blockchain has been studied. In this model, the transactions carried out in a normal workflow to purchase products are detailed as follows:

- In the client layer, when a client wants to buy a product, a transaction of funds from the client to the smart contract is carried out. Also, whenever a batch of items arrives at its final destination, the state of the batch is updated and a transaction is executed, in which it is updated the state of the batch, and the smart contract releases the funds transacted from the client to the owner of the product. This means that in a normal workflow, three transactions are carried out in this layer.

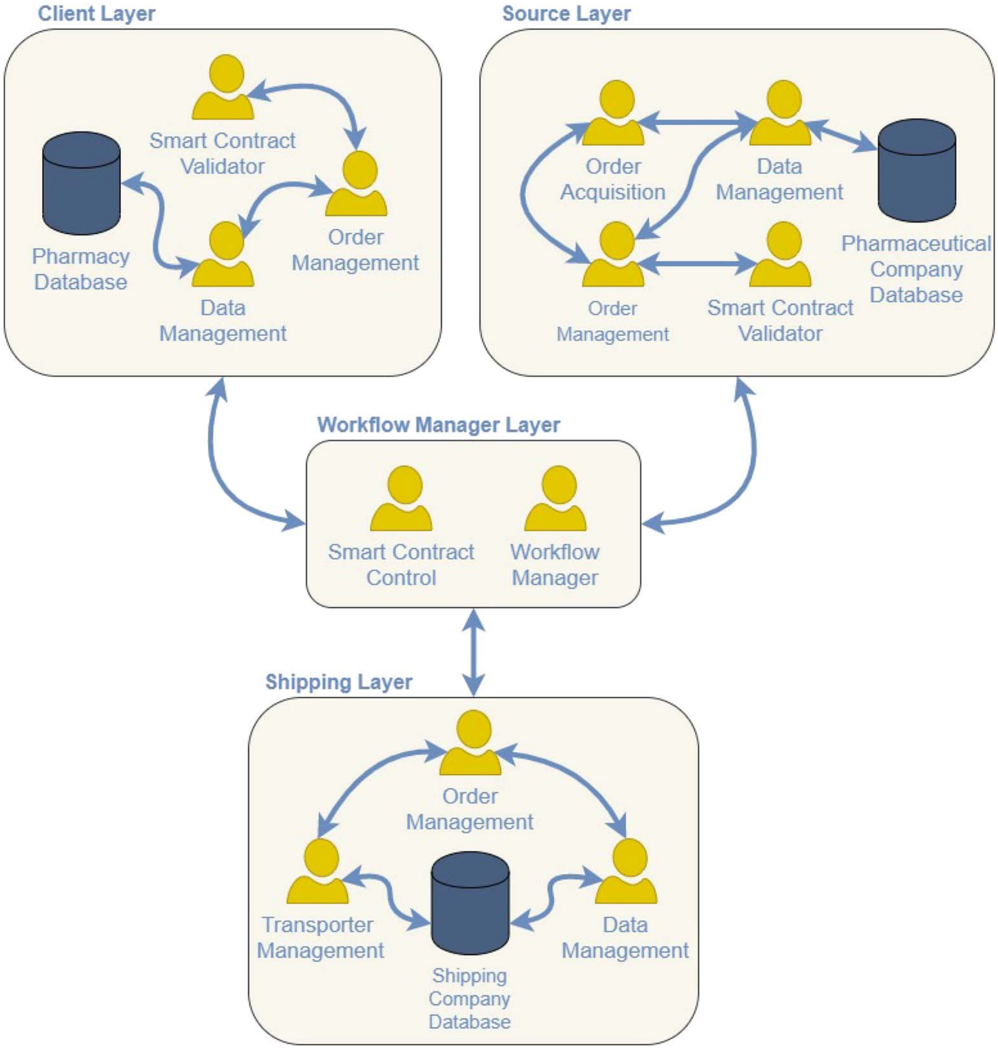

FIGURE 3 Multi-agent architecture. (i) Client layer: the pharmacies are found in this layer. (ii) Source layer: this layer contains pharmaceutical companies. (iii) Shipping layer: this layer manages transport companies. (iv) Workflow management layer: this layer contains an agent that controls the entire information flow and an agent which ensures that smart contract conditions are fulfilled.

– In the source layer, a transaction is carried out a transaction when a batch of products is put on sale, another when it is sold and when it is being shipped. The last transaction involves securing the payment made by the client in the smart contract, so that the seller does not receive the payment until it has been confirmed that the order has been delivered correctly. If nothing is wrong with the order, the funds are returned to the seller, making a total of five transactions in a normal execution.

- The workflow manager layer only makes transactions with the blockchain when an agent wants to be part of the platform and an agent leaves it. One transaction for each update of the agents status.
- The shipping layer only transfers the payment to the smart contract when a new order is being shipped. The funds are given to the seller in the case it has been any problem with the shipment. Otherwise, they are returned to the transporter.

After studying the interactions of the platform with the blockchain, we found out that a minimum of ten transactions are carried out when a batch of products are delivered from a seller to a final client. This number does not take into account the number of the transactions made in cases where a new seller, client or transporter wants to be a part of the platform.

To calculate the cost of executing the services of the blockahin network, we have to know the price of executing each transaction. In the case of Ethereum, the one chosen for this use case, and according to [45], the execution price of a transaction is equivalent to 0.1€, which multiplied by the number of transactions in a normal workflow of the system, the amount of money needed by all the stakeholders to keep the system up is 1€ per batch of products that are transacted from a stakeholder to another.

One of the reasons for which the Ethereum blockchain has been selected is because it offers the best support for the integration of the platform and moreover it uses the Python programming language, web3.py [23]. Also, if we assume that there are a hundred buyers and sellers, then hundreds of transactions are being carried out by the platform in a normal workflow iteration. Being said that, the time needed to perform an exchange of assets between seller and buyer is in the order of days, and the daily average number of transactions of the Ethereum blockchain is 610000 [17], then we can assume that the proposed platform can be managed by the Ethereum network.

In our study, it has been shown that the price for exchanging a batch of assets between different stakeholders is about 1€. If we have to compare to the traditional model that uses human intermediaries in the verification process [8], the workflow of our proposed platform is cheaper and faster.

5 Conclusion

This paper presents a new smart contract approach to improving logistics services. The novelty of this paper lies in the use of a blockchain for the storage of all the transaction of information in the logistical process. The proposed model makes use of smart contracts to manage the entire logistics process of a pharmaceutical supply chain more efficiently. By automating the processes with the use of smart contracts, human intermediaries are no longer needed.

Another novelty of this paper is the use of agents who verify that both parties abide to the terms of a smart contract. If the agents detect that either of the parties is not fulfilling the established conditions, a penalty is imposed and the agents keep money in the control entity until the conditions agreed upon are met. This makes our model more efficient than current models. Moreover, it is able to track and authenticate orders. A penalties pattern is introduced for breach of smart contracts.

Our model can be used to improve any logistics system that still relies in human intermediaries that verify payments and/or transactions between non-trusted parties. It is highly efficient and secure because it is automated by the multi-agent system. By incorporating blockchain, we provide the logistics system with solid security features. Shipments can be tracked, origin and destinations authenticated, and proof of all transactions can be stored and maintained unaltered in the blockchain.

Future lines of research include improving the multi-agent system by introducing new agents for the monitoring of procedures. In addition, our model could be enhanced by integrating a case-based reasoning system.

Acknowledgements

This work was developed as part of 'Virtual Ledger Technologies DLT/Blockchain y Cripto-IOT sobre organizaciones virtuales de agentes ligeros y su aplicación en la eficiencia en el transporte de última milla', ID SA267P18, project cofinanced by Junta Castilla y León, Consejería de Educación and FEDER funds. Also, the research work carried out by Yeray Mezquita is supported by the pre-doctoral fellowship from the University of Salamanca and Banco Santander.

References

[1] Academy Binance. What is a 51% attack? (October 2019). https://www.binance.vision/security/what-is-a-51-percent-attack, accessed: 04/10/2019.

[2] N. Z. Aitzhan and D. Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, **15**, 840–852, 2016.

[3] N. Z. Andrew. Blockchain fundamentals #1: what is a Merkle tree? (February 2018). https://medium.com/byzantine-studio/blockchain-fundamentals-what-is-a-merkle-tree-d44c529391d7, accessed: 01/10/2019.

[4] A. M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc., 2014.

[5] A. Back. Hashcash—a denial of service counter-measure, 2002.

[6] S. Banerjee and J. P. Hecker. A multi-agent system approach to load-balancing and resource allocation for distributed computing. In *First Complex Systems Digital Campus World E-Conference 2015*, pp. 41–54. Springer, 2017.

[7] L. Becerra-Bonache and M. D. J. López. Linguistic models at the crossroads of agents, learning and formal languages. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **3**, 67–87, 2014.

[8] R. Benjamin and R. Wigand. Electronic markets and virtual value chains on the information superhighway. *MIT Sloan Management Review*, **36**, 62, 1995.

[9] J. Bremer and S. Lehnhoff. Decentralized coalition formation with agent-based combinatorial heuristics. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **6**, 29–44, 2017.

[10] R. C. Cardoso and R. H. Bordini. A multi-agent extension of a hierarchical task network planning formalism. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **6**, 5–17, 2017.

[11] C. Carrascosa, J. Bajo, V. Julián, J. M. Corchado and V. Botti. Hybrid multi-agent architecture as a real-time problem-solving model. *Expert Systems with Applications*, **34**, 2–17, 2008.

[12] R. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto and J. M. Corchado. Non-linear adaptive closed-loop control system for improved efficiency in iot-blockchain management. *Information Fusion*, **49**, 227–239, 2019.

[13] R. Casado-Vara and J. M. Corchado. Blockchain for democratic voting: how blockchain could cast off voter fraud. *Oriental Journal of Computer Science and Technology*, **11**, 01–03, 2018.

[14] R. Casado-Vara, P. Novais, A. B. Gil, J. Prieto and J. M. Corchado. Distributed continuous-time

fault estimation control for multiple devices in iot networks. *IEEE Access*, **7**, 11972–11984, 2019.

[15] R. Casado-Vara, F. Prieto-Castrillo and J. M. Corchado. A game theory approach for cooperative control to improve data quality and false data detection in wsn. *International Journal of Robust and Nonlinear Control*, **28**, 5087–5102, 2018.

[16] R. Casado-Vara, A. Martin-del Rey, S. Affes, J. Prieto and J. M. Corchado. Iot network slicing on virtual layers of homogeneous data for improved algorithm operation in smart buildings. *Future Generation Computer Systems*, **102**, 965–977, 2020.

[17] ConsenSysConsenSys Ethereum by the numbers (December 2018). https://media.consensys.net/ethereum-by-the-numbers-3520f44565a9, accessed: 04/10/2019.

[18] J. A. G. Coria, J. A. Castellanos-Garzón and J. M. Corchado. Intelligent business processes composition based on multi-agent systems. *Expert Systems with Applications*, **41**, 1189–1205, 2014.

[19] Â. Costa, P. Novais, J. M. Corchado and J. Neves. Increased performance and better patient attendance in an hospital with the use of smart agendas. *Logic Journal of IGPL*, **20**, 689–698, 2011.

[20] V. Daza, R. Di, I. Klimek and M. Signorini. Connect: contextual name discovery for blockchain-based services in the iot. In *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6. IEEE, 2017.

[21] Q. DuPont. Experiments in algorithmic governance: a history and ethnography of “the dao,” a failed decentralized autonomous organization. In *Bitcoin and Beyond (Open Access)*, pp. 157–177. Routledge, 2017.

[22] B. O. Durić. Organisational metamodel for large-scale multi-agent systems: first steps towards modelling organisation dynamics. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **6**, 2017, 2017.

[23] EthereumEthereum A python interface for interacting with the Ethereum blockchain and ecosystem. https://web3py.readthedocs.io/en/stable/.

[24] M. Francisco, Y. Mezquita, S. Revollar, P. Vega and J. F. De Paz. Multi-agent distributed model predictive control with fuzzy negotiation. *Expert Systems with Applications*, **129**, 68–83, 2019.

[25] A. S. Gazafroudi, T. Pinto, F. Prieto-Castrillo, J. Prieto, J. M. Corchado, A. Jozi, Z. Vale and G. K. Venayagamoorthy. Organization-based multi-agent structure of the smart home electricity system. In *2017 IEEE Congress on Evolutionary Computation (CEC)*, pp. 1327–1334. IEEE, 2017.

[26] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf and S. Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3–16. ACM, 2016.

[27] N. Hackius and M. Petersen. Blockchain in logistics and supply chain: trick or treat? In *Proceedings of the Hamburg International Conference of Logistics (HICL)*, pp. 3–18. Epubli, 2017.

[28] M. A. Khan and K. Salah. Iot security: review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, **82**, 395–411, 2018.

[29] N. Kshetri. Can blockchain strengthen the internet of things? *IT Professional*, **19**, 68–72, 2017.

[30] K. Li, T. Zhou, B.H. Liu and H. Li. A multi-agent system for sharing distributed manufacturing resources. *Expert Systems with Applications*, **99**, 32–43, 2018.

[31] T. Li, S. Sun, M. Bolić and J. M. Corchado. Algorithm design for parallel implementation of the smc-phd filter. *Signal Processing*, **119**, 115–127, 2016.

[32] T. Li, S. Sun, J. M. Corchado and M. F. Siyau. A particle dyeing approach for track continuity

for the smc-phd filter. In *17th International Conference on Information Fusion (FUSION)*, pp. 1–8. IEEE, 2014.

[33] T. Li, S. Sun, J. M. Corchado and M. F. Siyau. Random finite set-based bayesian filters using magnitude-adaptive target birth intensity. In *17th International Conference on Information Fusion (FUSION)*, pp. 1–8. IEEE, 2014.

[34] A. C. E. Lima, L. N. de Castro and J. M. Corchado. A polarity analysis framework for twitter messages. *Applied Mathematics and Computation*, **270**, 756–767, 2015.

[35] C. C. Lo and Y. J. Chen. Secure communication mechanisms for gsm networks. *IEEE Transactions on Consumer Electronics*, **45**, 1074–1080, 1999.

[36] D. Massessi. Blockchain public/private key cryptography in a nutshell. (October 2018). https://medium.com/acoinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c, accessed: 04/10/2019.

[37] Y. Mezquita, A. González-Briones, R. Casado-Vara, P. Chamoso, J. Prieto and J. M. Corchado. Blockchain-based architecture: a mas proposal for efficient agri-food supply chains. In *International Symposium on Ambient Intelligence*, pp. 89–96. Springer, 2019.

[38] Y. Mezquita, D. Valdeolmillos, A. González-Briones, J. Prieto and J. M. Corchado. Legal aspects and emerging risks in the use of smart contracts based on blockchain. In *International Conference on Knowledge Management in Organizations*, pp. 525–535. Springer, 2019.

[39] S. Najafi, S. Talari, A. S. Gazafroudi, M. Shafie-khah, J. M. Corchado and J. P. Catalão. Decentralized control of dr using a multi-agent method. In *Sustainable Interdependent Networks*, pp. 233–249. Springer, 2018.

[40] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2008.

[41] PrasannaPrasanna What is the blockchain data structure? (November 2018). https://cryptoticker.io/en/blockchain-data-structure/, accessed: 01/10/2019.

[42] P. Rodríguez, N. Duque and D. A. Ovalle. Multi-agent system for knowledge-based recommendation of learning objects using metadata clustering. In *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pp. 356–364. Springer, 2015.

[43] S. Rodríguez, F. de La Prieta, D. I. Tapia and J. M. Corchado. Agents and computer vision for processing stereoscopic images. In *International Conference on Hybrid Artificial Intelligence Systems*, pp. 93–100. Springer, 2010.

[44] M. Rosenfeld. Analysis of hashrate-based double spending. Dec. 2012. https://www.bitcoil.co.il/Doublespend.pdf.

[45] D. Ryan. Calculating costs in ethereum contracts (May 2017). https://hackernoon.com/ether-purchase-power-df40a38c5a2f, accessed: 04/10/2019.

[46] G. Santos, T. Pinto, V. Zita, I. Praça and H. Morais. Enabling communications in heterogeneous multi-agent systems: electricity markets ontology. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, **5**, 15–42, 2016.

[47] F. I. P. Standards. Secure hash standard (August 2002). https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf, accessed: 02/25/2004.

[48] N. Szabo. Smart contracts. *Virtual School*, 1994.

[49] N. Szabo. The Idea of Smart Contracts. Nick Szabo's Papers and Concise Tutorials 6, 1997.

[50] D. I. Tapia, J. A. Fraile, S. Rodríguez, R. S. Alonso and J. M. Corchado. Integrating hardware agents into an enhanced multi-agent architecture for ambient intelligence systems. *Information Sciences*, **222**, 47–65, 2013.

[51] E. Tijan, S. Aksentijević, K. Ivanić and M. Jardas. Blockchain technology implementation in logistics. *Sustainability*, **11**, 1185, 2019.

[52] D. Valdeolmillos, Y. Mezquita, A. González-Briones, J. Prieto and J. M. Corchado. Blockchain technology: a review of the current challenges of cryptocurrency. In *International Congress on Blockchain and Applications*, pp. 153–160. Springer, 2019.

[53] J. Weise. *Public Key Infrastructure Overview*, pp. 1–27. Sun BluePrints OnLine, 2001.

[54] M. Wooldridge and N. R. Jennings. Intelligent agents: theory and practice. *The Knowledge Engineering Review*, **10**, 115–152, 1995.

[55] Y. Yuan and F. Y. Wang. Towards blockchain-based intelligent transportation systems. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 2663–2668. IEEE, 2016.

[56] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang. An overview of blockchain technology: architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564. IEEE, 2017.

Received 1 March 2019