Blockchain framework for IoT data quality via edge computing

Roberto Casado-Vara[*]
BISITE Digital Innovation Hub, University of Salamanca.
Edificio Multiusos I+D+i, 37007, Salamanca, Spain., Spain
rober@usal.es

Fernando de la Prieta
BISITE Digital Innovation Hub, University of Salamanca.
Edificio Multiusos I+D+i, 37007, Salamanca, Spain., Spain
fer@usal.es

Javier Prieto
BISITE Digital Innovation Hub, University of Salamanca.
Edificio Multiusos I+D+i, 37007, Salamanca, Spain., Spain
javierp@usal.es

Juan M. Corchado
BISITE Digital Innovation Hub, University of Salamanca.
Edificio Multiusos I+D+i, 37007, Salamanca, Spain., Spain
corchado@usal.es

ABSTRACT

Smart home presents a challenge in control and monitoring of its wireless sensors networks (WSN) and the internet of things (IoT) devices which form it. The current IoT architectures are centralized, complex, with poor security in its communications and with upstream communication channels mainly. As a result, there are problems with data reliability. These problems include data missing, malicious data inserted, communications network overload, and overload of computing power at the central node. In this paper a new architecture is presented. This architecture based in blockchain introduce the edge computing layer and a new algorithm to improve data quality and false data detection.

KEYWORDS

Blockchain, IoT, WSN, edge computing, data quality, false data detection, non linear control

ACM Reference Format:
Roberto Casado-Vara, Fernando de la Prieta, Javier Prieto, and Juan M. Corchado. 2018. Blockchain framework for IoT data quality via edge computing. In *The 1st Workshop on Blockchain-enabled Networked Sensor Systems (BlockSys'18), November 4, 2018, Shenzhen, China.* ACM, New York, NY, USA, Article 39, 6 pages. https://doi.org/10.1145/3282278.3282282

1 INTRODUCTION

IoT and blockchain are two topics which are causing a great deal of hype and excitement, not just in the technology circle but in the wide business world, too. Many people say they are ready to reshape all aspects of our lives, while others point out that there is a lot of hot air around both ideas, and much remains to be proved. However, the idea that putting them together could result in something even greater than the sum of their parts (not insignificant) is beginning to gain traction. At first, it makes a lot of sense. IoT is a term used to describe the current explosion of online data collection devices in our work and personal lives [21]. Blockchain is an encrypted and distributed computer archiving system designed to enable the creation of real-time, tamper-proof records. Put them together and, in theory, have a verifiable, secure and permanent method of recording data processed by smart machines on IoT.

There are various advantages to the idea of building smart machines that are able to communicate and operate through a blockchain [12]. Firstly, there is the issue of supervision. With data transactions occurring between multiple proprietary networks and operated by several organizations, a permanent, immutable record means that custody can be tracked as data, or physical assets, are transferred from one point in the supply chain to another [35]. Blockchain records are transparent by nature (i.e., activity can be tracked and analyzed by anyone authorized to connect to the network). If something fails, breaks down, data leaks where it shouldn't, then blockchain recording makes it easier to identify the weak link and take corrective action. Secondly, the use of encryption and distributed storage means that all parties involved in the supply chain can trust data. Machines should be able to securely record details of transactions between them without any human oversight. Without the private keys that provide write access to the blockchain (which in this case would be in the hands of machines), no human being can overwrite the registry with inaccurate information [32]. Thirdly, the smart contract support provided by some blockchain networks, such as Ethereum, allows for the creation of agreements that are implemented when the conditions are fulfilled. This can be very useful when it comes, for example, to authorising a system to make a payment, when the conditions indicate that a service has been provided. Fourthly, the blockchain has considerable scope for improving the global security of the IoT environment. For example, smart home devices have access to personal details about our lives and daily routines. This is data that must be shared with other machines and services to be useful to us [27]. But it also means that there is a significantly chance that hackers could attack us. Companies and governments investing in IoT also face this increased chance of data breach by foreign criminals, rivals or enemies. Allowing access to data on IoT devices to be controlled through blockchain would mean an additional layer of security that any malicious agent would have to avoid, and that is protected by some of the most robust encryption standards available.

[*] This is the corresponding author

BlockSys'18, November 4, 2018, Shenzhen, China
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-6050-0/18/11…$15.00
https://doi.org/10.1145/3282278.3282282

This paper presents a hybrid IoT architecture that allows decentralized data management via blockchain. For this purpose, the architecture has a computation distribution under the edge computing paradigm. This makes it possible to optimize the connection between IoT and blockchain. On the other hand, the other part of the hybrid system is data management with a big data ecosystem that facilitates the management of large amounts of data in blockchain. We believe that this hybrid architecture optimizes the current end-to-end architectures. This paper is organized as follows: in section 2 has the related work. Section 3 has the IoT based blockchain architecture, section 4 has the emperical results and section 5 has the conclusion.

2 RELATED WORK

A blockchain is a distributed data structure that is replicated and shared among the members of a network [22]. It was introduced with Bitcoin [26] to solve the double-spending problem [13]. As a result of how the nodes in Bitcoin (the so-called miners) mutually validate the agreed transactions, Bitcoin blockchain establishes the owners and states what they own [15]. A blockchain is built using cryptography. Each block is identified by its own cryptographic hash and each block refers to the hash of the previous block. This establishes a link between the blocks, forming a blockchain [3] [10] [7]. For this reason, users can interact with a blockchain by using a pair of public and private keys. Miners in a blockchain need to agree on the transactions and the order in which they have occurred. Otherwise the individual copies of this blockchain can diverge producing a fork; miners then have a different view of how the transactions have occurred, and it will not be possible to keep a single blockchain until the fork is not solved [18].

To achieve this a distributed consensus mechanism is required in every blockchain network [6]. Blockchain's way to solve the fork problem is that each blockchain node can link next block. Just a correct random number with SHA-256 has to be found [2] [11] [19] so you have number of zeros that the blockchain expects. Any node that can solve this puzzle has generated the so-called proof-of-work (pow) and gets to shape the chain's next block [26]. Since a one-way cryptographic hash function is involved, any other node can easily verify that the given answer satisfies the requirement. Notice that a fork may still occur in the network, when two competing nodes mine blocks almost simultaneously. Such forks are usually resolved automatically by the next block [29] [4].

On the other hand, an IoT are a network of sensors whose communications are transmitted by wireless signals. WSNs are used to collect and study a wide range of magnitudes, such as sound, humidity, temperature and many others [6] [8]. WSN is the preferred as the architecture of the sensor systems, but they are susceptible to the disadvantages caused by the limited lifetime of the operation. Unlike other sensor networks with physical support (wire), the use of WSN is limited by amount of energy it can store, its calculation capacities, memory, information flow and communication distance. WSN will be used to control and monitor a wide range of things [20] [24]. Some works are achieving good results in fields such as energy efficiency using WSN [5], control of operations [17], optimal routing in WSN [33], and some other applications such as social good [28]. Sensor networks can also be used with other technologies such as multi-agent systems to manage data [30], for data mining [31], multi-agent localization [33] and WSN [34] [9]. Clustering techniques will be used to find fraud cases. Among the machine learning algorithms that use clustering techniques, the most used technique to form clusters is the distance between the elements [16]. These algorithms are also being used for data mining [1].

Due of advantages offered by blockchain and WSN, applications are being created that combine both technologies. One of the first applications has been to authenticate and increase reliability in WSNs using blockchain [14] [25]. Other applications are also available with the Internet of Things and the global commerce [23]. Other applications of blockchain with WSN is to increase the security of the transactions. However, these applications have certain shortcomings because they are too general. In this paper a new architecture is presented. This architecture is based on the use of blockchain to improve data quality with a cooperative algorithm in the edge computing layer.

3 IOT BASED BLOCKCHAIN ARCHITECTURE FOR WSN CONTROL

In this paper we present a new architecture for monitoring and control IoT systems. This paper introduces a case study of a smart home. In this smart home there are a WSN which monitoring all the activities which occur in the smart home. This WSN sends the data to a blockchain. This allows data collected in the smart home and then stored in the blockchain to achieve all the advantages of blockchain. In the next paragraphs our new architecture for IoT monitoring and control is described. The smart devices that are equipped with sensors and a Raspberry Pi that controls these sensors. Each smart node is formed by different transceivers capable of capturing the data and incorporating it into the WSN. The sensor incorporates an accelerometer model LIS3DH capable of accurately measuring acceleration in different ranges (between 0 and +- 16g). This sensor is automatically adjusted to the usage conditions so it always maintains a constant accuracy. For temperature control a TC1047A ultra-low power consumption sensor is incorporated. The system also incorporates a positioning system through GNSS networks to geolocate data through the MAX-M8Q model of the u-blox manufacturer capable of receiving signals from the GPS, Galileo and GLONASS standards. For power consumption measurement, a non-invasive hall effect sensor is incorporated, the SCT-013-000 which is suitable for measuring power consumption up to 100A with a dielectric resistivity of 3KV. All this is controlled by an ATSAMR21G18A microcontroller (MCU) from Microchip manufacturer. This MCU is based on the ultra low power ARM Cortex-M0+ architecture and incorporates the IEEE 802.15.4 communication protocol so it is able to communicate on OpenThread network. A raspberry pi 3 is used as a technology edge router. To be able to communicate with the WSN, the raspberry pi 3 incorporates an OpenThread platform enabling device the CC2652 from the manufacturer Texas Instruments that facilitates the implementation of the WSN thanks to its open drivers. In this way, the raspberry collects the information from

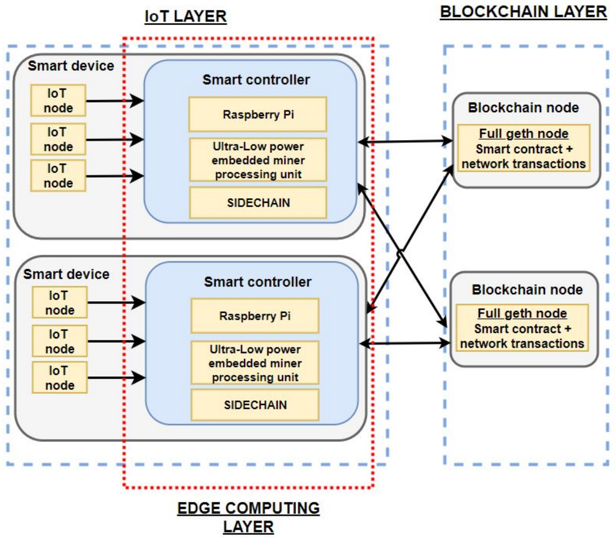

Figure 1: The figure show a new architecture for IoT monitoring and control via Blockchain.

the WSN and transmits it to the sidechain.

The smart controller manages the IoT nodes and all of their WSN nodes. Every IoT node collects data from its sensors. The Raspberry Pi then executes a smart contract in the main chain (blockchain). The smart controller has a miner processing unit to improve the computing power of the Raspberry pi. This module provides processing power to the Raspberry and enables it to perform some uncomplicated calculations in a reasonable amount of time. In this way, data can be transformed in the ETL (Extract Transform and Load) process from the IoT devices to the blockchain in the edge computing layer, instead of in the blockchain miners. This considerably reduces the energy consumption of the miners in transforming the data and building the blocks, since the smart controllers do the same with much lower energy consumption. This smart contract creates a sidechain that executes on the Raspberry Pi where all data collected by the WSN node of that smart device is stored. The smart contract authenticates the identity of the smart device and once it recognizes the WSN node as a member, the smart contract executes an event to send the data into the sidechain. Once the smart contract is validated (i.e., the data is completely inserted into the sidechain) the sidechain is inserted into the main chain. In this way, the blockchain is built with data collected by the smart devices. In order to build the blockchain, this new architecture presents the novelty of using sidechains (i.e., small blockchain pre-processing data) to build an intermediate layer between the IoT devices and the blockchain (i.e., edge computing layer). These sidechains optimize the transactions that are sent into the blockchain by performing data processing at the edge of the network, near the source of the data. This reduces communications between the WSN nodes (i.e., sensors) and the blockchain by performing the sidechains that have the WSN data. This approach requires leveraging resources that may not be continuously connected to a blockchain network and less resource wasting in the IoT layer. Edge computing pushes the applications, data and computing power away from the blockchain. As a computational paradigm, edge computing is also known as mesh processing, peer-to-peer computing, automatic and decentralized computing. The advantages of edge computing over current computing are: 1) the amount of data that needs to be moved over the network is much smaller. 2) edge computing eliminates (or reduces) centralized computing. 3) The ability to virtualize extends scalability.

Communications technology between the WSN and Raspberry Pi is called OpenThread. This technology is wireless and is based on the IEE 802.15.4-2006 standard. OpenThread uses the 2.4 GHz communications channel and assigns an IPv6 IP to each WSN so that every node is identified biunivocally. This protocol allows for data download individualized channels for communications, firmware updates, etc. The IPv6 protocol is used because in this way we avoid the IPv4 address allocation saturation that exists in the current WSN. Nowadays other protocols do not allow full duplex (i.e., bidirectional) communication as the data download from the network to the device is done through intermediaries (e.g., NAT, Gateways). As a novelty of this new architecture, the sensor is identified in the IPv6 standard. This sensor is authenticated throughout the network. This protocol allows the data collected by the sensor (and not other malicious data) to be entered into the sidechain.

The main objective of this paper is to improve the quality of data and false data detection, for them we have developed an algorithm based on game theory that runs on the edge computing layer of our new architecture on the data collected by the IoT nodes. In this way, it can be guaranteed that data stored in the blockchain is reliable, removing potential errors in the accuracy of the sensors or detecting false data. In the next paragraphs we describe the cooperative algorithm based on game theory. The previous step for the cooperative algorithm to work is to place the data received from the IoT sensors in a temperature matrix. The position of the data in the matrix depends on the position of the IoT devices, for this purpose, a mesh is made of the environment that monitors the IoT devices, and in this way the IoT devices can be ordered in the temperature matrix.

$$T_{n,n} = \begin{pmatrix} t_{s_{1,1}} & \cdots & t_{s_{1,n}} \\ \vdots & \ddots & \vdots \\ t_{s_{n,1}} & \cdots & t_{s_{n,n}} \end{pmatrix} \tag{1}$$

3.1 Mathematical formulation of the algorithm.

Let $n \geq 2$ denote the number of players in the game, numbered from 1 to n, and let N ={1, 2,...,n} denote the set of players. A coalition, S, is defined to be a subset of N, $S \subseteq N$, and the set of all coalitions is denoted by $\mathbb{S}$. A cooperative game in N is a function u (characteristic feature of the game) that assigns to each coalition $S_i \subseteq \mathbb{S}$ a real number $u(S_i)$. In addition one has the condition $u(\emptyset) = 0$. In our case, the game will be non-negative (the values of the characteristic function are always positive), monotonous (if more players are added to the coalition the value of the expected characteristic function does not change), simple and 0-normalized (players are obliged to cooperate with each other since individually they will obtain zero benefit).

In our case, the set of players is the set of ordered sensors S and the characteristic function u is defined as:

$$u : 2^n \longrightarrow \{0, 1\} \tag{2}$$

such that, for each coalition of sensors, u = 1 or 0 if that particular coalition can vote or not respectively (see eq.(2, 3)).

$$\mathbb{S} \ni S_i \longrightarrow u(S_i) = \{0, 1\} \in \mathbb{R} \tag{3}$$

3.2 Cooperative sensor coalitions

Cooperative games are defined by the fact that players can cooperate with each other in order to achieve a mutual benefit. Once the players have agreed to cooperate among themselves, a coalition should be formed. A coalition can be formed by any number of players. In our game, a single sensor cannot determine if its temperature is correct. Therefore, sensors are forced to cooperate in order to evaluate whether the temperature of the central sensor is correct in relation to their neighbourhood. Sensors work together in coalitions in order to cooperate for a mutual benefit (i.e., to verify that their temperatures are correct and to self-correct them if this is not the case). Sensors will work together by majority rule-based voting among the coalition members in the game presented in this paper. But not all sensors can form coalitions, so it is necessary to establish limitations for the allowed coalitions that could potentially be formed regarding the respective central sensor.

The stop condition of the game iterations is

The possible coalitions that the sensors will form, will be limited by their position, that is, the coalitions can only be formed by neighbouring sensors. Let's consider the matrix of the sensors and a pair of sensors $s_{i,j}$ y $s_{k,m}$ will be in the same neighbourhood if and only if:

$$\| (i-k)^2 - (j-m)^2 \| \leq 1 \tag{4}$$

that is, if each sensor to which the game is applied, is the center of a Von Neumann neighbourhood, its neighbours are those lying within a Manhattan distance (in the matrix) equal to one. In addition, the following conditions have to be fulfilled by the allowed coalitions:

(1) Coalition sensors have to be in the same neighborhood as defined in eq. 4.
(2) Coalitions cannot be formed by a single sensor.

3.3 A characteristic function to find *cooperative* temperatures.

In the proposed game, we want the neighbourhood coalitions to democratically decide the temperature of the main sensor. To do this, they will form coalitions that will decide on the final temperature of the sensor, which will be determined by whether they can vote or not in the process. From the characteristic function defined in eq.(2), if the value is 1(0), the coalition can vote (not vote) respectively. s_i is the main sensor with its associated temperature t_{s_i}, the characteristic function is built in the following way:

(1) First, the average temperature of all the sensors is calculated:

$$T^k_{s_i} = \frac{1}{V}\sum_i^V t_{s_i} \tag{5}$$

here $T^1_{s_i}$ represents the average temperature of the sensors' neighbourhood s_i (including it) in the first iteration of the game and V is the number of neighbours in the coalition.

(2) The next step is to compute an absolute value for the temperature difference between the temperatures of each sensor and the average temperature:

$$\overline{T}^k_{s_i} = \left(\frac{1}{V}\sum_i^V \mid t_{s_i} - T^k_{s_i} \mid^2\right)^{\frac{1}{2}} \tag{6}$$

(3) Using the differences in temperature values with regards to the average temperature $\overline{T}^k_{s_i}$ (see eq.(6)) a confidence interval is created and defined as follows:

$$I^k_{s_i} = \left(T^k_{s_i} \pm t_{(V-1,\frac{\alpha}{2})}\frac{\overline{T}^k_{s_i}}{\sqrt{V}}\right) \tag{7}$$

in Eq.(7) we use the Student's-t distribution with an error of 1%.

(4) In this step we use a hypothesis test. If the temperature of the sensor lies in the interval $I^k_{s_i}$, it belongs to the voting coalition, otherwise, it is not in the voting coalition:

$$u^k(s_1, \ldots, s_n) = \begin{cases} 1 & \text{if } t_{s_i} \in I^k_{s_i} \\ 0 & \text{if } t_{s_i} \notin I^k_{s_i} \end{cases} \tag{8}$$

(5) The characteristic function will repeat this process iteratively (k is the number of the iteration) until all the sensors in that iteration belong to the voting coalition. In each iteration k, the following payoff vector of the coalition S_j (with $1 \leq j \leq n$ where n is the number of sensors in the coalition) in the step k ($PV(S^k_j)$) is available:

$$PV(S^k_j) = (u^k(s_1), \ldots, u^k(s_n)) \text{ where } \sum_i^n u^k(s_i) \leq n \tag{9}$$

The stop condition of the game iterations is $PV(S^k_j) = PV(S^{k+1}_j)$ the process end. That is, let $PV(S^k_j) = (u^k(s_1), \ldots, u^k(s_n))$ and let $PV(S^{k+1}_j) = (u^{k+1}(s_1), \ldots, u^{k+1}(s_n))$. The iteration process ends when both payoff vectors contain the same elements. This process is shown in the following equation:

$$\begin{cases} u^k(s_1) = u^{k+1}(s_1) \\ \vdots \\ u^k(s_n) = u^{k+1}(s_n) \end{cases} \tag{10}$$

Then the game can find the solution that is defined in the following subsection.

3.3.1 *Solution concept of the cooperative game.*

Once the characteristic function has been applied to all sensors involved in this step of the game a payoff vector in the step k is available (see eq. 9). Since the proposed game is a cooperative game, the solution concept is a coalition of players that we have called game equilibrium (GE). The GE of the proposed game is defined as the minimal coalition with more than half of the votes cast. Below, we summarize the conditions that must be met by the winning coalition for the game to reach the GE. Let n be the number of players involved in this step of the game. Winning coalition must satisfy the following conditions:

(1) Sum of the elements of the coalition PV must be higher than half plus 1 of the votes cast:

$$\sum_{i}^{n} u^{k}(s_i) \geq \frac{n}{2} + 1 \tag{11}$$

(2) The coalition is maximal (i.e., coalition with the greatest number of elements, different from 0, in its payoff vector $PV(S_j^k)$).

Therefore, the solution to the proposed game is the coalition that verifies both conditions from among all possible coalitions that are formed at each step k of the game.

3.3.2 *Temperatures of the winning coalition.*

Once the characteristic function decides which is the winning coalition, it is possible to calculate the temperature of the main sensor. Let $\{s_1, \ldots, s_j\}$ be the winning coalition's sensors and $\{t_{s_1}, \ldots, t_{s_j}\}$ be their associated temperature.
The temperature that the game has voted to be the main sensor's temperature (MST) is calculated as follows:

$$MST = \max_{j \in |S_{winner}|} \{j * t_{s_i}\}_{s_i \in S_{winner}} \tag{12}$$

where $|\mathbb{S}|$ is the number of elements in the winning coalition. Therefore, the MST will be the maximum temperature that has the highest relative frequency. In case of a draw, it is resolved by the Lagrange criterion.

4 EMPIRICAL RESULTS.

As highlighted throughout the paper, this proposal focuses on the application of a distributed and self-organized GT game to the temperature data collected by a WSN from an indoor surface. Our main goal is to analyze the temperature data provided by each sensor and to verify the quality of this data assuming an error of 1%. Our game, was applied to a matrix containing the temperatures collected in a time $t = t_0$ by the WSN. However here we only focus on a time t_0 (i.e. we considered a static system). One of the main benefits of our game is that it is distributed and self-organized, which is a great advantage when dealing with data obtained by a WSN.

In figure 2, the initial temperature is shown in the first image, and in the rest of the images the iterations of the game until the GE is reached. In the successive images the temperature clusters are being formed, this can be observed by the changes in the color gradient. It can also be seen that some areas with inaccurate temperatures are smoothly self-corrected on the basis of the temperatures in their environment. This is the intended process, since the game is executing its iterations depending on the environment surrounding the sensor. This makes sense because the temperature of the sensor will be similar to the average temperature of the environment in which it is located. Also, we show the evolution of the temperature on the surface. To this end, we have represented the temperature on the z axis to facilitate visualization in the form of a surface. The first image shows the temperature measured by the sensors. The game is applied iteratively to every image until it reaches the game equilibrium. Notice that the proposed game transforms the temperature data according to its environment. If we consider this as a knowledge data discovery (KDD) process, the temperature collected by the sensors would be the target data (TD), the game performs the pre-processing and data transformation to the TD simultaneously. Resulting in some transformed data, which, when the game reaches the GE are the surface temperatures in the GE. In addition, since the game is self-organized and distributed, it can be applied to the data in the ETL (extract, transform and load) process without having to go through a central node first.

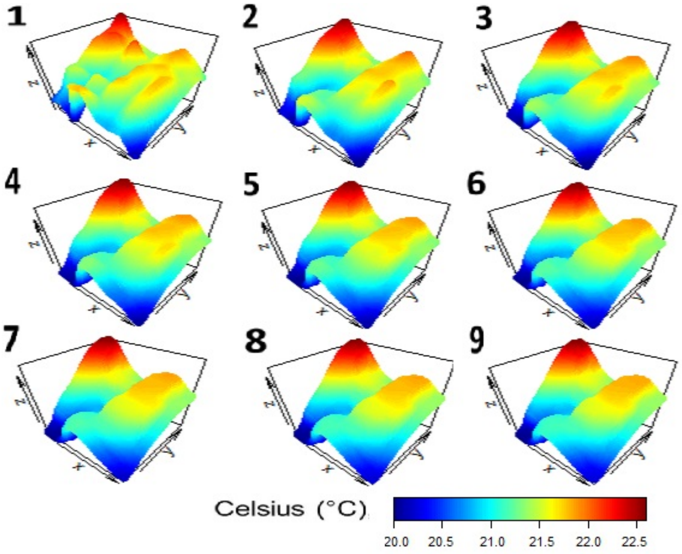

Figure 2: Evolution of surface temperatures over the different steps in the game until reaching game equilibrium.

5 CONCLUSION

This work proposes a distributed and self-organized cooperative algorithm using game theory. The algorithm has been applied to the data collected by a IoT devices. Furthermore, a blockchain-based architecture is proposed to improve data security. Novelty of this architecture is the fact that it proposes an edge computing layer where the algorithm is executed to improve data quality and false data detection.

ACKNOWLEDGMENTS

This work was supported by the Spanish Ministry, Ministerio de Economía y Competitividad and FEDER funds. Project: SURF, Intelligent System for integrated and sustainable management of urban fleets TIN2015-65515-C4-3-R.

REFERENCES

[1] Agrawal R., Gehrke J., Gunopulos D., Raghavan P., "Automatic subspace clustering of high dimensional data for data mining applications", Proc. ACM SIGMOD Int. Conf. Management of Data, pp. 94-105, (1998).

[2] (Aug. 1, 2002). Announcing the Secure Hash Standard. [Online]. Available: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[3] Antonopoulos A. M., Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc., 2014

[4] Becerra-Bonache L., Jiménez López M.D. (2014). Linguistic Models at the Crossroads of Agents, Learning and Formal Languages. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Salamanca, v. 3, n.4

[5] Biswas, S., Das, R., and Chatterjee, P. (2018). Energy-Efficient Connected Target Coverage in Multi-hop Wireless Sensor Networks. In Industry Interactive Innovations in Science, Engineering and Technology (pp. 411-421). Springer, Singapore.

[6] Casado-Vara R., Corchado J. M., Blockchain for Democratic Voting: How Blockchain Could Cast off Voter Fraud. Orient. J. Comp. Sci. and Technol;11(1). [Online]. Available from: http://www.computerscijournal.org/?p=8042

[7] Casado-Vara, R., Prieto, J., & Corchado, J. M. (2018, June). How Blockchain Could Improve Fraud Detection in Power Distribution Grid. In The 13th International Conference on Soft Computing Models in Industrial and Environmental Applications (pp. 67-76). Springer, Cham.

[8] Casado-Vara, R., González-Briones, A., Prieto, J., & Corchado, J. M. (2018, June). Smart Contract for Monitoring and Control of Logistics Activities: Pharmaceutical Utilities Case Study. In The 13th International Conference on Soft Computing Models in Industrial and Environmental Applications (pp. 509-517). Springer, Cham.

[9] Casado-Vara, R., Prieto-Castrillo, F., & Corchado, J. M. A game theory approach for cooperative control to improve data quality and false data detection in WSN. International Journal of Robust and Nonlinear Control.

[10] Cauê Cardoso R., Heitor Bordini R., (2017) A Multi-Agent Extension of a Hierarchical Task Network Planning Formalism. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Salamanca, v. 6, n. 2

[11] Chamoso, P., Rivas, A., Martín-Limorti, J. J., and Rodríguez, S. (2018). A Hash Based Image Matching Algorithm for Social Networks. In Advances in Intelligent Systems and Computing (Vol. 619, pp. 183–190).

[12] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2, 6-10.

[13] Double-Spending—Bitcoin WiKi, accessed on Mar. 15, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Double-spending

[14] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 618-623). IEEE.

[15] Eris Industries Documentation—Blockchains, accessed on Mar. 15, 2016. [Online]. Available: https://docs.erisindustries.com/explainers/ blockchains/

[16] Fan, Heng, et al. "Multi-level contextual rnns with attention model for scene labeling." IEEE Transactions on Intelligent Transportation Systems (2018).

[17] Farooq, M.O., Kunz, T.: Operating systems for wireless sensor networks: a survey. Sensors 11, 5900–5930 (2011)

[18] Greenspan G., (2015). Avoiding the Pointless Blockchain Project. [Online]. Available: http://www.multichain.com/blog/2015/11/avoidingpointless-blockchain-project/

[19] Hashcash-Bitcoin WiKi, accessed on Mar. 15, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Hashcash

[20] Huang, C.F., Tseng, Y.C.: A survey of solutions to the coverage problems in wireless sensor networks. J. Int. Technol. 6, 1–8 (2005)

[21] Huh, S., Cho, S., & Kim, S. (2017, February). Managing IoT devices using blockchain platform. In Advanced Communication Technology (ICACT), 2017 19th International Conference on (pp. 464-467). IEEE.

[22] Jörg Bremer, Sebastian Lehnhoff. (2017) Decentralized Coalition Formation with Agent-based Combinatorial Heuristics. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Salamanca, v. 6, n. 3

[23] Kupriyanovsky, Yulia, et al. "Smart container, smart port, BIM, Internet Things and blockchain in the digital system of world trade." International Journal of Open Information Technologies 6.3 (2018): 49-94.

[24] Kwame-Lante Wright, Martin Espinoza, Uday Chadha, Bhaskar Krishnamachari, SmartEdge: A Smart Contract for Edge Computing, BIoT 2018: The 1st International Workshop on Blockchain for the Internet of Things, held in conjunction with IEEE Blockchain, Halifax, Canada, 2018.

[25] Moinet, Axel, Benoît Darties, and Jean-Luc Baril. "Blockchain based trust & authentication for decentralized sensor networks." arXiv preprint arXiv:1706.01730 (2017).

[26] Nakamoto S., (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[27] Pan, J., & Yang, Z. (2018, March). Cybersecurity Challenges and Opportunities in the New Edge Computing+ IoT World. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (pp. 29-32). ACM.

[28] Prieto Tejedor, Javier; Chamoso Santos, Pablo; de la Prieta Pintado, Fernando; Corchado Rodríguez, Juan M. (September 2017). A generalized framework for wireless localization in gerontechnology. 17th IEEE International Conference on Ubiquitous Wireless Broadband ICUWB'2017. . IEEE.

[29] Rodríguez Marin P.A., Duque N., Ovalle D., (2015). Multi-agent system for Knowledge-based recommendation of Learning Objects. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, Salamanca, v. 4, n.1

[30] Rodríguez S., De Paz J.F., Villarrubia G., Zato C., Bajo J., Corchado , Multi-agent information fusion system to manage data from a WSN in a residential home. Information Fusion 23, 43-57 (2015).

[31] Rodríguez S., Zato C., Corchado J.M., Li T.,Fusion system based on multi-agent systems to merge data from WSN. Information Fusion (FUSION), 2014 17th International Conference on, 1-8 (2014)

[32] Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. IEEE Access, 6, 115-124.

[33] Sobral JVV., Rodrigues JJPC., Saleem K., de Paz J.F., Corchado J.M., A composite routing metric for wireless sensor networks in AAL-IoT, Wireless and Mobile Networking Conference (WMNC), 2016 9th IFIP, 168-173 (2016)

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

[35] Walker, M. A., Dubey, A., Laszka, A., & Schmidt, D. C. (2017, December). PlaTIBART: a platform for transactive IoT blockchain applications with repeatable testing. In Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things (pp. 17-22). ACM.

Received September 2018; revised September 2018; accepted September 2018