Authors’ Response to the Reviewers

Journal: Sensors
Manuscript ID: sensors-486217
Type: Article
Special Issue: Selected Papers from the 5th International Electronic Conference on Sensors and Applications
Title: Towards An Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-based System for Inventory and Traceability Applications in Big Data-driven Supply Chain Management
Authors: Tiago M. Fernández-Caramés *, Oscar Blanco-Novoa, Iván Froiz-Míguez, Paula Fraga-Lamas *

The authors would like to thank the reviewer for his/her valuable comments, which have certainly helped us to improve the manuscript. Please find below our detailed responses to the comments. In order to ease the labour of the reviewers we have colored in red the major differences with the previous version of the article.

I. RESPONSE TO REVIEWER NO. 1

The manuscript presents a UAV-based system equipped with several sensors and a UHF RFID reader capable of improving the performances and the traceability levels of traditional industry inventory systems as well as of automating specific tasks. The entire system exploits a blockchain approach based on a distributed ledger in order to ensure data trustworthiness and validation, too.

POSITIVE ASPECTS

- The combination of UAVs, RFID-based approaches and DLTs (i.e., Blockchain) is worth of investigation and very interesting

IMPROVABLE ASPECTS

(1)L25: I would suggest to use "paradigms and technological enablers" instead of "technologies"

Thank you for the suggestion. We corrected the sentence (now in line 28) as suggested.

(2)L161-164: I disagree with the assertion "RFID evolved towards NFC" as these two technologies coexist and it should be more properly to differentiate between far-field and near-field communication (where the former group encompasses UHF RFID systems and the latter category coincides to NFC).
We certainly agree with the reviewer observation. As a consequence, we rewrote the sentence (now in lines 167-169 so as to indicate that NFC is another technology for inventory applications that require short-distance readings.

(3)L204: reference 73 seems to me misplaced, as it should not be placed as the second reference in the big data section

Thank you for pointing such a mistake out. We have reordered the references to correct it.

(4)Page 6, Table 1: I strongly suggest the authors to modify the table as it follows:
- split column "Power/Main Features" into two columns: "Power type" and "Main Features"
- add one additional column named "Main Limitations"
- specify (for instance as a table footnote) that "Max range" values refer to optimal conditions
- max ranges proposed for BLE5 and NB-IoT are definitely over-estimated

Thank you for the suggestions. We modified Table 1 accordingly:

● We split Power/Main Features into two different columns.
● We added a new column “Main Limitations”
● We indicated in the column heading that the maximum range is related to optimal conditions.
● Regarding the Bluetooth 5 range, the official Bluetooth webpage (https://www.bluetooth.com/specifications/%20bluetooth-core-specification/bluetooth5) states that a 4x range is achieved respect to the previous Bluetooth release. We actually tested Bluetooth 5 in real environments (the results are yet to be published in another paper) and found that it is true: we were able to get (with Nordic transceivers) the RSSI from a receiver that was roughly 400 meters away, although it was not tested the maximum data rate at such a distance.
● Similarly, regarding the NB-IoT range, we used as a reference the following paper:

It is worth noting that some manufacturers plan to extend the range to 100 Km (https://www.zdnet.com/article/telstra-and-ericsson-expand-nb-iot-range-out-to-100km/), but we indicate in the table the most conservative figure of 35 Km.

(5)L247: Blockchain approaches are not the only way to achieve decentralized applications: microservices-based architectures can achieve the same purpose

We do agree with the reviewer. We rephrased the sentence (now in lines 270-290) so as to say that blockchain is one of the technologies that may allow for creating decentralized applications.

(6)Figure 4: definitely too big: please shrink it a little

Corrected.
NEGATIVE ASPECTS

(7) The main concern I have is related to the usage of the blockchain approach: since several other applications for managing huge data streams generated by RFID-based supply management activities are normally used nowadays (such as capturing applications based on complex events processors or even IoT-oriented cloud-based services from the most common public cloud providers), the authors should point out very clearly why their approach should be preferred to other, already existing, solutions. Moreover, the Ethereum testnet scenario is briefly described at the end of Section 4 while more detailed explanations would be advisable.

We agree with the reviewer on the fact that the advantages of the application of blockchain respect to other inventory solutions were not described clearly enough. To clarify this issue, the new version of the manuscript emphasizes in Section 3 (lines 270-290 and lines 305-313) the mentioned advantages.

In addition, we agree on the need for clarifying the Ethereum testnet scenario. Specifically, two different testnets were tested: Rinkeby and Ropsten.

- Rinkeby is a Proof-of-Authority (PoA) testnet created by the Ethereum team that makes use of the Clique PoA consensus protocol, where authorized signers are responsible for minting the blocks. In such a network blocks are created every 15 seconds and Ether cannot be mined (it is requested through a faucet).

- Ropsten is a Proof-of-Work (PoW) Ethereum testnet where Ether can be either mined or requested from a faucet. Ropsten's blocks are usually minted in less than 30 seconds and, although the testnet reproduces with more fidelity than Rinkeby Ethereum's mainnet production environment, it is prone to Denial-of-Service (DoS) attacks (e.g., by increasing the block gas limit while sending large transactions through the network), which makes synchronization slow and makes clients consume a lot of disk space.

These clarification have been added to the end of Section 4.2 (lines 383-396).

(8) Second, the authors claimed in the abstract that a distributed ledger is used "to store certain inventory data collected by UAVs, validate them, ensure their trustworthiness and make them available to the interested parties". Although these usages are compatible with the proposed enabling technology, very few details are provided throughout the text. More specifically, the authors should clarify:

1) what data typologies are amenable to be managed in this way and why this approach can be considered as a better solution if compared to current alternatives for those data typologies
2) what blockchain-mediated data validation steps have been performed
3) what data trustworthiness assessments have been made

Corrected. The new version of the manuscript, in Section 4.3 (lines 400-439), details how the inventory information is processed by the proposed architecture, while Figure 5 illustrates how inventory data is stored on the decentralized database and on Ethereum.

Regarding the specific reviewer questions to be clarified:
(1) The data types to be managed by the proposed storage and traceability solution are the same as in other traditional inventory solutions: sets of unique alphanumeric identifiers (UIDs). Thus, item UID association and information processing (e.g., to determine the number of items available of one specific type) need to be performed by an additional software layer that may be implemented through a CPS (as it is shown in Figure 2). This issue has been clarified in the last paragraph of Section 3 (in lines 305-313).

(2) The data validation steps are detailed in Section 4.3, in lines 423-429 and is illustrated in Figure 6. The validation process can be summarized as follows:

   a) When an entity wants to validate that the data stored in the decentralized database (OrbitDB) have not altered, it is performed a Get request to the corresponding Ethereum's smart contract.
   b) Such a request returns the inventory information stored on the blockchain and its hash.
   c) Then, the validation entity can compare the data stored by OrbitDB and the blockchain, and determine whether they have been modified.

(3) Data trustworthiness is enabled by four different mechanisms:

   a) Information integrity can be verified by checking its hash. In addition, Ethereum and OrbitDB act as timestamping services, so it can be easily verified when the data were inserted.
   b) Since the data stored on the blockchain cannot be tampered without leaving a trace, the authenticity of the inventory information stored on OrbitDB can be easily checked.
   c) Every user transaction within OrbitDB is protected by asymmetric cryptography mechanisms that make use of a public and a private key.
   d) Similarly, the data that is exchanged with Ethereum are managed by Infura, which protects them through an API key and a secret key.

Since this information is relevant for the reader, we have added it to the end of Section 4.3 (in lines 430-439).

(9)- Another negative aspect, specifically related to the management of the UAV configuration setup, pertains to the positioning of the reader's antennas on board: the authors should mention explicitly whether any consideration has been made in terms of potential disturbing effects induced by the UAV's propellers on the reader's antenna performances.

Although we consider really interesting the evaluation of the influence of the drone propellers on the RFID communications performance, we will carry it out in future analyses, since we consider that the aim of the current paper is to validate empirically the feasibility of the proposed architecture.

Nonetheless, since we do believe that the mentioned issue is actually relevant, we modified the paper (in Section 4.2, lines 344-347) to indicate that:

   ● The reader antennas were placed as far as possible from the hexacopter propellers, which was actually not indicated in the previous version of the manuscript.

   ● The location of the antennas may be further optimized.
Moreover, the considerations provided on SSI levels and their potential capability to help locating tags if an indoor GPS is available are too simplistic: several additional aspects (and issues) should be considered before claiming that the availability of SSIs can help to locate tags effectively (mutual effects between tags and surrounding materials, hostile EM environments, etc.)

We absolutely agree with the reviewer. The new version of the manuscript now indicates in Section 5.3 (in lines 497-504) that accurate positioning needs to consider multiple factors like the reflections, diffraction and refraction caused by surrounding materials, the presence of hostile electromagnetic sources, certain features of the scenario (e.g., presence of metals, water, exposure to liquids, acids, salinity, fuel or other corrosive substances, tolerance to high temperatures) or the actual reading distance, among others.

Therefore, starting from such considerations, I would suggest the authors to address these issues in a revised version of their manuscript.