Blockchain-based IoT Platform for Autonomous Drone Operations Management

Samir Dawaliby, Arezki Aberkane, Abbas Bradai

Blockchain-based IoT Platform for Autonomous Drone Operations Management

SAMIR DAWALIBY, Audensiel R&D, France
AREZKI ABERKANE, Audensiel R&D, France
ABBAS BRADAI, XLIM Laboratory, France

The growing number of unmanned aerial vehicles (UAVs), typically referred to as drones, poses new challenges on how to manage their operations in various internet of things (IoT) use cases such as surveillance and monitoring, weather prediction, agriculture, etc. The latter includes a massive number of devices that sometimes produce invalid messages due to lack of energy or system shutdown and needs to be autonomously monitored with drones in rural areas. In this paper, we develop a blockchain-based platform for managing drone IoT operations while maintaining trust and security. The test-bed consists of IoT devices, a drone and blockchain-enabled gateways through which drones are controlled to replace malfunctioning devices. The latter are detected using Z-score observation algorithm which launches a smart contract and sends the drone with clear operation order. The results obtained in realistic agriculture use case highlight the utility of our proposition in decreasing signaling and operation time, improving the percentage of successful maintenance operations and providing trust and security when managing drones in an autonomous manner.

Additional Key Words and Phrases: Unmanned aerial vehicles, Internet of things, Drone operations, Blockchain, Decentralized management

ACM Reference Format:
Samir Dawaliby, Arezki Aberkane, and Abbas Bradai. 2020. Blockchain-based IoT Platform for Autonomous Drone Operations Management. In *DroneCom'20: ACM MobiCom, September 25, 2020, London, UK*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Drones are autonomous flying robots that represent nowadays an integral part of the internet of things (IoT) ecosystem. The success behind enabling drones to support IoT communications is linked first of all to the success that mobile networks brought to IoT which has undergone an immense development. This success is also due to innovations in terms of image processing, huge capacities of data centers and the development of prediction algorithms to makr efficient and autonomous decisions. All these technologies integrated in drones-supported IoT networks enabled significant advances in moving towards a global connected infrastructure where IoT devices cooperate and share information using various wireless technologies (WiFi, LoRa, Sigfox, ZigBee, etc.). Drones fly to improve life experience with many applications such as agriculture and farming, rescue operations, pipeline inspections, video capturing and filming, delivering goods and medical supplies [4]. However, due to their increasing popularity, new challenges arised in terms of controlling drone flight places, reducing collisions and protecting UAVs from cyber attacks [13]. Legacy IoT architectures have many advantages in monitoring IoT networks, especially with the use of a broker entity with the cloud server that facilitates

Manuscript submitted to ACM

the sharing of drones usage between different service providers [1]. However, when moving towards decentralization, bids can be managed autonomously by replacing the broker with a blockchain [2]. The latter appeared as a revolutionary technology that mitigate these challenges and provide the desired level of transparency, trust, security and privacy [14].

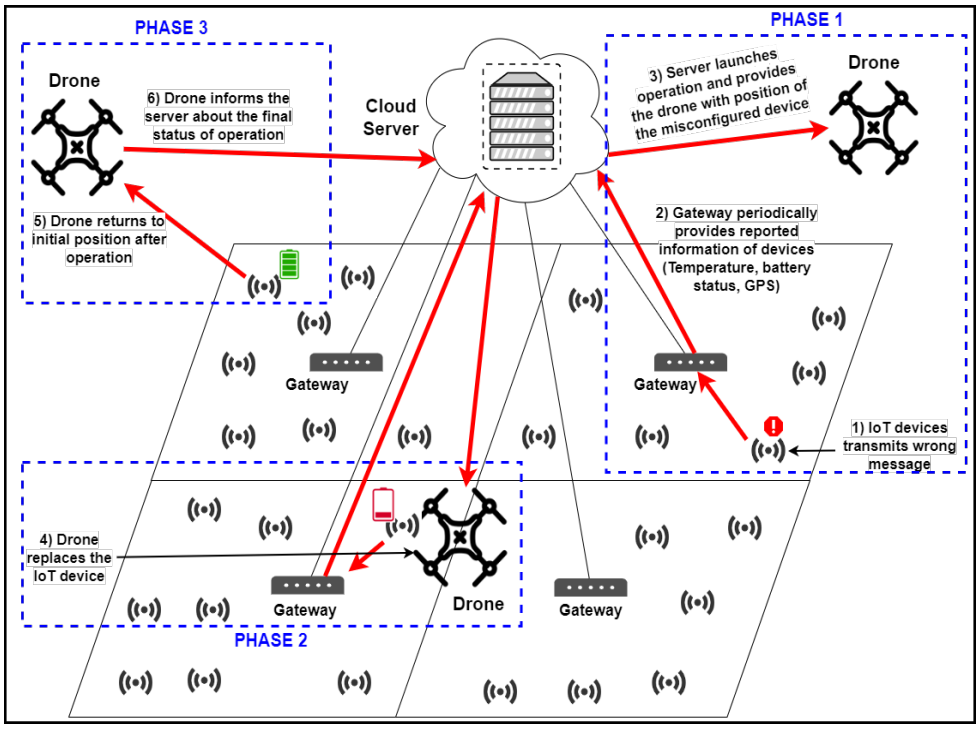


Fig. 1. Centralized architecture for managing drone operations

Multiple works are reviewed that focus on drones deployment strategies and blockchain integration in various IoT use cases [15]. One application is to control drone traffic based on geofencing [8] where virtual boundaries are created to partition the space and coordinate drone flights in a decentralized manner using blockchain. Moreover, blockchain-based solutions provide trust between UAVs and ground control stations [5]. Privacy and security are also improved when exchanging information between drones and ground control stations using blockchain [16]. It's a distributed, immutable, secure and encrypted ledger consulted by drones to receive operation orders and validate any transactions regarding flights and maintenance operations. Blockchain integration in drones network proved to be very efficient for data acquisition [11] where data are gathered from IoT devices using drones acting as relay nodes. Furthermore, one important feature for integrating blockchain in IoT is autonomy using smart contracts. The latter are self-sufficient programs stored in a decentralized manner and executed autonomously when certain conditions of a business process are met [9]. As the number of IoT devices rapidly grows, drones usage becomes more needed to operate and maintain nonfunctional IoT devices specially in rural areas where human intervention is expensive in terms of operation time and maintenance cost [12]. Hence, to cope with drones spatiotemporal limitations (speed limit, flight range, etc.), and to reduce the number of asynchronous operations, blockchain is adopted because it brings the

ability to move towards autonomous decentralized operations management while maintaining trust and security in drones networks.

Motivated by latest research directions [4] that highlight the need of a blockchain-based platform for drones management, we develop in this article a testbed that autonomously manages maintenance operations in IoT network and have not been yet introduced to the research community. To evaluate our platform, we consider a realistic agriculture use case where drone operations are autonomously managed starting from detecting erroneous information to controlling take-off, maintenance and landing phases. We develop a complete system that starts by analyzing data collected by sensors. The gateway detects next failures and malfunctioned devices using Z-score observation method that is shown to be very efficient in detecting erroneous messages [6]. The latter compares an information to the mean of data captured from neighbour IoT devices and evaluates how meaningful the measured data is based on specific thresholds configuration. Local gateways periodically store data on the cloud server.

Upon detection of an error, a smart contract [7] is dynamically executed that launches maintenance operation and transmits the required information to the nearby drone. The drone is able to recover the location of the defective sensor, plan the trajectory, position itself near the sensor and finally solve the problem by replacing the malfunctioned IoT device. The remainder of this paper is organized as follows. We devote Section II for describing drone operations management in IoT. In Section III, the proposed blockchain-based platform is introduced as well as a Z-score algorithm integrated into a smart contract to dynamically detect erroneous information and launch drones maintenance operations. Performance results carried out through realistic agriculture scenario are discussed in Section IV. Finally, Section V concludes the paper and presents our future work.

2 MANAGING DRONE OPERATIONS

Drones network control in legacy IoT architectures is generally centralized where IoT devices upload data to the cloud through nearby gateways. Here, IoT gateways only act as relay nodes that forwards data to the cloud which at its turn stores them on centralized servers. In this section, maintenance drone operations in legacy IoT networks, illustrated in **Fig. 1**, cross in rural areas three phases described below:

2.1 Detection of malfunctioned device

A failure of one or more IoT devices highly occur in wireless sensor network due to the rapid increase in the number of IoT devices deployed in rural areas. IoT devices fail to deliver valid messages due to internal factors such as configuration errors or lack of battery power. Physical damage that may happen to IoT boards may stop the device from uploading and reporting information due to external factors in extreme climatic conditions. Malfunctioned IoT devices should be rapidly detected in the monitored area. Therefore, the first phase of any monitoring operation is to detect erroneous values. The IoT device periodically reports the temperature, its geographical position and its battery life status to the nearby gateway before being forwarded to the centralized cloud server. This diversity of data may cause significant overhead to the blockchain network. This challenge is out of the scope of this paper but have been taken into consideration by other research works with solutions like data aggregation [10] transmitted by IoT devices, packets filtering [3] or block compression [17].

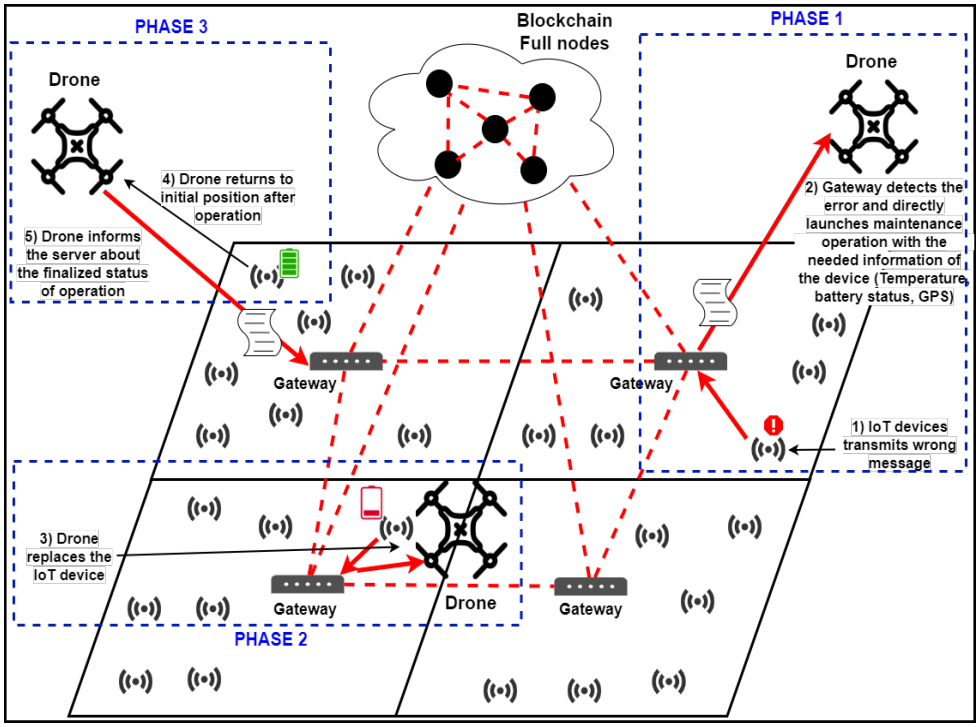


Fig. 2. Decentralized Blockchain-based architecture for managing drone operations

In the legacy architecture, the server compares each data value uploaded by a device to the other values received by its neighboring devices and detects the error using Z-score observation algorithm. the latter is a numerical measurement in terms of standard deviations from the mean and defines the captured value's relationship of an IoT device to the mean of a group of values of its neighbours. Based on this measurement, the server will be able to evaluate the reliability of the received packet. Upon detection of a malfunctioned device (erroneous information transmission or lack of battery power), the server checks and selects one of the available and closest drones to the incidence then launches maintenance operation by providing geographical position of the malfunctioned device to the drone.

2.2 Pre-maintenance operation

This section summarizes the pre-maintenance phase of any operations. Drones are initially IP-supported devices, connected to the centralized server and configured in stand-by mode. Upon receipt of maintenance order, the drone checks maintenance operation type and the geographical position of the device. Using its global positioning system (GPS), the drone flies and approaches near the position of the faulty sensor. However, GPS do not deliver a precise value. This forces the drone to activate the on-board camera, drop the arm and goes into searching mode to relocate the desired device. Once the sensor detected, the drone calculates the distance between the camera and the sensor, tries to minimize this distance to a value equal or lower than 1 cm, closes the clamp and replaces the malfunctioned device.

2.3 Post-maintenance operation

Drone returns to initial position after operation and announces the end of the maintenance to the server. The latter updates geographical position of the drone and register the new identity of the IoT device as well as its position and battery life status.

3 THE BLOCKCHAIN-BASED PLATFORM

Drones bring numerous advantages in controlling areas that are difficult to reach. However, despite these advantages, identity validation of a drone assigned a maintenance mission is not straightforward and gets even more complicated with the increasing number of drones and IoT devices. This motivates the need for autonomy and decentralization using Ethereum blockchain technology [18] to transform the centralized IoT architecture into a decentralized network that provides security, trust and autonomy.

The key components in the proposed blockchain-based architecture illustrated in **Fig. 2** are: 1) *The cloud server* acting as *blockchain full-nodes*. The latter are *miners* and electrically-powered devices with high computational capacities responsible on packing transactions into blocks and validating new blocks after running Proof of Work (PoW) consensus algorithm. 2) *The IoT gateway* acting as *blockchain light-nodes* and stores smart contracts programmed to dynamically detect erroneous messages or lack of battery power and launch maintenance operations. 3) *The Drones* are considered as flying devices with the ability of recharging their batteries when being at the central base station. Drones are registered and connected to the blockchain and interacts with the IoT gateways using smart contracts. 4) *IoT devices* are mainly battery-powered sensors that periodically transmit data to the cloud through IoT gateways.

The difference within this architecture is that erroneous messages instead of being detected at the server level, they are detected by the smart contracts installed on IoT gateways. Each GW is capable of detecting malfunctioned devices, updating battery, storing data on blockchain and dynamically launching the drone to execute maintenance operation. An additional advantage for integrating blockchain in drones-supported IoT network is the ability of dynamically managing operations without the need for human interventions. This is done by managing IoT devices and drones using Ethereum blockchain and smart contracts. To maintain security in the platform, public keys are added on all contracts as well as signatures. This prevent any malicious attack from manipulating the storage of smart contracts. The latter are programmed with solidity and explained in details as follows:

3.1 Tracking contract

On this smart contract, IoT devices periodically reports temperature values measured in the field and send them to the gateways acting as blockchain light-nodes. An Ethereum account is created for each IoT device, the latter sends three input values: the measured temperature value, the public key and the signature to be able to directly detects the identity of the sender device.

3.2 Operation Policy contract

On this smart contract, operation policies are written in details to be able to control when to execute, modify or abort operations. In this context, maximum and minimum threshold values are set in an empirical manner in order to eliminate wrong values coming from faulty sensors. The temperature of sensors placed in an agriculture environment cannot

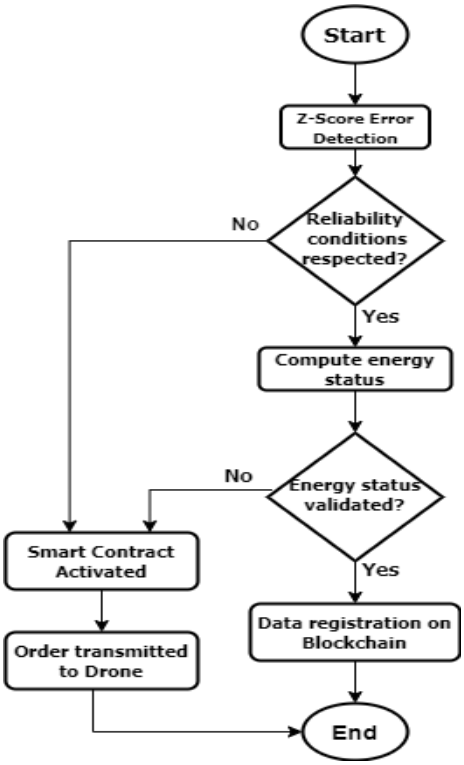


Fig. 3. Smart Contract Activation Algorithm

drop below 20 °C or exceed 70 °C. Moreover, we define 10% of battery life thresholds that indicates the need for IoT device replacement. Once contract conditions are met, gateways execute flight operation to drones by providing exact geographical position of the malfunctioned IoT device.

3.3 Drone management contract

This smart contract controls drones movement during take-off and landing. It also controls device replacement phase when it first enters area scanning mode. Based on the distance between the device and the drone, it opens drone's arm and replaces the device. Once the maintenance operation ends, drones inform the IoT gateway about new device installation and register its identity and public key. Interactions between smart contracts are summarized in **Fig. 3**. The program starts with data cleaning followed by a dynamic observation method that detects when temperature value seems suspicious for an IoT device compared to its neighbours. We chose to implement Z-score method that have shown to be more efficient in detecting errors and frauds [6]. Based on the output of Z-score algorithm, smart contract defines if the value is erroneous or not then it moves to check battery life status and validate the respect of the programmed threshold conditions. If any of the conditions were not respected, operation contract is dynamically activated and executed on the drone to launch the maintenance and replace the malfunctioned device. After the completion of maintenance operation, the drone returns to the base station and updates energy and gateway positioning. The latter finally places the transaction to the miners for validation.

4 SIMULATIONS AND RESULTS

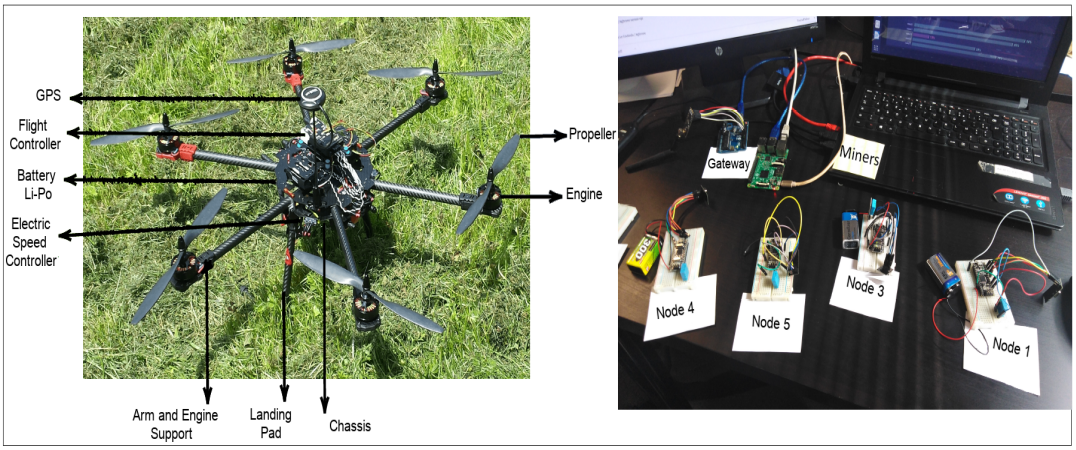


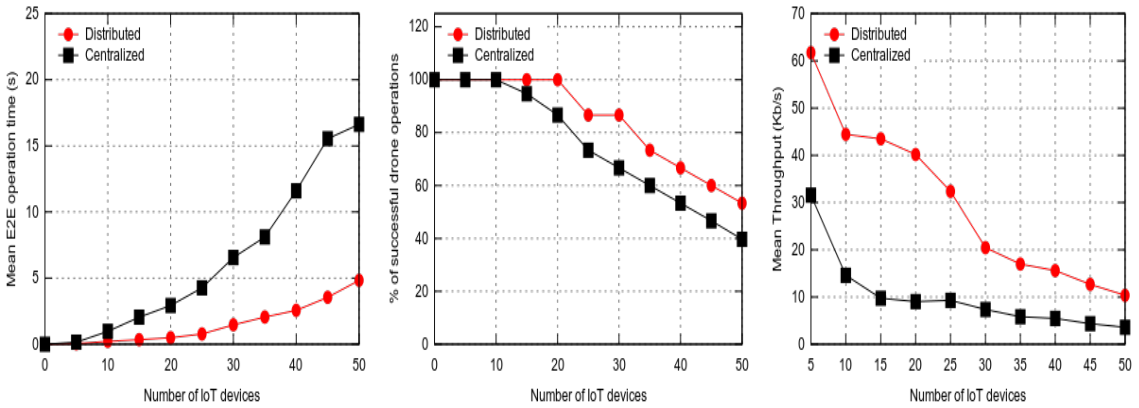
Fig. 4. Experiment testbed: a) Hexacopter Drone; b) Blockchain-based platform

To evaluate the proposed blockchain-based platform for drones network, a realistic testbed is applied in a realistic agriculture use case. Compared with traditional systems supported with satellites, drones usage in smart farming and agriculture is very effective because it gives to the farmer a bird's eye view of the field. In particular, drones usage enables a global survey of the field with an overall view of the monitored area and optimizes farming time instead of wasting time searching and moving from a device to another. The farmer has to be positioned in an area close to the field in order to receive precise evaluations measurements. However, in rural areas, the task becomes more complicated to manage specially when IoT devices are placed in areas where it's difficult for a farmer to reach and replace a malfunctioned IoT device. This motivates the main advantage of this platform that will remove the need for farmer's intervention and dynamically detects errors, launches the operation and replaces the device without farmer's intervention.

The proof of concept implementation is illustrated in **Fig. 4**. We use an hexacopter drone occupied with 6 motors chosen based on our experiments to generate a power allowing the carrying of heavy loads for a long time, which is essential since the drone will have to carry loads up to 1.5 kg in addition to its own weight (1.3 kg). When the device approaches from the IoT device, the drone must be stable and precise, the 6 motors ensure better reaction to different climatic disturbances approaching the target. During the flight, taking account of the size and the weight, the biggest danger would is having a drone falling that could damage the material with high landing speed. With this structure, the loss of an engine automatically stops its opposite pair in order to maintain balance. The last criteria for the drone is the size of its layout. The drone is expected to IoT sensors and actuators. Hence, the platform should be large enough to be able to carry the device easily and efficiently. Hexacopters are generally considered as large drones with sufficient layout size capable of doing the task assigned for this prototype.

The networking part of the proposed platform, illustrated in **Fig. 4b**, consists of *Crossbow Mica 2* battery-powered IoT devices embedded with GPS and configured to periodically transmit data to the IoT gateway. The latter is built with

a Raspberry Pi (RPi) 3 with *16 GB* microSD connected to GPS and running Go-lang-based Ethereum *Geth* client to the private Ethereum network using programmed smart contracts. The gateway periodically receives data and forwards the packets to the miners to validate new blocks in the private network. In this context, we used two laptops with *3.40 GHz Intel Core^{TM} i7-3770 CPU* and *16 GB RAM*. On each machine, a miner account is initialized with the same genesis block, and acts as full node on the private Ethereum blockchain.



(a) Mean E2E operation time (b) Percentage of successfull drone operations (c) Mean throughput

Fig. 5. Performance Study between centralized and blockchain-supported decentralized achitectures

We realize the experiment in a realistic agriculture field where IoT devices are randomly uploading small packet data to their nearby IoT gateways in a periodic manner. We fix two IoT gateways and we constantly increase the number of devices till it reaches 50 devices in the field. IoT devices are randomly positioned over a field of 1.5 KM radius following to a uniform random distribution. The goal is to develop more the study over a larger area with also a higher number of IoT devices. In the following performance study illustrated in **Fig. 5**, the *"centralized"* network architecture is compared to the *"distributed"* blockchain-supported drones network. We compare both architectures and evaluate the performance of the proposed platform in terms of operation time, percentage of successful operations and throughput.

4.1 Mean End-to-End Operations Time

The impact of enabling decentralization is clearly highlighted in **Fig. 5a**. With both architecture, the mean End-to-End (E2E) operation delay increased due to the increasing number of IoT devices. However, one can directly note the advantage of the *"distributed"* blockchain-based in reducing the overall operation time. Instead of sending all signaling and placing intelligence on the cloud server as it happens with the *"centralized"* architecture, drones directly interacts with local IoT gateways and dynamically launches maintenance operation saving lots of signaling and operation time.

4.2 Percentage of Successful Operations

Further improvement is achieved in the percentage of successful operations illustrated in **Fig. 5b**. Due to the increasing result achieved in the mean end-to-end operation time, drones were able to achieve more maintenance operations

knowing that their number is limited. The task was easier to achieve with the *"distributed"* blockchain architecture because decentralization gave more room for maintenance operation to be achieved in the most efficient way possible.

4.3 Mean Throughput

In **Fig. 5c**, increasing the number of IoT devices decreases throughput to values in the order of few Kb/s. This returns to the increasing congestion in the IoT network. However, the utility of the proposition is highlighted in the decreasing behavior of mean throughput when we compare the *"centralized"* to the *"distributed"* architecture. The former decreases faster due to the higher congestion and end-to-end delay whereas the latter had better performance due to the direct interaction between blockchain nodes.

5 CONCLUSION AND FUTURE WORK

UAVs proved to be very useful in monitoring IoT areas where it's hard for humans to arrive and repair faulty sensors. In this article, we propose a blockchain-based platform for UAVs management through which drones are controlled to replace malfunctioning devices. We provide a global overview of the blockchain-based IoT platform as well as the smart contracts programmed for controlling drone flights and maintenance tasks. We compare the performance of the decentralized blockchain-based platform to the traditional centralized architecture and we highlight the efficiency of this proposition in reducing the overall operation time and the percentage of maintenance operation successfully realized. In the future, we will work towards improving our platform to support a higher number of IoT devices and to work on improving its coverage with better placement strategies. Moreover, we believe that current performance can still be improved by using prediction algorithm instead Z-score that is currently used to detect faulty sensors. This should improve communications reliability and reduce further end-to-end operation time. Maintenance operations and devices replacement will be dynamically operated with smart contracts and adapted faster to failures that may happen in agriculture or any other use cases suffering from similar management challenges.

REFERENCES

[1] Jacques Bou Abdo, Jacques Demerjian, Hakima Chaouchi, Kabalan Barbar, and Guy Pujolle. 2013. Broker-based cross-cloud federation manager. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*. IEEE, 244–251.

[2] Jacques Bou Abdo and Sherali Zeadally. 2020. Multi-Utility Market: Framework for a Blockchain Exchange Platform for Sustainable Development. arXiv:2007.07096 [cs.CY]

[3] Eman M Abou-Nassar, Abdullah M Iliyasu, Passent M El-Kafrawy, Oh-Young Song, Ali Kashif Bashir, and Ahmed A Abd El-Latif. 2020. DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access* 8 (2020), 111223–111238.

[4] Tejasvi Alladi, Vinay Chamola, Nishad Sahu, and Mohsen Guizani. 2020. Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications* (2020), 100249.

[5] Ezedin Barka, Chaker Abdelaziz Kerrache, Hadjer Benkraouda, Khaled Shuaib, Farhan Ahmad, and Fatih Kurugollu. 2019. Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure. *Transactions on Emerging Telecommunications Technologies* (2019), e3706.

[6] Ganga Bhavani and Christian Tabi Amponsah. 2017. M-Score and Z-Score for detection of accounting fraud. *Accountancy Business and the Public Interest* (2017), 68–86.

[7] Vitalik Buterin et al. 2014. A next-generation smart contract and decentralized application platform. *white paper* 3, 37 (2014).

[8] Tamraparni Dasu, Yaron Kanza, and Divesh Srivastava. 2018. Geofences in the sky: herding drones with blockchains and 5G. In *Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. 73–76.

[9] Tiago M Fernández-Caramés, Oscar Blanco-Novoa, Iván Froiz-Míguez, and Paula Fraga-Lamas. 2019. 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. *Sensors* 19, 10 (2019), 2394.

[10] Zhitao Guan, Xin Lu, Naiyu Wang, Jun Wu, Xiaojiang Du, and Mohsen Guizani. 2020. Towards secure and efficient energy trading in IIoT-enabled energy Internet: A blockchain approach. *Future Generation Computer Systems* 110 (2020), 686–695.

[11] Anik Islam and Soo Young Shin. 2019. BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things. *Journal of Communications and Networks* 21, 5 (2019), 491–502.

[12] Tara Lemmey and Stanislav Vonog. 2016. Management of drone operations and security in a pervasive computing environment. US Patent 9,292,705.

[13] Chao Lin, Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo, Alexey Vinel, and Xinyi Huang. 2018. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Communications Magazine* 56, 1 (2018), 64–69.

[14] Jun Lin, Zhiqi Shen, Chunyan Miao, and Siyuan Liu. 2017. Using blockchain to build trusted lorawan sharing server. *International Journal of Crowd Science* (2017).

[15] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito. 2018. Blockchain and iot integration: A systematic survey. *Sensors* 18, 8 (2018), 2575.

[16] Tarun Rana, Achyut Shankar, Mohd Kamran Sultan, Rizwan Patan, and Balamurugan Balusamy. 2019. An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 162–167.

[17] Ashish Sardesai, Dante J Pacella, Lachlan Maxwell, Venkata Josyula, and Mani Tadayon. 2020. Blockchain compression using summary and padding blocks. US Patent App. 16/224,966.

[18] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 2014 (2014), 1–32.