A Lightweight Reputation System for UAV Networks

Simeon Ogunbunmi[1], Mohsen Hatmai[1], Ronghua Xu[2], Yu Chen[1(✉)], Erik Blasch[3], Erika Ardiles-Cruz[3], Alexander Aved[3], and Genshe Chen[4]

[1] Binghamton University, Binghamton, NY 13902, USA
ychen@binghamton.edu
[2] Michigan Technological University, Houghton, MI 49931, USA
[3] The U.S. Air Force Research Laboratory, Rome, NY 13441, USA
[4] Intelligent Fusion Tech, Inc., Germantown, MD 20876, USA

Abstract. Unmanned Aerial Vehicles (UAVs) have become indispensable components in the modern Internet of Things (IoT) ecosystem and are increasingly popular for various applications, including delivery, transporting, inspection, and mapping. However, the reliability, security, and privacy of UAV devices are among the public's top concerns as they operate close to each other and other objects. This paper proposes a **LI**ghtweight **B**lockchain-based **RE**putation (LIBRE) system to improve the reliability and performance of a UAV network by monitoring, tracking, and selecting the most appropriate individuals to carry out tasks. In the LIBRE system, a reputation score is assigned to each newly registered UAV device with limited network access. Exclusive access is, therefore, given once the reputation is ascertained based on the behavior and the feedback given by peer nodes that have interacted with it. An algorithm was proposed to calculate the reputation score updated in the Blockchain to provide fairness, immutability, and auditability. A proof-of-concept prototype of LIBRE system architecture was implemented on a private Ethereum Blockchain, and the extensive experimental study has validated the effectiveness of the LIBRE scheme.

Keywords: Unmanned Aerial Vehicles (UAVs) · Reputation System · Reliability · Lightweight · Ethereum Blockchain

1 Introduction

From 2018 to 2023, the market of Unmanned Aerial Vehicles (UAVs), which are also referred to as Drones, has grown from 69 billion dollars to 141 billion dollars

This work was partially supported by the U.S. National Science Foundation (NSF) under Grant No. 2141468, and the U.S. Air Force Research Laboratory (AFRL) Summer Faculty Fellowship Program (SFFP) via contracts FA8750-15-3-6003, FA9550-15-001, and FA9550-20-F-0005. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U. S. Air Force.

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2024
Published by Springer Nature Switzerland AG 2024. All Rights Reserved
Y. Chen et al. (Eds.): SmartSP 2023, LNICST 552, pp. 114–129, 2024.
https://doi.org/10.1007/978-3-031-51630-6_8

[13]. Because of many attractive features, drones have been widely adopted for both civilian and military applications including delivery, transporting, inspection, surveillance, and mapping [5,7,17]. In particular, data received through the UAV devices is essential and crucial for carrying out emergency operations [2]. Different from other robotic vehicles, UAVs have demonstrated higher mobility and adaptivity, which are required for tasks conducted in remote worksites, inconvenient or hazardous locations, or areas that lack communication infrastructure [29], leaving alone the capability of collecting high-quality images for complex tasks. Essentially, each UAV unit is a complex Internet of Things (IoT) system, which consists of sensors, antennae, embedded software, and a two-way communication module. The whole system functions seamlessly to ensure the Quality of Service (QoS) and the Quality of Experience (QoE) for applications like remote control and monitoring [9,27].

The proliferation of UAV applications also made UAV networks attractive targets. The past decades have witnessed variant attacks against UAV systems on confidentiality, reputation, privacy, security, and reliability [1]. Compared to regular computers, UAV systems are more vulnerable to physical and cyber threats due to their constrained computing resources and limited power supply [13]. To manage behavioral evidence and enforce authorization, an effective access control layer is required in addition to authentication [4]. During encrypted data exchange between UAV systems and unauthorized entities, sensitive and private information, such as position, payload, and flight time, is made public [11], making them highly vulnerable to attacks.

The reliability and credibility of UAV networks are of paramount importance. A reputation system aggregates the interactions among nodes and enables the establishment of profiles that reflect system-level and individual-level performance [10]. Reputation scores serve as indicators of security, privacy, and decision-making confidence, providing valuable insights into the level of trustworthiness. Since its introduction as a decentralized and transparent ledger technology with characteristics such as audibility, immutability, traceability, and transparency, Blockchain has garnered recognition as a promising solution to enhance privacy and security in data transmission [6,27]. By incorporating peer-to-peer and cryptography consensus algorithms, Blockchain has achieved transparency characteristics between different non-trusted entities [22].

This paper introduces a **LI**ghtweight **B**lockchain-based **RE**putation (LIBRE) system to enhance the reliability and performance of UAV networks. LIBRE achieves this by monitoring, tracking, and selecting the most suitable individuals for task execution. This protocol effectively eliminates malicious nodes from the UAV network, allowing the network to reach a consensus when assessing the overall system reliability [16]. The major contributions are listed below:

- A light-weight reputation system architecture is introduced with the details of its key components and functionalities;
- A reputation contract to determine malicious or harmful devices that cause attacks on the system was proposed; and
- A proof-of-concept prototype of LIBRE architecture is implemented and tested, which validated the proposed architecture.

The rest of the paper is structured as follows: Sect. 2 provides a concise overview of the background knowledge and related works on UAV networks and reputation systems. The proposed LIBRE design rationale and architecture are presented in Sect. 3, and the experimental results are reported in Sect. 4. Finally, Sect. 5 concludes the paper with a brief discussion of the ongoing efforts.

2 Background and Related Works

This section provides a brief overview of the background knowledge and related works on Blockchain networks for UAVs, and the implementation of reputation systems using different frameworks, models, and consensus protocols.

2.1 Blockchain in UAV Networks

Blockchain is based on a distributed database with a scalable list of data entries. The information block includes the timestamp, encrypted hash value, and data transaction from the preceding linked block [21]. In a blockchain network, when nodes exchange information or assets, they initiate a transaction. The source node creates a transaction file, which is broadcast to the network or specific nodes for validation. Validated transactions are grouped into blocks and added to the blockchain based on the consensus mechanism employed [20]. Numerous researchers and organizations have contributed to the creation and improvement of blockchain technology since it was first introduced with Bitcoin. Building on the outlining of the original concept, there are variant blockchain systems and versions that have been developed by diverse researchers today. Blockchain technology has tremendous potential in various fields where trust is essential between mutually dependent parties. Its applications include not just electronic cash exchange systems like Bitcoin and Litecoin [3], but also rendering and enabling secure communication amongst robotic swarm systems or even data marketplaces [26]. There is sufficient literature that covers the taxonomy on the use of blockchain for authentication in IoT networks [19] and the challenges of adopting blockchain in IoT devices alongside some of their solutions to these challenges [18].

Specifically, the integration of Blockchain technology has proven effective in mitigating various attacks in UAV systems, including Sybil attacks, Man-in-the-Middle attacks, jamming, Distributed Denial of Service (DDoS) attacks, and more [25]. Integrating blockchain enables establishing trust and ensuring data immutability and transparency within UAV systems. Several studies have highlighted the effectiveness of Blockchain in enhancing security and integrity. The Autonomous Intelligent Robot Agent (AIRA) protocol is introduced to address the limitations of a centralized system [15]. This protocol utilizes blockchain, specifically the Ethereum platform, to manage economic interactions in a multi-agent system. AIRA protocol combines smart contracts, Robot Operating System, InterPlanetary File System for data storage and Docker for virtualization. Transactions in the system involve both Ethereum tokens and custom tokens

[15]. The AIRA protocol was implemented in the Drone Employee project, where UAVs were utilized for navigation, regulatory compliance, and economic activities. The process involved service requests, smart contract creation, service acceptance by UAV agents, and approval of air corridors by agent dispatchers [15].

To address the constraints of IoT devices and support UAV-based applications to securely and autonomously receive sensor data, a decentralized platform within the air-to-ground heterogeneous network is suggested [12], which enables information storage and trading. A novel blockchain architecture is introduced that effectively addresses computation and storage overhead while maintaining privacy, security, and lightweight characteristics [12].

The significance of blockchain in the context of UAV-assisted IoT is highlighted and a data collection system is proposed in [28], which emphasizes security and energy efficiency. Blockchain is introduced as a fundamental component that enables UAVs to serve as edge data collection nodes. By leveraging blockchain technology, the UAVs facilitate long-term network access for IoT devices through regular cruises and recharging [28]. This integration of blockchain with UAV-assisted IoT showcases the importance of blockchain in creating a comprehensive framework that incorporates UAV edge computing, UAV charging, and secure data handling.

Focusing on the common security and privacy concerns in IoT, a framework is proposed that combines blockchain with IoT to address these issues effectively [30]. By integrating blockchain technology, the framework offers robust security and privacy measures, ensuring the integrity of IoT data and supporting various functionalities such as authentication and decentralized payment. Potential solutions are also presented based on blockchain and Ethereum to tackle security challenges in IoT devices [30], including data sharing, data integrity, authentication, access control, and privacy. The use of blockchain serves as a promising solution to enhance the overall security of IoT systems.

Blockchain technology plays a crucial role in addressing the issues associated with centralized solutions by introducing the UGG/IPP and LPP algorithms for dynamic encryption [21]. A decentralized architecture is proposed that leveraged hash functions to enhance storage and processing efficiency utilizing blockchain. The significance of blockchain in this context lies in its capability to provide a secure and tamper-resistant framework for storing and managing identities. The proposed architecture, with its periodic updates and calculation of real identities, showcased improved system performance, reduced processing time, and enhanced privacy protection [21].

2.2 Reputation Systems

Trust and reputation systems are critical in a variety of fields, including online platforms, social networks, and distributed systems. They provide for the evaluation of the trustworthiness and trust of entities such as users, service providers, or peers based on their previous behavior, interactions, and feedback. Researchers

have extensively researched the design, analysis, and assessment of trust and reputation systems in journal publications to improve security, minimize assaults, and improve decision-making processes.

A trust and reputation model is crucial for protecting large distributed sensor networks in IoT/CPS from malicious node attacks. Such a model fosters collaboration among distributed entities, aids in detecting untrustworthy entities, and assists in decision-making processes. After thoroughly exploring trust establishment processes and comparing various methods, a trust and reputation model called TRM-IoT is designed to promote cooperation among IoT/CPS network things based on their behaviors [8]. The model's accuracy, robustness, and efficiency are validated through extensive simulations, demonstrating its effectiveness in ensuring reliable and lightweight trust management in IoT/CPS networks [8].

Researchers also proposed solutions for trust and reputation systems based on Fog computing [23]. It utilizes Fog nodes to evaluate trust levels among IoT devices, allowing interactions only with devices that meet a predefined trust threshold. This evaluation process helps to prevent malicious devices from impacting the system and compromising the quality of service while also safeguarding against various attacks such as Bad Mouthing, On-Off, and Self Promoting attacks [23]. The paper includes simulation results demonstrating the system's behavior under these attacks. Additionally, the proposed solution is well-suited for large-scale IoT systems. A comparison with related works reveals that the proposed model outperforms previous approaches in terms of its suitability for IoT systems and security.

An event-based reputation model is introduced aimed at filtering false event messages in a multi-UAV network [14]. The proposed solution recognized two distinct roles for each event and implemented a dynamic mechanism for role development, reputation, and evaluation. The mechanism helped to determine the trustworthiness of incoming messages and prevents the spread of false event messages among UAVs in the network [14]. By employing this approach, the system can effectively mitigate the impact of false information and maintain the reliability of event communication in the multi-UAV environment.

An enhanced condensed hierarchical clustering method was proposed that utilizes user preference similarity to enhance the accuracy of recommendation trust [24]. This approach employed a cloud model-based technique to measure similarities between users and then applied a hierarchical clustering method to group users into different domains based on their similarities. This process obtained the final recommendation trust, which includes both intra-domain and extra-domain recommendation trust [24]. The overall trust in cloud services is evaluated by considering both direct trust and recommended trust. Through simulation experiments, the paper validated the accuracy and superiority of the clustering algorithm. The experimental results demonstrated that the cloud service selection method enhances transaction success rates and allows users to choose more satisfactory cloud services.

3 LIBRE: Rationale and Architecture

Aiming at assurance and reliability of UAV systems, LIBRE leverages reputation system and Blockchain technology to enhance QoS and security requirements in drone-based applications, like package delivery, smart surveillance, environment monitoring, etc. Figure 1 demonstrates the LIBRE system architecture that consists of four sub-systems: i) UAV network; ii) identity authentication; iii) reputation system; and iv) Blockchain fabric.

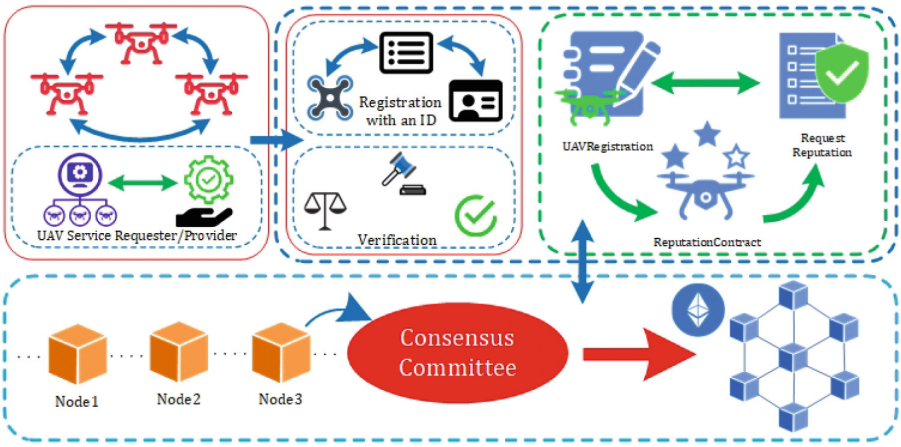

Fig. 1. LIBRE System Architecture Overview.

3.1 The UAV Network

The UAV network serves as a physical infrastructure for LIBRE system, which allows UAVs to connect, share data, and carry out specific functions to provide intelligent air mobility applications. Key components and functions are described as follows.

– *Unmanned Aerial Vehicles*: Unmanned Aerial Vehicles (UAVs) also known as drones are responsible for sensing the environment, collecting data, and communicating with ground stations. Unmanned Aerial Vehicles (UAVs) have the potential to radically improve speed, safety, and integration while completely transforming communication and transportation networks. Drones are UAVs that execute activities and services on the network. However, current events have shown how vulnerable UAVs are to attacks made feasible by faulty or malicious equipment operating within communication networks. To protect UAVs in the airspace and lessen the risk of cyber attacks, this emphasizes the urgent need for cybersecurity measures. Introducing a secure and reliable networking architecture for UAV data, blockchain is a concept that addresses this.

- *UAV Service Providers*: UAV Service Providers are nodes that provide services needed in the system and have the node registered on the network by interacting with the registration contract. They are responsible for the maintenance and operation of the UAVs, as well as the provision of flight services to users. They are used in making UAVs to perform tasks such as aerial photography, surveillance, and delivery.
- *Ground Stations*: The ground stations are the stationary points on the ground that control the UAVs. They are in charge of delivering commands to the UAVs, receiving data from them, and providing power to them. The ground stations serve as control centers for overseeing and directing drone operations for simplifying data sharing and control centers or communication hubs for managing and coordinating drone operations.

3.2 UAV Identity Authentication:

This component is in charge of ensuring the authenticity and identity verification of UAVs in the network. It employs mechanisms to validate the identification of each UAV, often through digital signatures, cryptographic keys, or other secure means. Only registered, verified, and authenticated UAVs are able to access the network and participate in its activities. This authentication mechanism assists in the prevention of unauthorized access, potential security breaches, and the involvement of malicious or untrustworthy entities.

3.3 Reputation System

The reputation system is critical to ensuring quick and secure service exchanges inside the UAV network. Because of their demonstrated track record of dependability and competency, providers with higher reputation scores are most likely to be preferred for services. By assessing and regulating the dependability and performance of UAVs, the reputation system is a fundamental component of the architecture that fosters reliability and accountability among UAV network members. Its purpose is to evaluate and maintain the reputation of the UAV service providers based on their behavior, dependability, and adherence to network rules. It tracks each UAV's activities and performance and assigns reputation ratings based on their actions and results. Provider reputation ratings may reflect factors such as performance, responsiveness, task completion, interactions, honesty, promptness in executing obligations, and adherence to safety regulations.

3.4 Blockchain

Blockchain is a decentralized network that provides a space where no one organization has total authority. This enhances the network's fault tolerance and resilience since different drones may communicate and cooperate without depending on a centralized authority. Additionally, blockchain provides trust and transparency through its transparent and immutable ledger. In a drone network, this ensures secure recording of flight data, including location, altitude,

and mission parameters. Transparency builds trust among network participants and safeguards the integrity of the collected data.

3.5 Architecture and Algorithm

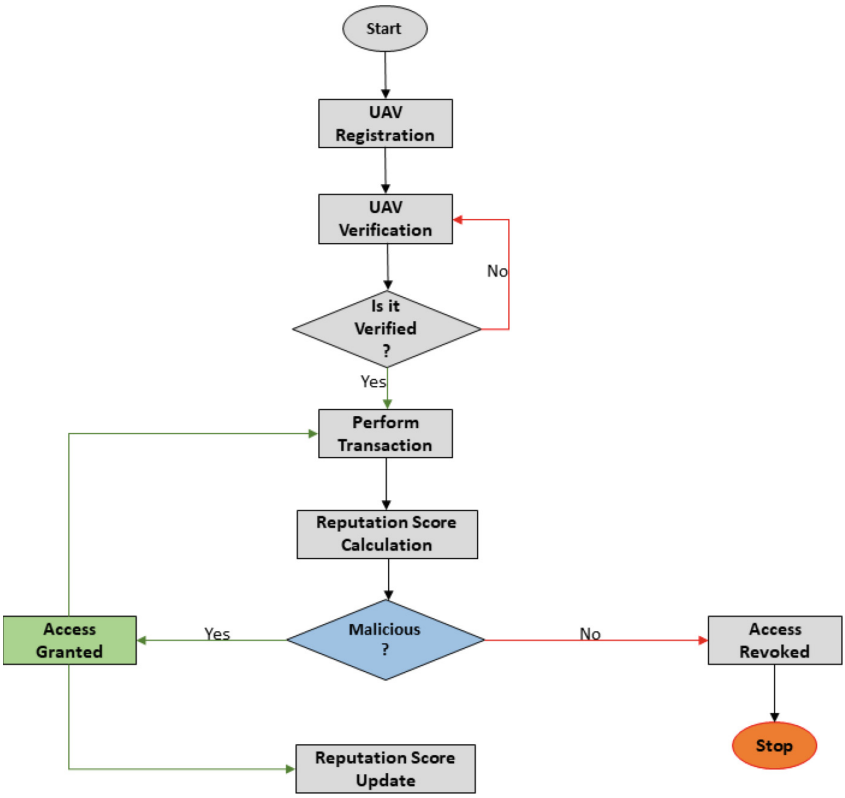

Fig. 2. The process of gaining access to a network.

To manage the registration, verification, reputation calculation, and updating of the reputation scores for service providers in UAV systems, the LIBRE system architecture was implemented. With Remix IDE using Solidity version 0.8.20, the solidity code was compiled using Remix VM (Shangbai), and the Reputation Calculation Equation (Eq. 1) was used in this design to calculate the reputation score of each device after each successful transaction made by each provider based on their weight factors, rating and the number of tasks completed. Separate smart contracts were developed to ensure separate reputation operations for the UAV providers. For service providers, the ReputationSystem contract maintains the reputation system and reputation management.

The ReputationContract contract provides a different approach to determining reputation, taking into account elements like ratings, tasks completed, and weight into consideration. Two interfaces were implemented by the smart contracts to outline the functions of each smart contract used. the IReputationSystem which was implemented by the Reputation Contracts, while the IUAVRegistration was implemented by the UAVRegistration contracts. The functions of the smart contracts used for registration, verification and reputation calculations, and updating in the design are discussed as follows:

UAVRegistration Contract: The reputation system interface (IReputationSystem) is used in the UAVRegistration contract to implement the UAV registration, and verification, and initiate the reputation score updating process. From the reputation system contract, an initial UAV's reputation score is generated. This smart contract allows the registration of the service provider with a given specific name using a string parameter representing the UAV to be registered. It is important to note that an empty name can not be accepted as a specific name needs to be given to each registered UAV. It also checks if the UAV is registered or verified by the name and the address used during registration. Once the registration and verification of the provider are completed, it sets the reputation score and the prior reputation to zero which is mapped using the name and address as the key. It returns a boolean output of the verification function to be true if the UAV device is verified and returns false if not verified. Transactions can not be done without a complete verification of the UAV device as shown in Fig. 2.

Reputation Contract: The reputation score of a device can be increased or decreased, which substantially affects the reputation, trustworthiness and the scores of the UAV devices either positively or negatively after the Prior Reputation calculation has been calculated as regarded in Eq. (1). Reviews/feedback are given after each successful transaction based on different metrics, e.g., delivery level, performance, delivery time, meeting the set rules and regulations, and reliability while we set our metrics to be timeliness and quality of delivery as we assume that the quality of the service deliver is assumed to be highly effective than the timeliness of the delivery, thereby, the weight factor of quality of delivery and timeliness of delivery is assumed to be 6 and 4 respectively. The feedback given is based on the rating and weight factors and it is calculated and updated using the reputation contract. The Reputation Score of each device is therefore calculated using the equation in Eq. (1) by finding the summation of all the prior reputation scores as regarded in Eq. (1) and then finding the division of this sum with the total amount of task it has completed.

$$PR = \frac{(WQ * RQ) + (WT * RT)}{10} \tag{1}$$

Algorithm 1. UAVRegistration

```
registered_names ← {}
verified_uavs ← {}
procedure registerUAV(name)
    if name ≠ None and name ∉ registered_names and name ∉ verified_uavs then
        registered_names[name] ← False
    end if
end procedure
procedure verifyUAV(name)
    if name ∈ registered_names and name ∉ verified_uavs then
        verified_uavs[name] ← True
        delete registered_names[name]
    end if
end procedure
function isUAVRegistered(name)
    return name ∈ registered_names
end function
function isUAVVerified(name)
    return name ∈ verified_uavs
end function
```

$$RS = \sum_{1}^{n} \frac{PR}{TT} \tag{2}$$

where:

WQ: the weight factor of Quality of Delivery
RQ: the reputation score of Quality of Delivery
WT: the weight factor of Timeliness
RT: the reputation score of Timeliness
TT: the Total Task Completed
PR: the Prior Reputation
RS: the Reputation Score

A node with a lower reputation score indicates that it has the potential or has already produced services that cause attacks and harm to the system, thereby the access of the node or such service provider is revoked to prevent malicious attacks on the system. A malicious provider can pass through the registration and verification process without being detected as malicious but can be detected once service is been rendered on the system. The calculated reputation score is then updated and saved on the blockchain to ensure the immutability, transparency, and decentralization of the system.

Algorithm 2. ReputationContract

```
struct UAV
struct Rating
mapping(address = UAV)
mapping(address = Rating[])
public reputationScores;
mapping(address = uint256) public priorReputations;
constant MAX_SCORE = 5;
constant MAX_RATING = 5;
constant MAL_THRESHOLD = 2;
constant WEIGHT_QUALITY = 6;
constant WEIGHT_TIMELINESS = 4;
function submitRating(...)
end function
function calculateReputationScore(...)
end function
```

4 Experimental Results

4.1 Experimental Setup

The algorithms were tested using multiple scenarios of UAV systems and various outputs based on the algorithm provided in Sect. 4. This is done with the Remix IDE environment, a web-based integrated development environment, that was employed for writing, testing, and deploying the smart contracts, which gives valuable logs for checking the status and results of each operation when debugged. The simulation was done on the Windows 10 operating system. Python 3 is the programming language employed in this implementation. A 500 GB SSD drive was used to meet storage requirements, ensuring quick access to data and low latency during operations and a 1 Gbps network link enabled flawless communication between nodes. Ethereum, a well-known and widely utilized blockchain platform, served as the foundation technology for building and testing our smart contracts. In order to simulate the real-time interaction inherent to blockchain-based systems, nodes interacted with one another through the use of smart contracts issued on the Ethereum blockchain. Some of our nodes served as Service Providers providing UAV services, while others were allocated specialized duties. Five nodes were selected for the simulation and the reputation score was computed by taking into account the nodes shown in Fig. 3. The reputation values for the 5 nodes are calculated using Equations (1) and (2) with a reputation score of 5 being considered as being reliable and reputation score below 3 is considered as malicious to the system and sending fake and wrong messages to the network.

4.2 Results

After implementing the framework, precise results of a node's reputation are produced, which may be used to assess whether or not the node is to be trusted.

According to Fig. 3, Node 1 and Node 2 have a balanced reputation in that they provide both real and fake services in a balanced manner. Also, Node 3's reputation is continually being stabilized as a result of its constant genuine service to the system with a constant rating being given to it. Because of its unreal services, Node 5 reputation is continually deteriorating and unreal. However, Node 4 has a fluctuating reputation score as a result of having to deliver both real and fake services to the system making the curves decrease as well as increase. The level at which the communications are regarded trustworthy is assumed to be 3.0, and relevant steps are performed. Devices that have a reputation score below this limit are deemed untrustworthy and malicious to the system, thereby they are discarded so as to prevent an attack on the system. Whether the node is accepted or rejected, the reputation of each node is updated as shown in the flow chart in Fig. 2. The closest the reputation score is to 5 which is assumed to be the optimum reputation score, the most trustworthy the device is.

The processing time for registration, verification, and rating process of each Unmanned Aerial Vehicle are plotted in Fig. 4. The graph shows that the processing time of UAVs during registration takes an average of 3 s to be completed for all the UAVs. This illustrates that differences in UAV models or other parameters have no significant effect on the registration process. A constant processing time suggests that the registration system is well-designed and efficient for the model. With an average processing time of 3 s, the registration procedure for all UAVs is fast. An efficient registration system is essential for UAV operations since it allows for quick deployment and eliminates downtime. It would also be beneficial to compare the processing times of the verification and rating proce-

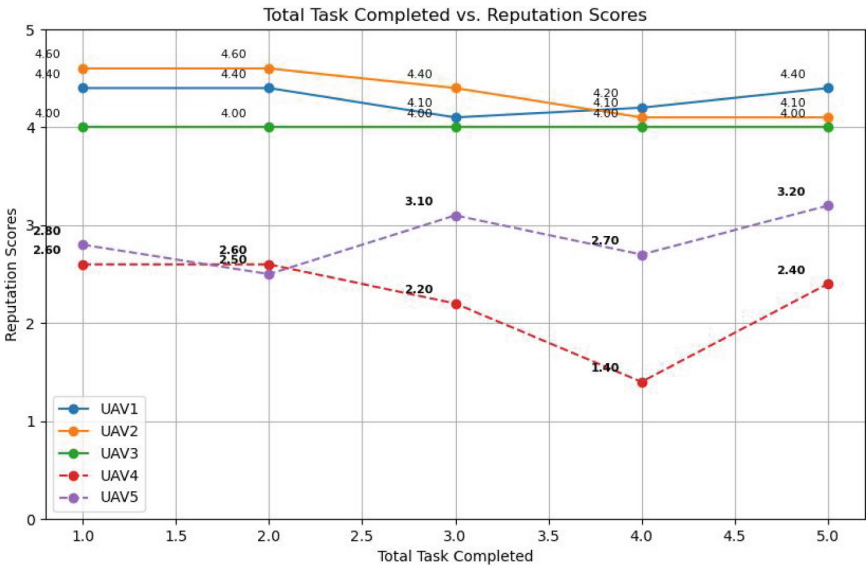

Fig. 3. Total task completed versus Reputation score

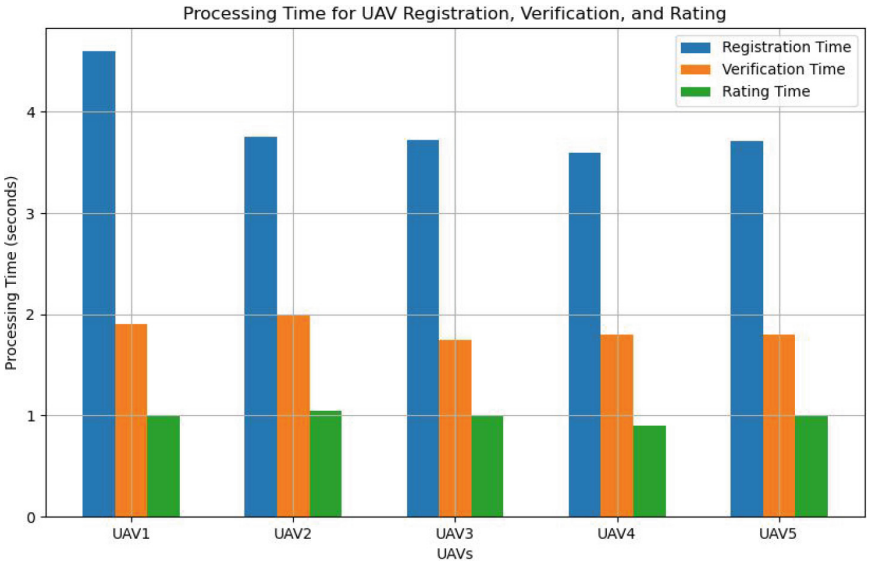

Fig. 4. Processing time (second) versus UAVs

dures because they are both consistent and efficient. This can help enhance and identify possible bottlenecks in UAV operations.

The verification technique takes an average of 2 s for each of the 5 UAVs, whereas the rating procedure takes 1 s according to Fig. 4. The fact that these processing times are minimal and quick indicates that the verification and rating processes are both efficient. The timely completion of these tasks can contribute to the overall efficiency of UAV operations. When the processing times are compared, we can see that the verification and rating operations are both faster than the registration process, which takes an average of 3 s. This suggests that the registration process may be more complicated or include more steps than verification and rating.

4.3 Discussions

Registration Reputation. The requester node gives feedback on the service provider nodes it has interacted with. This approach will fail if the service provider is not registered in the smart contract. Furthermore, the smart contract's state is restored if the submitted reputation values are outside of the expected range.

However, if a UAV device has already been registered and verified on the system, any attempt to register the account again either by its name or by the address will cause the transaction to be reversed to its initial state while printing out an error message "UAV is already registered".

When a UAV device with no prior registration history aims at performing some transactions on the network, a reversion to its initial state occurs indicating that the UAV has not been registered.

ReputationContract Reputation. The aggregation of the past feedback and present feedback after being calculated using the reputation calculation was computed and updated on the Reputation Contract. This node acted in good behavior by delivering honest and consistent evaluations in the majority of its reputation score submissions.

Figure 3 shows that after the rating was submitted for each UAV the reputation score was calculated. Plotting the reputation score per total task completed, it shows the interaction between the service providers after each successful transaction which shows the behaviors of both the malicious devices and the non-malicious devices.

Challenges of Blockchain on the UAV Network. Integrating blockchain into UAV networks is still facing many challenges, even if a lightweight-designed blockchain like Microchain. In ongoing efforts, we continue tailoring the blockchain to fit in the resource-constrained UAVs from aspects below:
Energy Efficient: UAV networks are resource-constrained devices Blockchain computational processes are intensive, and a large amount of energy is being consumed during computations most especially for UAV devices operating in real-time scenarios leading to the draining of the battery energy as fast as possible.
Connectivity: Most UAV operations occur in remote areas or hostile environments. Thereby connection to the blockchain networks in these environments continuously is challenging which can enhance synchronization issues.
Storage: Resource constraint features of UAV devices make it an issue when considering the storage of the devices. Having to store blockchain ledger on these resource-constrained devices is a trade-off and seems impractical as a result of the limited storage capacity which might hinder the up-to-date update of the blockchain.
Scalability: As a result of the huge amount of data being sent and received in a real-time scenario of UAV systems, scalability is a great issue on blockchain networks because if the transactions load, and may find it hard to handle this amount of data or load.

5 Conclusions

In this paper, we proposed a **LI**ghtweight **B**lockchain-based **RE**putation (LIBRE) system to enhance the reliability and performance of UAV networks. LIBRE system enables a UAV network to register, verify assignments, and update the reputation score of a UAV service provider after assessing and observing its behavior and services provided based on the feedback received. Reputation scores are calculated using the blockchain-based algorithm that guarantees

the reliability, immutability, and auditability of the score after being updated. Based on the output of the reputation score calculated using the Reputation Calculation Equation, there is either an increase or decrease in the global reputation score which is visible to the public when the calculation and updating has been done. Based on the reliability, security, and privacy of UAV networks have been great issues being researched. A blockchain which is a type of lightweight distributed ledger technology system that uses fewer nodes to ensure faster consensus and transaction processing was implemented in the system as an underlying protocol for the reputation system. This lightweight method benefits UAV systems since it concentrates on systems with fewer resources.

References

1. Abdelmaboud, A.: The internet of drones: requirements, taxonomy, recent advances, and challenges of research trends. Sensors **21**(17), 5718 (2021)
2. Alladi, T., Chamola, V., Sahu, N., Guizani, M.: Applications of blockchain in unmanned aerial vehicles: a review. Veh. Commun. **23**, 100249 (2020)
3. Bansal, G., Hasija, V., Chamola, V., Kumar, N., Guizani, M.: Smart stock exchange market: a secure predictive decentralized model. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2019)
4. Battah, A.A., Iraqi, Y., Damiani, E.: A trust and reputation system for IoT service interactions. IEEE Trans. Netw. Serv. Manage. **19**(3), 2987–3005 (2022)
5. Bhoi, S.K., Jena, K.K., Jena, A., Panda, B.C., Singh, S., Behera, P.: A reputation deterministic framework for true event detection in unmanned aerial vehicle network (UAVN). In: 2019 International Conference on Information Technology (ICIT), pp. 257–262. IEEE (2019)
6. Bodkhe, U., et al.: Blockchain for industry 4.0: a comprehensive review. IEEE Access **8**, 79764–79800 (2020)
7. Caro, M.P., Ali, M.S., Vecchio, M., Giaffreda, R.: Blockchain-based traceability in agri-food supply chain management: a practical implementation. In: 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), pp. 1–4. IEEE (2018)
8. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., Wang, X.: TRM-IoT: a trust management model based on fuzzy reputation for internet of things. Comput. Sci. Inf. Syst. **8**(4), 1207–1228 (2011)
9. Chen, N., Chen, Yu.: Smart city surveillance at the network edge in the era of IoT: opportunities and challenges. In: Mahmood, Z. (ed.) Smart Cities. CCN, pp. 153–176. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76669-0_7
10. Debe, M., Salah, K., Rehman, M.H.U., Svetinovic, D.: IoT public fog nodes reputation system: a decentralized solution using Ethereum blockchain. IEEE Access **7**, 178082–178093 (2019)
11. Fortino, G., Fotia, L., Messina, F., Rosaci, D., Sarné, G.M.: Trust and reputation in the internet of things: state-of-the-art and research challenges. IEEE Access **8**, 60117–60125 (2020)
12. Ge, C., Ma, X., Liu, Z.: A semi-autonomous distributed blockchain-based framework for UAVs system. J. Syst. Architect. **107**, 101728 (2020)
13. Hassija, V., et al.: Fast, reliable, and secure drone communication: a comprehensive survey. IEEE Commun. Surv. Tutorials **23**(4), 2802–2832 (2021)

14. Jena, K.K., Bhoi, S.K., Behera, B.D., Panda, S., Sahu, B., Sahu, R.: A trust based false message detection model for multi-unmanned aerial vehicle network. In: 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 324–329. IEEE (2019)
15. Kapitonov, A., Lonshakov, S., Krupenkin, A., Berman, I.: Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs. In: 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), pp. 84–89. IEEE (2017)
16. Kong, L., Chen, B., Hu, F.: Lap-BFT: Lightweight asynchronous provable byzantine fault-tolerant consensus mechanism for UAV network. Drones **6**(8), 187 (2022)
17. Lagkas, T., Argyriou, V., Bibi, S., Sarigiannidis, P.: Uav IoT framework views and challenges: towards protecting drones as "things". Sensors **18**(11), 4015 (2018)
18. Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W.: Blockchain's adoption in IoT: The challenges, and a way forward. J. Netw. Comput. Appl. **125**, 251–279 (2019)
19. Mohsin, A.H., et al.: Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. Comput. Stand. Interfaces **64**, 41–60 (2019)
20. Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Das, G.: Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consum. Electron. Mag. **7**(4), 6–14 (2018)
21. Qureshi, K.N., Jeon, G., Hassan, M.M., Hassan, M.R., Kaur, K.: Blockchain-based privacy-preserving authentication model intelligent transportation systems. IEEE Trans. Intell. Transp. Syst. **24**, 7435–7443 (2022)
22. Resnick, P., Zeckhauser, R.: Trust among strangers in internet transactions: empirical analysis of Ebay's reputation system. In: The Economics of the Internet and E-commerce, vol. 11, pp. 127–157. Emerald Group Publishing Limited (2002)
23. Shehada, D., Gawanmeh, A., Yeun, C.Y., Zemerly, M.J.: Fog-based distributed trust and reputation management system for internet of things. J. King Saud Univ.-Comput. Inf. Sci. **34**(10), 8637–8646 (2022)
24. Wang, Y., Wen, J., Zhou, W., Tao, B., Wu, Q., Tao, Z.: A cloud service selection method based on trust and user preference clustering. IEEE Access **7**, 110279–110292 (2019). https://doi.org/10.1109/ACCESS.2019.2934153
25. Wang, Z., Xiong, R., Jin, J., Liang, C.: Airbc: a lightweight reputation-based blockchain scheme for resource-constrained UANET. In: 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 1378–1383 (2022). https://doi.org/10.1109/CSCWD54268.2022.9776299
26. Xu, R., Ramachandran, G.S., Chen, Y., Krishnamachari, B.: BlendSM-DDM: BLockchain-ENabled secure microservices for decentralized data marketplaces. In: 2019 IEEE International Smart Cities Conference (ISC2), pp. 14–17. IEEE (2019)
27. Xu, R., Wei, S., Chen, Y., Chen, G., Pham, K.: Lightman: a lightweight microchained fabric for assurance-and resilience-oriented urban air mobility networks. Drones **6**(12), 421 (2022)
28. Xu, X., Zhao, H., Yao, H., Wang, S.: A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT. IEEE Internet Things J. **8**(4), 2431–2443 (2021). https://doi.org/10.1109/JIOT.2020.3030080
29. Yaacoub, J.P., Noura, H., Salman, O., Chehab, A.: Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things **11**, 100218 (2020)
30. Yu, Y., Li, Y., Tian, J., Liu, J.: Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wirel. Commun. **25**(6), 12–18 (2018). https://doi.org/10.1109/MWC.2017.1800116