drones

MDPI

Article

Drones and Blockchain Integration to Manage Forest Fires in Remote Regions

Dena Mahmudnia [1], Mehrdad Arashpour [2,*], Yu Bai [2] and Haibo Feng [3]

[1] Civil Engineering Department, Sadjad University of Technology, Mashhad 91881-48848, Iran
[2] Department of Civil Engineering, Monash University, Clayton, Melbourne, VIC 3800, Australia
[3] Department of Mechanical and Construction Engineering, Northumbria University, Newcastle NE2 1XE, UK
* Correspondence: mehrdad.arashpour@monash.edu

Abstract: Central management of fire stations and traditional optimization strategies are vulnerable to response time, a single point of failure, workload balancing, and cost problems. This is further intensified by the absence of modern communication systems and a comprehensive management framework for firefighting operations. These problems motivate the use of new technologies such as unmanned aerial vehicles (UAVs) with the capability to transport extinguishing materials and reach remote zones. Forest fire management in remote regions can also benefit from blockchain technology (BC) due to the facilitation of decentralization, tamper-proofing, immutability, and mission recording in distributed ledgers. This study proposed an integrated drone-based blockchain framework in which the network users or nodes include drones, drone controllers, firefighters, and managers. In this distributed network, all nodes can have access to data; therefore, the flow of data exchange is smooth and challenges on spatial distance are minimized. The research concluded with a discussion on constraints and opportunities in integrating blockchain with other new technologies to manage forest fires in remote regions.

Keywords: blockchain; smart contract; drone; forest fire

Citation: Mahmudnia, D.; Arashpour, M.; Bai, Y.; Feng, H. Drones and Blockchain Integration to Manage Forest Fires in Remote Regions. *Drones* **2022**, *6*, 331. https://doi.org/10.3390/drones6110331

Academic Editor: Diego González-Aguilera

Received: 21 September 2022
Accepted: 26 October 2022
Published: 30 October 2022

1. Introduction

Different ecosystems such as forests and grasslands provide a natural resource and maintain resilience and natural cycles. These environments are characterized by a wide variety of attributes. Specific attributes of each ecosystem need to be monitored to properly assess their health. These certain attributes are aligned with their ecosystem stressors. The main stressor for forests is "climate change", and the second most important is "fire disturbance" [1]. Since traditional methods in ecosystem health monitoring had limitations, the combination of Geographic Information System (GIS) with remote sensing became more and more popular for monitoring various spatiotemporal scales. These technologies allow up-to-date monitoring and prediction of forest disturbance risks [2]. Forest fires in remote regions pose severe threats to ecosystems and are considered important drivers of climate change with adverse impacts on the environment [3]. There is a need for an emergency response to detect the exact location of fires in remote regions and prevent them from turning into a disaster [4]. However, in the field of firefighting, departments are slow to implement novel technologies due to restrictive protocols and uncertainty about value addition [5]. Therefore, many studies have been conducted to improve scientific methods to save the environment, ecosystems, and risks to the public [6]. In this regard, to reduce the destructive effects of forest fires in remote regions, researchers have used wireless sensor networks and machine-learning models [7]. Furthermore, operational models and forest fire simulations have been created to predict fire behavior [8]. The other technique for forest fire detection is using satellite imagery and forest fire modeling considering spatial parameters [9]. Recently, deep-learning frameworks have been utilized to predict forest fire progression and protect human lives [10]. Due to the dangerous nature of firefighting operations, using robots in extinguishing fires in remote regions has been of particular interest [11].

Unmanned aerial vehicles (UAVs) and drones are able to autonomously fly without a human pilot and are remotely controlled [12]. One of the drone usages is in a warehouse to scan items and products and communicate to managers for any appropriate action [13]. Recently, drones have achieved an important role in the logistics sector since they have some advantages such as time-saving by getting away from the traffic and environmental friendliness by reducing carbon footprint. However, since drone management relies on machine-learning techniques, there are some limitations, for example, employing a highly skilled person that increases costs. Another issue is a limited battery problem that can be handled by drone-charging facilities, but it can lead to a significant initial cost. Accordingly, it is necessary to define the factors that may play a remarkable role in the adoption of drones in different industries [14].

Drones can effectively monitor operations to avoid undesirable results when natural disasters occur. They can be a tool to obtain "aerial photography" used for the investigation of disaster management [15]. Aerial pictures of operations facilitate detailed descriptive analysis of equipment [16] and give helpful clues for scene understanding [17]. Moreover, these robotic vehicles can carry payloads and fly to remote regions [18]. Multidrones need interaction to share data such as locations, paths, tasks, and purposes. Complex interactions between drones and stations can be supported by artificial intelligence (AI), the Internet of Things (IoT), and cloud or edge computing [19]. Modern technologies can minimize casualties and damages, enable quick responses, and prevent false alarms. However, information systems confront a primary challenge since they require trust in centralized management that cannot effectively protect data from unauthorized access [20]. Therefore, there is a need for distributed networks to access information and facilitate data exchange in a secure procedure [21].

To address these issues, blockchain technology (BC) can efficiently facilitate collaboration among devices [22]. Blockchain, introduced by Satoshi Nakamoto in 2008, electronically records data in digital formats [23]. This technology has been increasingly adopted for various purposes, including forest fire surveillance [24]. There are many challenges for a drone network because of its distributed nature; thus, there is a need for blockchain-based platforms to control drone functions and provide trust and security for the network [25,26]. Moreover, since there is a possibility of false alarms while applying UAVs to detect fires in a particular area, AI algorithms using blockchain can record a history of transparent alarms received to assess the truthfulness of UAV performance [27,28].

This study developed a blockchain solution to prevent multidrone collisions during combating fire. The main objective of the proposed framework is to present a complete picture of how BC can support the management of drone operations for delivering extinguishing materials and monitoring the mission in forest fires in remote regions. Toward the main research objectives, the following contributions to the body of knowledge are made:

- Proposing a framework architecture aiming at applying blockchain for combating forest fires;
- Discussing two cases for drone management to combat fire, i.e., delivering materials to suppress fires and monitoring the firefighting operations in the forest area;
- Reporting the research challenges in using blockchain for putting out forest fires.

This study primarily focused on managing drone functions to combat fire outbreaks in remote regions with BC. The remainder of this paper is presented as follows. Related studies are discussed in Section 2, and the proposed framework of the system is explained in Section 3. Section 4 offers blockchain applications in two cases of firefighting operations. Challenges are described in Section 5. Finally, research conclusions are presented in Section 6.

2. Related Work and Background

2.1. Blockchain Technology

BC has been considered a "trust machine" since the technology can realize multiuser participation in both an open and semi-open network and create trust among users [29]. Moreover, the network based on the blockchain can protect personal privacy. In this regard, patent data access based on BC was introduced to control data access by the encryption algorithm [30]. The core design patterns of BC include a consensus mechanism, used to reach the required agreement on specific data, chained data blocks, the space for storing data, encryption technology, and protecting sensitive data from hacking [31]. Researchers reviewed the features of BC and investigated its effective role in solving interaction problems [32]. One of the unique features of blockchain is the consensus mechanism applied in a decentralized network to guarantee that different nodes can achieve the final agreement on data content or a decision. Both authorized and unauthorized nodes can reach consensus mechanisms. The second type of mechanism contains proof of knowledge (POK), crash fault tolerance (CFT), proof of work (POW), and proof of stake (POS) [33].

Consensus algorithms can be used in blockchain to authorize all network users to uphold a chain of blocks for stored data. These blocks contain historical transaction information, connected through a hash algorithm. Blockchain architecture contains public and private access based on the network's permissions level [34]. Cryptography technology, including hash algorithm, zero-knowledge proof, and asymmetric encryption, ensures data privacy protection in a blockchain network. In a blockchain network, each block has a unique hash that, if its information is changed, the hash value will be changed. Then, the next block will not recognize the new block. This feature of blockchain makes it very difficult to tamper with the recorded data [35].

Since 1997, cryptographers have presented the concept of smart contracts [36]. One of the first BC applications was the Ethereum platform that enabled smart contract codes to be run on a blockchain network. Once the determined requirements in the digital contract are fulfilled, the contract is automatically executed. Smart contracts implemented on a blockchain network guarantee secure data sharing [37]. These further minimize unpredictable conditions, facilitate trust-based interaction, and reduce transaction costs [38].

2.2. Drone Technology

Aerial support is a critical firefighting tool releasing a considerable amount of extinguishing material [39]. However, such kinds of ways to suppress wildfire can cause a risk to firefighters' lives: firefighters risk entrapments [40]. Since a limited-size fire can be easier to suppress and control than a flame that has already spread, unmanned aerial vehicles (UAVs) can be more valuable in such conditions. In the last few years, the application of UAVs, commonly called drones, in surveillance has increased. Several studies investigated the use of drones in forest fire detection and suppression [41]. In the following, the various aspects of using drones in fire control are reviewed.

One of the important steps in controlling forest fires is predicting the firefront advance that raises awareness. In this case, a research study developed a system for the patrolling planning of UAVs to monitor fires in forests. To this purpose, researchers applied a route point scheduling logic combining features of the region with real-time measurements [42]. Another idea to detect a fire at the early stage is to use the animal's body in the forest to deploy IoT-based sensors. Tehseen et al. came up with the idea to gather data and send them to the station. They also used drones for real-time visualization and graph theory to create an efficient model [43].

In the case of extinguishing forest fires, Aydin et al. presented the use of drones equipped with fire-extinguishing balls. They analyzed the factors involved to increase the efficiency of fire-extinguishing balls including the optimal number of balls and the best distance for dropping the balls [44]. In another study, scholars depicted a unique clustering approach to detect a forest fire and transmit data on the fire to a base station through wireless communication. Moreover, their approach is efficient for managing the energy challenges of UAVs [45]. Ausonio et al. presented a conceptual framework to compute the water flow rate based on the total number of drones by considering the decisive factors in the evolution of fires [46].

2.3. Applications of Blockchain in Monitoring

BC has been gradually applied for monitoring purposes to handle the issues of central systems. For example, many organizations and governments adopted electronic medical records (EMRs) based on cloud computing [47]. EMRs have several advantages, but they suffer from central management. Records stored in centralized systems may result in tampering, fraud, or unauthorized publication. Therefore, researchers designed an EMR system based on BC to improve their security [20]. Vahdati et al. presented an IoT, blockchain, and AI architecture to manage the coronavirus disease (COVID-19) [48]. Codes relying on a blockchain-based smart contract are autonomously executed, which establishes trust between the participants involved and enhances the efficiency of any workflow [49]. Hathaliya et al. presented a healthcare architecture based on a permissioned blockchain and reduced the patient's time and cost through remote patient monitoring (RPM) [50]. Ratta et al. used BC and IoT in healthcare systems to improve the functionality of the medical sector in drug traceability, RPM, and medical record management [51]. Personal health records are sensitive and essential to be saved during data exchange inside the system; therefore, another study presented a network to use BC to improve efficiency in multiple healthcare monitoring systems [52].

Also, monitoring can play an essential role in the system workflow of using renewable energy, in which the secure management of node transactions can reduce system failure [53]. Data about inbound or outbound energy can be part of a smart contract stored in blockchain [54]. Accordingly, an energy management framework was proposed to establish trust among users and enforce autonomous monitoring to improve aggregated grid services without relying on centralized systems [55]. An authorization system based on blockchain technology can facilitate access to customer data and resource trading; the system improves reliable monitoring management and optimization of worldwide consumption [56].

By growing the use of UAVs, new challenges in managing their operations have emerged. The critical issue of working with UAVs that needs to be addressed is the possibility of crashes. As a result, to avoid the collision, there is a need to design a network based on blockchain to identify obstacles. Accordingly, a swarm system was designed to maximize the motion safety of drones [57]. In this regard, a blockchain-based platform could increase trust and security during the operation of drones [58]. Another study introduced an improved architecture based on a chain code to manage and monitor IoT devices employing a private blockchain [59]. Furthermore, Datta and Sinha presented a framework for EdgeDrone and BC to improve forest fire surveillance by relying on secured data delivery. They designed an edge-computing architecture including three layers: the IoT layer, edge layer, and a cloud server continually connecting with the edge layer. The leader selection algorithm used in this study to improve energy conservation is important in a wildfire IoT environment with constrained resources. Furthermore, the researchers minimized energy consumption by a drone trajectory algorithm. A comprehensive analysis of QoS parameters displayed a delay reduction of 66% [24]. Another application of the blockchain-based framework for drones is optimizing the scheduling for UAVs' battery problems. Therefore, researchers [60] designed a secure drone charging system based on blockchain to authenticate charging stations.

As mentioned above, the previous studies have applied new technologies to control forest fires in different phases; detection, prevention, and suppression. Inspired by the relevant studies, the authors of the current paper presented a management framework based on blockchain to manage drones in a fire operation.

3. Proposed Framework Solution

When combating fires in remote regions, the integration of smart contracts based on blockchain and UAV collaboration makes operations easy to control and more robust to a single point of failure. Blockchain can efficiently control drone performance, support collaboration to avoid an operation failure, secure it, and ensure drones remain in the mission area. Data in a blockchain-based network are public for each node, and therefore, not only does each node has access to other nodes' data, but it also controls its attack detection. As a result, the single point of failure challenge is mitigated [61]. For ceasing wildfire in remote regions, the current paper focused on examining the achieved solutions by BC and identifying decentralized drone mission challenges. Figure 1 presents the process of uploading mission status reports to the blockchain network.

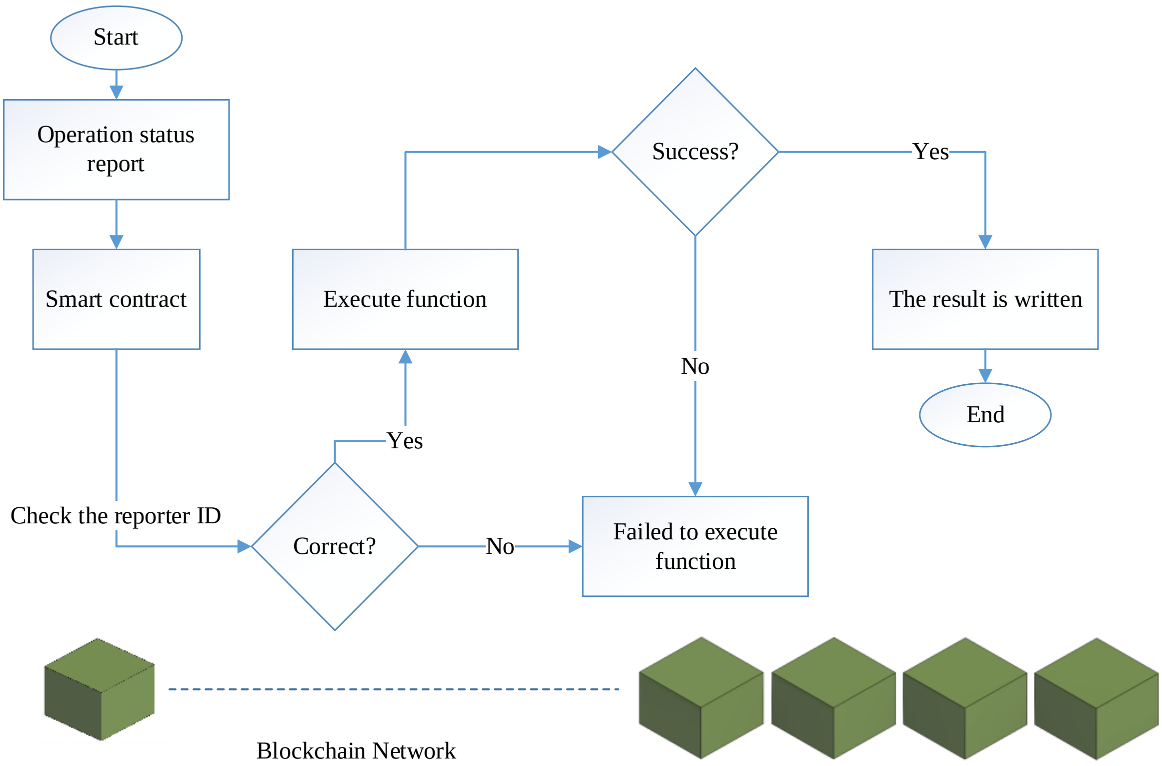

Figure 1. Process of uploading mission status reports to blockchain network.

The UAVs can deliver extinguishing materials to a specific place in real time and improve the emergency response to suppress the fire. Therefore, drones help firefighters respond and find the direction of the fire spread [62]. The drone's function for combating wildfire is summarized, as seen in Figure 2.

The nodes based on joint planning need to reach a common aim of the operation. Since decision-making in a distributed network is complex, autonomous solutions can solve the challenge [63]. Moreover, unit testing is used to analyze the correctness of individual components in smart contracts. A unit test can provide an obvious reflection of mistakes if the test fails [64]. Blockchain technology offers an effective solution to ensure that all users are connected to share their data in a decentralized fashion. The proposed framework enables the drone's performance under control through the smart contract. In this procedure, the drone controller and the manager in the fire station follow the terms of the smart contract security system.

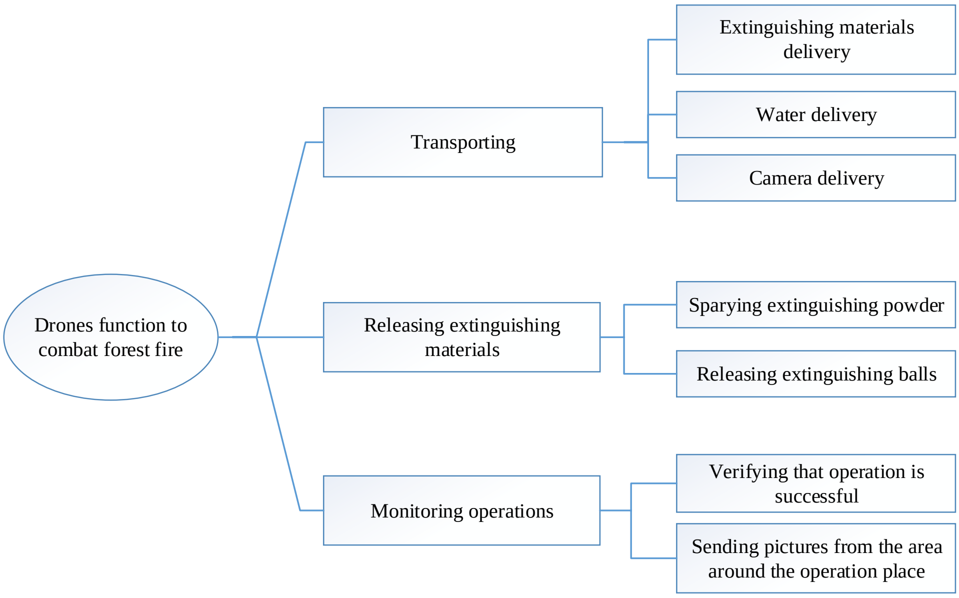

Figure 2. Drones function to combat forest fires.

A drone consists of a frame, motor propellers, an electric motor controller, a power distribution board, a flight controller, a battery, a receiver or Bluetooth, a camera, a video transmitter, and some sensors. There are multiple sensors attached to a drone. For example, the pressure sensor measures the altitude or the distance between the ground and the drone; the GPS locates the drone's position. Firefighting drones supported by thermal cameras improve vision via the smoke and quickly navigate. Generally, an average communication range of a drone is 8 km. It can fly for 30 min, and its speed can reach 96 km/h [65]. Drones facilitate fire suppression by transporting fire extinguishers such as foam, powder, and carbon dioxide extinguishers (CO2) [66] (Figure 3); and monitoring the operation by carrying cameras and capturing pictures to inform the status of the fire outbreak. They are equipped with a payload drop mechanism to release the spheres against fires. When a drone reaches the flame, the controller can release the balls to suppress the flame [46,67].

(**a**) (**b**)

Figure 3. Drones with extinguishing materials: (**a**) powder; (**b**) balls.

4. Applications of the Presented Approach

In an untrusted environment, data sharing by drones may lead to security breaches, which blockchain can address. Attribute-based encryption (ABE) is one of the most common public key-based verification schemes. The verification mechanism utilizes a smart contract to access public-key cryptography to improve accounts' security [68]. The drone needs to generate a random key to encrypt the collected data and the key by ABE; then, it can upload the data and send the ciphertext to the fire station. When the drone sends data or a request to the blockchain, the validation of the request needs to be evaluated. If the drone receives verification from the blockchain, it can upload the ciphertext to the network.

4.1. Drone for Suppressing Fires

The proposed algorithm for suppressing fires in remote regions by drones is shown in Figure 4. The framework includes three stages: receiving alarms, blockchain, and orders. In the receiving stage, alarms sent from the camera installed in a forest area are received; the alarm includes fire size and fire location. The smart contract confirms the requirements. Then, the established block with encrypted data, including drone ID, fire location, and delivery time, will be stored in the blockchain. All information recorded in the blockchain network is secure and trustworthy.

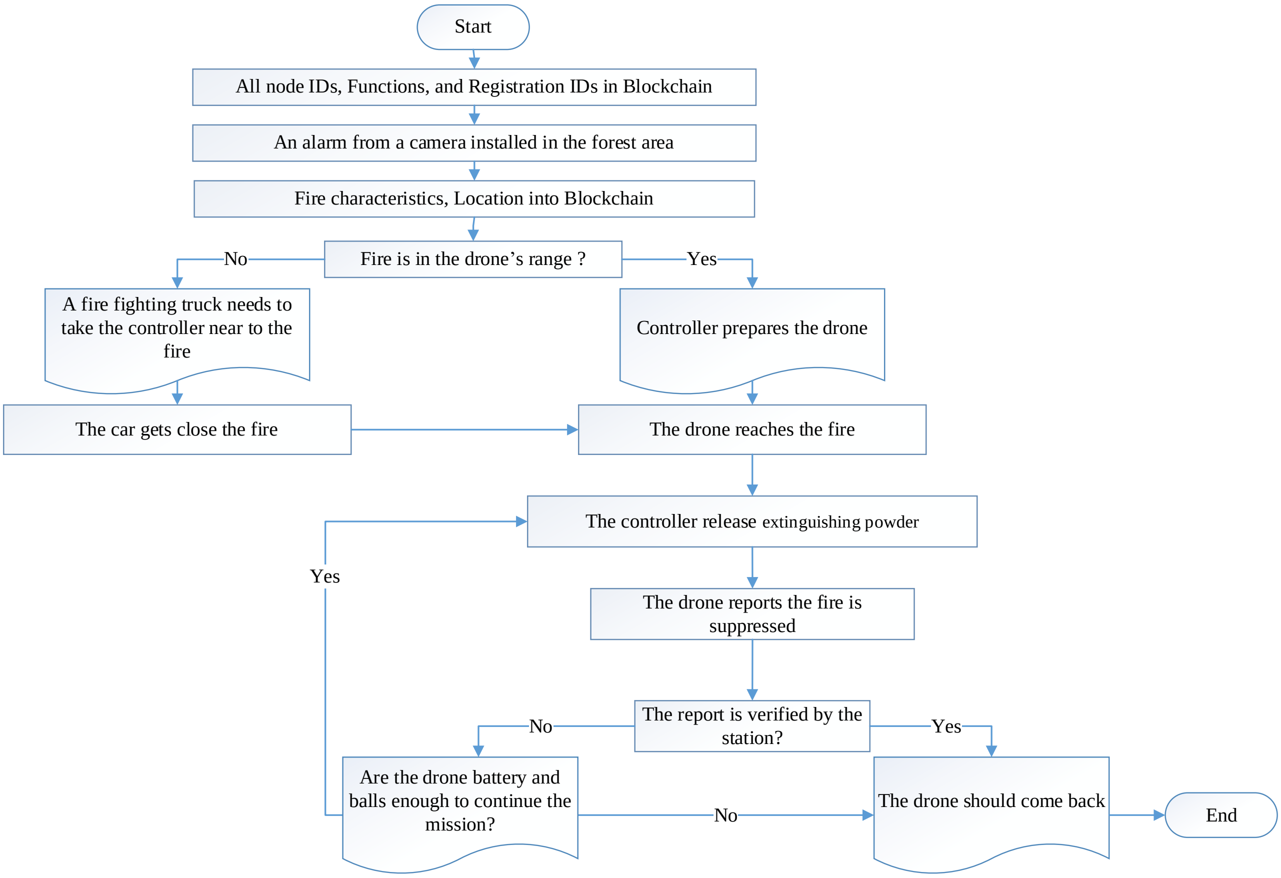

Figure 4. Flowchart of delivering extinguishing materials to combat a fire.

The procedure of the network, which is seen in Figure 5, includes the following:

- Sending an alarm by a camera installed in the forest area near the station;
- Deciding the place of starting the operation, based on the distance of the fire from the station;
- Registering the identification number of the selected drone into the network;
- Starting the operation and monitoring the status of equipment and the progress of the mission.

The drones need to be coordinated in remote regions to maintain their trajectory to reach the fire point. Once the extinguishing materials of the drone are almost finished, the drones return to their base. Eventually, once the fire is successfully suppressed, the mission is concluded.

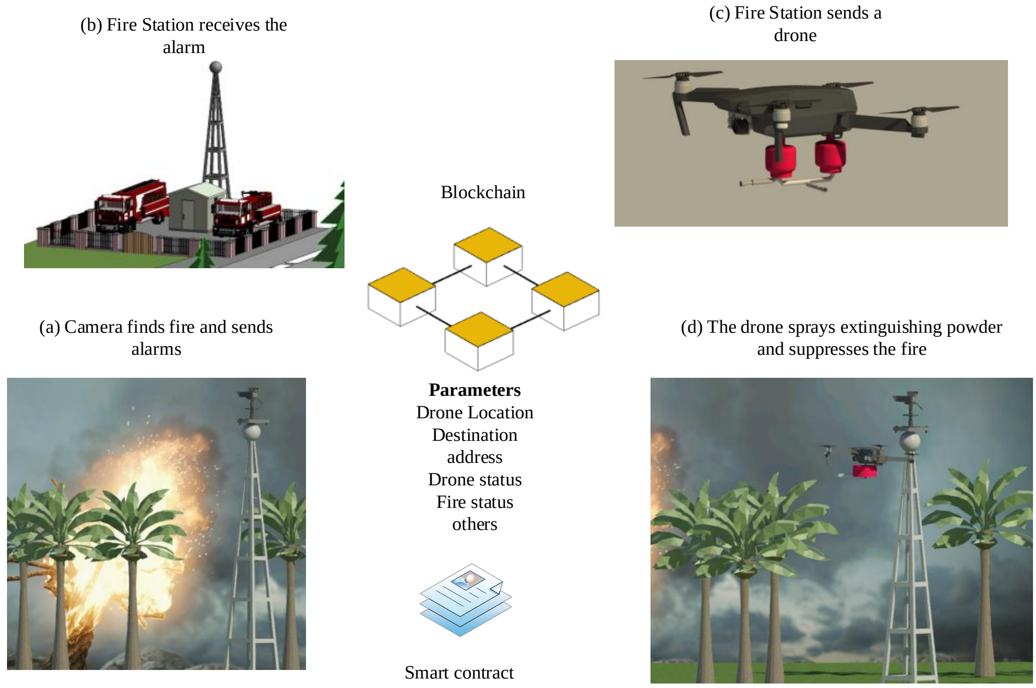

Figure 5. Steps of operation of fire suppression using a drone.

4.2. Drone for Monitoring the Operation

To ensure fire safety operations, drones are equipped with cameras and can communicate with the station. The monitoring data gathered by the drones can report the status of the mission by sending data to simultaneously update its location to inform the fire station about its condition and the fire status. The blockchain is a decentralized technology known as a meta controller and can manage the drone's function in a decentralized fashion.

This section proposes a management framework for drone collaboration based on blockchain. According to this framework, drones are the tools to manage and control the mission, not suppress the fire. The management framework includes three layers: verifying identities, managing the operation, and tracking tasks.

Verifying identities: The nodes of this study are a selected drone, a manager in the fire station, and firefighters; the nodes record their identification number, which a smart contract can confirm in the blockchain. When verifying node addresses, the smart contract defines whether the verification request meets the criteria. If the smart contract does not authorize the identification address, the blockchain discards the request. For example, the function of "checkFirefighters" can only be executed by the manager; thus, if an unknown address runs the function, the function cannot be executed, and an error will be returned. After running the function, its information (Table 1) is recorded in a block, then the block is added to the network.

Table 1. Example of transaction details.

Type	Description
Function	checkFirefighters
Executed by	Manager
Manager address	0xCE3B046f5F795e45176278Cf431584DBad02674D
Transaction index	22
Transaction Hash	0x5c8f2a2f951b3f6747484e273c8bc839c8a9410a8eebe134ceb9f18b7c63913d

Managing the operations: The drone needs to report the firefighters' location, wind direction, and fire status. As mentioned before, the image data are not transmitted to the blockchain. The InterPlanetary File System (IPFS) is used as decentralized storage to store the hash values of image data imported from the Decentralized Application (DApp) [69]. Back to the previous example, the function "checkFirefighters" causes the drone to send pictures of each firefighter. If one of them is in trouble, the station and other firefighters can be informed of an alarm. As mentioned in the previous section, when the battery's capacity is almost finished, the drone needs to return to the station; a new drone will continue the mission. Figure 6 presents the algorithm for monitoring the framework of the firefighting operation with blockchain technology.

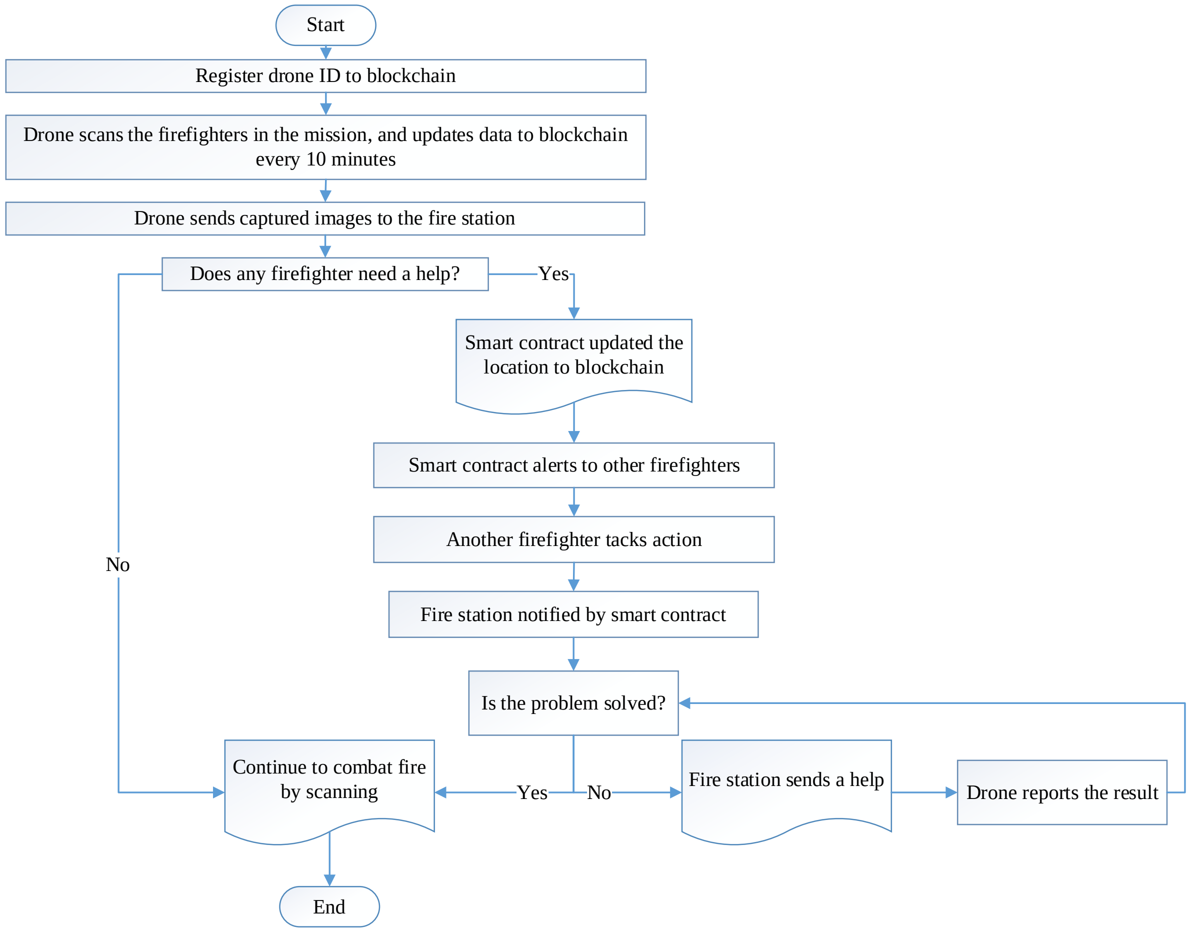

Figure 6. Flowchart of monitoring collaboration to combat fire.

Tracking tasks: Since the data are recorded in distributed ledgers, every operation step can be tracked. This feature offered by BC helps firefighters locate faulty equipment during the mission, track responsibility goals, and improve the structure of the firefighting system (see Figure 7).

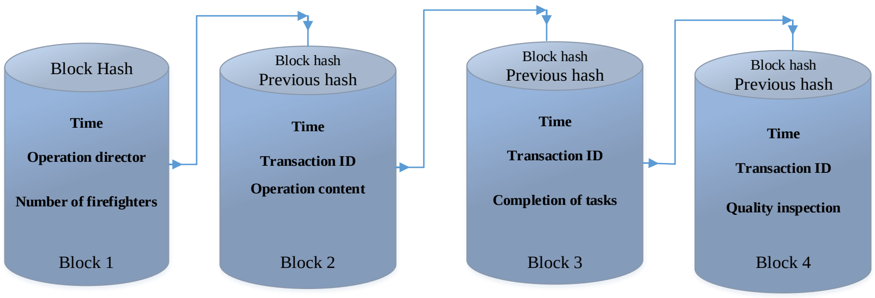

Figure 7. Representational blockchain for tracking tasks of the operation.

5. Discussion and Challenges

In the last few decades, drone technology has paved the way for avoiding human presence, especially during forest fires, by monitoring delivery extinguisher materials. This study proposed a framework for decentralized drone collaboration using BC in combating fire in remote regions. The data reported from the operation place are constantly and automatically recorded on the blockchain to fully monitor operations. Since it can run without any third-party interference, the cost of manual validation will be reduced, and the security of the data will be increased. In particular, since the images captured by cameras need memory with high capacity, they cannot be efficiently transmitted into the blockchain.

To ensure complete fire suppression, text data, such as the drone battery status reports, wind direction reports, and amount of used extinguishing material reports, are reported during the mission. The texts are reported on time by the drone. When a firefighter is in danger or gets stuck, the drone can detect the dangerous situation with a high-resolution camera in the drone's body. Then the drone immediately sends an alert to the fire station. Furthermore, the drone is required to immediately send the wind direction report after reaching the fire area. Therefore, blockchain manages the operation to control the drone's status and protect the mission from a cyber-attack. Moreover, every single task in the process is performed under the supervision of the fire station. Figure 8 illustrates drone applications for monitoring and suppressing fire in remote regions using blockchain.

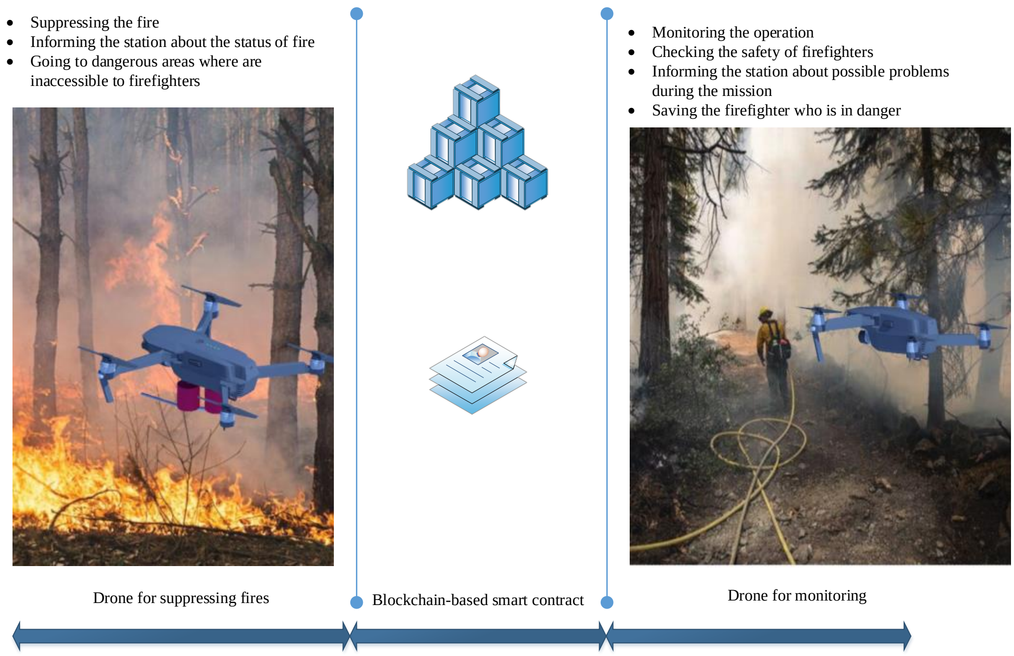

Figure 8. Drone-based blockchain applications.

Some constraints and limitations in implementing the proposed framework in remote regions need to be reported. The lifecycles of blockchain technology are one of the limitations of the framework. Blockchain networks depend on high computational power to run smart contracts on drones. Therefore, faster and more energy-efficient drone processors are needed to obtain maximum outcomes from a limited energy resource [70]. Another limitation of blockchain is transaction throughput [33]. Since the smart contracts deployed on a blockchain network are immutable, the developers need to be careful about the correctness of the codes. Any fault codes in the smart contract may damage the blockchain network.

Distributed ledger management is a complex task not only in public but also in private or consortium blockchains. The issues include determining the individuals who write the codes, govern, and manage the blockchain. There is a need to conduct many research studies in this field to improve proper technical criteria, policies, rules, and regulations for the professional deployment of BC in drone networks.

Moreover, UAVs and drones are equipped with various sensors that can create massive data; thus, the processing of this amount of data on drones, which have a battery constraint, can lead to a suboptimal solution [71]. As a result, collected data from IoT devices may affect drone resources. In addition, because of the presence of several sensors of drones, there may be a possibility of reading adverse data from surroundings by the sensors; thus, the drone may be damaged or misguided.

6. Conclusions

Blockchain technology provides decentralization, immutability, data privacy, and transparency. In this article, a drone application system equipped with BC for safe and real-time firefighting management in remote regions has been introduced. The proposed framework is applicable in firefighting missions based on BC and smart contracts. Drones can suppress the fire, and the fire station manager controls their function on a smart contract. Deployment of drones based on BC improves the efficient control of mission steps to maximize the safety of operations in remote regions. The proposed architecture of system nodes improves the security of the process by preventing information from being tampered with and enhances the ability of data analysis in the management system. The text data are recorded in the transaction information in a blockchain network. Furthermore, operation supervision can be facilitated by a visualization platform, which allows for manageable access to transaction data. There are, however, challenges around the large volume of imagery data and storing them in blockchain networks. In this paper, frameworks for delivering and monitoring were designed to handle the data in the blockchain. The frameworks have the potential to facilitate fire management in remote areas. Furthermore, the flexible deployment and robust information analysis can assist in safe fire suppression missions.

Author Contributions: D.M. and M.A.: contributed to the design of the study. D.M., M.A., Y.B., and H.F.: collected the data. D.M. and M.A.: analyzed and interpreted the data. D.M. and M.A.: drafted the manuscript. Y.B. and H.F.: reviewed the manuscript. All authors read, commented, and approved the final manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: The authors are grateful for the support from the Australian Research Council (ARC) through the Linkage project (LP180101080).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no competing interests.

References

1. Soubry, I.; Doan, T.; Chu, T.; Guo, X. A Systematic Review on the Integration of Remote Sensing and GIS to Forest and Grassland Ecosystem Health Attributes, Indicators, and Measures. *Remote Sens.* **2021**, *13*, 3262. [CrossRef]
2. Zaitseva, E.; Stankevich, S.; Kozlova, A.; Piestova, I.; Levashenko, V.; Rusnak, P. Assessment of the Risk of Disturbance Impact on Primeval and Managed Forests Based on Earth Observation Data Using the Example of Slovak Eastern Carpathians. *IEEE Access* **2021**, *9*, 162847–162856. [CrossRef]
3. Sannigrahi, S.; Pilla, F.; Basu, B.; Basu, A.S.; Sarkar, K.; Chakraborti, S.; Joshi, P.K.; Zhang, Q.; Wang, Y.; Bhatt, S.; et al. Examining the effects of forest fire on terrestrial carbon emission and ecosystem production in India using remote sensing approaches. *Sci. Total Environ.* **2020**, *725*, 138331. [CrossRef] [PubMed]
4. Toledo-Castro, J.; Caballero-Gil, P.; Rodríguez-Pérez, N.; Santos-González, I.; Hernández-Goya, C.; Aguasca-Colomo, R. Forest Fire Prevention, Detection, and Fighting Based on Fuzzy Logic and Wireless Sensor Networks. *Complexity* **2018**, *2018*, 1639715. [CrossRef]
5. Bashoor, M. Chief Concerns: Technology & Tradition. Available online: https://www.powerdms.com/policy-learning-center/technology-in-the-fire-service (accessed on 1 June 2017).
6. Arif, M.; Alghamdi, K.K.; Sahel, S.A.; Alosaimi, S.O.; Alsahaft, M.E.; Alharthi, M.A.; Arif, M. Role of Machine Learning Algorithms in Forest Fire Management: A Literature Review. *Int. J. Robot. Autom* **2021**, *5*, 212–216. [CrossRef]
7. Dampage, U.; Bandaranayake, L.; Wanasinghe, R.; Kottahachchi, K.; Jayasanka, B. Forest fire detection system using wireless sensor networks and machine learning. *Sci. Rep.* **2022**, *12*, 46. [CrossRef] [PubMed]

8. Pais, C.; Carrasco, J.; Martell, D.L.; Weintraub, A.; Woodruff, D.L. Cell2Fire: A Cell-Based Forest Fire Growth Model to Support Strategic Landscape Management Planning. *Front. For. Glob. Change* **2021**, *4*, 692706. [CrossRef]
9. Naderpour, M.; Rizeei, H.M.; Khakzad, N.; Pradhan, B. Forest fire induced Natech risk assessment: A survey of geospatial technologies. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 106558. [CrossRef]
10. Ban, Y.; Zhang, P.; Nascetti, A.; Bevington, A.R.; Wulder, M.A. Near Real-Time Wildfire Progression Monitoring with Sentinel-1 SAR Time Series and Deep Learning. *Sci. Rep.* **2020**, *10*, 1322. [CrossRef]
11. Innocente, M.S.; Grasso, P. Self-organising swarms of firefighting drones: Harnessing the power of collective intelligence in decentralised multi-robot systems. *J. Comput. Sci.* **2019**, *34*, 80–101. [CrossRef]
12. Ferrandez, S.M.; Harbison, T.; Weber, T.; Sturges, R.; Rich, R. Optimization of a truck-drone in tandem delivery network using k-means and genetic algorithm. *J. Ind. Eng. Manag.* **2016**, *9*, 15. Available online: http://inis.iaea.org/search/search.aspx?orig_q=RN:48050833 (accessed on 26 April 2016). [CrossRef]
13. Walmart Testing Warehouse Drones to Catalog and Manage Inventory. Available online: https://www.supplychain247.com/article/walmart_testing_warehouse_drones_to_manage_inventory (accessed on 3 June 2016).
14. Raj, A.; Sah, B. Analyzing critical success factors for implementation of drones in the logistics sector using grey-DEMATEL based approach. *Comput. Ind. Eng.* **2019**, *138*, 106118. [CrossRef]
15. Yadav, V.; Damle, M.; Pathak, P.; Pal, P.R. Humanitarian Impact of Drones in Healthcare and Disaster Management. *Int. J. Recent Technol. Eng.* **2019**, *7*, 201–205.
16. Arashpour, M.; Kamat, V.; Heidarpour, A.; Hosseini, M.R.; Gill, P. Computer vision for anatomical analysis of equipment in civil infrastructure projects: Theorizing the development of regression-based deep neural networks. *Autom. Constr.* **2022**, *137*, 104193. [CrossRef]
17. Arashpour, M.; Ngo, T.; Li, H. Scene understanding in construction and buildings using image processing methods: A comprehensive review and a case study. *J. Build. Eng.* **2021**, *33*, 101672. [CrossRef]
18. Alladi, T.; Chamola, V.; Sahu, N.; Guizani, M. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* **2020**, *23*, 100249. [CrossRef]
19. Alsamhi, S.H.; Almalki, F.A.; AL-Dois, H.; Shvetsov, A.V.; Ansari, M.S.; Hawbani, A.; Gupta, S.K.; Lee, B. Multi-Drone Edge Intelligence and SAR Smart Wearable Devices for Emergency Communication. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6710074. [CrossRef]
20. Alrebdi, N.; Alabdulatif, A.; Iwendi, C.; Lian, Z. SVBE: Searchable and verifiable blockchain-based electronic medical records system. *Sci. Rep.* **2022**, *12*, 266. [CrossRef]
21. She, W.; Liu, Q.; Tian, Z.; Chen, J.-S.; Wang, B.; Liu, W. Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 38947–38956. [CrossRef]
22. Dorigo, M. Blockchain technology for robot swarms: A shared knowledge and reputation management system for collective estimation. In Proceedings of the 11th International Conference, 4–6 April 2018; p. 425.
23. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://metzdowd.com (accessed on 20 July 2019).
24. Datta, S.; Sinha, D. BESDDFFS: Blockchain and EdgeDrone based secured data delivery for forest fire surveillance. *Peer Peer Netw. Appl.* **2021**, *14*, 3688–3717. [CrossRef]
25. Chang, Z.; Guo, W.; Guo, X.; Chen, T.; Min, G.; Abualnaja, K.M.; Mumtaz, S. Blockchain-Empowered Drone Networks: Architecture, Features, and Future. *IEEE Netw.* **2021**, *35*, 86–93. [CrossRef]
26. Satheesh Kumar, M.; Vimal, S.; Jhanjhi, N.Z.; Dhanabalan, S.S.; Alhumyani, H.A. Blockchain based peer to peer communication in autonomous drone operation. *Energy Rep.* **2021**, *7*, 7925–7939. [CrossRef]
27. Calvaresi, D.; Mualla, Y.; Najjar, A.; Galland, S.; Schumacher, M. Explainable multi-agent systems through blockchain technology. In Proceedings of the International Workshop on Explainable, Transparent Autonomous Agents and Multi-Agent Systems, Montreal, QC, Canada, 13–14 May 2019; pp. 41–58.
28. David, G.; Mark, S.; Jaesik, C.; Timothy, M.; Simone, S.; Guang-Zhong, Y. XAI—Explainable artificial intelligence. *Sci. Robot.* **2019**, *4*, eaay7120. [CrossRef]
29. The Trust Machine- The Technology Behind Bitcoin Could Transform How the Economy Works. Available online: https://www.economist.com/leaders/2015/10/31/the-trust-machine (accessed on 31 October 2015).
30. Li, H.; Li, M. Patent data access control and protection using blockchain technology. *Sci. Rep.* **2022**, *12*, 2772. [CrossRef] [PubMed]
31. Frankenfield, J. What Is a Smart Contract? Investopedia 2021. Available online: https://www.investopedia.com/terms/s/smart-contracts.asp (accessed on 25 June 2019).
32. Mahmudnia, D.; Arashpour, M.; Yang, R. Blockchain in construction management: Applications, advantages and limitations. *Autom. Constr.* **2022**, *140*, 104379. [CrossRef]
33. Zhang, Y.; Wang, T.; Yuen, K.-V. Construction site information decentralized management using blockchain and smart contracts. *Comput. Civ. Infrastruct. Eng.* **2021**, *37*, 1450–1467. [CrossRef]
34. Mao, D.; Hao, Z.; Wang, F.; Li, H. Novel Automatic Food Trading System Using Consortium Blockchain. *Arab. J. Sci. Eng.* **2018**, *44*, 3439–3455. [CrossRef]
35. Yuan, K.; Yan, Y.; Xiao, T.; Zhang, W.; Zhou, S.; Jia, C. Privacy-Protection Scheme of a Credit-Investigation System Based on Blockchain. *Entropy* **2021**, *23*, 1657. [CrossRef]

36. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday.* **1997**, 2. [CrossRef]
37. Gürsoy, G.; Brannon, C.M.; Gerstein, M. Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts. BMC Med. *Genomics* **2020**, *13*, 74. [CrossRef]
38. Eenmaa, H.; Schmidt-Kessen, M. Smart Contracts: Reducing Risks in Economic Exchange with No-Party Trust? *Eur. J. Risk Regul.* **2019**, *10*, 245–262. [CrossRef]
39. Thompson, M.; Calkin, D.; Herynk, J.; Mchugh, C.; Short, K. Airtankers and wildfire management in the US Forest Service: Examining data availability and exploring usage and cost trends. *Int. J. Wildland Fire* **2013**, *22*, 223–233. [CrossRef]
40. Butler, B. Wildland firefighter safety zones: A review of past science and summary of future needs. *Int. J. Wildland Fire* **2014**, *999*, 1. [CrossRef]
41. Floreano, D.; Wood, R.J. Science, technology and the future of small autonomous drones. *Nature* **2015**, *521*, 460–466. [CrossRef]
42. Giuseppi, A.; Germanà, R.; Fiorini, F.; Delli Priscoli, F.; Pietrabissa, A. UAV Patrolling for Wildfire Monitoring by a Dynamic Voronoi Tessellation on Satellite Data. *Drones* **2021**, *5*, 130. [CrossRef]
43. Tehseen, A.; Zafar, N.A.; Tariq Ali, F.J.; Alkhammash, E.H. Formal Modeling of IoT and Drone-Based Forest Fire Detection and Counteraction System. *Electronics* **2022**, *11*, 128. [CrossRef]
44. Aydin, B.; Selvi, E.; Tao, J.; Starek, M.J. Use of Fire-Extinguishing Balls for a Conceptual System of Drone-Assisted Wildfire Fighting. *Drones* **2019**, *3*, 17. [CrossRef]
45. Bharany, S.; Sharma, S.; Frnda, J.; Shuaib, M.; Khalid, M.I.; Hussain, S.; Iqbal, J.; Ullah, S.S. Wildfire Monitoring Based on Energy Efficient Clustering Approach for FANETS. *Drones* **2022**, *6*, 193. [CrossRef]
46. Ausonio, E.; Bagnerini, P.; Ghio, M. Drone Swarms in Fire Suppression Activities: A Conceptual Framework. *Drones* **2021**, *5*, 17. [CrossRef]
47. Sakellariou, S.; Tampekis, S.; Samara, F.; Sfougaris, A.; Christopoulou, O. Review of state-of-the-art decision support systems (DSSs) for prevention and suppression of forest fires. *J. For. Res.* **2017**, *28*, 1107–1117. [CrossRef]
48. Vahdati, M.; Gholizadeh HamlAbadi, K.; Saghiri, A.M. IoT-Based Healthcare Monitoring Using Blockchain. In *Applications of Blockchain in Healthcare*; Namasudra, S., Deka, G.C., Eds.; Springer: Singapore, 2021; pp. 141–170. [CrossRef]
49. Mhaisen, N.; Fetais, N.; Erbad, A.; Mohamed, A.; Guizani, M. To chain or not to chain: A reinforcement learning approach for blockchain-enabled IoT monitoring applications. *Future Gener. Comput. Syst.* **2020**, *111*, 39–51. [CrossRef]
50. Hathaliya, J.; Sharma, P.; Tanwar, S.; Gupta, R. Blockchain-Based Remote Patient Monitoring in Healthcare 4.0. In Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing (IACC), Tiruchirappalli, India, 13–14 December 2019; pp. 87–91. [CrossRef]
51. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives. *J. Food Qual.* **2021**, *2021*, 7608296. [CrossRef]
52. Barka, E.; Dahmane, S.; Kerrache, C.A.; Khayat, M.; Sallabi, F. STHM: A Secured and Trusted Healthcare Monitoring Architecture Using SDN and Blockchain. *Electronics* **2021**, *10*, 1787. [CrossRef]
53. Khan, A.A.; Laghari, A.A.; Liu, D.-S.; Shaikh, A.A.; Ma, D.-D.; Wang, C.-Y.; Wagan, A.A. EPS-Ledger: Blockchain Hyperledger Sawtooth-Enabled Distributed Power Systems Chain of Operation and Control Node Privacy and Security. *Electronics* **2021**, *10*, 2395. [CrossRef]
54. Górski, T.; Bednarski, J.; Chaczko, Z. Blockchain-based renewable energy exchange management system. In Proceedings of the 2018 26th International Conference on Systems Engineering (ICSEng), Sydney, NSW, Australia, 18–20 December 2018; pp. 1–6. [CrossRef]
55. Van Cutsem, O.; Ho Dac, D.; Boudou, P.; Kayal, M. Cooperative energy management of a community of smart-buildings: A Blockchain approach. *Int. J. Electr. Power Energy Syst.* **2020**, *117*, 105643. [CrossRef]
56. Alcarria, R.; Bordel, B.; Robles, T.; Martín, D.; Manso-Callejo, M.-Á. A Blockchain-Based Authorization System for Trustworthy Resource Monitoring and Trading in Smart Communities. *Sensors* **2018**, *18*, 3561. [CrossRef]
57. Majd, A.; Loni, M.; Sahebi, G.; Daneshtalab, M. Improving Motion Safety and Efficiency of Intelligent Autonomous Swarm of Drones. *Drones* **2020**, *4*, 48. [CrossRef]
58. Dawaliby, S.; Aberkane, A.; Bradai, A. Blockchain-Based IoT Platform for Autonomous Drone Operations Management. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; pp. 31–36.
59. Košťál, K.; Helebrandt, P.; Belluš, M.; Ries, M.; Kotuliak, I. Management and Monitoring of IoT Devices Using Blockchain. *Sensors* **2019**, *19*, 856. [CrossRef]
60. Torky, M.; El-Dosuky, M.; Goda, E.; Snášel, V.; Hassanien, A.E. Scheduling and Securing Drone Charging System Using Particle Swarm Optimization and Blockchain Technology. *Drones* **2022**, *6*, 237. [CrossRef]
61. Rathore, S.; Wook Kwon, B.; Park, J.H. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *J. Netw. Comput. Appl.* **2019**, *143*, 167–177. [CrossRef]
62. Firefighting Drones Help Localities Battle Blazes in the Wild and in Cities. Available online: https://edms.energy.gov/Articles/Firefighting%20Drones%20Help%20Localities%20Battle%20Blazes%20in%20the%20Wild%20and%20in%20Cities.aspx (accessed on 21 December 2021).
63. Alsamhi, S.H.; Lee, B.; Guizani, M.; Kumar, N.; Qiao, Y.; Liu, X. Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: Framework and proposed solutions. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4255. [CrossRef]

64. Roan, A. How to Test Ethereum Smart Contracts. Better Programming. Available online: https://betterprogramming.pub/how-to-test-ethereum-smart-contracts-35abc8fa199d (accessed on 23 March 2020).
65. How fast can Drones Fly? Available online: https://dronesgator.com/how-fast-can-drones-fly (accessed on 25 October 2022).
66. Fire Extinguishers. Available online: https://en.wikipedia.org/wiki/Fire_extinguisher (accessed on 15 September 2022).
67. Kumar, M.; Cohen, K.; HomChaudhuri, B. Cooperative Control of Multiple Uninhabited Aerial Vehicles for Monitoring and Fighting Wildfires. *J. Aerosp. Comput. Inf. Commun.* **2011**, *8*, 1–16. [CrossRef]
68. Feng, C.; Yu, K.; Bashir, A.; AI-Otaibi, Y.; Lu, Y.; Chen, S.; Zhang, D. Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach. *IEEE Netw.* **2020**, *35*, 130–137. [CrossRef]
69. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 1–36. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 29 October 2021).
70. Li, B.; Fei, Z.; Zhang, Y. UAV Communications for 5G and Beyond: Recent Advances and Future Trends. *IEEE Internet Things J.* **2019**, *6*, 2241–2263. [CrossRef]
71. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538. [CrossRef]