applied sciences

MDPI

Article

Competing Miners: A Synergetic Solution for Combining Blockchain and Edge Computing in Unmanned Aerial Vehicle Networks

Jacob Mathias Nilsen [1], Jun-Hyun Park [1], Sangseok Yun [2], Jae-Mo Kang [1,*] and Heechul Jung [1,*]

[1] Department of Artificial Intelligence, Kyungpook National University, Daegu 41566, Korea; jacobmnilsen@gmail.com (J.M.N.); wnsgus126@knu.ac.kr (J.-H.P.)
[2] Department of Information and Communications Engineering, Pukyong National University, Busan 48513, Korea; ssyun@pknu.ac.kr
* Correspondence: jmkang@knu.ac.kr (J.-M.K.); heechul@knu.ac.kr (H.J.)

Abstract: Edge computing (EC) is very useful and particularly promising for many practical unmanned aerial vehicle (UAV) applications. Integrating the blockchain to this technology strengthens privacy protection and data integrity and also prevents data from being easily leaked. However, the required operations in the blockchain are computationally heavy because a blockchain requires devices to solve a complicated proof-of-work (PoW) puzzle to add new data (i.e., a block) to the blockchain. Solving a PoW requires substantial amounts of time and energy, which are big concerns for UAVs. In this article, we suggest a synergetic solution to address this issue based on multiple competing miners in a blockchain. Specifically, we present two novel frameworks for combining the blockchain and EC to effectively overcome several critical limitations when applying the blockchain to UAV and EC tasks, respectively. The goal of both of these proposed frameworks is to reduce both the time spent on mining and the energy consumption for the EC. We first look at the fundamentals of the blockchain with competing miners. Then, our proposed frameworks are described with experimental results, through which important insights are drawn. We finally discuss application scenarios for our proposed frameworks, the related technical challenges, and future research directions.

Keywords: blockchain; competing miners; edge computing; Internet of Things; proof-of-work; unmanned aerial vehicle

Citation: Nilsen, J.M.; Park, J.-H.; Yun, S.; Kang, J.-M.; Jung, H. Competing Miners: A Synergetic Solution for Combining Blockchain and Edge Computing in Unmanned Aerial Vehicle Networks. *Appl. Sci.* **2022**, *12*, 2581. https://doi.org/10.3390/app12052581

Academic Editor: Agostino Forestiero

Received: 9 February 2022
Accepted: 28 February 2022
Published: 2 March 2022

1. Introduction

1.1. Blockchain

The blockchain, which was first conceptualized in 2008 [1], has been proven to outperform other centralized ledger approaches that suffer from low efficiency owing to bottleneck, single point of failure, security attacks, and moral hazards [2]. Specifically, the blockchain is an open distributed (yet secured) database where data are distributed across many devices and the chain (i.e., sequence of data) is entirely decentralized. This means that no single user or participant has control over the blockchain, which implies that the data cannot easily be faked or changed without being logged in the history of the chain, unlike the centralized approach.

The blockchain strengthens the integrity and validity of the data by using a demanding computation-heavy puzzle called the proof-of-work (PoW). The computational process required to solve the PoW puzzle is called mining, and the time spent on mining a block depends on the difficulty degree (or level) of the PoW puzzle. A normal or standard blockchain employs only a single miner per device in the network, and this miner solely has to solve the computationally heavy PoW puzzle to infer the hash value of the block. The critical problem of the blockchain with a single miner is that it often requires large amounts of time and energy for mining, which is indeed very challenging for mobile devices (e.g., IoT sensors and unmanned aerial vehicles (UAVs) in practical applications).

The above-mentioned problem has also been introduced in earlier studies [3,4]. One possible way to resolve this problem could be to make the transactions in the blockchain quicker by increasing the mining speed. In this article, we propose a framework of two or more competing miners (i.e., two or more miners in the blockchain that try to solve the same PoW hash for a specific block the fastest) to improve the mining time. Recent studies that research the improvement of mining time are faint. The studies that are available include using an inner for-loop [3] as well as implementing parallel mining [4] for speeding up blockchain mining. The study that introduces parallel mining [4] is the closest we found compared to our framework of competing miners. In [4], however, the results were not significant enough, and thus, in this work, we try to improve the mining time even further by employing competing miners instead of parallel miners (i.e., two or more miners in the blockchain that try to solve the hash on the same transactional data but with different nonce values for each miner).

1.2. Edge Computing in UAV Networks

With traditional cloud computing, data have to be sent all the way to the cloud, which often has a high time latency, resulting in slow processing rates. To solve this issue, edge computing (EC) has been proposed. With EC, the data can be processed on the edge, which is not only much closer to where the data are being created but also better than the original approach for preserving privacy [5,6]. In EC, local data centers and servers are deployed by a service provider at the edge of mobile networks, such as the base stations of radio access networks [2]. These data centers often have sufficient computational resources to be able to handle heavy tasks. One of the key considerations of EC is overcoming network latency.

Because many Internet of Things (IoT) applications and UAVs require fast response time (i.e., the time required to offload and compute data), sending data all the way to the cloud as in traditional cloud computing may result in serious problems in practice. For instance, a safety control system that operates an industrial machine may need to stop immediately if a human is too close. A delayed response time may cause serious harm to the person or damage the machine. Autonomous vehicles/UAVs face the same problem because they usually require a fast response time below 20 ms [7]. This short response time cannot be achieved by traditional cloud computing, but moving the processing of the sensor or device to the edge (i.e., EC) can be a promising and viable way to achieve the desired response time.

Another major concern for traditional cloud computing is its cost. As we can see in Figure 1, with EC, the data can be properly filtered and processed before they are sent to the cloud such that the network cost of data transmission is effectively reduced while also reducing the cost of cloud storage. For example, a mobile temperature device sensor that reports a reading of 20 °C every second might not be informative, but once it starts reading 40 °C, the data become more informative. If the traditional cloud architecture is combined with EC, then the users can reduce the latency by uploading continuously to the close edge server. When uploads reach a set number, the edge server can filter these data and then send it to the cloud for storing. However, in EC, because UAVs are most often deployed in the public to gather data [7–9], some privacy concerns still exist; for example, the data can be exposed to malicious secrecy attacks or overhearing by eavesdroppers and/or possibly by other mobile devices as well as UAVs. In particular, during the offloading process from UAVs to the edge server, data are vulnerable to an attack.

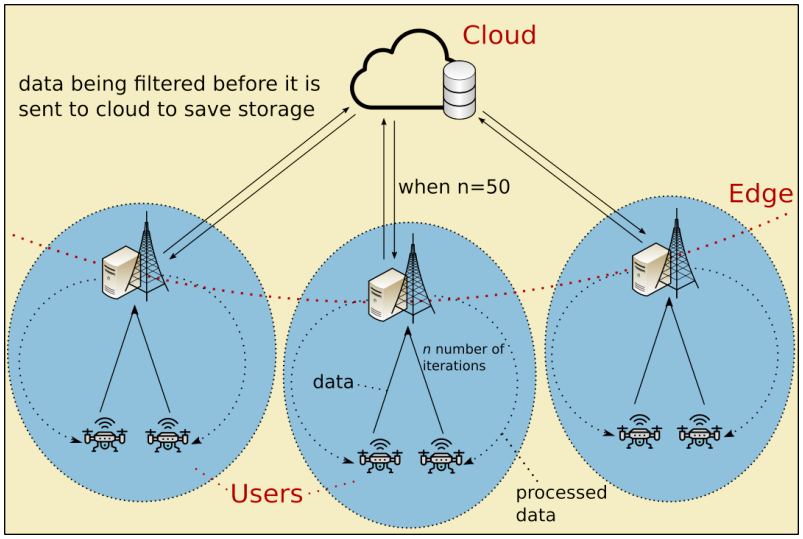

Figure 1. EC combined with cloud.

1.3. Blockchain Combined with Edge Computing in UAV Networks

The blockchain is a very promising and emerging solution to resolve the security issue of EC in many practical applications, such as IoT [10], autonomous vehicles [11], smart homes [12], and healthcare [13]. However, owing to the heavy computational burden for solving the PoW, some resource-limited nodes, such as UAVs/mobile devices, need to use considerable processing power and sacrifice considerable time to participate in mining and consensus processes [14], which is indeed a major challenge in applying the blockchain to EC applications as well as UAVs and other mobile applications [2]. In this study, we investigate how such issues can be effectively addressed by employing competing miners in the blockchain.

EC is very promising and useful to alleviate the computational burden of devices because computing tasks can be offloaded to the edge servers having more computational resources. Although the blockchain is being recognized as an appealing solution for EC (and vice versa), its potential benefits and synergetic aspects have not yet been fully revealed, especially in terms of latency and energy consumption. To the best of our knowledge, very few reports [2,15–17] have studied the issue of the blockchain in EC. However, in those studies, the simplistic situation of only a single miner is considered. In addition, in those studies, the focus is not on improving the energy consumption and latency of the EC network, as we propose with our framework, but to improve the security and aid the blockchain with computational resources. In addition, we have found no current papers that study the issue of the amount of computational resources needed in a blockchain-empowered UAV network. Performing a blockchain operation requires a lot of computational resources, which are very limited on UAVs. Therefore, in this paper, we conduct research on how these issues could be resolved.

1.4. Study Overview

In this study, we first describe the basic overview and key concepts of the blockchain with competing miners. Then, we present the raw results of competing miners in a blockchain for improving the mining time. These results are compared to the other available results in Hazari et al. [4], where parallel mining was introduced. The results from the mentioned paper can be further improved by our proposed framework, which could outperform existing research and create an improved baseline for being combined with other technologies.

Following this, we present our proposed frameworks for combining the blockchain and EC. Two possible scenarios are considered. In the first scenario, the computing task of solving the PoW puzzle in the blockchain is offloaded from UAVs to edge servers, and the

goal is to reduce the time spent on mining with the aid of EC while simultaneously increasing the security of the data. The proposed framework for this scenario will be referred to as the EC-enabled blockchain network with multiple competing miners, which is called an EC-enabled blockchain. This framework can actually be considered a generalization of the concept of the blockchain with competing miners proposed by Xiong et al. [2].

In the second scenario, we exploit the blockchain for offloading data from UAVs to edge servers by employing competing miners hierarchically. Our novel framework proposed for this scenario will be referred to as blockchained EC with hierarchical competing miners, or as blockchained EC for short. The goal of blockchained EC is to improve the security of the offloaded data while reducing energy consumption and latency on the UAVs. Furthermore, we present experimental results for both frameworks with some important insights. Finally, several important application scenarios for our proposed frameworks are discussed, followed by a description of related technical challenges and future research directions.

2. Related Works

2.1. Parallel PoW Mining

The ability to reduce the time spent on mining a PoW puzzle can have great benefits, as it will result in less energy and time consumption, opening up more opportunities and combinations with different technologies (i.e, technologies that are dependent on low energy and time usage). It is very hard to reduce the time spent on mining, and thus, this topic has remained mostly untouched, except for in [3,4,18]. The authors in Adewumi et al. [3] suggest implementing a population-based inner for-loop approach, as introduced in their earlier research [18], instead of using the standard brute force approach. Another technique that has been researched is parallel PoW mining [4]. The authors in this paper improve the standard brute force approach by adding parallel miners. The proposed method is designed so that all parallel miners use the same transaction data but with a different nonces, ensuring that no two miners perform the same work. To ensure this, they implement a manager that has control over the subordinates (i.e., parallel miners). This manager has to ensure that no two miners use the same nonce value and that all miners use the same transactional data. The manager also has the overview of which miner finishes which block and gives the mining reward accordingly. This paper is also the only one that provides numerical results for mining speed in its experiments.

2.2. Blockchain in UAV Networks

The authors in [19] introduce a way to make UAV networks safer by using the blockchain to secure them. They mention that even with the advantages of 5G networks, there are still some vulnerabilities in security, especially when extracting data from UAVs. This problem is also addressed in [20], where the authors focus on the data collected from IoT devices. Both of the papers agree that using a blockchain network is great for storing the data securely against attacks, as the data is encrypted and well hidden behind hashes. The authors in [21,22] discuss the issues of UAVs in healthcare and how these issues can be solved with the blockchain. They touch upon the subject of the UAV systems having security, reliability, latency, and storage cost issues and how these problems can be solved with their solution. Specifically, in [22], the authors focus on path planning for the UAVs to provide privacy-preservation in Healthcare 4.0. The authors in [23–26] discuss the issue of UAVs in data acquisition schemes in IoT and how the data are so open and vulnerable to malicious attacks. They introduce how a blockchain can help with making the data more secure, which is vital in IoT networks, where many important data are shared. All of these papers that use the PoW approach use a single miner to encrypt and store the data.

3. Concept and Working Principle of Competing Miners in a Blockchain

3.1. Proof-of-Work

The blockchain has a few different processes of how to verify the integrity and validity of the data in the chain [27]. The most common process is the PoW. This process allows the transactions inside a blockchain to be verified without the use of a third party.

The PoW is the most commonly used process amongst the blockchains. It was reported in 2016 that the PoW was being used in more than 90% of the total existing digital cryptocurrencies [27]. The PoW is based on cryptography, which is an advanced form of mathematics. However, since advanced mathematical equations are used, only powerful computers are able to solve the PoW if the difficulty is set too high. This results in not only a significant amount of electricity used but also a very limited number of transactions that can be processed at the same time. In Table 1 we can see the transaction speed of different existing cryptocurrencies, each with different settings on their verification process.

Table 1. Transaction speed of different cryptocurrencies.

Cryptocurrency	Transactions per Second	Average Transaction Confirmation Time
Bitcoin	3–7	25 min
Ethereum	15–20	2 min
Ripple	1500	4 s
Bitcoin Cash	61	60 min
Cardano	5–7	3–5 min
Litecoin	26	30 min
Monero	4	30 min
Neo	1000	15–20 s
Dash	48	2–10 min

The Definition of Difficulty

In the PoW, difficulty is a measurement of how difficult it is to mine a block in a blockchain. Setting the difficulty level to high means that it would take additional computing power to be able to verify the transactions entered on a blockchain. This process is also called mining. In cryptocurrency, difficulty is used as a parameter to keep the average time between blocks steady as the network's hash power changes.

Having a high difficulty level can be of significant importance because of the security it provides. When a hash is created, it starts with the difficulty of 0. This is because the hash is deterministic, meaning that it will remain the same as long as the data on which the hash is created are the same. In other words, there is no added complexity to the solving of the hash. To add difficulty to a hash, the PoW uses something called a nonce, which is an abbreviation of "number only used once". Nonces are added at the start of the hash as random strings, and the level of difficulty determines how many nonces are added. Since the nonce is a random unpredictable string, the complexity multiplies every time a new nonce is added. Figure 2 shows what a PoW hash with a difficulty level of 5 will typically look like.

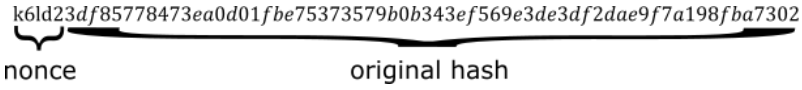

Figure 2. PoW hash.

The original hash will always stay the same, while the nonce will increase or decrease based on the difficulty level set by the blockchain.

3.2. The Concept of Competing Miners

Figure 3 shows the concept of a blockchain with competing miners on each participant. (In the EC-enabled blockchain, the participant refers to the edge server. In blockchained EC, it refers to a UAV.) A blockchain with competing miners works as follows:

- First, the data created by a participant are sent to multiple competing miners (not a particular single miner, as in the traditional blockchain) to solve the PoW and create a block (step (1) in Figure 3).
- Second, the data are mined by a set amount of competing miners per participant, where they compete on being the first to mine the data into a block (step (2) in Figure 3; in this case, K = 2 miners).
- Third, after mining is finished, the block is sent back to the participant for identification (step (3) in Figure 3). Specifically, if two or more miners complete the mining task almost at the same time, then the participant has to identify which miner completed it first.
- Finally, the participant then broadcasts the mined block to the other participants in the network by performing a cross verification (step (4) in Figure 3), and the cross-verified block is then added to the blockchain (step (5) in Figure 3).

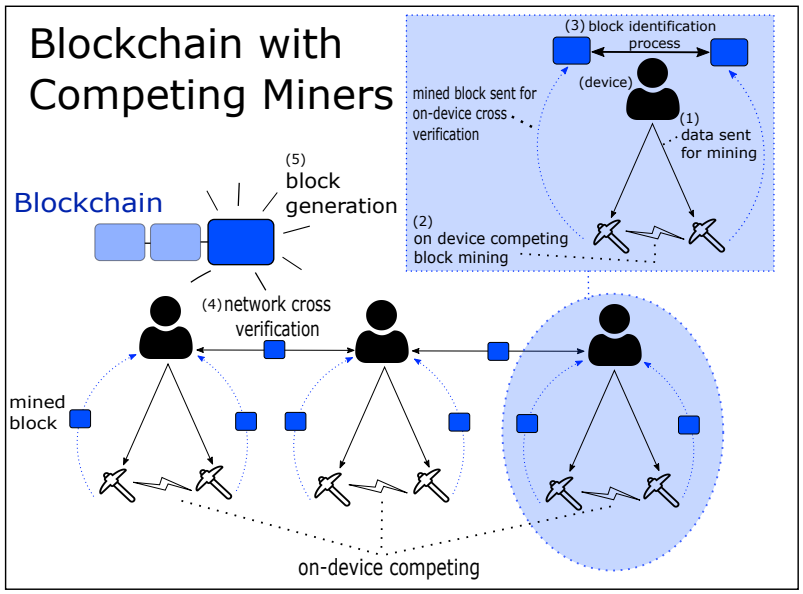

Figure 3. The concept of blockchain with competing miners.

A blockchain with multiple competing miners requires much less time for solving the PoW compared to a traditional blockchain that employs only a single miner. This significant benefit in turn enables a lower latency and less energy consumption for many EC applications, such as IoT [28,29], autonomous vehicles and UAVs [11], and healthcare [30]. The details will be investigated in the following sections. The intuitive reason for this benefit is as follows: In the blockchain, the miner solves the PoW by randomly guessing the hash value, which means that the time spent for completing the mining task is random. Thus, if we employ more miners in the blockchain, then the chance of solving the PoW more quickly increases. Mathematically, this result can be shown as follows: Let t_i denote the time spent by miner i for completing the mining task. If there are a total of K miners, the completion time is (approximately) given by $t = \min\{t_1, t_2, \cdots, t_K\}$, which is a random sequence that is monotonically decreasing in the number K of miners. Thus, t decreases as K increases.

The idea behind lower energy consumption is that with more miners, the time spent on mining reduces. Therefore, less computing resources are used, which results in less energy consumed. However, the computing capabilities of a device come to a limit. In other words, employing too many miners, more than the device can handle, in the end, requires too many computing resources, which can result in more energy being used.

4. Proposed Frameworks with the Utilization of Competing Miners

4.1. The Impact of Competing Miners in a Blockchain

As discussed in the earlier sections, having miners compete with each other on device (i.e., UAV) is expected to require much less time for solving the PoW compared to a traditional blockchain that employs only a single miner. In our proposed framework, to improve the mining speed, we employ two or more miners on device and make them compete with each other. The miners are all split into different processes, which makes it easier for a manager to have control over them. They are all trying to solve the same PoW hash, and when a miner solves the PoW hash, it gets a reward as an incentive and the other miners are stopped so that no extra computing resources are used. Our proposed improvement is compared to the conventional improvement made in Hazari et al. [4], where the miners are set to solve different PoW hashes but on the same block.

Experiments and Results

To ensure that our research and the research with the parallel miners are fairly compared, we conducted the experiments based on the premises set in Hazari et al. [4]. The CPU clock speed was set to 2.2 GHz with 4GB allocated RAM on a Windows operating system. The blockchain was made in Python and each miner was given just 10% of the total resources available. The numerical results from the experiments that were conducted are presented by Table 2 and Figure 4.

Table 2. Comparison of parallel miners vs. competing miners in average mining time per difficulty level.

Avg Mining Time (Seconds)/Difficulty	Single (1) Miner	3 Parallel Miners	5 Parallel Miners	3 Competing Miners	5 Competing Miners
D = 5	60	53	45	23	18
D = 6	24	180	160	159	90
D = 7	895	710	590	531	450

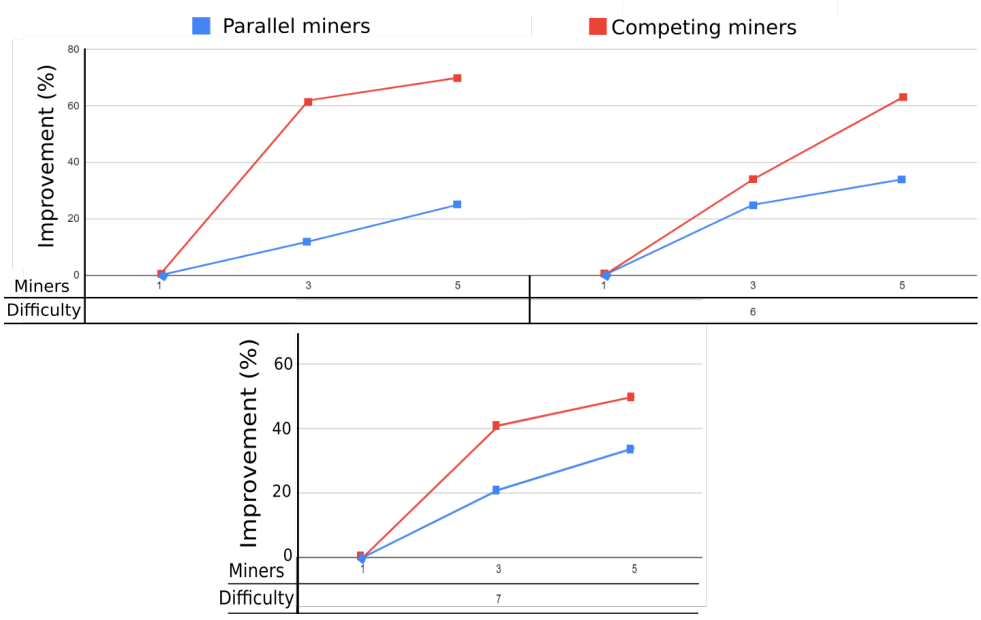

Figure 4. Improvement percentage of parallel and competing miners compared to a single miner.

In Table 2, we can observe how our proposed method of competing miners compares to that of parallel miners proposed in Hazari et al. [4]. The results are given by the average time to mine a block by each difficulty level D. By a quick glance, we can easily see that the proposed scheme of competing miners achieves a better and faster mining time than the opposition. At a low difficulty level, the proposed scheme with competing miners has an average mining speed that is more than double as fast as the parallel miners, which

is an amazing improvement. Looking at the higher difficulty levels, we discover that the competing miners still have a better performance, but the gap seems to be closing in.

This is also depicted in Figure 4, where both of the frameworks are put against each other to see how much, in percentage, they improve compared to the single miner at each difficulty level. The huge difference we see in Table 2 is confirmed by the large gap between the lines in this graph, where the framework of competing miners reaches a maximum of 70% improvement from the case of a single miner.

When comparing the competing miners with the parallel miners, we find some interesting insights. To begin with, the framework of competing miners performs much better than that of parallel miners at a lower difficulty level than it does when the difficulty increases. The biggest gap is at three miners solving the PoW with difficulty level set to 5. In this parameter, the competing miners achieve a substantial 50% higher improvement than the parallel miners. However, increasing the difficulty seems to decrease the gap between the two frameworks. A possible reason behind this can be the limitations of computing resources set by the author in Hazari et al. [4]. This experiment was only given a limited amount of resources, which resulted in problems when scaling and wanting to solve more complex equations. Owing to this, we believe that when given an unlimited amount of computing resources, the competing miners would continue to perform better with high improvement percentage, since it would not be limited any longer, and therefore continue to outperform the parallel miners.

In the following sections, we will present two novel frameworks for combining the blockchain and EC, namely, the EC-enabled blockchain and blockchained EC, respectively. In both of our proposed frameworks, multiple competing miners (rather than a single miner) are employed in the blockchain to reduce the time spent on mining, latency, and energy consumption for EC.

4.2. EC-Enabled Blockchain Network with Multiple Competing Miners

The critical limitation of the blockchain for practical IoT/UAV applications (such as transportation and autonomous driving) is that to solve the PoW puzzles and reach a consensus, a huge amount of computing resources (such as time and energy) is required at the IoT/UAVs, which, however, have strictly limited computing capability with limited energy. If multiple competing miners are employed in the blockchain, the required computing resources are quite high. As we introduced in Section 1.2, EC is very promising and useful to alleviate the computational burden of devices because computing tasks can be offloaded to the (nearest) edge servers, since the edge servers have more computational resources and are not limited by energy. Motivated by this, in this article, we suggest using EC as a means to overcome the above-mentioned limitations of the blockchain. Specifically, in an EC-enabled blockchain, the required mining tasks in the blockchain are offloaded to edge servers and each edge server further employs multiple competing miners to substantially reduce the time spent on mining. This novel framework is called the EC-enabled blockchain and is depicted in Figure 5.

As depicted in Figure 5, in the EC-enabled blockchain, the data acquired by each device for mining are offloaded to an edge server. By employing competing miners, the edge server then performs the mining task; after which, the mined data are added to the blockchain. By offloading the mining tasks, the computational burden of the device owing to the mining task can be substantially reduced, as the mining tasks are carried out completely on edge servers, which have enough computing resources and thus the capability to execute the mining task even with many competing miners. Because of the sufficient computing resources and capability, the edge server can generally employ a number of competing miners (much more miners than on the device); thus, the time spent on mining can be substantially reduced. In addition, since all the tasks are being executed on the edge server, the communication time between the edge device and the edge server remain the same for each task, both on the framework proposed in Xiong et al. [2] and in our proposed framework. For this reason, we have chosen to only show the benefits of using

EC's computational resources to aid in blockchain mining. Furthermore, by combining EC with the blockchain, there will be a significant improvement when it comes to security. Having the data stored in a blockchain network eliminates the single point of failure (i.e., when all of the data is being stored in a single place, thus leading to a high security risk if that place is hacked or compromised), which can be a problem when storing important data on the cloud. The data are stored on all participants that are connected to the blockchain network, and even though one participant is a victim to malicious attacks, the data will still be safe until the whole network is compromised. An attacker would need to control more than half of all the devices in the network before getting access to the encrypted data, which is practically impossible [31].

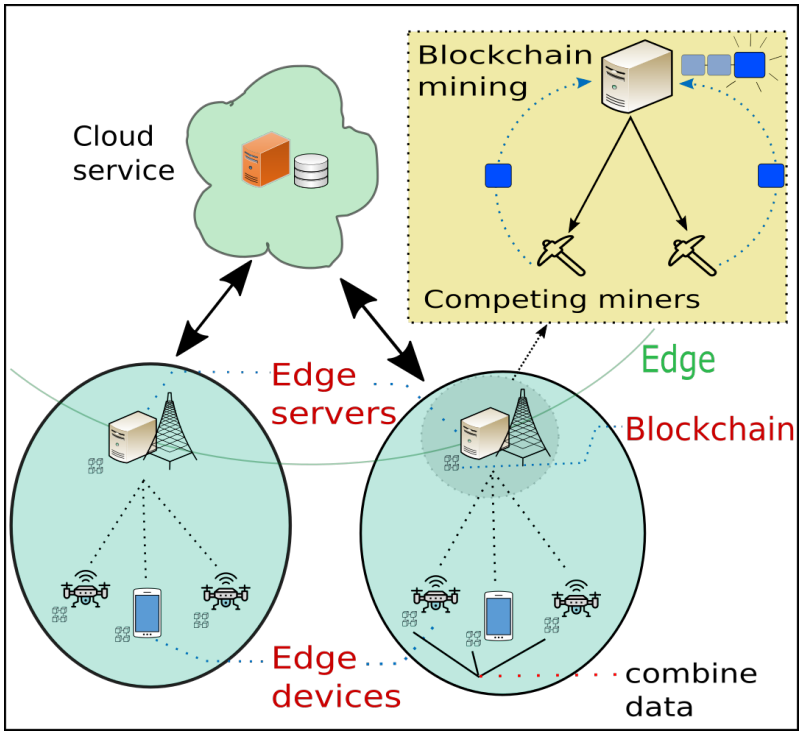

Figure 5. EC-enabled blockchain network with multiple competing miners.

Experiments and Results

To confirm the above-mentioned benefits, in Figure 6, the time spent on mining on the edge server is plotted against the number of mining tasks for the case of competing miners. The numerical simulations were performed on a Windows operating system with a Ryzen 7 series 3700x CPU. We created a simple blockchain in Python where we could change the difficulty for every simulation. The blockchain included from and to addresses, an amount in currency, data to be sent, and the hash of the previous block. To make the simulations as similar and fair as possible, we ran all of the experiments on the same parameters, which we copied from Xiong et al. [2]. The difficulty level of the PoW, which was described in Section 2.1 (denoted by D), was set to D = 5. We could also specify the number of mining tasks in our blockchain, where, in this case, we simulated up to 100 mining tasks per scenario.

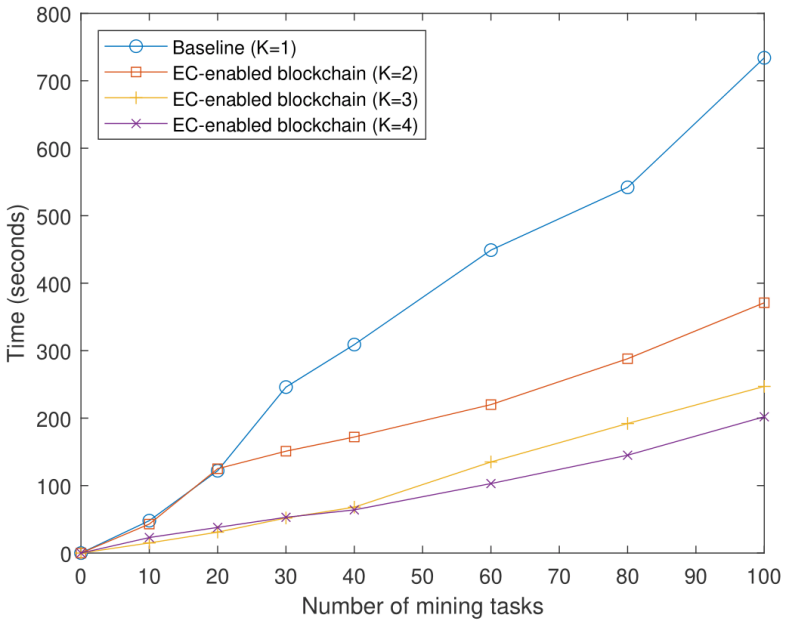

Figure 6. Time spent for the mining tasks on the edge server in the EC-enabled blockchain versus the number of mining tasks for different numbers (K) of competing miners.

As shown in Figure 6, the blockchain with multiple competing miners considerably outperforms the baseline (i.e., the blockchain with a single miner). Additionally, from Figure 6, the following observations can be made, and some interesting insights can be drawn. First, for the case of a small number of mining tasks (e.g., when it is less than 20 or 30), the blockchain with two miners achieves almost the same performance as the baseline; thus, there is not a significant performance gain in this regime. Interestingly, we also observe that when the number of mining tasks is small, the case of three miners performs better than the case of four miners.

Finally, for the case of a large number of mining tasks (e.g., when the number of mining tasks exceeds 20 or 30), even a blockchain with two miners considerably outperforms the baseline; specifically, its time spent on mining is almost two times faster than that of the baseline. This is in agreement with our earlier analysis in Section 2. Additionally, in this regime, the case of four miners yields the best performance, as expected.

In this framework, there are some positive sides when addressing scalability. As we observe with the case of a small number of mining tasks, there is no significant performance gain. Therefore, in some practical applications with a small number of mining tasks, or equivalently, a small number of devices, employing only a single miner is sufficient and there is no need to employ multiple competing miners for efficiency. Meanwhile, when the number of mining tasks is small, the case of three miners performs better than the case of four miners. Thus, in practice, one should carefully and judiciously choose the number of miners according to the number of mining tasks. From the results shown in Figure 6, one can expect that in practical applications with a large number of mining tasks (or devices), there will be a significant and meaningful performance gain; thus, one should employ multiple competing miners for better performance. In addition, as explained in Section 3.2, by adding the blockchain to EC, the security is increased. Moreover, single point of failure is eliminated, making the network more robust when dealing with malicious attacks. It clearly shows how much EC can benefit from adding the blockchain with competing miners to its network, not only in faster mining speed but also when it comes to security.

4.3. Blockchained EC with Hierarchical Competing Miners

EC typically involves the following two phases: (i) first, the device offloads its data to the closest edge server (i.e., offloading phase); (ii) the edge server performs the computing

task for the offloaded data (i.e., computing phase). The practical and critical issue of EC is that the offloading phase is exposed to eavesdropping and is even vulnerable to some malicious secrecy attacks. To resolve this issue and strengthen the security during the offloading phase of EC, in this article, we suggest applying the blockchain to the offloading phase of the EC. In particular, we employ multiple competing miners hierarchically. This novel framework is called blockchained EC and is depicted in Figure 7.

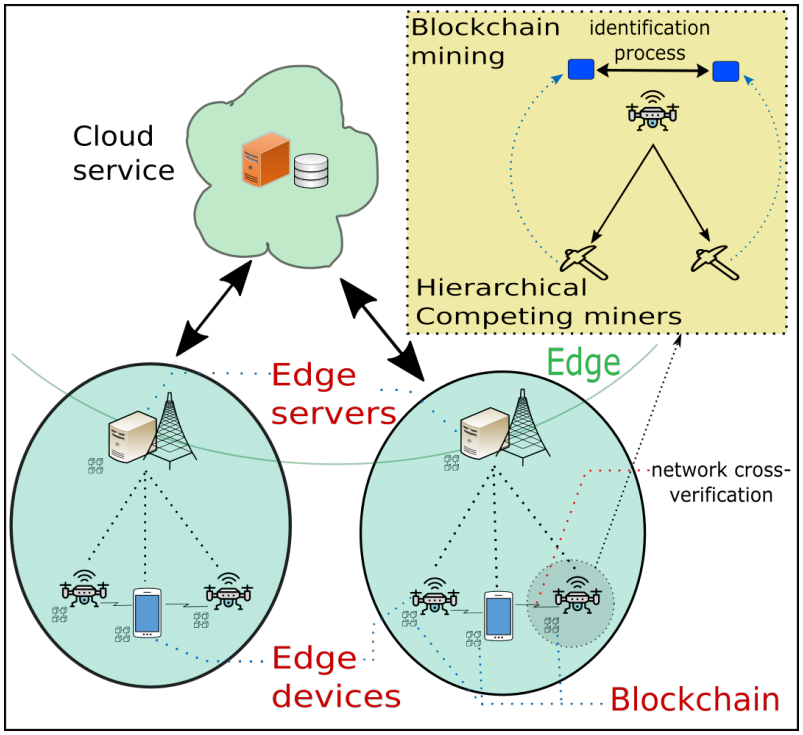

Figure 7. Blockchained EC with hierarchical competing miners.

As shown in Figure 7, blockchained EC works as follows: First, the data acquired by each device are sent to other devices in the same network to start the mining task. In each device, we employ multiple competing miners (rather than a single miner) for better support. When the competing miners on each device finish the mining task, they send the mined block to the device for identification. Afterwards, the devices in the network compete again with each other. Through this competition, the block mined first is identified and is finally added to the blockchain. Overall, in blockchained EC, the competition occurs first over the miners on each device and then over the devices in the network, consequently forming a hierarchy of competitions. Through this framework, the security could be significantly increased, not only by encrypting the data before it leaves the devices but also by eliminating the single point of failure as explained in Section 3.2.

Experiments and Results

The experiments in this section used the same CPU, experiment environment, methods, and base parameters as those used in Section 4.2. We first ran experiments on different numbers of mining tasks to see if the offloading time was different for a higher number of tasks, and the results are depicted in Figure 8. In Figure 8 the experiment was done on K = 1 to 4 miners. However, since our framework does not focus on lowering the offloading time but on lowering the total latency overall, there was no difference in offloading time for different amounts of competing miners. As we can observe, there is a stable rise in offloading time as the number of mining tasks increases. At a low number of mining tasks, the offloading time is around 0.02 s, while it increases to 0.14 s at a high number of mining tasks.

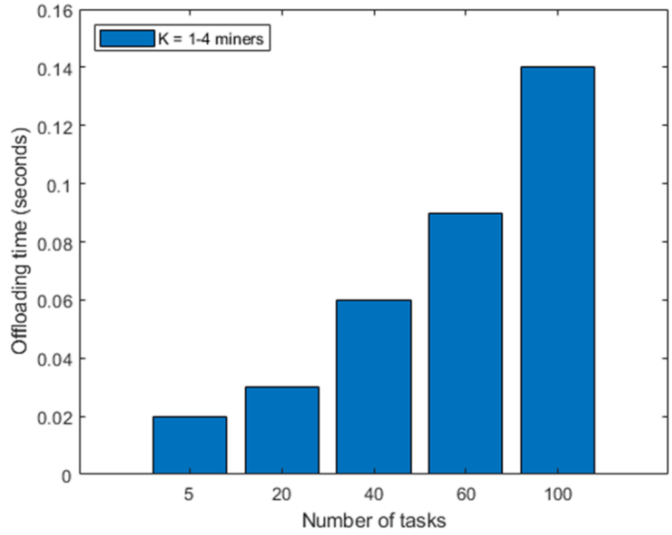

Figure 8. Offloading time for each number of mining tasks.

Based on the discussions in Section 2, one can naturally expect that hierarchically competing miners can achieve a higher performance compared with the case of only a single miner and even for the case of competing miners solely on each device. To confirm this, in Figures 9 and 10, the average latency required for mining and offloading in blockchained EC and the corresponding energy consumption are plotted for various values of difficulty level D. For these figures, we consider an EC network with three devices and one edge server. Additionally, the number K of hierarchical competing miners ranged from two to four and the number of mining tasks was set to 100. At most, four miners were used to make the experiments more realistic, as most UAVs do not have enough resources (i.e., processing power) to employ more miners. In Figures 9 and 10, the performance for the case of K = 1 is also presented as a baseline. In Figure 9, the combined times from blockchain mining and the offloading time are added together and shown as average latency.

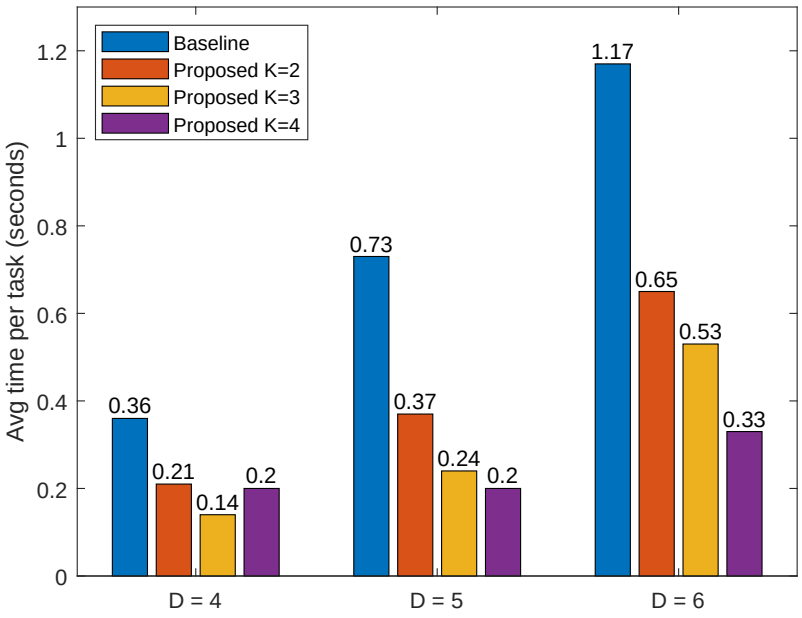

Figure 9. Average latency required for mining and offloading in blockchained EC versus difficulty level D for different numbers (K) of hierarchical competing miners.

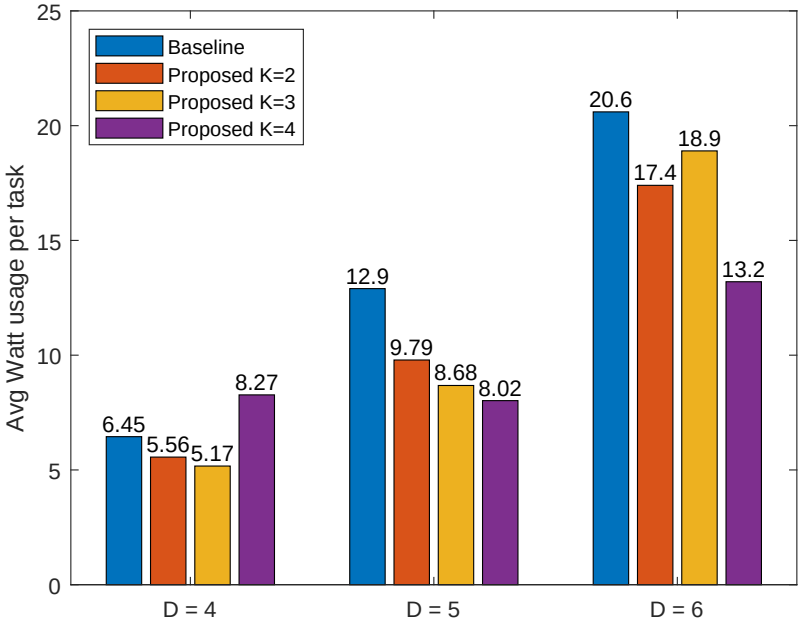

Figure 10. Average energy consumption versus difficulty level D for different numbers (K) of hierarchical competing miners.

According to the results shown in Figures 9 and 10, blockchained EC performs much better than the baseline in terms of latency and energy consumption. As expected, the case of four miners yields the best performance at the high difficulty level (i.e., D = 6). Interestingly, however, we observe that at the low difficulty level (i.e., D = 4), the case of three miners yields the best performance (rather than the case of four miners).

Finally, in Table 3, by comparing the performance of the baseline and blockchained EC with K = 3 when D = 4, we find that the latter is 157% (i.e., 2.5 times) faster than the former in terms of latency. When D = 5, we can observe that K = 4 is, incredibly, 231% (i.e., 3.3 times) faster than the baseline, which is a significant improvement. In our last experiment, when D = 6, we find that blockchained EC with K = 4 still outperforms the others, with an amazing 254% (i.e., 3.5 times) faster mining speed.

Table 3. Average latency by K = 1, 2, 3, 4 with faster than the baseline presented in percentage.

Avg Latency (Seconds)	D = 4	D = 5	D = 6
Baseline (single miner)	0.36	0.73	1.17
Blockchained EC (K = 2)	0.21 (71%)	0.37 (97%)	0.65 (80%)
Blockchained EC (K = 3)	0.14 (157%)	0.25 (192%)	0.53 (120%)
Blockchained EC (K = 4)	0.20 (80%)	0.22 (231%)	0.33 (254%)

When compared to the watt usage, the biggest difference is observed with K = 3 miners, as shown in Table 4. When K = 3 miners are used, the energy consumption is 24% less than the baseline, while using K = 4 miners interestingly proves to consume more energy than the baseline. When D = 5 and D = 6, the case of K = 4 outperforms the others, with 60% and 56% less energy usage, respectively, than that of the baseline of only a single miner, which validates the effectiveness and superiority of our proposed framework.

Table 4. Average watt usage by K = 1, 2, 3, 4, with less usage than the baseline presented in percentage.

Avg Usage (Watt)	D = 4	D = 5	D = 6
Baseline (single miner)	6.45 W	12.9 W	20.6 W
Blockchained EC (K = 2)	5.56 W (16%)	9.79 W (31%)	17.4 W (18%)
Blockchained EC (K = 3)	5.17 W (24%)	8.68 W (48%)	18.9 W (9%)
Blockchained EC (K = 4)	8.27 W (−22%)	8.02 W (60%)	13.2 W (56%)

This framework has some problems with scalability, as the edge devices do not have the same opportunities as the edge servers in adding more competing miners to further improve the results. However, seeing as the results show such good numbers, employing a maximum of four miners would be sufficient for applications using this framework. In addition, to confirm the analysis made in Section 2, we observe that for every miner added, the increased energy consumed does not exceed 35%. Therefore, with the multiple competing miners being able to solve the PoW at faster rates (i.e., more than 35% faster), there is lower energy consumption overall. Furthermore, adding the blockchain before the offloading phase makes a significant improvement when it comes to security. Even if the devices that gather data are being put out in the public, the offloading process will not suffer from security threats. In a standard EC network, the offloading phase has no extra security added to it, but with the blockchain, the data are encrypted and validated before leaving the device, which results in higher security and confirms the significance of our proposed framework.

5. Discussion and Conclusions

To the best of our knowledge, there are no current papers that address the issue of energy consumption and latency reduction in a blockchained UAV network. The majority of the papers touch on the subject of improving security [19,20] but do not take into account the amount of computing resources which is needed to complete these operations. Therefore, we think that this research is a very important topic to introduce to UAV networks that might suffer from less computational resources.

In the following sections, we will explain some application scenarios where our proposed frameworks can be applied to help with the security and lessen the computational demand of the blockchain. Further on, we discuss some future research directions.

5.1. Application Scenarios

There are several important application scenarios to which the proposed frameworks presented in the previous section could be applied. Among them, in this section, we discuss two major and popular scenarios for UAVs.

The first one we consider is about vehicle-to-vehicle communication. Since the UAVs are deployed out in public, there might not be a data center they can communicate with that is close. However by implementing a blockchain to the UAV, as performed in blockchained EC, the data gathered on the UAV can be shared among other UAVs in the vicinity. The authors in [32] discuss some important security concerns for this situation and also illustrate some potential solutions for this problem. The blockchained EC framework can also work as a solution for some of the problems they discuss.

The authors in [9] introduce some concerns regarding energy consumption and security issues for UAVs. Some UAVs are put into public to gather sensitive data which should not fall into the wrong hands. Eavesdropping is a serious concern that cannot easily be avoided unless there is a system that strengthens the security on the UAVs. Both EC-enabled blockchain and blockchained EC focus on making the data gathered more

secure, while the latter additionally focuses on reducing energy consumption, which can work as a solution for the problem raised in [9].

UAVs can be used for many different and meaningful applications, one of them being transportation. The authors in [33] introduce how UAVs can be used for transportation in smart cities. On the positive side, a UAV can be used as an accident agent that reports any accidents happening in the area it is surveilling. The UAV can also be used as a roadside unit or an additional police eye. In this scenario, the UAV could communicate with cars on the road to alert them about dangers ahead. It could also communicate with the local police to let them know if there is any suspicious activity going on or if any car is speeding. However, in these scenarios, the data it gathers should be kept private. This is where blockchained EC can come in and be integrated to make the data secure and safe from malicious attack, while at the same time, it tries to keep the computational aspect as low as possible with competing miners.

Artificial intelligence is an important technology that can be applied to almost any other technology. In UAV networks, artificial intelligence, or better yet, deep learning, can be applied to different UAV operations. The authors in [34] conducted research on implementing deep learning to UAVs to counter the way some other people use UAVs maliciously. UAVs can be combined with object detection to easily detect different things. On the good side, these would be suspicious activities, while on the bad side, this could be used to find hideouts of people running from war. In their paper [34], the authors propose a way to counter the malicious activities by using deep learning. While doing so, the data that they will collect could be very sensitive, and therefore, securing this data is a huge priority. In these scenarios, both of our proposed frameworks could work in a good integration with the existing deep learning model. The blockchain makes the data secure and encrypted, which means that the wrong people will not obtain it. In addition, since the UAVs probably have to stay out for a period of time, they will have limited batteries and computational capabilities. With the competing miners framework, this issue can be resolved to an extent and the owner can also adjust the security level based on how many computing resources are available.

5.2. Technical Challenges

One of the goals of the EC in practice is reducing computational complexity. When the blockchain is applied to EC, the required computational complexity further increases, owing to the PoW. If the difficulty level is high, the time spent on mining can be long, which can result in slow response of the EC. With this in mind, blockchained EC can improve the security and privacy of EC but at the cost of increased complexity, which is actually one of the critical issues for EC. Additionally, with competing miners in the blockchain, a duplicate uploading issue may occur. Specifically, if some of the competing miners finish their mining tasks within 2 ms, they would both upload to the corresponding participant without having time to terminate the other miner. There are several effective approaches to circumvent the above challenges. First, one very promising and effective solution to address the latency issue of blockchained EC is to lower the difficulty level for a much faster mining process than that of a higher difficulty level.

Second, to solve the duplicate uploading issue, one can perform an additional process that can accurately identify the block. One possible approach for this is to verify the block that was created first and to delete the other block so that the correct block is added to the chain. There is a chance that the communication link between the device and the edge servers could be compromised, either through a malicious attack or some fault in the system. If this problem occurs, the device would not be able to send or receive data from the edge server. Using the blockchain when sending data is a proven good security measure where existing data cannot easily be edited and new data cannot easily be added to the chain. One possible solution to this problem is implementing a method that allows the device and edge server to hold onto the encrypted data until the communication link is back to normal and trust in the network is restored.

5.3. Future Research Directions

Because the blockchain can be combined and is synergetic with many different technologies in IoT and artificial intelligence (AI), there are several interesting and important research directions of the blockchain for those technologies. First, an area for further research involves possibilities of implementing the competing miners in IoT and/or AI technologies while analyzing the resulting performance. Moreover, further research can be conducted in federated learning, which is a state-of-the-art mechanism to train an AI model in a decentralized manner [35]. It would be important and interesting to implement the proposed frameworks of the blockchain with competing miners to better support AI services by making the training data even more secure while reducing the mining time and energy consumed on devices.

6. Conclusions

In this study, we first introduced the idea of competing miners for UAV applications and compared it to existing research. Then, we introduced two novel approaches for combining the blockchain and EC. One approach is the EC-enabled blockchain with multiple competing miners, where the computing task of solving the PoW puzzle in the blockchain is offloaded from UAVs to edge servers to reduce the time spent on mining with the aid of EC. The other is blockchained EC with hierarchically competing miners, where the blockchain is exploited for offloading data from UAVs to edge servers to improve the security of the offloaded data while reducing energy consumption and latency for EC. The superiority and effectiveness of the competing miners and the two frameworks were confirmed by our numerical results. Several application scenarios were discussed, followed by a discussion of the technical challenges and future research directions.

We can make several important conclusions based on our results. First, compared to existing approaches, our proposed approaches are proven to be beneficial due to low energy consumption, latency, and computational resources, rendering our approaches highly useful and effective in practice. Furthermore, it is important to note that at the low difficulty level, one should judiciously select the number of competing miners.

Author Contributions: Conceptualization and methodology, J.M.N.; resources and data curation, J.-H.P.; writing—original draft preparation, J.M.N.; writing—review and editing, J.-M.K., H.J. and S.Y.; supervision, J.-M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2020R1I1A3073651) and in part by the MSIT (Ministry of Science, ICT), Korea, under the High-Potential Individuals Global Training Program (2021-0-01571) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 17 July 2021).
2. Xiong, Z.; Zhang, Y.; Niyato, D.; Wang, P.; Han, Z. When mobile blockchain meets edge computing. *IEEE Commun. Mag.* **2018**, *56*, 33–39. [CrossRef]
3. Adewumi, T.P.; Liwicki, M. Inner For-Loop for Speeding Up Blockchain Mining. *Open Comput. Sci.* **2020**, *10*, 42–47. [CrossRef]
4. Hazari, S.S.; Mahmoud, Q.H. A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 916–921.
5. Satyanarayanan, M. The emergence of edge computing. *Computer* **2017**, *50*, 30–39. [CrossRef]

6. Corcoran, P.; Datta, S.K. Mobile-edge computing and the internet of things for consumers: Extending cloud computing and services to the edge of the network. *IEEE Consum. Electron. Mag.* **2016**, *5*, 73–74. [CrossRef]
7. Zhou, F.; Hu, R.Q.; Li, Z.; Wang, Y. Mobile Edge Computing in Unmanned Aerial Vehicle Networks. *IEEE Wirel. Commun.* **2020**, *27*, 140–146. [CrossRef]
8. Hong, S.-J.; Han, Y.; Kim, S.-Y.; Lee, A.-Y.; Kim, G. Application of Deep-Learning Methods to Bird Detection Using Unmanned Aerial Vehicle Imagery. *Sensors* **2019**, *19*, 1651. [CrossRef]
9. Liu, Y.; Dai, H.-N.; Wang, Q.; Shukla, M.K.; Imran, M. Unmanned aerial vehicle for internet of everything: Opportunities and challenges. *Comput. Commun.* **2020**, *155*, 66–83. [CrossRef]
10. Khan, M.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
11. Narbayeva, S.; Bakibayev, T.; Abeshev, K.; Makarova, I.; Shubenkova, K.; Pashkevich, A. Blockchain technology on the way of autonomous vehicles development. *Transp. Res. Procedia* **2020**, *44*, 168–175. [CrossRef]
12. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.
13. Dwivedi, A.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
14. Choi, J.-Y. A study on the application of blockchain to the edge computing-based Internet of Things. *J. Digit. Converg.* **2019**, *17*, 219–228.
15. Stanciu, A. Blockchain based distributed control system for edge computing. In Proceedings of the 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2017. pp. 667–671.
16. Liu, S.M.; Yu, F.R.; Teng, Y.; Leung, V.C.M.; Song, M. Computation offloading and content caching in wireless blockchain networks with mobile edge computing. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11008–11021. [CrossRef]
17. Rahman, M.A. Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE Access* **2018**, *6*, 72469–72478. [CrossRef]
18. Adewumi, T.P. Inner loop program construct: A faster way forprogram execution. *Open Comput. Sci.* **2018**, *8*, 115–122. [CrossRef]
19. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538. [CrossRef]
20. Islam, A.; Shin, S.Y. BUS: A Blockchain-Enabled Data Acquisition Scheme with the Assistance of UAV Swarm in Internet of Things. *IEEE Access* **2019**, *7*, 103231–103249. [CrossRef]
21. Gupta, R.; Shukla, A.; Mehta, P.; Bhattacharya, P.; Tanwar, S.; Tyagi, S.; Kumar, N. VAHAK: A Blockchain-based Outdoor Delivery Scheme using UAV for Healthcare 4.0 Services. In Proceedings of the IEEE INFOCOM 2020, Toronto, ON, Canada, 6–9 July 2020; pp. 255–260.
22. Aggarwal, S.; Kumar, N.; Alhussein, M.; Muhammad, G. Blockchain-Based UAV Path Planning for Healthcare 4.0: Current Challenges and the Way Ahead. *IEEE Netw.* **2021**, *35*, 20–29. [CrossRef]
23. Islam, A.; Shin, S.Y. BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things. *J. Commun. Netw.* **2019**, *21*, 491–502. [CrossRef]
24. Lei, K.; Zhang, Q.; Lou, J.; Bai, B.; Xu, K. Securing ICN-Based UAV Ad Hoc Networks with Blockchain. *IEEE Commun. Mag.* **2019**, *57*, 26–32. [CrossRef]
25. Rana, T.; Shankar, A.; Sultan, M.K.; Patan, R.; Balusamy, B. An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology. In Proceedings of the 2019 9th International Conference on Cloud Computing, Noida, India, 10–11 January 2019; pp.162–167.
26. Gai, K.; Wu, Y.; Zhu, L.; Choo, K.-K.R.; Xiao, B. Blockchain-Enabled Trustworthy Group Communications in UAV Networks. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4118–4130. [CrossRef]
27. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; ; Capkun, S. On the Security and Performance of Proof of Work Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), Vienna, Austria, 24–28 October 2016; pp. 3–16.
28. Damianou, A.; Angelopoulos, C.M.; Katos, V. An architecture for blockchain over edge-enabled IoT for smart circular cities. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 465–472.
29. Kumar, T.; Harjula, E.; Ejaz, M.; Manzoor, A.; Porambage, P.; Ahmad, I.; Liyanage, M.; Braeken, A.; Ylianttila, M. BlockEdge: Blockchain-edge framework for industrial IoT networks. *IEEE Access* **2020**, *8*, 154166–154185. [CrossRef]
30. Akkaoui, R.; Hei, X.; Cheng, W. EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access* **2020**, *8*, 113467–113486. [CrossRef]
31. 51% Attack Definition. Available online: https://www.investopedia.com/terms/1/51-attack.asp (accessed on 22 July 2021).
32. Shang, B.; Liu, L.; Ma, J.; Fan, P. Unmanned Aerial Vehicle Meets Vehicle-to-Everything in Secure Communications. *IEEE Commun. Mag.* **2019**, *57*, 98–103. [CrossRef]
33. Menouar, H.; Guvenc, I.; Akkaya, K.; Uluagac, A.S.; Kadri, A.; Tuncer, A. UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges. *IEEE Commun. Mag.* **2017**, *55*, 22-28. [CrossRef]

34. Menouar, H.; Guvenc, I.; Akkaya, K.; Uluagac, A.S.; Kadri, A.; Tuncer, A. Deep Learning on Multi Sensor Data for Counter UAV Applications—A Systematic Review. *Sensors* **2019**, *19*, 4837.
35. Kim, H.; Park, J.; Bennis, M.; Kim, S. Blockchained on-device federated learning. *IEEE Commun. Lett.* **2020**, *24*, 1279–1283. [CrossRef]