JYX

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Chang, Zheng; Guo, Wenlong; Guo, Xijuan; Chen, Tao; Min, Geyong; Abualnaja, Khamael M.; Mumtaz, Shahid

Title: Blockchain-Empowered Drone Networks : Architecture, Features, and Future

Year: 2021

Version: Accepted version (Final draft)

Copyright: © IEEE 2021

Rights: In Copyright

Rights url: http://rightsstatements.org/page/InC/1.0/?language=en

Please cite the original version:

Chang, Z., Guo, W., Guo, X., Chen, T., Min, G., Abualnaja, K. M., & Mumtaz, S. (2021). Blockchain-Empowered Drone Networks : Architecture, Features, and Future. IEEE Network, 35(1), 86-93. https://doi.org/10.1109/MNET.011.2000202

Blockchain-Empowered Drone Networks: Architecture, Features, and Future

Zheng Chang, *Senior Member, IEEE,* Wenlong Guo, Xijuan Guo, Tao Chen, *Senior Member, IEEE,* Geyong Min, *Senior Member, IEEE,* Khamael M. Abualnaja, and Shahid Mumtaz *Senior Member, IEEE*

Abstract

The future mobile communication system is expected to provide ubiquitous connectivity and unprecedented services over billions of devices. The flying drone, also known as unmanned aerial vehicle (UAV), is prominent in its flexibility and low-cost, and emerges as a significant network entity to realize such ambitious targets. However, the distributed nature makes the operation of a large scale drone network confront many challenges, such as vulnerability to security threats and privacy leakage. To address these problems, in this article, we propose to utilize the blockchain concept to the development of drone network. Under proposed blockchain-empowered drone networks (BeDrone), the drones that are deployed for service provisioning, can act as the miners of blockchain, and acquire the computing resources from each other or edge computing node whenever needed. Recommendations and future research directions for designing BeDrone are introduced with a focus on the game theoretic incentive mechanism for resource allocation and acquisition. Performance evaluations are conducted to illustrate the benefits of the proposed architecture on developing blockchain-envisioned drones.

Index Terms

UAV; drone; blockchain; resource allocation

I. Introduction

The increasing demand for high quality wireless services urges the future wireless communication system to provide ubiquitous connectivity and coverage over all kind of mobile devices. To realize the vision of unlimited access to wireless data anywhere and anytime for anything, the recent emerging drone-based flying platforms are expected to break the limitations of traditional network infrastructure [1]. The drone, also known as Unmanned Aerial Vehicle (UAV), has attracted many attentions recently due to its prominent in flexibility, configuration, and low-cost deployment [2]. An on-demand drone-based mobile communication system can provide a cost- and energy-efficient solution to complement the current wireless network [2].

In addition to extending territorial cellular network, drones are expected to be harnessed for public, civil and military applications, such as surveillance, disaster management, medical supplies, public safety and transportation management. Moreover, advances in sensor and other technologies have widen the functions of drone network to include many new applications, such as prediction and sensing. As one can found in Fig. 1, the requirement of large number of network-based services in the smart city may be complemented by the usages of a large scale of different types of drones over the air, such as medical drones, delivery drones, cellular drones, and sensing drones. What's more, the drones equipped with different sensors can be applied to other application area, such as smart industry, smart agriculture and smart grid. Therefore,

Z. Chang is with School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, and also with Faculty of Information Technology, University of Jyväskylä, P.O.Box 35, FIN-40014 Jyväskylä, Finland. W. Guo and X. Guo are with College of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China. T. Chen is with VTT Technical Research Centre of Finland, Espoo, Finland. G. Min is with Department of Computer Science, University of Exeter, Exeter, EX4 4QF, U.K.. Khamael M. Abualnaja is with Taif University, Saudi Arabia and S. Mumtaz is with Inst. de Telecomun., Portugal.

This work is supported by NSFC (No. 62071105), NSF of Hebei (No. E2017203351) and Key Research and Development Project of Hebei (No. 19252106D).

Fig. 1: UAV network in a smart city environment

the drones will become indispensable in the era of Internet of Things (IoT) and surely play a profound rule in the evolution of wireless network.

While having potential to significantly advance the development of many different technologies, the inherent nature of drone network requires considerable research efforts in order to be successfully implemented. There are some examples:

- The drones are usually with inconsistent energy supply, which leads to the fact that they are commonly resource-starved. Flying over the air contributes a large part of overall energy consumption, and leaves less space for other operations. Thus, comparing with the cellular network, the drone-based network will be with limited radio and computational resource/capabilities due to short of energy.
- The distribute nature and lack of resources makes the drone network vulnerable for attack. With no doubt, centralized control and distributed execution may pose profound security threats. A single point of failure can result in the disability of the whole network.
- Due to its high mobility architecture, the topology and links of the drone network keep changing over the time horizon. In addition, depending on the applications, the drones may move with different velocities, which means that there will be a large amount of signalling overhead between the distant central controller and the drones, and stringent requirements on the transmission latency.

As one can observe, to fully explore the potential benefits of drone network and obtain a secure and distributed architecture, advanced approaches and mechanisms are needed. Blockchain, which was mainly used for crypto-currency technology, may provide promising solutions for the management of drone network. As a well-known decentralized ledger-based system, blockchain is able to provide secure transactions and trust in a trustless network environment. Correspondingly, blockchain has recently evolved to wide computer and Internet applications from digital currency due to its transparent, retrospective, tamper-resistant, and decentralized features. In general, blockchain ledger comprises of three main concepts which are transaction, block and chain. All the valuable information that are broadcasted within blockchain can be treated as transaction. A block can be seen as storage that packs specific data about cryptographic transactions. Based on its hash value, the identity of each block is unique, and it is referenced by the next block. Such a procedure constructs a link among the blocks, which essentially creates a chain of blocks. As described, two processes are involved in the generation of blockchain. The first one is computing, which also refers to the consensus process, e.g., solving the Proof of Work (PoW) in Bitcoin. The node (or so called miner) in blockchain executes some computation tasks to obtain an unverified block. The second one is reporting/releasing. When the nodes successfully address the consensus protocol, it can report the result to blockchain for verification. The miners will reach consensus when the verification is correct and then obtain rewards caused by the computing for consensus process (or so called mining). As we can see, the blockchain has its great potential to provide a secure IoT platform, especially the number of devices is large. In this work, concept and features of Blockchain-empowered Drone Network (BeDrone), as presented in Fig. 2, are introduced to shed light on the secure and efficient management of drone network.

BeDrone is able to reap the benefits of blockchain and address the confront challenges of drone network due to its advantages of anonymity, privacy-preserving, and decentralization. In the BeDrone, the drones can act as the miners of the blockchain, and record all the operational data. Moreover, edge computing will be integrated, which is considered as an alternative solution for providing computational and storage resource whenever needed. There are several benefits of introducing blockchain and edge computing to drone network, which are briefly listed as follows.

- Firstly, with blockchain-based decentralization, the communication overhead and burden of central controller could be released. Moreover, the impact of single point of failure is also significantly reduced.
- Secondly, security and privacy of the drone network can be enhanced by encryption algorithm and consensus mechanism of blockchain. By leveraging consensus, one or some drones can be identified.
- Besides, as blockchain is essentially a public ledger and all the drones can audit its stored information, BeDrone provides a trust platform for further data processing.

To explore the advantages of blockchain on the design of drone network, in this article, we introduce the BeDrone architecture and present game-theoretic incentive scheme for the resource allocation and trading in the BeDrone. The reminder of this paper is organized as follows. First, a brief survey about design of drone network and the application of mobile blockchain are provided. The architecture of BeDrone is provided, along with its features and challenges. Moreover, we utilize the game theory and present a resource trading scheme for the BeDrone management, and evaluate its performance. Finally, we explore the future direction and conclude this work.

II. Overview of Drone Network and Mobile Blockchain

It can be found that the drone network will become a significant complementary to the current territorial cellular infrastructure [1] [2]. In addition, as the drone-based platform is highly flexible, it can be used for many mission-critical applications concerning civil life, such disaster management and surveillance [1] [3]. Because of all these potential advantages, the dedicated research efforts on the drone-based network or communications system have mainly concentrated on the drone coordination, placement and resource optimization [1]. Recently, the integration of drone and edge computing has also received considerable research interests [4] [5]. Generally, applying edge computing to the IoT system is able to bring the computational resources closer to the network users [6]. In this context, the drones are usually considered as edge computing nodes providing computational resources to the ground users or as the relays forwarding computing task to the edge node in their vicinity.

Meanwhile, apart from being dedicated to digital currency, blockchain has recently evolved to broad IoT applications due to its transparent, retrospective, tamper-resistant, and decentralized features [7]. Recently, there are increasing research interests on exploring the blockchain in the edge computing system [8]- [12]. The integration of blockchain and edge computing enables the management of network access, computation and storage at the edge, which can enrich the network services and applications in a secure manner [8] [9]. To further accelerate the blockchain applications in the IoT and edge computing paradigms, there are some efforts on investigating the computational offloading schemes where the IoT devices can act as the miners and offload the computational requests (e.g. for solving the PoW) to the nearby edge nodes [10] [11]. Similarly, some researchers explore the game-theoretic approaches to investigate how the service provider set the price and rent the computational resources to the miners [12] [13]. The integration of

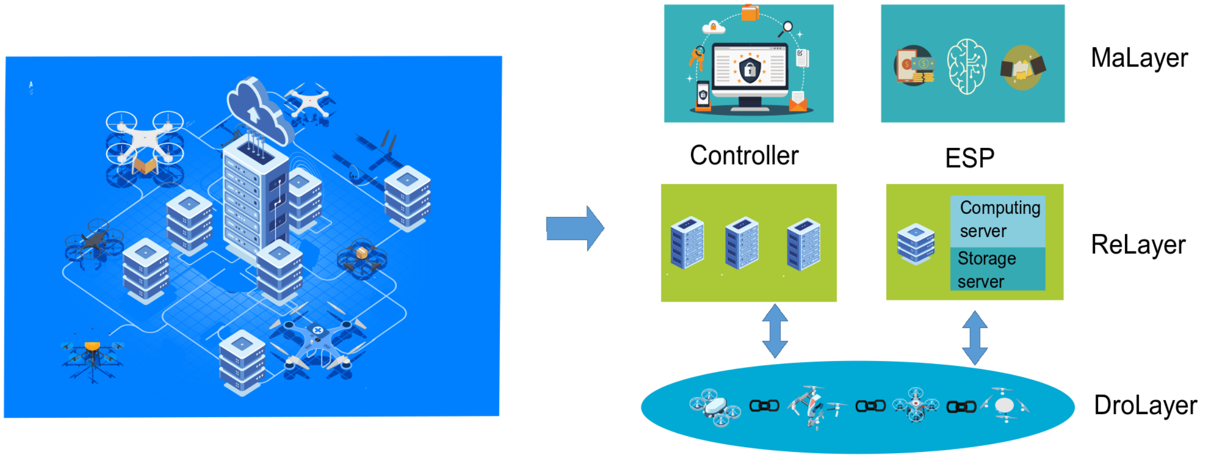

Fig. 2: Blockchain-empowered Drone Network (BeDrone)

blockchain and edge computing has a great potential to provide secure and efficient solutions for the drone network paradigm. However, although some works dedicate to using blockchain-based resource sharing scheme among drones [14], there are seldom works discussing the potential of using blockchain for drone network and operations, which motivates us to explore in this direction.

III. Architecture of BeDrone

To reap the benefits of blockchain on designing the drone network, we introduce the architecture and concept of BeDrone in this section. We first present the system model, features and applications. The implementation issues and challenges are then discussed.

A. System Model

As described, mining is the core of blockchain-based system and requires considerable computing and storage capabilities. Before adding or publishing to the blockchain, some complex computation problems, e.g., PoW puzzle, are solved to secure the integrity and validity of transactions. Correspondingly, security and privacy of the system depend on the overall mining and consensus mechanisms, which is highly affected by the computing and storage capabilities of the miners.

As drones are usually resource-limited, edge computing can play a crucial role in the BeDrone. The drones can rent computing and storage resources from edge service provider (ESP) to carry on the blockchain process. In practice, the trade between the drones and ESPs can be performed in the way that the drones offload the computation tasks to the edge nodes for execution. The BeDrone system has three layers: the management layer (MaLayer), the resource layer (ReLayer), and the drone layer (DroLayer). In the DroLayer, drones are deployed over a relatively large area and are able to communicate with each other over dedicated communication channels. They not only need to execute their own missions, but also record their missions or operation data. These drones are the potential miners in the blockchain. In the ReLayer, the actual authority of blockchain process and the resource trading and allocation are performed. In the MaLayer, the ESP is able to manage its resources and make the decision, in addition to the authorization process by the controller. The functions of main entities in the BeDrone are summarized as follows.

- **Drone**: The drones are mainly deployed for performing various missions, such as extending territorial cellular network, data collection and surveillance. The operation records and other type of data can

Algorithm 1 Implementation of BeDrone

1: **System Initialization and Key Generation:** Each drone will be registered on the trusted authority (e.g., controller) and be a legitimate entity obtaining certificate and public/privacy key. The certificate of the drone is relevant to the registration information which can uniquely identify itself, such as the license plate number. A set of wallet addresses stored in the account pool will be given to the drones by the authority. Drone executes the system initialization and downloads the last wallet data from the storage of edge nodes, which is able to store all history transaction records.

2: **Creation of Transactions:** The transactions could be the operational data, collected data or any useful data that can be shared among all the drones in a certain period. For instance, a drone for logistic or traffic management can share the encrypted surrounding/road information among each other.

3: **Building Blocks and Finding PoW:** The drones which have collected a set of transactions pack the transactions into a block and performs mining. Each drone competes to create a block by finding a valid PoW and the mined block is then broadcast to notify other drones in the blockchain.

3: **Block Verification with Consensus Process:** All of the drones audit the transaction records, referred as the consensus process. The consensus generates an unique hash value for each block in blockchain. This cryptographic value is used to connect the previous block in the blockchain for traceability and verification.

4: **Establishing a new block:** If the block is proved effective by majority of the drones, the transaction information will be stored in the appended block at the end of the current blockchain. The blocks are added to the blockchain in a linear chronological order. Finally, the drones are rewarded in a certain way.

be added to the formulated blockchain to ensure the security and privacy. As the drones are with limited-resources in computing units and energy battery, in order to relieve the computation-intensive challenge of establishing a blockchain, the drones can require resources from the edge nodes in proximity. Moreover, some powerful drones can also act as resource providers by renting its resources to others. Essentially, these drones can be considered as edge nodes as well. Thus, in this work, we consider edge nodes owned by the ESP are the main resource providers.

- **Controller/Authority**: A controller is essential for a drone network and it is for responsible for network control and initialization. It can carry out encryption process by managing the drones' identities and authorizations. It also generates parameters and cryptographic keys. Note that in this system, the Controller/Authority only acts as the initializer for identity authorization and key parameters before establishing the blockchain of drone network. The controller remains offline and has no impact after the blockchain has been built which indicates that decentralization of the blockchain will not be disrupted.
- **ESP/edge node**: As shown in Fig. 2, an edge node basically compromises of two components, i.e., a storage server and and a computing server. Upon request, the computing server provides computational resources to the drones to complete the process of block generation and validation. In addition, the storage server can store the real-time transactions records and also trading-related information, such as the price announcement and service demand, if needed. With a properly designed incentive mechanism, the ESPs who own the edge nodes and resources can set the price, and make the decision on how to provide resources to the drones.

B. Features and Implementation

The considered scenario has a wide application area, including cellular drone network, surveillance, weather estimation, remote sensing, medical supplies, public safety and transportation management. In these applications, the operational and collected data of drone will be crucial for the network management. The security and privacy of these data will be profound as the single leakage may cause the damage of the whole network. In the proposed system, the drones will act as the miners of the blockchain, and they will request for computing resources from ESP when its hash power is insufficient.

The main operation processes of blockchain in BeDrone is described as follows. First, the drone sends the request to the whole network when a transaction happens. Second, when the security of transaction could be verified, the blockchain begins to execute the transaction. The generation of block begins, and the drones participate in the computing of new blocks by using hash power. The interaction between drones and ESP/edge computing system is needed. The drones can purchase or rent the resources from the ESP, for executing the computation tasks. The amount of purchased resource depends on task requirement, the associated cost and the received reward. The ESP can also announce the price of its resources resources during the interaction. Therefore, a resource allocation and trading scheme is needed here to support the drones with limited computing capability. New blocks would reach consensus after obtaining the results of, e.g., PoW, and miners can receive the rewards. Finally, the blockchain network transmits the data to drones for the next actions. The implementation process is described in Algorithm 1.

C. Challenges on Limitation of Resource

Note that during the whole process, due to the limited-computing power, drone can turn to ESP for edge computing service, which means that integrating the edge computing is essentials. Exploring the blockchain in the drone network will provide a promising solution for coping with the security and privacy threats of drones. In the blockchain-based system, the computing capability is the key to the performance. Then as the drones are usually with limited resources and different tasks, how to incentivize the drones to participate the blockchain process and obtain the computational resources from ESP is the major challenge to realize the BeDrone. In this aspect, we will propose a novel Stackelberg game-based incentive mechanism in order to find the optimal pricing for the ESP and purchase strategy for the drones, respectively.

IV. Resource Allocation and Trading in BeDrone

A. Game Formulation

As described, computing resource acquisition is pivotal for the success of BeDrone. Thus, the development of resource allocation and trading scheme in BeDrone is of great importance. In this section, to incentive the ESP to provide its computing resources and encourage the drones to participate the blockchain, the interactions between these two parties are explored. Game theory is well known for its capability of describing and analyzing interactive decision situations. During last decades, there has been a growing interest in applying game-theoretic approaches to investigate the resource allocations in wireless communication system. In this work, incentive mechanism is explored via single-leader multiple-follower Stackelberg game model, where ESP is the leader and drones are the followers.

Accordingly, a two-stage Stackelberg game is introduced to investigate the relations and interactions between the ESP and drones. The objective of the formulated game is to find an optimal pricing strategy for the ESP (leader), assuming that the drones (followers) are rational and can react set the purchase strategy to optimize their objective functions. In the first stage, the ESP sets the price $\mathcal{Q} = \{q_1, q_2...\}$ for each drone based on the its provided services. The utility/profit of the ESP is denoted as u_{esp} which is related to the pricing and cost. The objective of the first stage is to maximize u_{esp} via optimizing pricing and purchase strategies.

The main target of the second stage is for the drones to determine the demand for resources, according to the price strategy of the ESP, the associated cost and possible rewards. In the BeDrone, reward R of a drone can consist of three parts: fixed reward, performance reward and the participant reward. The performance reward is related to the size of block and the participant reward is related to degree of participation (computing capability). We can assume the purchase strategy (resource demand) of drone i is s_i and its utility/profit is u_i. The objective is then to maximize the utility of these drones via optimizing pricing and purchase strategies.

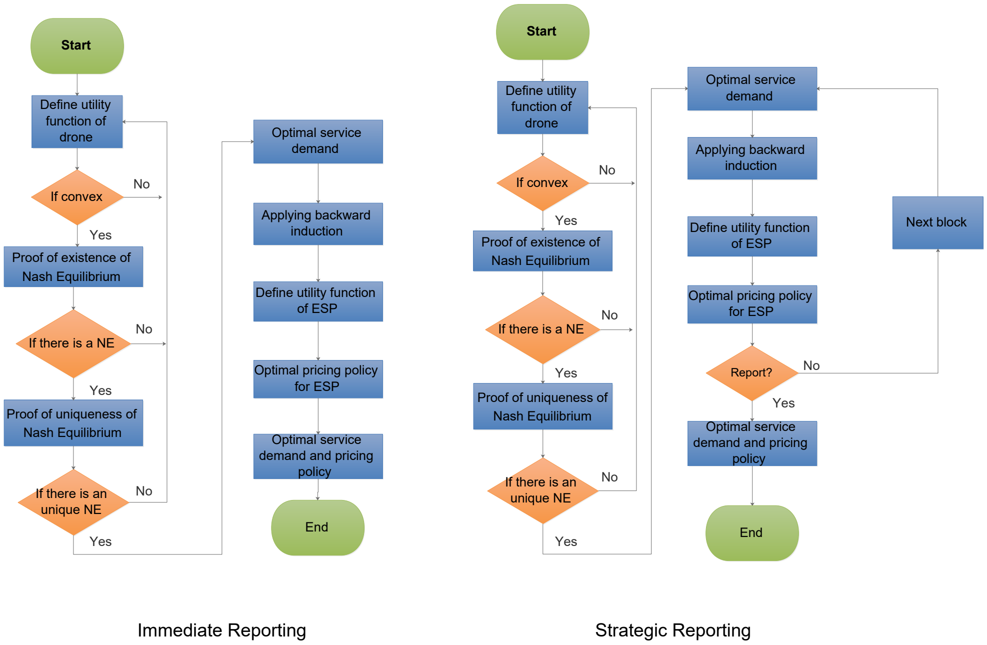
Start
Define utility function of drone
If convex
No
Yes
Proof of existence of Nash Equilibrium
If there is a NE
No
Yes
Proof of uniqueness of Nash Equilibrium
If there is an unique NE
No
Yes
Optimal service demand
Applying backward induction
Define utility function of ESP
Optimal pricing policy for ESP
Optimal service demand and pricing policy
End
Immediate Reporting
Start
Define utility function of drone
If convex
No
Yes
Proof of existence of Nash Equilibrium
If there is a NE
No
Yes
Proof of uniqueness of Nash Equilibrium
If there is an unique NE
No
Yes
Optimal service demand
Applying backward induction
Define utility function of ESP
Optimal pricing policy for ESP
Report?
No
Yes
Optimal service demand and pricing policy
End
Next block
Strategic Reporting

Fig. 3: Flow of the resource trading

We can see in order to reach the Stackelberg equilibrium (SE) of the formulated game, a two-stage iterative algorithm is needed. In the first stage, the ESP present its price strategy for its computing resources upon requests. In the section stage, the drones with demand can compete for these resources in a non-cooperative fashion. The backward induction is used to find the SE of the formulated game. When the Nash equilibrium (NE) of the sub-game in second stage is reached, the ESP shows its reaction by renew its price strategy according to the purchase strategies of drones. Through the analysis of the game in each stage, the local optimal strategy can be reached and the global optimal solution of the whole game is derived.

The developed game theoretic approach is expected to adapt to the features of BeDrone. Thus, in the following, two different mining mechanisms which are differed by reporting process in blockchain are specifically investigated. The first mining mechanism, refereed as Immediate Reporting (IR), works in the way that after successfully computing, the drone will report immediately. The other one, which is called Strategical Reporting (SR), allows the drones to temporarily hide their solutions and report strategically after successfully computing.

B. Game Analysis of IR and SR

1) Game Analysis of IR: As for the IR, the existence and uniqueness of NE of the second stage should be found at first. In the IR, the utility of the drone is related to the reward and cost. We assume that the defined utility function $u_{i,IR}$ is continuous and strictly convex with respect to (w.r.t) s_i. Then based on the results and discussions in [12], we can find the existence of NE. Moreover, the uniqueness of the NE is also of interest and should be explored. This is due to the fact if there are multiple Nash equilibria, coordinating all the drones to converge to the same NE will be difficult. According to the discussions in [15], and utility function $u_{i,IR}$ is continuous and strictly convex, an unique NE exists in the IR. With knowledge of the existence and uniqueness of NE, the optimal strategy of drones can be obtained by applying Karush-Kuhn-Tucker (KKT) conditions and Lagrangian method under possible constraints.

Then we turn to the game analysis of the first stage, the pricing strategy of ESP depends on the requests of the drones, i.e., $\mathcal{S} = \{s_1, s_2...\}$. Thus, after obtaining the solution of the second stage, we can derive the pricing of ESP with the objective to obtain the optimal utility. Here, it is also assumed that u_{esp} is a convex function w.r.t. q_i. Accordingly, a $\mathcal{Q}^*$ that enables the ESP to achieve the optimal utility must exist [15]. Similarly, the KKT conditions and Lagrangian method can be applied to obtain the optimal q_i^*.

With the optimal purchase strategy s_i^* of drone i, the optimal pricing of the resources to each drone q_i^* can be obtained. Therefore, both the ESP and drones can obtain the optimal utilities under the combination of strategies ($\mathcal{S}^*$, $\mathcal{Q}^*$), which is essentially the SE of the game. To this end, the backward induction method is then applied to find the SE of this two-stage Stackelberg game to reach a global optimal solution. Once the optimal purchase strategy of the drones is solved, we can obtain the pricing strategy of the ESP.

2) Game Analysis in SR: When drones are in the blockchain process, some of them may prefer not to report their results of transactions intermediately due to the their stronger hash power. Instead, they can choose to temporarily hold their solutions. Then, SR mining scheme, instead of IR, is applied here for the drones with a certain level of hash power to achieve a better reward. However, the drone may suffer from using SR scheme as the others can report their results before. That is, although using SR can make the drone achieve a better reward, the drone may encounter more risk to generate a chain of abandoned blocks.

In the SR, after successfully mining block m, droner i can obtain a profit $u_{i,SR}^m$ that is related to reward, cost, the probability that the drone successfully announces the solutions of the PoW and the profit that obtained by computing $(m-1)$ blocks. While we also consider a continuous and convex utility function w.r.t s_i, similar to the previous study, the existence and uniqueness of a NE can be found. The optimal purchase strategy is achieved by addressing a set of equations that are formed by applying KKT conditions, etc, e.g., letting the partial derivative of $u_{i,SR}^m$ w.r.t. variable s_i equals to zero. To find the optimal pricing of the ESP, the optimal purchase strategies of the drones, the derived s_i is needed. As defined, the utility u_{esp} of the ESP is strictly convex w.r.t. q_i. After finding the optimal purchase strategy $\mathcal{S}^*$ of all the drones, the optimal pricing $\mathcal{Q}^*$ of ESP can be achieved by applying the KKT condition. The backward induction is then used to find the SE of the overall game, which can optimize the utilities of both parties.

The flowchart containing incentive processes of both IR and SR schemes is summarized in Fig. 3. As analyzed, we can see that SE exist for both IR and SR schemes given the defined utility function, which indicates for both mining schemes, optimal strategies ($\mathcal{S}^*$, $\mathcal{Q}^*$) respectively exist.

V. Case study and Performance Evaluation

In this section, we present a case study to validate the performance of the proposed mechanisms. To simplify the evaluation, we assume the drones are not with hash power which means that all the hash power should be purchased from the ESP. As stated, the reward that drone can obtain consists of fixed reward, performance reward and participant reward. Here, in order to find the impact of different award factors, we consider the reward R is defined as

$$R = R_f + \beta\pi + \gamma\alpha_i,$$

where R_f is the fixed reward, β is a evaluation factor, π is the size of block and γ is an evaluation factor for the participate award. α_i which indicates computing capability, is the hash power proportion of miner i in the whole network.

Fig. 4 shows a three dimension plot about the relations among price of ESP, computing capability and the profit of the drone for the SR scheme. In Fig. 4, a stronger computing capability leads to a higher profit when the price is fixed. This is because participation reward is determined by the computing capability when solving the PoW puzzle, and the reward is dominant in this case. We can also observe that when the price increases, the profit decreases under the condition of fixed computing capability. It can also be found that the profit can increase with the increase of computing capability if the price does not change too much, which indicates computing capability has a better impact on the profit.

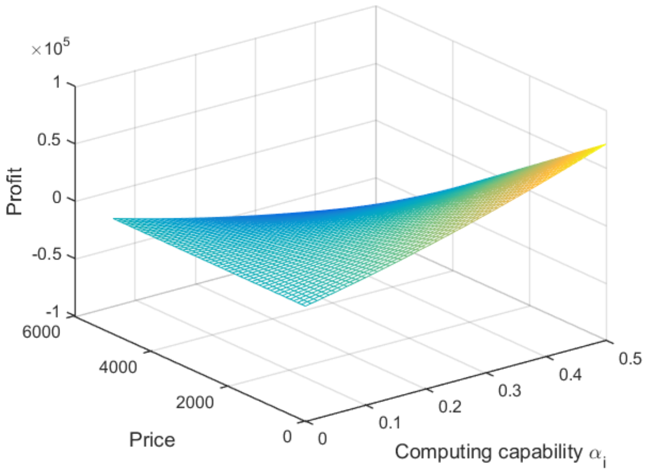

Fig. 4: Price & computing capability vs. profits

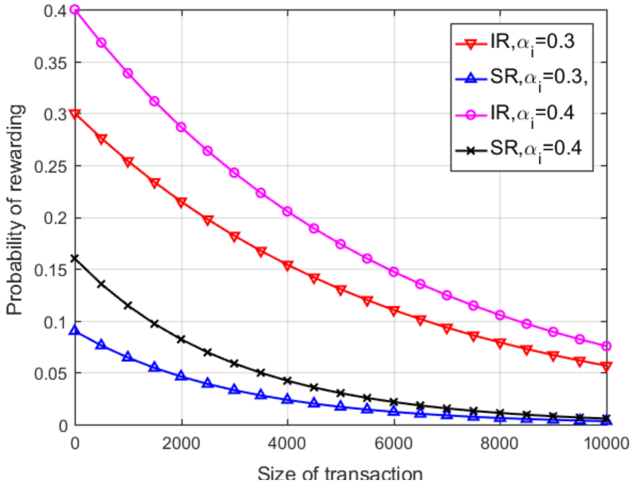

Fig. 5: Transaction size vs. the probability of rewarding

Fig. 5 explores the rewarding probability of both IR and SR schemes when considering different computing capabilities and transaction sizes. In general, the rewarding performance when using IR scheme is better than using the SR scheme. As the transaction size increments, the reporting/rewarding probability reduces which is caused by the incremental complexity of computing. It can also be found that as more hash power can be advocated for computing, and the growth of computing capability leads to a better performance. Moreover, if a bigger transaction size or more drones are considered, more resources can be allocated to the drones with demand by using the incentive schemes.

VI. Future Research Directions

As we can see, there is a great research potential to integrate the blockchain and edge computing to the development of drone networks. However, there are still many challenges ahead concerning computational resources, algorithm development, efficiency, privacy and security. In the following, we present the obstacles that may prevent the design of our proposed architecture and point out possible research directions.

A. Prediction of State of the Drones

In the BeDrone, accurate knowledge of the status (such as demand, link quality position and data acquisition) of the drones is beneficial for carrying out the resource trading process. As the drone system is highly dynamic, the status of each drone is not easy to be preciously and timely evaluated. Thus, it will be possible to explore machine learning or some other advanced techniques to dynamically predict the drones' status and make more accurate decisions. However, applying advanced learning technique requires considerable computational resources and data input. Therefore, sophisticated optimization schemes are preferred to alleviate the computational burden and make the decision-making process more accurate.

B. Ultra-reliable Transmission in Drone Network

In the traditional propagation phase, a mined block may fail to be propagated or broadcast due to the possible high mobility and latency among the drones. Besides, the topology of the drones will be changed in a high velocity, which can also make the blockchain process challenging. In addition, the control signalling between the drones and controller is crucial for the drone control and the secure key generations etc. There will be frequent communications among the drones, and between the drones and edge nodes. Thus, the communication overhead of such a drone platform will be relatively high. In addition, the quality of radio links and access control also impact the communications within BeDrone, which may pose extra bottleneck to the information exchange between edge computing units and drones, and consensus process. Therefore, ultra-reliable and efficient transmission schemes within the drone network are worth of considerable and dedicated efforts.

C. Development of Edge Computing System

The edge computing framework should be further improved to increase the data rate or decrease the latency to avoid the requests being discarded from the transmission point-of-view. Besides, the current incentives in the edge computing system is formulated as two-stage Stackelberg game, which can't maximize the social welfare of drones and service providers. Therefore, as one the future research direction, social welfare optimization scheme can be further developed and more different types of service providers can be taken into consideration.

D. Game Formulation

There are some potential threats which may impact the incentive mechanism of the BeDrone. Firstly, drones/miners may not be completely rational, which results in the failure of the incentive mechanism. In addition, drones who own stronger computing capability may choose to strategically release the calculated solution to obtain more profits by hiding a chain of blocks, which leads to ”withholding block attack”. Moreover, selfish drone is primarily an attack on the mining and incentive mechanism. Therefore, it would be better to further explore the sophisticated game theoretic approaches to the development of BeDrone.

E. Application Cases

As one can observe, the proposed architecture and developed schemes can be adapted to a wide range of application scenarios of the drone network. Nevertheless, different scenarios may require modifications and/or extensions to the current architecture and presented scheme. For example, contract theory can be further extended to optimize the pricing policy and maximize the profit in a certain trade in energy harvesting drones. To explore and consider additional features of the drone network will be vital for adopting the proposed architecture to a wider market.

VII. Conclusion

In this article, we have introduced the concept of blockchain-empowered drone network (BeDrone), and integration of BeDrone with edge computing. The distributed nature makes the operation of large-scale drone network confronts many challenges, including vulnerability to security threats and privacy leakage, and so on. To address these problems caused, we propose to utilize blockchain concept to the development of drone network. Under proposed blockchain-empowered drone network, the drones which are deployed for service provisioning, can act as the miners in the blockchain, and are able to acquire the computing resources from each other or edge computing node whenever needed. Recommendations for designing such a system and future research directions are introduced with a focus on the game theoretic incentive mechanism for resource acquisition. Performance evaluations are conducted to illustrate the benefits of proposed architecture on developing blockchain envisioned drones.

References

[1] L. Gupta, R. Jain, and G. Vaszkun, ”Survey of Important Issues in UAV Communication Networks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123-1152, Second quarter 2019.

[2] Z. Zhou, J. Feng, C. Zhang, Z. Chang, Y. Zhang and K. Huq, ”SAGECELL: Software-defined Space-Air-Ground Integrated Moving Cells,” *IEEE Communications Magazine*, vol. 56, no. 8, pp. 92-99, Aug. 2018.

[3] X. Liu et al., ”Transceiver Design and Multihop D2D for UAV IoT Coverage in Disasters,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1803-1815, April 2019.

[4] Y. Liu, K. Xiong, Q. Ni, P. Fan and K. B. Letaief, ”UAV-assisted Wireless Powered Cooperative Mobile Edge Computing: Joint Offloading, CPU Control and Trajectory Optimization,” *IEEE Internet of Things Journal*. doi: 10.1109/JIOT.2019.2958975

[5] S. Garg, A. Singh, S. Batra, N. Kumar and L. T. Yang, ”UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles,” *IEEE Network*, vol. 32, no. 3, pp. 42-51, May/June 2018.

[6] Y. Gu, Z. Chang, M. Pan, L. Song, and Z. Han, ”Joint Radio and Computational Resource Allocation in IoT Fog Computing, ” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7475-7484, August 2018.

[7] S. Nakamoto, ”Bitcoin: a peer-to-peer electronic cash system,” White paper, 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[8] R. Yang, F. R. Yu, P. Si, Z. Yang and Y. Zhang, ”Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508-1532, Second quarter 2019.

[9] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He and Y. Zhang, ”Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond,” *IEEE Network*, vol. 33, no. 3, pp. 10-17, May/June 2019.

[10] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, ”Computation Offloading and Content Caching in Wireless Blockchain Networks With Mobile Edge Computing,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11008-11021, Nov. 2018.

[11] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, Z. Zheng and Y. Zhang, ”Cooperative and Distributed Computation Offloading for Blockchain-Empowered Industrial Internet of Things,” *IEEE Internet of Things Journal*, pp. 1-1, May. 2019.

[12] Z. Chang, W. Guo, X. Guo, Z. Zhou, and Tapani Ristaniemi, ” Incentive Mechanism for Edge Computing-based Blockchain,” *IEEE Transactions on Industrial Informatics*, 2020, DOI 10.1109/TII.2020.2973248.

[13] J. Qiu, D. Grace, G. Ding, J. Yao and Q. Wu, ”Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator’s Perspective,” *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451-466, Jan. 2020.

[14] A. Asheralieva and D. Niyato, ”Distributed Dynamic Resource Management and Pricing in the IoT Systems with Blockchain-as-a-Service and UAV-Enabled Mobile Edge Computing,” *IEEE Internet of Things Journal*, 2020. doi: 10.1109/JIOT.2019.2961958

[15] Z. Han, D. Niyato, W. Saad, T. Baar, and A. Hjrungnes, Game Theory in Wireless and Communication Networks Theory, Models, and Applications. Cambridge University Press, NY, 2000.

Zheng Chang [SM] received the B.Eng. degree from Jilin University, Changchun, China in 2007, M.Sc. (Tech.) degree from Helsinki University of Technology (Now Aalto University), Espoo, Finland in 2009 and Ph.D degree from the University of Jyväskylä, Jyväskylä, Finland in 2013. From June to Auguest 2013, he was a visiting student at Tsinghua University and from April to May 2015. He was a visiting researcher at University of Houston, TX, USA. His research interests include IoT, machine learning, and green communications.

Wenlong Guo received his master degree at Yanshan University in 2018 and is now pursing for PhD degree in College of Information Science and Engineering at Yanshan University, Qinhuangdao, China. His research interests include blockchain, UAV, cloud computing and mobile computing.

Xijuan Guo received a PhD degree from Yanshan University. She is now a professor at College of Information Science and Engineering, Yanshan University, Qinhuangdao, China. Her research interests include high performance computing, cloud computing, image processing, wireless communications.

Tao Chen [SM] is a senior researcher at VTT, Finland, an honorary professor at the University of Kent, United Kingdom, and an adjunct professor at the University of Jyvskyl, Finland. He has more than 20 years of experience in the telecommunications sector. He has been the project coordinator and technical manager of large EU funded projects on 5G. His current research interests include AI for wireless communications, software defined networking for 5G mobile networks, dynamic spectrum access, and energy efficiency and resource management in heterogeneous wireless networks.

Geyong Min [SM] is a professor of high performance computing and networking with the Department of Computer Science within the College of Engineering, Mathematics and Physical Sciences at the University of Exeter, United Kingdom. His research interests include computer networks, wireless communications, parallel and distributed computing, ubiquitous computing, multimedia systems, modeling and performance engineering.

Shahid Mumtaz [SM] received his M.S. and Ph.D. degrees in electrical and electronic engineering from Blekinge Institute of Technology, Sweden, and the University of Aveiro, Portugal, in 2006 and 2011, respectively. He has been with the Instituto de Telecomunicaes since 2011, where he currently holds the position of auxiliary researcher and adjunct positions with several universities across the Europe-Asian Region. He is also a visiting researcher at Nokia Bell labs. He is the author of four technical books, 12 book chapters, and 150+ technical papers in the area of mobile communications.