Article:

Qiu, Junfei, Grace, David orcid.org/0000-0003-4493-7498, Ding, Guoru et al. (2 more authors) (2020) Blockchain-Based Secure Spectrum Trading for Unmanned Aerial Vehicle Assisted Cellular Networks : An Operator's Perspective. IEEE Internet of Things Journal. 8851203. pp. 451-466. ISSN 2327-4662

https://doi.org/10.1109/JIOT.2019.2944213

Blockchain-Based Secure Spectrum Trading for Unmanned Aerial Vehicle Assisted Cellular Networks: An Operator's Perspective

Junfei Qiu, David Grace, *Senior Member, IEEE,* Guoru Ding, *Senior Member, IEEE,*
Junnan Yao, and Qihui Wu, *Senior Member, IEEE*

***Abstract*—Unmanned aerial vehicles (UAVs) are envisioned to be widely deployed as an integral component in the next generation cellular networks, where spectrum sharing between the aerial and terrestrial communication systems will play an important role. However, there exist significant security and privacy challenges due to the untrusted broadcast features and wireless transmission of the UAV networks. This paper endeavors to resolve the security issues through proposing a novel privacy-preserving secure spectrum trading and sharing scheme based on *blockchain* technology. Specifically, from the operator's perspective, a pricing-based incentive mechanism is firstly introduced, in which a primary mobile network operator (MNO) leases its owned spectrum to a secondary UAV network in exchange for some revenue from the UAV operators. To address the potential security issues, a *spectrum blockchain* framework is then proposed to illustrate detailed operations of how the blockchain helps to improve the spectrum trading environment. Under this framework, a Stackelberg game is formulated to jointly maximize the profits of the MNO and the UAV operators considering uniform and non-uniform pricing schemes. Security assessment and numerical results confirm the security and efficiency of our schemes for spectrum sharing in UAV-assisted cellular networks.**

***Index Terms*—Unmanned aerial vehicle, cellular network, spectrum trading, blockchain, security and privacy, Stackelberg game.**

I. INTRODUCTION

A. Background and Motivation

In recent years, unmanned aerial vehicles (UAVs) have attracted increasing interest and are expected to be an important complementary part of future wireless communication networks due to their remarkable advantages of low cost, high mobility and deployment flexibility [1]–[3]. They can be deployed either as aerial base stations to enhance the network capacity and expand the coverage for existing terrestrial networks [4], [5], or as mobile user equipment to carry out delivery or surveillance tasks in the sky [6], [7].

Despite many potential applications, to fully reap the benefits of deploying UAVs for communication purposes, some core technical challenges still need to be faced with. On the one hand, most UAVs in the market basically operate on the unlicensed spectrum (e.g., the industrial, scientific and medical bands), which is usually of limited data rate, unreliable and vulnerable to interference, thus severely restricting the potential performance of UAVs [8]. On the other hand, there always exist significant security and privacy threats for UAV-assisted wireless communications due to the untrusted broadcast features and wireless transmission of UAV networks. However, these problems have not been well studied in existing works. These observations motivate us to focus on investigating the spectrum usage for UAV-assisted cellular networks while considering the security and privacy issues in this paper.

B. Related Work

Due to the scarcity of wireless spectrum, UAVs always need to share the spectrum with existing communication systems (e.g., cellular networks with licensed spectrum). However, traditional spectrum sharing mechanisms through spectrum sensing [9], [10] or spectrum databases [11] are actually not efficient for UAV-assisted cellular networks, because spectrum sensing is generally imperfect and subject to sensing errors while spectrum databases are based on centralized management. It is challenging to apply these methods into UAV networks to achieve distributed and reliable communications. To deal with these challenges, some researchers attempt to exploit the property-right spectrum sharing techniques operating based on an agreement where the spectrum owners lease or share their spectrum to the unlicensed ones in exchange for some certain services [12], [13]. However, these works do not take into account the practical challenges of UAV deployments for cellular services from the perspective of operators. In fact, UAVs and ground base stations often belong to multiple different operators, each selfishly seeking to maximize their individual benefit. In general, the cellular network operators will be not willing to share their own spectrum to the UAV networks, since the total usable bandwidth of the cellular networks is limited, and sharing part of the total bandwidth with UAVs may harm the capacity of the cellular base stations. Thus, to promote the adoption of spectrum sharing, some incentive mechanisms should be developed to motivate the mutual cooperation between the operators.

This work is supported in part by the National Natural Science Foundation of China under Grant 61871398, and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20160080.

J. Qiu and D. Grace are with the Department of Electronic Engineering, University of York, York YO10 5DD, U.K. (e-mail: dr.junfei.qiu@gmail.com, david.grace@york.ac.uk).

G. Ding and J. Yao are with the College of Communications Engineering, Army Engineering University, Nanjing 210007, China (e-mail: dr.guoru.ding@ieee.org, tms3216@qq.com).

Q. Wu is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China (e-mail: wuqihui2014@sina.com).

Incentive mechanism design has been extensively studied for networking problems, such as caching [14], [15], traffic/computation offloading [16], [17], cooperative communications [18], etc. However, none of them consider the UAV-assisted application scenarios. Besides, existing incentive mechanisms with high complexity and centralized control may not be suitable for UAV networks when considering the energy constraint and distributed features of UAV networks. Recently, Hu *et al.* in [19] investigated the use of contract theory to formulate the spectrum trading problem between the macro base station manager and the UAV operators to encourage the macro base station manager to lease its owned bandwidth to the UAVs. However, there are significant security and privacy challenges for such peer-to-peer (P2P) spectrum trading in UAV-assisted cellular networks for the following reasons. i) It is insecure for mobile network operators (MNOs) to carry out large-scale spectrum trading in an untrusted and nontransparent trading environment, where malicious UAV operators could heavily threaten cellular network's security through malicious exploitation, e.g., falsification, advertising fraudulent spectrum demands, etc. ii) In traditional centralized spectrum trading, there is an intermediary managing the trading among the operators, which may suffer from problems such as single point of failure and privacy leakage.

In recent years, *blockchain technology* [20]–[22] has attracted growing attention of researchers, which may provide possible solutions addressing the above challenges because of its advantages of decentralization, anonymity and trust. Blockchain is a decentralized ledger-based storage method, which provides a unique tool for secure transactions in a distributed manner without trusted agents [23]. Moreover, in blockchain-based networks, each node manages a copy of whole or part of a database from the system. These advantages enable spectrum trading to be executed in a decentralized, transparent, and secure market environment. Some recent works have explored blockchain to address the transaction security issues for local P2P networks, such as the blockchain-based anonymous rewarding scheme for vehicle-to-grid networks in [24], and utilizing blockchain for crowdsourcing to preserve the privacy of the participants in [25], [26]. However, these methods can not be directly employed in localized spectrum trading for energy-limited UAV networks due to the challenges of the high computation cost associated with establishing a blockchain. Recently, there are several works attempting to apply blockchain into UAV networks. For example, Zhu *et al.* in [27] used blockchain to construct a decentralized information storage platform for air-to-ground industrial networks. In [28], a neural-blockchain based drone-caching approach was designed to ensure ultra-reliable communications. However, spectrum sharing or trading is not considered in these works. Moreover, they also do not propose efficient solutions to deal with the high cost for building a blockchain.

C. Contributions

Motivated by the aforementioned observations, in this paper, we exploit the consortium blockchain technology to develop a secure spectrum trading system named *spectrum blockchain* for UAV-assisted cellular networks. A consortium blockchain is a special blockchain with multiple pre-selected nodes to establish the distributed shared database with moderate cost [29], [30]. To deal with the computation-intensive blockchain creation and verification process, mobile edge computing is applied to help to offload the computation task to proximate authorized edge computing nodes. Under the mobile edge computing aided consortium blockchain framework, secure spectrum trading between the MNO and the UAV operators with privacy protection can be achieved in a distributed manner. Moreover, since spectrum pricing along with the amount of traded spectrum need to be optimized in the spectrum blockchain, a Stackelberg game is formulated to jointly maximize the profits of the MNO and the UAV operators.

Specifically, the contributions of this paper are summarized as follows:

- A pricing-based incentive mechanism is firstly presented to motivate the MNO to open its owned spectrum for UAV networks, in which the MNO acts as a spectrum seller and leases the idle spectrum to a secondary UAV network in exchange for some revenue from the UAV operators.
- To address the potential security and privacy issues caused by malicious attacks in the spectrum trading process, a spectrum blockchain framework is proposed to illustrate the detailed operations of how the blockchain can help to improve the transaction security without relying on a third party.
- Under the blockchain framework, a Stackelberg game is formulated to obtain the optimal spectrum pricing and purchasing strategies, which can jointly maximize the revenue of the MNO and the UAV operators.
- Two pricing schemes are investigated, including *non-uniform pricing* in which different spectrum prices are assigned to different UAV operators, and *uniform pricing* in which the same price applies to all the UAV operators. In addition, we develop a non-uniform pricing algorithm and a distributed spectrum price bargaining algorithm respectively for the two different pricing cases to achieve the optimal solutions.

The rest of this paper is organized as follows. The system model for spectrum trading is introduced in Section II. Detailed operations of spectrum blockchain are illustrated in Section III. In Section IV, a Stackelberg game is formulated to obtain the optimal pricing and purchasing strategies, considering two different pricing schemes. Security assessment and numerical results are shown in Section V before the paper is concluded in Section VI.

II. SYSTEM MODEL FOR SPECTRUM TRADING

A. Network Model

We consider a heterogeneous network, in which one cellular base station owned by the MNO is overlaid with a number of UAVs possessed by different UAV operators. The set of UAV operators is denoted by $\mathcal{N}$, $\mathcal{N} = [1, 2, \cdots, N]$. Since UAVs always operate on unlicensed spectrum with limited capacity that restricts their performances to provide better services for local mobile users, UAV operators have a strong wish to be allowed to share spectrum with the MNO. Nevertheless, the quality of experience (QoE) of cellular users may diminish if UAVs take up some spectrum owned by cellular base station for serving cellular users. Thus, it is difficult for a MNO to be so altruistic to allow UAV users to access licensed spectrum without any remuneration.

To deal with the above issues, an incentive mechanism can be designed to motivate the cooperation between MNO and UAV operators in which the MNO can lease some idle bandwidth to UAVs in exchange for a certain level of profit (e.g., revenue) from the UAV networks while the UAVs will benefit from enhanced quality of service with licensed spectrum. In this way, both systems can increase their own interest and a *win-win situation* can be achieved. Therefore, in this section, a pricing-based incentive mechanism is introduced to promote spectrum sharing between the cellular and UAV networks. In particular, we investigate the spectrum leasing problem and design an incentive mechanism at the data (message) level from a network operator's perspective, in which each UAV operator can temporally buy some licensed spectrum from the MNO to provide better services for its local mobile users. Detailed design considerations are given as follows.

B. Utility Function for the Incentive Mechanism

For the MNO, we define μ_i as the price for each unit of bandwidth provided to the UAV operator i. Let b_i denote the spectrum that UAV operator i intends to purchase. Under the pricing-based incentive mechanism, the MNO's objective is to maximize its revenue obtained from selling the spectrum to the UAV operators. Mathematically, the utility function of the MNO can be modelled as

$$U_{MNO}\left(\boldsymbol{\mu}, \boldsymbol{b}\right) = \sum_{i=1}^{N} \mu_i b_i, \tag{1}$$

where $\boldsymbol{\mu}$ is the spectrum price vector with $\boldsymbol{\mu} = \left[\mu_1, \mu_2, \cdots, \mu_N\right]^T$, and $\boldsymbol{b}$ is a vector of bandwidth purchased by UAV operators with $\boldsymbol{b} = \left[b_1, b_2, \cdots, b_N\right]^T$. Note that $\forall i$, b_i is actually a function of μ_i, i.e., $b_i \triangleq f_i\left(\mu_i\right)$, which indicates that the amount of the spectrum that each UAV operator is willing to buy is dependent on its assigned bandwidth price. Besides, it is assumed that the total available idle bandwidth of the MNO is Q, i.e., the aggregate allocated spectrum for all the UAV operators should not be larger than Q, which can be expressed as $\sum\limits_{i=1}^{N} b_i \le Q$.

From the spectrum purchaser's perspective, each UAV operator i requests spectrum from the MNO according to the real requirement for serving its own users for a specific application. Without loss of generality, in this paper, the utility function of an arbitrary UAV operator is defined as

$$U_i\left(b_i, \mu_i\right) \triangleq \mathcal{R}\left(b_i, d_i\right) - \mathcal{C}\left(b_i, \mu_i\right), \tag{2}$$

where $\mathcal{R}\left(b_i, d_i\right)$ is the payoff/benefit gained from allocated spectrum, with d_i denoting the basic bandwidth demand of UAVs which reflects the service type, and $\mathcal{C}\left(b_i, \mu_i\right)$ is the cost incurred due to buying the spectrum. Note that each UAV operator's utility function consists of two parts: payoff and cost. In the following, we present how to model them under the proposed incentive mechanism.

Payoff: The payoff of a UAV operator i is the benefit or reward gained from allocated spectrum. In this paper, the payoff is modeled as

$$\mathcal{R}\left(b_i, d_i\right) = g_i \mathcal{H}\left(b_i, d_i\right), \tag{3}$$

where $\mathcal{H}\left(b_i, d_i\right)$ is the spectrum obtainment gain, and g_i is a positive coefficient converting the spectrum obtainment gain into monetary reward. Here, we define g_i as the spectrum coins that the UAV operator i possesses to pay for the spectrum received from the MNO. The spectrum coin is one kind of digital cryptocurrency which is employed to facilite the spectrum trading between the MNO and the UAV operators. More details about the spectrum coins will be given in Section III. Intuitively, the more spectrum you are allocated, the more gain you should receive. Thus, $\mathcal{H}\left(b_i, d_i\right)$ should be an increasing function of b_i. Besides, UAV operators should also take into account the real demands of serving users when purchasing bandwidth due to considering the cost of buying spectrum. In this paper, a log function is used to model the spectrum obtainment gain, i.e.,

$$\mathcal{H}\left(b_i, d_i\right) = \log_2\left(1 + \frac{b_i}{d_i}\right). \tag{4}$$

Though other functions (such as linear or exponential functions) can also be used to model the spectrum obtainment gain, log functions are shown in literature to be more suitable to representing the relationship between the network performance and a large class of elastic data traffic [31], [32]. It is observed from (4) that when the amount of received spectrum is zero ($b_i = 0$), the obtained gain $\mathcal{H}$ is also equal to zero, while the gain increases with the increasing of allocated spectrum. Moreover, $\mathcal{H}\left(b_i, d_i\right)$ can also reflect the degree of "happiness" of the UAV operator if receiving bandwidth b_i under the demand d_i. These indicate that (4) is able to capture the relationship between the UAV operators' benefit and the received bandwidth.

Cost: $\mathcal{C}\left(b_i, \mu_i\right)$ denotes the cost incurred when UAV operator i purchases spectrum from the MNO. In general, the cost increases with the increasing of the amount of obtained spectrum. Thus, it can be easily modeled as

$$\mathcal{C}\left(b_i, \mu_i\right) = \mu_i b_i. \tag{5}$$

Therefore, the utility function of an arbitrary UAV operator can be written as

$$U_i\left(b_i, \mu_i\right) = g_i \log_2\left(1 + \frac{b_i}{d_i}\right) - \mu_i b_i. \tag{6}$$

Obviously, with a larger bandwidth b_i, UAV operator i can obtain a more satisfactory system performance, however, this also increases the cost. Therefore, optimal strategies are needed for a rational operator to balance the cost and achieved benefit in order to maximize its utility.

C. Security Threats

In the above subsection, we focus on designing a pricing-based incentive mechanism for spectrum trading between the cellular and UAV networks. However, this monetary approach always needs to rely on trusted centers that may not only leak operators' privacy, but also be vulnerable to attack. In addition, due to the untrusted broadcast features and wireless transmission of the UAV networks, there also exist significant trust issues which may threaten system security and privacy. Typically, three kinds of attackers or adversaries may appear:

1) Malicious spectrum provider: A malicious cellular operator who advertises fraudulent spectrum leasing services without enough available spectrum.

2) Malicious spectrum buyer: A malicious UAV operator who pretends that it has not received any spectrum from the cellular operator and refuses to pay.

3) Malicious trusted third party: The malicious trust center may not only disclose the MNO's privacy but tamper the UAV operators' credit value (e.g., spectrum coins) for profit.

To deal with these security threats, distributed and trusted management schemes are needed to identify and defend against malicious peers. To this end, we exploit blockchain technology to provide a trusted environment to enhance secure spectrum trading among the operators.

III. SPECTRUM BLOCKCHAIN

Blockchain is a P2P decentralized ledger, which is designed to efficiently record transactions among participants in a verifiable and permanent way, without relying on a trusted center. Blockchain technology enables spectrum trading to be executed in a distributed, transparent and secure market environment. Thus, in this section, a blockchain-enabled *spectrum blockchain* framework is proposed to support secure spectrum trading between the cellular and UAV operators.

A. Overview of Spectrum Blockchain

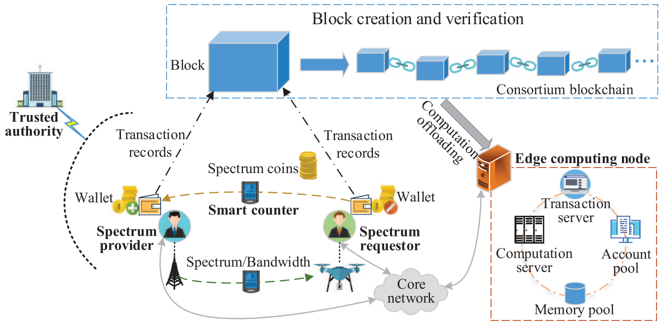

Fig. 1. Framework of spectrum blockchain.

The core issue of the blockchain is a computational processing called "*mining*" (consensus), in which a set of participants called "*miners*" need to solve a complex computation problem, i.e., proof-of-work puzzle, to confirm and secure the integrity and validity of transactions before adding the records into the blockchain. The security and privacy of the blockchain depend on the distributed consensus mechanism managed by these miners. However, in a traditional public/permissionless blockchain (such as Bitcoin and Ethereum), the consensus stage is executed by all nodes (miners) which leads to high cost. To relieve the computation-intensive challenge of establishing a blockchain, unlike existing works, in this paper, we use consortium blockchain technology to perform distributed spectrum trading. A consortium blockchain is a special permissioned blockchain in which the consensus process is executed on pre-selected nodes with moderate cost[1]. Thus, it is more suitable and feasible for energy-constraint UAV networks. Moreover, to further solve the high computing power needed in blockchain creation, we leverage edge computing as a network enabler to offload the computation-intensive proof-of-work puzzles to proximate edge computing nodes. Compared to traditional cloud computing [34], [35], edge computing brings network resources (e.g., computation or storage resources) closer to the users which can effectively shorten the transmissions delay and reduce the energy consumption [36]. The practicality of integrating edge computing and blockchain comes from both the same decentralized infrastructure and the same functions of storage and computation [37].

The consortium blockchain-based secure spectrum trading framework is shown in Fig. 1, which consists of the following major entities.

- *Trusted authority (TA)*: The TA is responsible for initializing the whole spectrum trading system, generating public parameters and cryptographic keys, and managing the operators' identities. Note that the TA only serves as a parameter initializer to provide identity authorization and certificate issuance of entities before running spectrum blockchain. It will remain offline for most of the time. That is to say, this role does not conflict with the decentralization of the blockchain.
- *Spectrum provider and requestors*: UAV operators act as spectrum requestors to purchase bandwidth from the spectrum provider. The MNO acts as spectrum provider and leases its own idle licensed spectrum to UAV operators in return for reward.
- *Edge computing nodes*: It is assumed that there are edge devices (nodes) in the system which can provide computing and storage services. As shown in Fig. 1, each edge computing node consists of four components: a transaction server, an account pool, a memory pool and a computation server. The transaction server collects the real-time spectrum requests from the UAV operators and the price announcements from the MNO, and transmits the trading-related information among the MNO and the UAV operators via the core network. Here, a digital cryptocurrency named spectrum coin works as UAV operators' digital assets to purchase spectrum from the MNO. Each UAV operator has a virtual wallet to manage personal spectrum coins. The account pool in the edge computing nodes records and stores spectrum coins in the personal wallet of UAV operators, and the numerical value of the amount of available spectrum of MNO. The

---

[1] As for consortium blockchain, Hyperledger is one of the most famous application platforms [33].

memory pool stores all the transaction records of local operators. The computation server provides computing power for the process of block generation and validation.

- *Smart counters*: A built-in smart counter in each entity records the amount of traded spectrum in real time. The UAV operators pay the MNO according to the records of smart counters.

In the framework, the spectrum trading between the UAV operators and the MNO are forwarded based on blockchain technology, in which all the transactions should be announced to the audit edge computing nodes for verification through broadcasting, instead of direct transactions among them. In this way, a secure spectrum trading environment can be established, which guarantees transaction security and privacy protection. The detailed mechanism of operation is given in Section III-C.

B. Design Goals

Based on the proposed blockchain-enabled spectrum trading scheme, the following properties are expected to be achieved:

- **Operator authentication**. Operators should be authenticated in an anonymous way so that no adversary can impersonate a registered operator.
- **Privacy**. The requests, announcements and transactions do not leak any personal information about their sources (i.e., anonymity).
- **Traceability**. The TA can track the identity of a operator in case of a dispute or something unexpected occurs.
- **Reliability**. According to the design idea of blockchain, every operator can manage a copy of the whole block chains of transactions, and each transaction is related to the phases of spectrum trading. Thus, an entity is unable to modify the transactions without authorization.
- **Data confidentiality and integrity**. The contents of any trading messages should be protected from the operators, edge computing nodes, and other entities. All accepted messages should be transmitted without being altered.

C. Operation Details of Blockchain-based Secure Spectrum Trading

As depicted in Fig. 2, there are mainly three parts for the operation of the spectrum blockchain for secure spectrum trading. (i) *Reputation-based miner selection*. Since not all the edge nodes are trusted in the system, those malicious edge nodes may falsely modify or discard transaction records during their mining process. Thus, it is necessary to design a secure and efficient reputation management scheme for the edge computing nodes and select the candidates with high reputation acting as active miners to ensure a reliable consensus process. (ii) *Block mining and generation*. The selected edge computing nodes then act as miners to collect the transaction records from the MNO and the UAV operators, and perform block generation. (iii) *Block verification with consensus process*. A new generated block needs to be audited by the miners via the consensus mechanism before storing it. As long as most miners agree on the block data, this block can be added into the spectrum blockchain. More details are given in the subsequent discussions.

1) System initialization: In the spectrum blockchain, to guarantee the data integrity and unforgeability, an elliptic curve digital signature algorithm and asymmetric cryptography [38] are utilized for system initialization. Every operator becomes a legitimate entity with proprietary registration information after passing identity authentication by a TA, such as a government department. A UAV operator i can firstly get its certificate $Cert_i$ from the TA and the $Cert_i$ is used to uniquely identify itself through binding its registration information, e.g., identity ID_i and license plate number. Then UAV operator i joins the spectrum blockchain network with its $Cert_i$ and obtains its public/private key pair (PK_i, SK_i) and wallet address add_i. Here, each UAV operator's account includes its account balance Bal_i, certificate $Cert_i$, current spectrum coin value g_i, public/private key pair (PK_i, SK_i) and wallet address add_i. The MNO's account contains its account balance Bal_{MNO}, available spectrum, public/pricate key pair (PK_{MNO}, SK_{MNO}) and wallet address add_{MNO}. The asymmetric cryptography scheme for ensuring the authenticity and integrity of information transmission is expressed as

$$Dec_{PK_i}\left(Sig_{SK_i}\left(H\left(m\right)\right)\right) = H\left(m\right), \qquad (7)$$

where Sig_{SK_i} is the digital signature of sender i with private key, Dec_{PK_i} is to decode the signed data with sender i's public key, $H\left(m\right)$ is the hash digest of message m [39]. When executing system initialization, each operator uploads its wallet addresses being used to the account pool of its nearest edge computing node. Operators check the integrity of their account and download data about their account from a memory pool in the edge computing nodes. The memory pool stores all transaction records in the spectrum blockchain.

2) Reputation-based miner selection: Since not all edge devices/nodes are trusted, an edge node that wants to be a miner candidate needs to firstly submit its identity-related information to the TA. The TA verifies the validity of the edge node by estimating its average reputation according to feedback information about the reputation opinions from operators. Only if its average reputation is higher than a trust threshold or ranked at the forefront, the edge node can be issued a legitimate certificate and act as a miner to perform mining task. Here, to calculate edge nodes' reputation, a subjective logic model based on historical interactions between the edge nodes and operators is utilized, which is a framework for probabilistic information fusion operated on subjective beliefs about the world [40]. The subjective logic uses the term "opinion" to indicate the representation of a subjective belief, and models positive statements, negative statements and uncertainty. It also provides a broad range of logical operators to combine and relate different opinions [41]. Thus, the subjective logic model is a suitable mechanism to quantify the edge computing nodes' reputation. The basic procedure of using a subjective logic model for reputation calculation is given as follows.

Considering an operator ope_i and an edge node e_j, the operator may interact with the edge node during the spectrum trading. The trustworthiness (i.e., local opinion) of ope_i to e_j in the

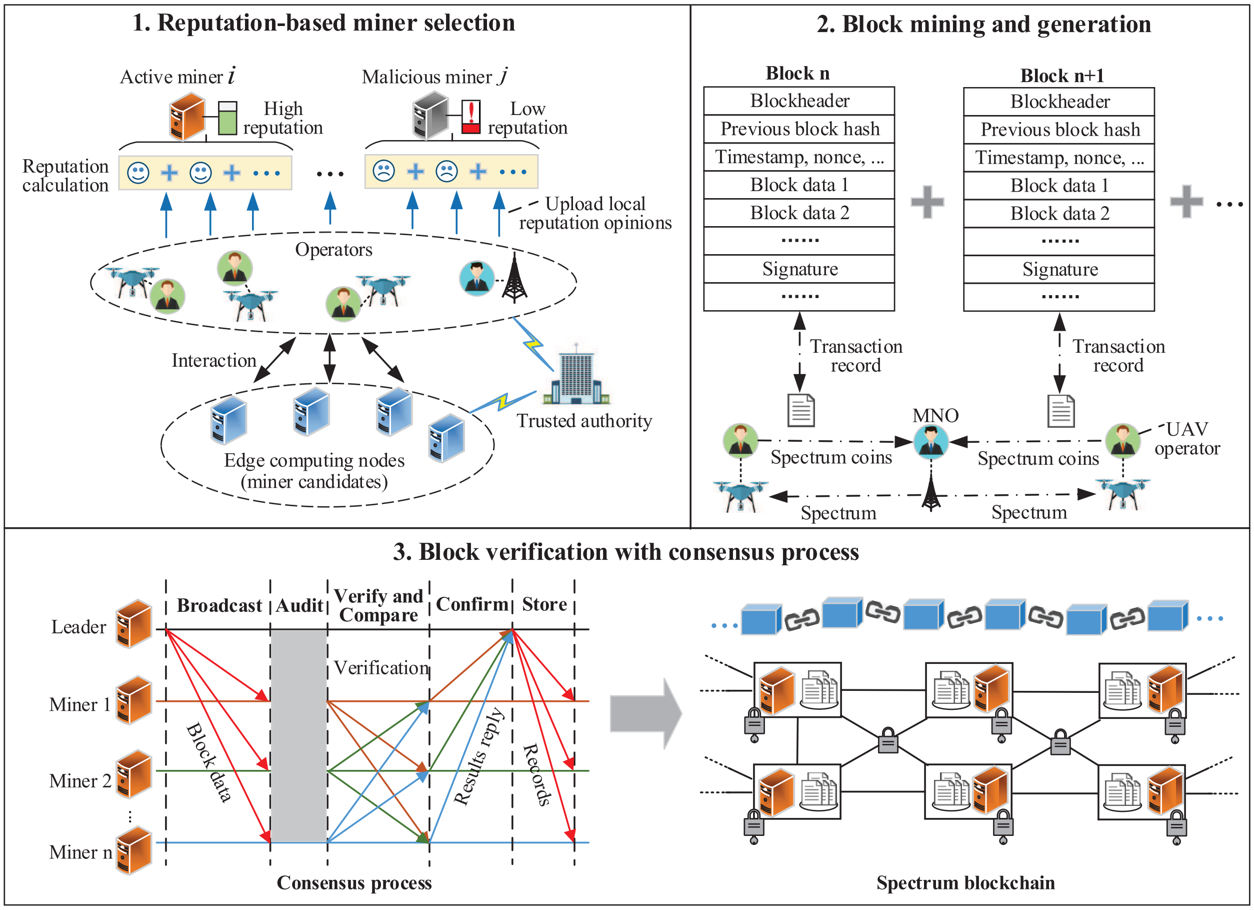

Fig. 2. Operation procedure of the blockchain-based secure spectrum trading.

subjective logic can be formally expressed as a local opinion vector $\omega_{i\to j}$, i.e., $\omega_{i\to j} := \{bel_{i\to j}, dis_{i\to j}, uncer_{i\to j}\}$, where $bel_{i\to j}$, $dis_{i\to j}$ and $uncer_{i\to j}$ represent the belief, distrust, and uncertainty, respectively. Here, $bel_{i\to j}, dis_{i\to j}, uncer_{i\to j} \in [0,1]$ and $bel_{i\to j} + dis_{i\to j} + uncer_{i\to j} = 1$. According to the subjective logic model, we have

$$\begin{cases} bel_{i\to j} = (1 - uncer_{i\to j})\,\frac{N_{PI}}{N_{PI}+N_{NI}}, \\ dis_{i\to j} = (1 - uncer_{i\to j})\,\frac{N_{NI}}{N_{PI}+N_{NI}}, \\ uncer_{i\to j} = 1 - succe_{i\to j}, \end{cases} \tag{8}$$

where N_{PI} is the number of positive interactions, while N_{NI} is the number of negative interactions. The positive interaction means that the operators believe that the services provided by edge computing nodes are relevant and useful. The communication quality $succe_{i\to j}$ of a link between ope_i and e_j, i.e., the successful transmission probability of data packets, determines the uncertainty of local opinion vector $uncer_{i\to j}$. According to $\omega_{i\to j}$, the reputation value $rep_{i\to j}$ represents the expected belief of operator ope_i that edge node e_j is trusted and behaves in the spectrum blockchain network, which can be expressed as

$$rep_{i\to j} = bel_{i\to j} + \phi uncer_{i\to j}, \tag{9}$$

where $\phi \in [0,1]$ is the given constant indicating an effect level of the uncertainty for reputation. Operators can calculate all edge nodes' reputation based on (8) and (9). Moreover, to achieve higher credibility and accuracy, a multi-weight subjective logic model can be exploited to characterize the local opinions, considering different influencing factors such as interaction frequency, interaction timeliness and interaction effects, while taking into account the recommended opinions from other operators. Further studies about the multi-weight subjective logical model can refer to the literature [40], [41].

After calculating the reputation opinions, each operator votes for y candidates from the edge nodes as the potential miners according to its local ranking of reputation opinions for edge nodes. Then, the top k candidates with the highest reputation are selected to be active miners. These active miners will be authorized by the TA and join in the spectrum blockchain to carry out trading-related tasks.

3) Trading spectrum between MNO and UAV operators: UAV operators send spectrum requests to the transaction server of a nearby miner (i.e., selected edge node). The transaction server in the edge node counts the total spectrum demands and broadcasts these demands to the MNO. The edge node works as a spectrum broker and sets a pricing-based incentive mechanism (as shown in Section II) to attract MNO for participation in the spectrum trading. Motivated by the incentive mechanism, the MNO determines its initial spectrum to be leased and the corresponding price and gives responses to the transaction server. The transaction server then coordinates and matches the spectrum supply and demand among the operators. According to the pricing-based incentive mechanism in Section II, it can be seen that both MNO and UAV operators are rational and selfish in the process of spectrum trading, in which all of the them attempt to maximize their own benefits. Thus, to balance spectrum demand and supply in our spectrum blockchain, a solution for analyzing and determining the optimal spectrum price for MNO and the optimal spectrum requests for UAV operators is necessary. Here, a game theoretic method is used to execute spectrum negotiations and transactions between the seller and the buyers. More details about the optimal spectrum trading strategies based on game theory will be given in Section IV.

After spectrum trading, a UAV operator transfers spectrum coins from its wallet to the wallet address given by the MNO. The MNO obtains the latest blockchain data from the memory pool of edge nodes to verify this payment activity. The UAV operators generate new transaction records, and the MNO verifies and digitally signs the transaction records and thus uploads the records to blockchain miners for audit.

4) Block mining and generation: Edge nodes collect all local transaction records between spectrum seller and buyers during a certain period, and then encrypt and digitally sign these records to guarantee authenticity and accuracy. As shown in part 2 of Fig. 2, all the transaction records are packaged into blocks. A block consists of a transaction set, a timestamp, a hash value of pre-block and other information that are significant to record. For traceability and verification, each block has a unique and cryptographic hash to prior blocks in the spectrum blockchain. Similar to that in Bitcoin, the edge nodes try to find their own valid proof-of-work about data audit (i.e., a hash value meeting a certain level of difficulty) [42]. Each edge node calculates the hash value of its block based on a random nonce value φ, timestamp, transactions' merkel root, and historical block hash value and so on (denoted as $previous_{data}$), which is written as:

$$Hash\left(\varphi + previous_{data}\right) < N_{difficulty}, \tag{10}$$

where $N_{difficulty}$ is a number that can be adjusted by the system to control the speed of finding out the specific nonce value φ [43]. Each authorized edge node (miner) in the spectrum blockchain competes to create a block by finding a valid proof-of work (i.e., nonce value φ). After a valid proof-of-work is found, the fastest miner works as a leader and broadcasts the block and the specific nonce value to other edge nodes in the spectrum blockchain for audit and verification. If other edge nodes agree on the block, data information in this new block will be added to the spectrum blockchain in a linear and chronological order, and the fastest miner is awarded by spectrum coins.

5) Block verification with consensus process: To ensure that each authorized node in the system has a copy of the recognized version of the whole blockchain, the audit stage, i.e., the block verification with consensus process should be carried out. To this end, a distributed consensus algorithm is proposed in Algorithm 1 to reach consensus efficiently in the spectrum blockchain. More details are given as follows.

Algorithm 1 Distributed consensus algorithm

```
The miner leader broadcasts the $Block\_data$ to all edge nodes;
for all edge computing nodes do
    if its own data do not contain the block information then
        Compare its own data with data in the block;
        if all the data are identical then
            Set $verify\left(Block\_data\right) = True$;
        else
            Set $verify\left(Block\_data\right) = False$;
        end if
        Broadcast its audit result to other edge nodes for mutual supervision and verification;
        Each edge node compares its result with others and sends a reply back to the leader;
    else if its own data contain the block data then
        No action;
    end if
end for
The leader analyzes the received replies from edge nodes;
if all the edge nodes approve the block then
    The leader will send records including current audited block data and a corresponding signature to all authorized edge nodes for storage;
else if some edge nodes do not agree on the block then
    The leader checks the audit results and sends the block data to these edge nodes once again for audit;
end if
Discard the block that fails to pass the verification;
Go back to the step of block generation for next round of audit.
```

As shown in part 3 of Fig. 2, the miner leader firstly broadcasts block data $Block\_data$, timestamp, and the specific φ to other authorized edge nodes for audit. In order to achieve mutual supervision and verification, these edge nodes check the block data and broadcast their audit results with signatures to each other. After receiving the audit results, each edge node compares its result with others and sends a reply back to the miner leader. The reply is made up of the edge node's signatures, audit result, comparison result, and the records of received audit results. The leader performs statistics analysis of received replies from edge nodes. If the block data is approved by all the edge nodes, i.e., reaching consensus, the leader will broadcast records including current audited block data and a corresponding signature to all authorized edge nodes for storage. Then, the new block is added into the consortium blockchain in a linear and chronological order, which contains a cryptographic hash to the prior block. At the same time, every node synchronizes its local copy of the blockchain with the new block. However, if some edge nodes do not agree on the block data, the leader needs to check the audit results, and send the ledger update requests to these edge nodes once again for audit if necessary. At last, the block that fails to pass the verification will be discarded, and the implementation phase goes back to the step of block mining and generation for next round of consensus process.

IV. OPTIMAL SPECTRUM TRADING STRATEGIES

In this section, we present the problem definition for the spectrum pricing and the amount of traded spectrum between the MNO and the UAV operators, and analyze the optimal strategies that are made in Section III-C to maximize the utilities of both sides during the spectrum blockchain management process.

A. Problem Formulation

In Section II, a pricing-based incentive mechanism is introduced to motivate the spectrum trading between the cellular networks and the UAV networks. Since both MNO and UAV operators are selfish and rational entities who try to pursue personal utility maximization in a distributed manner, it is obvious that game theory is the most suitable tool to analyze the problem. The game should involve two phases, in which the MNO firstly announces the initial price of the spectrum to be leased and the UAV operators then request the spectrum according to the price. Thus, it is reasonable to formulate the process as a Stackelberg game [44], [45].

A Stackelberg game is a strategic game that consists of a leader and several followers competing with each other on certain resources. In this paper, we formulate the MNO as the leader, and the UAV operators as the followers. The leader (i.e., MNO) needs to finally find the optimal spectrum price $\boldsymbol{\mu}$ to maximize its revenue within its limited available spectrum. Every follower (i.e., UAV operator) will respond with the best amount of spectrum request (i.e., b_i) based on the price given by the leader. The optimization problems can be formulated as follows.

Leader's spectrum pricing:

$$\max_{\boldsymbol{\mu}\succcurlyeq 0} U_{MNO}\left(\boldsymbol{\mu},\boldsymbol{b}\right), \tag{11}$$

$$\text{s.t.} \sum_{i=1}^{N} b_i \le Q. \tag{12}$$

Follower's spectrum purchasing:

$$\max_{b_i\ge 0} U_i\left(b_i,\mu_i\right), \tag{13}$$

where $U_{MNO}\left(\boldsymbol{\mu},\boldsymbol{b}\right)$ and $U_i\left(b_i,\mu_i\right)$ are defined in (1) and (6), respectively.

The above problems together form a Stackelberg game. The objective is to find the Stackelberg Equilibrium (SE) point(s) from which neither the leader (MNO) nor the followers (UAV operators) have incentives to deviate. For the proposed Stackelberg game, the SE is defined as follows.

Definition 1 (Stackelberg Equilibrium). *Let $\boldsymbol{\mu}^*$ be a solution for the spectrum pricing problem and b_i^* be a solution for the spectrum purchasing problem of the ith UAV operator. Then the point $(\boldsymbol{\mu}^*,\boldsymbol{b}^*)$ is a SE for the proposed Stackelberg game if for any $(\boldsymbol{\mu},\boldsymbol{b})$ with $\boldsymbol{\mu}\succcurlyeq 0$ and $\boldsymbol{b}\succcurlyeq 0$, the following conditions are satisfied:*

$$U_{MNO}\left(\boldsymbol{\mu}^*,\boldsymbol{b}^*\right) \ge U_{MNO}\left(\boldsymbol{\mu},\boldsymbol{b}^*\right), \tag{14}$$

$$U_i(b_i^*,\boldsymbol{\mu}^*) \ge U_i(b_i,\boldsymbol{\mu}^*). \tag{15}$$

Note that the same or different prices can be charged to the UAV operators, which here are referred to as the *uniform and non-uniform* pricing schemes, respectively. In the following, we use the backward induction method to analyze the Stackelberg game under these two pricing schemes.

B. Non-Uniform Pricing Scheme

The non-uniform pricing scheme is firstly considered, in which the MNO can set different unit prices for leasing spectrum to different UAV operators. If the spectrum price for a UAV operator i is donated as μ_i, the optimal spectrum purchasing problem can be written as

$$\underline{\textit{Problem 1:}}\ \max_{b_i\ge 0} g_i\log_2\left(1+\frac{b_i}{d_i}\right)-\mu_i b_i. \tag{16}$$

It is observed that the objective function is a concave function over b_i, and the constraint is affine. Thus Problem 1 is a convex optimization problem. For a convex optimization problem, the optimal solution must satisfy the Karush-Kuhn-Tucher (KKT) conditions. Therefore, by solving the KKT conditions, the optimal solution for Problem 1 can be obtained in the following theorem.

Theorem 1. *For a given bandwidth price μ_i, the optimal solution for Problem 1 is given by*

$$b_i^* = \left\{ \begin{array}{cl} \frac{g_i}{\mu_i \ln 2}-d_i, & \text{if } \mu_i < \frac{g_i}{d_i \ln 2}, \\ 0, & \text{if } \mu_i \ge \frac{g_i}{d_i \ln 2}. \end{array} \right. \tag{17}$$

Proof: Please refer to Appendix A. ■

From the Theorem 1, it is observed that if the bandwidth price is too high, i.e., $\mu_i \ge \frac{g_i}{d_i \ln 2}$, UAV operator i will not buy any bandwidth, which indicates that operator i will not participate in the game. Besides, under the same spectrum price, more bandwidth is allocated to the UAV operator with higher spectrum coins for the same demand type. Substituting (17) into MNO's optimal pricing strategies, i.e., combining (11) and (12), the optimization problem at the MNO side can be written as

$$\underline{\textit{Problem 2:}}\ \max_{\boldsymbol{\mu}\succcurlyeq 0} \sum_{i=1}^{N}\left(\frac{g_i}{\ln 2}-\mu_i d_i\right)^{+}, \tag{18}$$

$$\text{s.t.} \sum_{i=1}^{N}\left(\frac{g_i}{\mu_i \ln 2}-d_i\right)^{+} \le Q, \tag{19}$$

where $(\cdot)^{+} \triangleq \max\left(\cdot,0\right)$. Note that the objection function is a convex function of $\boldsymbol{\mu}$, while the maximization of a convex function is generally non-convex which is difficult to solve. However, it is shown in the following that the above problem can be converted to a series of convex subproblems.

For UAV operator i ($i=1,2,\cdots,N$), we introduce the following indicator function

$$\chi_i = \left\{ \begin{array}{l} 1,\ \text{if } \mu_i < \frac{g_i}{d_i \ln 2}, \\ 0,\ \text{otherwise}. \end{array} \right. \tag{20}$$

Then, the Problem 2 can be reformulated as

$$\text{Problem 2a:} \quad \max_{\boldsymbol{\chi},\, \boldsymbol{\mu} \succcurlyeq 0} \sum_{i=1}^{N} \chi_i \left(\frac{g_i}{\ln 2} - \mu_i d_i \right), \tag{21}$$

$$\text{s.t.} \sum_{i=1}^{N} \chi_i \left(\frac{g_i}{\mu_i \ln 2} - d_i \right) \le Q, \tag{22}$$

$$\chi_i \in \{0,1\}, \forall i, \tag{23}$$

where $\boldsymbol{\chi} \triangleq [\chi_1, \chi_2, \cdots, \chi_N]^T$. It is observed that the above problem is still non-convex due to $\boldsymbol{\chi}$. Nevertheless, for a given indicator vector $\boldsymbol{\chi}$, it is easy to verify that Problem 2a is convex. Under this observation, we consider a special case of Problem 2a by assuming that the total available bandwidth of MNO is sufficient large (i.e., Q is large enough) such that all the requests from the UAV operators are admitted. As a result, the indicators for all UAV operators are equal to 1, i.e., $\mu_i < \frac{g_i}{d_i \ln 2}$, $\forall i$. Then, Problem 2a can be further converted to a minimization problem as

$$\text{Problem 2b:} \quad \min_{\boldsymbol{\mu} \succcurlyeq 0} \sum_{i=1}^{N} \mu_i d_i, \tag{24}$$

$$\text{s.t.} \sum_{i=1}^{N} \frac{g_i}{\mu_i \ln 2} \le Q + \sum_{i=1}^{N} d_i. \tag{25}$$

It is not difficult to see that the above objective function now becomes convex, and minimization of convex function is a convex optimization problem. The optimal solution is given by the following proposition.

Proposition 1. *The optimal solution to Problem 2b is given by*

$$\mu_i^* = \frac{1}{\ln 2} \sqrt{\frac{g_i}{d_i}} \frac{\sum_{i=1}^{N} \sqrt{g_i d_i}}{Q + \sum_{i=1}^{N} d_i}, \forall i \in \{1, 2, \cdots, N\}. \tag{26}$$

Proof: Please refer to Appendix B. ■

The optimal solution of Problem 2b can be related to the original optimization problem, i.e., Problem 2, in the following proposition.

Proposition 2. *The bandwidth prices given by (26) are the optimal solutions of Problem 2 if and only if the following condition holds:*

$$Q > \frac{\sum_{i=1}^{N} \sqrt{g_i d_i}}{\min_i \sqrt{\frac{g_i}{d_i}}} - \sum_{i=1}^{N} d_i. \tag{27}$$

Proof: Please refer to Appendix C. ■

Combining with the above results obtained from a number of subproblems, the original problem can now be addressed. The optimal solution of Problem 2 is given by the following theorem.

Theorem 2. *Assuming that all the UAV operators are sorted in the order $\frac{g_1}{d_1} > \frac{g_2}{d_2} \cdots \frac{g_{N-1}}{d_{N-1}} > \frac{g_N}{d_N}$, the optimal solution for Problem 2 can be expressed as*

$$\boldsymbol{\mu}^* = \begin{cases} \frac{q_N}{\ln 2} \left[\sqrt{\frac{g_1}{d_1}}, \sqrt{\frac{g_2}{d_2}}, \cdots, \sqrt{\frac{g_N}{d_N}} \right]^T, & \text{if } Q > Y_N \\ \frac{q_{N-1}}{\ln 2} \left[\sqrt{\frac{g_1}{d_1}}, \cdots, \sqrt{\frac{g_{N-1}}{d_{N-1}}}, \infty \right]^T, & \text{if } Y_N \ge Q > Y_{N-1} \\ \vdots & \vdots \\ \frac{q_1}{\ln 2} \left[\sqrt{\frac{g_1}{d_1}}, \infty, \cdots, \infty \right]^T, & \text{if } Y_2 \ge Q > Y_1 \end{cases}, \tag{28}$$

where $q_K = \frac{\sum_{i=1}^{K} \sqrt{g_i d_i}}{Q + \sum_{i=1}^{K} d_i}$, and $Y_K = \frac{\sum_{i=1}^{K} \sqrt{g_i d_i}}{\sqrt{\frac{g_K}{d_K}}} - \sum_{i=1}^{K} d_i$, $\forall K \in \{1, 2, \cdots, N\}$.

Algorithm 2 Non-uniform spectrum pricing and purchasing algorithm

```
Input: the number of UAV operators $N$, basic bandwidth demand $d_i$ ($i \in \mathcal{N}$) for each UAV operator, total amount of available idle spectrum $Q$, and $g_i$;
Output: Non-uniform spectrum price vector $\boldsymbol{\mu}$ and bandwidth purchasing vector $\boldsymbol{b}$;
    Spectrum Pricing
 1: Based on the spectrum blockchain network, an authorized miner acts as a trusted coordinator and local computation center, and sets $K = N$.
 2: for $K = N \to 1$ do
 3:     Sort the $K$ operators such that $\frac{g_1}{d_1} \ge \cdots \ge \frac{g_{K-1}}{d_{K-1}} \ge \frac{g_K}{d_K}$.
 4:     Compute $q_K = \frac{\sum_{i=1}^{K} \sqrt{g_i d_i}}{Q + \sum_{i=1}^{K} d_i}$ and compare $q_K$ with $\sqrt{\frac{g_K}{d_K}}$.
 5:     if $q_K > \sqrt{g_K / d_K}$ then
 6:         Remove the operator $K$ from the game, set $K = K - 1$, and go to step 4.
 7:     else
 8:         Go to step 9.
 9:         With $q_K$ and $K$, the spectrum price $\mu_i$ for operator $i$ is given by
            $\mu_i = \begin{cases} \frac{q_K}{\ln 2} \sqrt{\frac{g_i}{d_i}}, & \text{if } i \le \text{K} \\ \infty, & \text{otherwise.} \end{cases}$
10:     end if
11: end for
12: A miner broadcasts the price vector to the UAV operators in the spectrum blockchain.
    Spectrum Purchasing
13: After receiving the spectrum prices, the UAV operators decide the amount of their spectrum request according to (17).
14: The miner collects the spectrum demand information from the UAV operators and provides feedback to the MNO.
15: The MNO finally leases the spectrum bandwidth to the UAV operators while the UAV operators transfer the corresponding spectrum coins to the MNO through the blockchain network with security and privacy protection.
```

Proof: From the Proposition 2, it is observed that the UAV operators which cannot fulfill the condition (27), are removed from the game and the bandwidth price for these operators will be set to ∞. If $Q > Y_N$, the optimal bandwidth price for each UAV operator is already obtained by Proposition 2. For the other intervals of Q, e.g., $Y_{N-1} < Q \leq Y_N$, the proof of the optimality for the corresponding $\boldsymbol{\mu}^*$ can be obtained similarly as Proposition 2, and is thus omitted. The proof of Theorem 2 thus follows. ■

Now, the Stackelberg game for the non-uniform pricing scheme is completely solved. With the optimal solution obtained in Theorem 1 and Theorem 2, the SE for the proposed Stackelberg game is given as follows.

Theorem 3. *The SE for the Stackelberg game formulated in the Problems 1 and 2 is* $(\boldsymbol{\mu}^*, \boldsymbol{b}^*)$*, where* $\boldsymbol{\mu}^*$ *is given by (28), and* $\boldsymbol{b}^*$ *is given by (17).*

In practice, the unique SE can be achieved in a centralized manner as in [45]. However, it is observed from the Theorem 2 that, to obtain the optimal spectrum price vector $\boldsymbol{\mu}^*$, the MNO has to collect and measure the network state information to compute and compare $\sqrt{g_i/d_i}$ for each individual UAV operator i. This will lead to high computation complexity and communication overhead for the MNO and the UAV operators. Fortunately, owning to the distributed ledger benefit of blockchain, such information can be safely collected and processed by the edge computing nodes and then shared in the whole network. Moreover, based on the special structure of (28), to further relieve the burden, we propose an optimal non-uniform pricing scheme for the MNO and the corresponding spectrum purchasing scheme for each UAV operator by Algorithm 2. Through leveraging the blockchain and exploiting miners acting as local coordinators and trusted computation center, an efficient implementation solution can be available.

C. Uniform Pricing Scheme

In this subsection, the uniform pricing scheme is considered, in which the MNO charges all the UAV operators the same unit price for their bandwidth requests, i.e., $\mu_i = \mu, \forall i$. With a uniform price μ, the optimal bandwidth request for UAV operators can be easily obtained from (17) by replacing μ_i with μ, which is given by the following theorem.

Theorem 4. *For a given uniform bandwidth price* μ*, the optimal bandwidth request solution for UAV operators is given by*

$$b_i^* = \begin{cases} \frac{g_i}{\mu \ln 2} - d_i, & \text{if } \mu < \frac{g_i}{d_i \ln 2}, \\ 0, & \text{if } \mu \geq \frac{g_i}{d_i \ln 2}. \end{cases} \tag{29}$$

Then, at the MNO's side, similar to Problem 2, the optimal pricing problem can be expressed as

$$\underline{\textit{Problem 3:}} \ \max_{\mu > 0} \sum_{i=1}^{N} \left(\frac{g_i}{\ln 2} - \mu d_i \right)^+, \tag{30}$$

$$\text{s.t.} \ \sum_{i=1}^{N} \left(\frac{g_i}{\mu \ln 2} - d_i \right) \leq Q. \tag{31}$$

It is observed that Problem 3 has similar formation as Problem 2, and its solution can be found in the same way. Details are thus omitted here for brevity.

Algorithm 3 Distributed spectrum price bargaining algorithm

```
• Step 1: The MNO sets the initial spectrum price $\mu$, and sends the $\mu$ to a nearby miner in the blockchain network. The miner records the information and broadcasts the price to all the UAV operators.
• Step 2: Each UAV operator computes its optimal bandwidth request $b_i^*$ based on (29) for the given $\mu$, and gives responses back to the miner.
• Step 3: The miner records the feedback from the UAV operators and measures the total bandwidth requests $\sum_{i \in \mathcal{N}} b_i$, and then transmits the related data to the MNO. The MNO compares the total demand with its available spectrum $Q$. Assume that $\tau$ is a small positive constant that controls the algorithm accuracy, and $\Delta\mu > 0$ is a small step size.
if $\sum_{i \in \mathcal{N}} b_i > Q + \tau$ then
    The MNO increases the price by $\Delta\mu$;
else if $\sum_{i \in \mathcal{N}} b_i < Q - \tau$ then
    The MNO decreases the price by $\Delta\mu$;
end if
After that, the MNO sends the new spectrum price to the miner. Then, the miner updates the price and broadcasts it to UAV operators. The corresponding transactions are recorded and verified in the spectrum blockchain to guarantee the security.
• Step 4: Step 2 and Step 3 are repeated until $\left|\sum_{i \in \mathcal{N}} b_i - Q\right| \leq \tau$.
```

Theorem 5. *Assuming that all the UAV operators are sorted in the order* $\frac{g_1}{d_1} > \frac{g_2}{d_2} \cdots \frac{g_{N-1}}{d_{N-1}} > \frac{g_N}{d_N}$*, the optimal solution for Problem 3 is given by*

$$\mu^* = \begin{cases} \tilde{\mu}_N, & \text{if } Q > \tilde{Y}_N \\ \tilde{\mu}_{N-1}, & \text{if } \tilde{Y}_N \geq Q > \tilde{Y}_{N-1} \\ \vdots & \vdots \\ \tilde{\mu}_1, & \text{if } \tilde{Y}_2 \geq Q > \tilde{Y}_1 \end{cases}, \tag{32}$$

where $\tilde{\mu}_K = \frac{\sum_{i=1}^{K} g_i}{\left(Q + \sum_{i=1}^{K} d_i\right) \ln 2}$ *and* $\tilde{Y}_K = \frac{d_K \sum_{i=1}^{K} g_i}{g_K} - \sum\limits_{i=1}^{K} d_i$, $\forall K \in \{1, 2, \cdots, N\}$.

From Theorem 5, it is not difficult to observe that when the total available bandwidth margin Q is given, the optimal price strategy is unique. Thus, the SE for this Stackelberg game is also unique and given as follows.

Theorem 6. *The SE for the Stackelberg game formulated with the uniform pricing scheme is* $(\mu^*, \boldsymbol{b}^*)$*, where* μ^* *is given by (32), and* $\boldsymbol{b}^*$ *is given by (29).*

For the uniform pricing scheme, to obtain the SE of the proposed Stackelberg game, some insights about the optimization problem are introduced at first. It can be observed from Problem 3 that both the objective function and the left hand side of the constraint condition (31) are monotonically decreasing functions of μ. Thus, when the constraint condition is satisfied with equality, the objective function can be maximized. Based on this fact, a distributed spectrum price bargaining algorithm is proposed in Algorithm 3 to implement the proposed game.

It can be seen that Algorithm 3 is a distributed algorithm which greatly reduces the amount of information that needs to be exchanged in the network, as compared to centralized approach. The convergence of the spectrum price bargaining algorithm is guaranteed by the following facts: (i) the optimal spectrum price is always obtained when the total idle bandwidth of the MNO is fully allocated; (ii) the left hand side of (31) is a decreasing function of μ; and (iii) the SE for the proposed Stackelberg game is unique for a given Q.

V. SECURITY ASSESSMENT AND NUMERICAL RESULTS

In this section, a security assessment of our proposed spectrum blockchain is firstly given. After that, several numerical examples are provided to evaluate the performances of the spectrum trading strategies based on the approach of spectrum pricing.

A. Security Assessment

Unlike traditional communication security and privacy protection, our proposed method can ensure spectrum trading security by leveraging consortium blockchain technology which can provide a defensive ability against many potential security attacks. More details about the security assessment for the spectrum blockchain are listed as follows.

- *Without reliance on a trusted intermediary*: In our spectrum blockchain, operators trade spectrum in a distributed P2P manner, unlike conventional trading schemes that have to rely on a globally trusted center. This can efficiently solve the security threats caused by the centralized mechanisms such as single point of failure, privacy leakage, and denial of service attacks.
- *Privacy protection*: This feature is guaranteed by the fact that the trading information is sent in the encrypted format among the operators and the edge computing nodes. Without knowledge of the secret key of the sender, it is impossible to derive the original private message from the operators.
- *Wallet security*: As each operator has a unique wallet corresponding to its spectrum coin account, without authorized keys and certificates, no adversary can open an operator's wallet, stealing or distorting spectrum coins from the wallet.
- *Prevention of replay attack*: Each transaction is digitally signed with a unique identifier. Therefore, transactions with the same identifier will be rejected by the consensus servers (i.e., pre-selected edge computing nodes), and thus replay attacks are prevented.
- *Transaction authentication*: All transactions recorded in blockchain have been publicly audited and authenticated by high-reputation authorized edge computing nodes. Moreover, each block has a unique and fixed hash value, which can be used to protect the order and the information of blocks. Since modifying any contents of any block will cause a change to the hash values of the other blocks, it is impossible for an adversary to tamper or forge a transaction due to overwhelming cost.
- *Traceability*: When a dispute happens in the spectrum blockchain network, the TA will check one public ledger to find out the corresponding real identity of the illegal or misbehaved operator from the anonymous certificate $Cert$ and registered ID, and revoke its public key. Thus, the traceability can be guaranteed.

B. Numerical Results

In this subsection, the simulation results are presented to demonstrate the performances of the proposed pricing-based spectrum trading scheme. An air-ground spectrum sharing for UAV-assisted cellular network with one MNO and three UAV operators is considered. In order to illustrate the impact of spectrum coins and spectrum demands of UAV operators on the system performance, two different cases are investigated. In the first case (i.e., the first three examples), it is assumed that the spectrum coins of all the UAV operators are the same while their basic spectrum demands for serving users (i.e., application types) are different. Without loss of generality, the spectrum coins of all the UAV operators are assumed to be the same with $g_1 = g_2 = g_3 = 1$. The bandwidth demands of these UAV operators at the current time are different with $[d_1, d_2, d_3] = [5, 10, 15]$ units[2]. In the second case (i.e., the last example), the UAV operators have the same spectrum demands with different spectrum coins.

Example 1. *Uniform Pricing vs. Non-Uniform Pricing:* In this example, the performance comparison between the two schemes of uniform pricing and non-uniform pricing is examined. Fig. 3 and Fig. 4 show the MNO revenue and the sum-revenue of UAV operators, respectively, versus the total available bandwidth Q at the MNO, with uniform or non-uniform pricing. It is observed that for the same Q, the revenue of the MNO under the non-uniform pricing scheme is in general larger than that under the uniform pricing scheme, while the reverse is generally true for the sum-revenue of UAV operators. These observations indicate that, from the perspective of revenue maximization for the MNO, the non-uniform pricing is preferable compared to uniform pricing. On the other hand, the uniform pricing scheme is indeed optimal for the sum-revenue maximization of the UAV operators.

In addition, it is worth noting that when Q is sufficiently small, the revenues of the MNO become equal for the two pricing schemes, so are the sum-revenues of UAV operators. This is because when Q is very small, there is only one UAV operator active in the network, and thus by comparing (28) and (32), the non-uniform pricing scheme is same as the uniform pricing counterpart in the single-UAV operator case. Besides, it is expected that when Q is sufficiently large, the revenues of the MNO converge to the same value for the two pricing schemes. This can be explained as follows. For the non-uniform pricing scheme, it is observed from (28) that arbitrary spectrum price μ_i becomes very small with very large Q, and thus the objective function of Problem 2 converges to $\sum_{i=1}^{N} \frac{g_i}{\ln 2}$ as $Q \rightarrow \infty$. On the other hand, for the uniform pricing

---

[2] Since this paper considers spectrum trading purely from the data level, there is no specific unit for the bandwidth, which can be a general parameter.

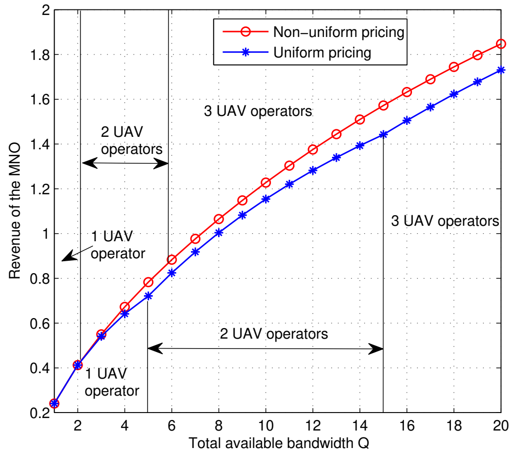

Fig. 3. Revenue of the MNO vs. Q.

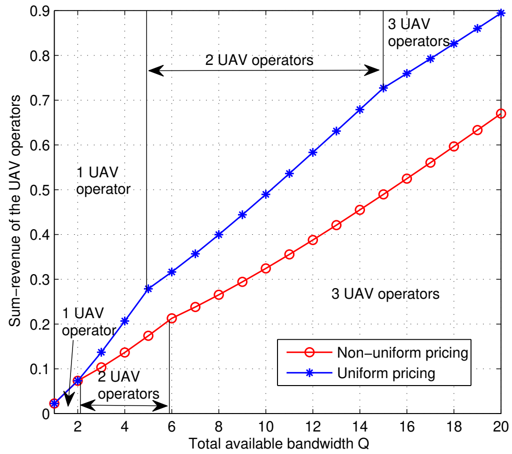

Fig. 4. Sum-revenue of the UAV operators vs. Q.

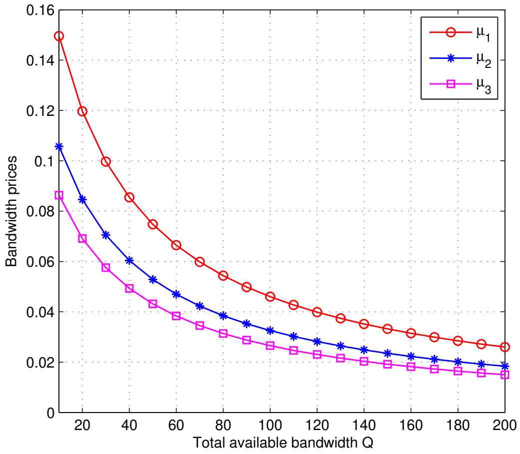

Fig. 5. Bandwidth prices vs. Q under non-uniform pricing.

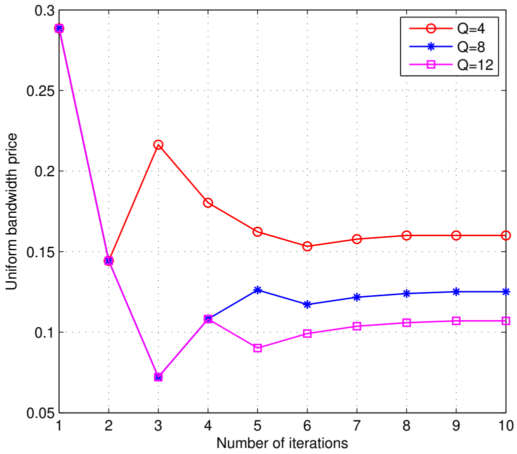

Fig. 6. Convergence performance of the distributed spectrum price bargaining algorithm.

scheme, when Q approaches infinity, the revenue of the MNO will also converge to $\sum_{i=1}^{N} \frac{g_i}{\ln 2}$. Thus, there exists a same upper bound for the two different pricing schemes.

Example 2. *Comparison of Bandwidth Prices for UAV Operators under Non-Uniform Pricing:* In this example, we examine the optimal bandwidth prices for the UAV operators with the variation of Q under non-uniform pricing. First, it is observed from Fig. 5 that, for the same Q, the bandwidth price for UAV operator 1 is the highest, while that for UAV operator 3 is the lowest. This is true due to the fact that $\frac{g_1}{d_1} > \frac{g_2}{d_2} > \frac{g_3}{d_3}$, where a larger $\frac{g_i}{d_i}$ indicates that the corresponding UAV operator can achieve a higher profit with the same amount bandwidth allocated. Therefore, the operator with a larger $\frac{g_i}{d_i}$ has a willingness to pay a higher price to buy the spectrum. Secondly, it is observed that the differences between the bandwidth prices decrease with the increasing of Q. The reason is that when Q increases, it can be seen from (28) that $\frac{\sum_{i=1}^{N}\sqrt{g_i d_i}}{Q+\sum_{i=1}^{N} d_i}$ decreases. Last, it is observed that the prices for all UAV operators decrease with the increasing of Q, which can be easily inferred from (28). Intuitively, this can be explained by the practical rule of thumb that if a seller has a large amount of goods to sell, it would like to price lower to stimulate consumption.

Example 3. *Convergence Performance of Distributed Bandwidth Price Bargaining Algorithm:* In this example, the convergence performance of the distributed bandwidth price bargaining algorithm (i.e., Algorithm 3) is investigated. Actually, the distributed bargaining algorithm can be implemented though the bisection method, for which the implementation procedure is given as follows. First, the MNO initializes a lower bound μ_L and an upper bound μ_H of the bandwidth price. Then, the MNO computes $\mu_M = (\mu_H + \mu_L)/2$ and sends the μ_M to a nearby miner (i.e., authorized edge computing node) through the blockchain network. The miner records the information and broadcasts it to all the UAV operators. After receiving μ_M, UAV operators compute their optimal bandwidth requests and give responses back to the miner. The miner measures the total bandwidth requests $\sum_{i\in\mathcal{N}} b_i$ and transmits the feedback information to the MNO. If $\sum_{i=1}^{N} b_i < Q$, the

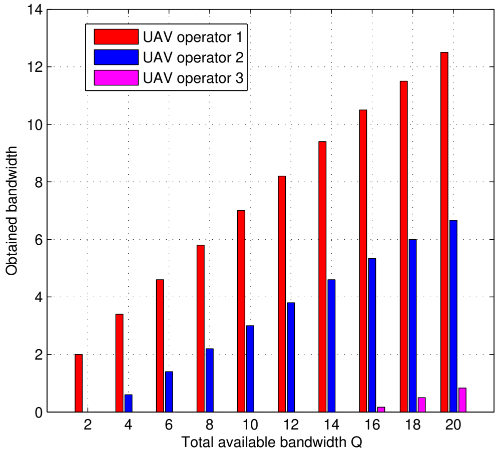

Fig. 7. Bandwidth allocation vs. Q.

MNO sets $\mu_H = \mu_M$; otherwise, the MNO sets $\mu_L = \mu_M$. Then, μ_M is recomputed based on the new lower and upper bounds. The algorithm stops when $\left|\sum_{i=1}^{N} b_i - Q\right|$ is within the desired accuracy. It is observed from Fig. 6 that the distributed bargaining algorithm can converge within 9 iterations for all values of Q.

Example 4. *Relationship between Bandwidth Allocation and Available Idle Spectrum:* In this example, the spectrum demands of all the UAV operators are assumed to be the same with $d_1 = d_2 = d_3 = 5$ units while the spectrum coins are different with $[g_1, g_2, g_3] = [3, 2, 1]$. The bandwidth assignments for the three UAV operators with variation of Q are shown in Fig. 7. It is observed from Fig. 7 that the UAV operators with more spectrum coins have a higher priority in bandwidth obtainment. When the available bandwidth Q is small, the MNO will reject the request from the operators with low spectrum coins, and provide the limited resource to the operators with high spectrum coins. When the available bandwidth Q is large, the MNO will try to meet every operator's request. However, operators with more spectrum coins are given a higher priority in obtaining the bandwidth. It is also observed that with the increasing of Q, the bandwidth assigned for each operators increases. This is due to the fact that the MNO's utility is maximized only when it leases all its available idle spectrum to the UAV operators.

VI. CONCLUSION

In this paper, a consortium blockchain enabled secure spectrum trading framework is exploited for UAV-assisted cellular networks, where MNO and UAV operators are able to trade spectrum in a credible environment without relying on a trusted third party. Under this framework, a Stackelberg game model is adopted to jointly study the utility optimization for the MNO and UAV operators. Non-uniform spectrum pricing and uniform spectrum pricing schemes are discussed. Additionally, a non-uniform pricing algorithm with low complexity and a distributed uniform pricing bargaining algorithm are respectively designed to obtain the optimal solutions under the two pricing schemes. A security assessment shows that our proposed spectrum blockchain improves transaction security and privacy protection. Numerical results illustrate that the pricing-based incentive mechanisms are effective and efficient for spectrum trading. In future work, it is interesting to extend the utilization of blockchain for broader applications in UAV-assisted cellular networks, while taking into account more UAV features such as deployment optimization, trajectory planning and energy constraint.

APPENDIX A
PROOF OF THEOREM 1

Since the Problem 1 is a convex optimization problem, the duality gap between this problem and its dual optimization problem is zero. Thus, we can deal with Problem 1 by solving its dual problem.

The Lagrangian of the Problem 1 can be written as

$$\mathcal{L}\left(b_i, \alpha\right) = g_i \log_2\left(1 + \frac{b_i}{d_i}\right) - \mu_i b_i + \alpha b_i, \tag{33}$$

where α is nonnegative dual variable associated with the constraint $b_i \geq 0$.

The dual function is then defined as $h\left(\alpha\right) = \max_{b_i \geq 0} \mathcal{L}\left(b_i, \alpha\right)$, and the dual problem is given by $\min_{\alpha \geq 0} h\left(\alpha\right)$. Then, the KKT conditions can be written as follows:

$$\frac{\partial \mathcal{L}\left(b_i, \alpha\right)}{\partial b_i} = \frac{g_i}{\left(b_i + d_i\right) \ln 2} - \mu_i + \alpha = 0,\ \forall i, \tag{34}$$

$$\alpha \geq 0,\ b_i \geq 0,\ \forall i, \tag{35}$$

$$\alpha b_i = 0. \tag{36}$$

From (34), it follows

$$b_i = \frac{g_i}{\left(\mu_i - \alpha\right) \ln 2} - d_i. \tag{37}$$

Suppose $b_i > 0$ when $\mu_i \geq \frac{g_i}{d_i \ln 2}$. Then from (36), it follows that $\alpha = 0$. Therefore, (37) reduces to $b_i = \frac{g_i}{\mu_i \ln 2} - d_i$. Then $b_i > 0$ results in $\mu_i < \frac{g_i}{d_i \ln 2}$. This contradicts the presumption. Therefore, from (35), it follows

$$b_i = 0,\ \text{if}\ \mu_i \geq \frac{g_i}{d_i \ln 2}. \tag{38}$$

Suppose $b_i = 0$ when $\mu_i < \frac{g_i}{d_i \ln 2}$. Then, from (37), it follows $\mu_i = \frac{g_i}{d_i \ln 2} + \alpha$. Since $\alpha \geq 0$, it follows $\mu_i \geq \frac{g_i}{d_i \ln 2}$. This contradicts the presumption. Thus, $b_i \neq 0$ for this set of μ_i. Then, from (36), it follows $\alpha = 0$. Therefore, from (37), it follows

$$b_i = \left(\frac{g_i}{\mu_i \ln 2} - d_i\right),\ \text{if}\ \mu_i < \frac{g_i}{d_i \ln 2}. \tag{39}$$

Theorem 1 is thus proved.

APPENDIX B
PROOF OF PROPOSITION 1

By introducing the dual variables associated with the bandwidth price and amount of total available spectrum constraints, the Lagrangine of Problem 2b is given by

$$\mathcal{L}(\boldsymbol{\mu},\eta,\boldsymbol{\gamma}) = \sum_{i=1}^{N}\mu_i d_i + \eta\left(\sum_{i=1}^{N}\frac{g_i}{\mu_i \ln 2} - \sum_{i=1}^{N} d_i - Q\right) - \sum_{i=1}^{N}\gamma_i\mu_i, \tag{40}$$

where η and γ_i are the nonnegative dual variables associated with the constraints $\sum_{i=1}^{N}\frac{g_i}{\mu_i \ln 2} \le Q + \sum_{i=1}^{N} d_i$ and $\mu_i \ge 0$, respectively.

The dual optimization problem is expressed as the maximization of the Lagrangian

$$\mathcal{V}(\boldsymbol{\mu},\eta,\boldsymbol{\gamma}) = \max_{\boldsymbol{\mu}\succcurlyeq 0}\mathcal{L}(\boldsymbol{\mu},\eta,\boldsymbol{\gamma}). \tag{41}$$

The dual problem is then given by $\min_{\eta\ge 0,\boldsymbol{\gamma}\succcurlyeq 0}\mathcal{V}(\boldsymbol{\mu},\eta,\boldsymbol{\gamma})$. The duality gap is zero for the convex problem addressed here, and thus solving its dual problem is equivalent to solving the original problem. Thus the optimal solution needs to satisfy the following KKT conditions:

$$\frac{\partial\mathcal{L}(\mu,\eta,\gamma)}{\partial\mu_i} = d_i - \frac{\eta g_i}{{\mu_i}^2 \ln 2} - \gamma_i = 0, \forall i, \tag{42}$$

$$\eta\left(\sum_{i=1}^{N}\frac{g_i}{\mu_i \ln 2} - \sum_{i=1}^{N} d_i - Q\right) = 0, \tag{43}$$

$$\gamma_i\mu_i = 0, \tag{44}$$

$$\eta \ge 0, \gamma_i \ge 0, \mu_i \ge 0, \forall i, \tag{45}$$

$$\sum\nolimits_{i=1}^{N}\frac{g_i}{\mu_i \ln 2} - Q - \sum\nolimits_{i=1}^{N} d_i \le 0. \tag{46}$$

From (42), we can derive

$${\mu_i}^2 = \frac{\eta g_i}{(d_i - \gamma_i)\ln 2}, \forall i. \tag{47}$$

To further analyze the dual problem, we firstly provide the following two lemmas.

Lemma 1. $\gamma_i = 0, \forall i$.

Proof: Suppose that $\gamma_i \neq 0$ for any arbitrary i. Then, from (44), we can derive that $\mu_i = 0$. Then, since $g_i > 0$, from (47), it follows that $\eta = 0$. Substituting $\eta = 0$ into (47), we have $\mu_i = 0, \forall i$. However, this result contradicts the condition in (46). Thus, the asumption that $\gamma_i \neq 0$ for any given i does not hold, and we thus have $\gamma_i = 0, \forall i$. ∎

Lemma 2. $\sum_{i=1}^{N}\frac{g_i}{\mu_i \ln 2} - Q - \sum_{i=1}^{N} d_i = 0$.

Proof: Suppose that $\sum_{i=1}^{N}\frac{g_i}{\mu_i \ln 2} - Q - \sum_{i=1}^{N} d_i \neq 0$. Then, from (43), it follows that $\eta = 0$. Substituting $\eta = 0$ into (47), we have $\mu_i = 0, \forall i$, which contradicts the condition in (46). Therefore, the aforementioned assumption does not hold, and we thus have $\sum_{i=1}^{N}\frac{g_i}{\mu_i \ln 2} - Q - \sum_{i=1}^{N} d_i = 0$. ∎

From Lemma 1, we have $\gamma_i = 0$ for arbitrary i. Since $\mu_i \ge 0$, thus from (47), it follows $\mu_i = \sqrt{\frac{\eta g_i}{d_i \ln 2}}, \forall i$. According to Lemma 2, it follows that $Q + \sum_{i=1}^{N} d_i = \sum_{i=1}^{N}\frac{g_i}{\mu_i \ln 2}$. Substituting $\mu_i = \sqrt{\frac{\eta g_i}{d_i \ln 2}}$ into it, we can derive

$$\sqrt{\eta} = \frac{\sum_{i=1}^{N}\sqrt{\frac{g_i d_i}{\ln 2}}}{Q + \sum_{i=1}^{N} d_i}. \tag{48}$$

Then, it follows

$$\mu_i = \frac{1}{\ln 2}\sqrt{\frac{g_i}{d_i}}\frac{\sum_{i=1}^{N}\sqrt{g_i d_i}}{Q + \sum_{i=1}^{N} d_i}. \tag{49}$$

Thus, Proposition 1 is proved.

APPENDIX C
PROOF OF PROPOSITION 2

This proof consists of two parts: the necessity proof and the sufficiency proof, which are given as follows.

Part I: Sufficiency. The optimal solution to the Problem 2b is given by (26) with the assumption that that all the indicator functions are equal to 1, i.e., $\mu_i < \frac{g_i}{d_i \ln 2}, \forall i \in \{1, 2, \cdots, N\}$. Submitting (26) into these inequalities yields

$$\sqrt{\frac{g_i}{d_i \ln 2}}\frac{\sum_{i=1}^{N}\sqrt{\frac{g_i d_i}{\ln 2}}}{Q + \sum_{i=1}^{N} d_i} < \frac{g_i}{d_i \ln 2}, \forall i \in \{1, 2, \cdots, N\}. \tag{50}$$

Then, (50) can be rewritten as $Q > \frac{\sum_{i=1}^{N}\sqrt{g_i d_i}}{\sqrt{g_i/d_i}} - \sum\limits_{i=1}^{N} d_i, \forall i \in \{1, 2, \cdots, N\}$. Furthermore, the inequalities given above can be compactly written as

$$Q > \frac{\sum_{i=1}^{N}\sqrt{g_i d_i}}{\min_i\sqrt{\frac{g_i}{d_i}}} - \sum_{i=1}^{N} d_i. \tag{51}$$

Thus, the sufficiency of the condition in (27) is proved.

Part II: Necessity. This part can be proved by contradiction. For the ease of exposition, we assume that UAV operators are sorted by the following order: $\frac{g_1}{d_1} > \cdots \frac{g_{N-1}}{d_{N-1}} > \frac{g_N}{d_N}$. Then, in Proposition 2, the condition becomes $Q > Y_N$, where

$$Y_N = \frac{\sum_{i=1}^{N}\sqrt{g_i d_i}}{\sqrt{\frac{g_N}{d_N}}} - \sum_{i=1}^{N} d_i. \tag{52}$$

Now, suppose $Y_{N-1} < Q \le Y_N$, where Y_{N-1} is shown later in (56). Suppose that $\boldsymbol{\mu}^*$ given by (26) is still optimal for Problem 2 with $Y_{N-1} < Q < Y_N$. Then, since $Q \le Y_N$, from (26) we have $\mu_N^* \ge \frac{g_N}{d_N \ln 2}$ and thus $\left(\frac{g_N}{\mu_N^*} - d_N\right)^+ = 0$. From Problem 2, it then follows that $\mu_1^*, \ldots, \mu_{N-1}^*$ is the optimal solution of the following problem

$$\max_{\boldsymbol{\mu}\succcurlyeq 0}\sum_{i=1}^{N-1}\left(\frac{g_i}{\ln 2} - \mu_i d_i\right)^+, \tag{53}$$

$$\text{s.t.} \sum_{i=1}^{N-1}\left(\frac{g_i}{\mu_i \ln 2} - d_i\right)^+ \le Q. \tag{54}$$

It is easy to observe that the above problem has the same structure as the Problem 2. Therefore, according to Proposition 1 and the proof of previous Part I, the optimal solution for this problem can be given by

$$\mu_i^* = \frac{1}{\ln 2}\sqrt{\frac{g_i}{d_i}}\frac{\sum_{i=1}^{N-1}\sqrt{g_i d_i}}{Q + \sum_{i=1}^{N-1} d_i}, \forall i \in \{1, 2, \cdots, N-1\}, \tag{55}$$

with the condition that $Q > Y_{N-1}$, where Y_{N-1} is expressed as the threshold for Q above which $\mu_i^* < \frac{g_i}{d_i \ln 2}, \forall i \in \{1, 2, \cdots, N-1\}$ holds, i.e.,

$$Y_{N-1} = \frac{\sum_{i=1}^{N-1} \sqrt{g_i d_i}}{\sqrt{\frac{g_{N-1}}{d_{N-1}}}} - \sum_{i=1}^{N-1} d_i. \tag{56}$$

Comparing the optimal bandwidth price solution shown in (55) with that given in (26), we can find that they are different from each other, which contradicts with our assumption that $\boldsymbol{\mu}^*$ is still the optimal solution for Problem 2 with the condition $Y_{N-1} < Q \leq Y_N$. Thus, we can conclude that only if the condition $Q > Y_N$ satisfies, the bandwidth prices given by (26) are the optimal solutions for Problem 2.

Combining the results obtained in Part I and Part II, it is concluded that the bandwidth prices given by (26) are the optimal solutions of Problem 2 if and only if $Q > \frac{\sum_{i=1}^{N} \sqrt{g_i d_i}}{\min_i \sqrt{g_i / d_i}} - \sum_{i=1}^{N} d_i$. Thus, Proposition 2 is proved.

REFERENCES

[1] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[2] M. Mozaffari, W. Saad, M. Bennis, Y. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart. 2019.

[3] J. Qiu, D. Grace, G. Ding, M. D. Zakaria, and Q. Wu, "Air-ground heterogeneous networks for 5G and beyond via integrating high and low altitude platforms," *IEEE Wireless Commun.*, to be published, 2019.

[4] M. Mozaffari, A. Taleb Zadeh Kasgari, W. Saad, M. Bennis, and M. Debbah, "Beyond 5G with UAVs: Foundations of a 3D wireless cellular network," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 357–372, Jan. 2019.

[5] Y. Zeng, J. Xu, and R. Zhang, "Energy minimization for wireless communication with rotary-wing UAV," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2329–2345, Apr. 2019.

[6] Y. Zeng, J. Lyu, and R. Zhang, "Cellular-connected UAV: Potential, challenges, and promising technologies," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 120–127, Feb. 2019.

[7] S. Zhang, Y. Zeng, and R. Zhang, "Cellular-enabled UAV communication: A connectivity-constrained trajectory optimization perspective," *IEEE Trans. Wireless Commun.*, vol. 67, no. 3, pp. 2580–2604, Mar. 2019.

[8] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.

[9] F. Shen, G. Ding, Z. Wang, and Q. Wu, "UAV-based 3D spectrum sensing in spectrum-heterogeneous networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5711–5722, Jun. 2019.

[10] W. Xu, S. Wang, S. Yan, and J. He, "An efficient wideband spectrum sensing algorithm for unmanned aerial vehicle communication networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1768–1780, Apr. 2019.

[11] S. Bhattarai, J. J. Park, B. Gao, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Trans. Cogn. Commun. Netw.*, vol. 2, no. 2, pp. 110–128, Jun. 2016.

[12] J. Lyu, Y. Zeng, and R. Zhang, "UAV-aided offloading for cellular hotspot," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3988–4001, Jun. 2018.

[13] L. Wang, H. Yang, J. Long, K. Wu, and J. Chen, "Enabling ultra-dense UAV-aided network with overlapped spectrum sharing: Potential and approaches," *IEEE Netw.*, vol. 32, no. 5, pp. 85–91, Sep. 2018.

[14] J. Yao and N. Ansari, "Caching in energy harvesting aided internet of things: A game-theoretic approach," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3194–3201, Apr. 2019.

[15] W. Huang, W. Chen, and H. V. Poor, "Request delay-based pricing for proactive caching: A Stackelberg game approach," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 2903–2918, Jun. 2019.

[16] S. Hong and H. Kim, "QoE-aware computation offloading to capture energy-latency-pricing tradeoff in mobile clouds," *IEEE Trans. Mobile Comput.*, vol. 18, no. 9, pp. 2174–2189, Sep. 2019.

[17] M. Li, T. Q. S. Quek, and C. Courcoubetis, "Mobile data offloading with uniform pricing and overlaps," *IEEE Trans. Mobile Comput.*, vol. 18, no. 2, pp. 348–361, Feb. 2019.

[18] N. Zhao, Y. Liang, and Y. Pei, "Dynamic contract incentive mechanism for cooperative wireless networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, Nov. 2018.

[19] Z. Hu, Z. Zheng, L. Song, T. Wang, and X. Li, "UAV offloading: Spectrum trading contract design for UAV-assisted cellular networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6093–6107, Sep. 2018.

[20] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart. 2016.

[21] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[22] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart. 2019.

[23] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[24] H. Wang, Q. Wang, D. He, Q. Li, and Z. Liu, "BBARS: Blockchain-based anonymous rewarding scheme for V2G networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3676–3687, Apr. 2019.

[25] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, J. Liu, Y. Xiang, and R. H. Deng, "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1251–1266, Jun. 2019.

[26] X. Xu, Q. Liu, X. Zhang, J. Zhang, L. Qi, and W. Dou, "A blockchain-powered crowdsourcing method with privacy preservation in mobile environment," *IEEE Trans. Comput. Social Syst.*, to be published, 2019. DOI: 10.1109/TCSS.2019.2909137.

[27] Y. Zhu, G. Zheng, and K. Wong, "Blockchain-empowered decentralized storage in air-to-ground industrial networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3593–3601, Jun. 2019.

[28] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K. R. Choo, "Neural-blockchain based ultra-reliable caching for edge-enabled UAV networks," *IEEE Trans. Ind. Informat.*, to be published, 2019. DOI: 10.1109/TII.2019.2922039.

[29] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.

[30] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart. 2019.

[31] X. Kang and Y. Wu, "Incentive mechanism design for heterogeneous peer-to-peer networks: A Stackelberg game approach," *IEEE Trans. Mobile Comput.*, vol. 14, no. 5, pp. 1018–1030, May 2015.

[32] L. Duan, J. Huang, and B. Shou, "Duopoly competition in dynamic spectrum leasing and pricing," *IEEE Trans. Mobile Comput.*, vol. 11, no. 11, pp. 1706–1719, Nov. 2012.

[33] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which and how," *IEEE Commun. Surveys Tuts.*, to be published, 2019. DOI: 10.1109/COMST.2019.2928178.

[34] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, and B.-G. Kim, "Algorithms for efficient digital media transmission over IoT and cloud networking," *J. Multimedia Inf. Syst.*, vol. 5, no. 1, pp. 27–34, Mar. 2018.

[35] K. E. Psannis, C. Stergiou, and B. B. Gupta, "Advanced media-based smart big data on intelligent cloud systems," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 77–87, Jan./Mar. 2019.

[36] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.

[37] 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 Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart. 2019.

[38] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Sec. Comput*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[39] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.

[40] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[41] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[42] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[43] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[44] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press, 2012.

[45] X. Kang, R. Zhang, and M. Motani, "Price-based resource allocation for spectrum-sharing femtocell networks: A Stackelberg game approach," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, pp. 538–549, Apr. 2012.

Junfei Qiu received his B.S. degree in electronic and information engineering from Wuhan University of Science and Technology, Wuhan, China, in 2013 and his M.S. degree in information and communication engineering from the College of Communications Engineering, Nanjing, China, in 2016. He is currently pursuing the Ph.D. degree at the Department of Electronic Engineering, University of York, York, United Kingdom. His research interests include unmanned aerial vehicle (UAV) communications, blockchain, machine learning, and big data analytics over wireless networks. He was recognized as an Exemplary Reviewer for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS in 2018. He has served as a Technical Program Committees (TPC) member for many international conferences and workshops such as the IEEE ICARES 2019, IEEE ICIIP 2019, IEEE GLOBECOM Workshop 2016, IEEE ICC Workshops 2016 and 2017.

David Grace (M'00-SM'13) received his PhD from University of York in 1999, with the subject of his thesis being 'Distributed Dynamic Channel Assignment for the Wireless Environment'. Since 1994 he has been a member of the Department of Electronic Engineering at York, where he is now Professor (Research), Head of Communication Technologies Research Group, and Director of the Centre for High Altitude Platform Applications. Current research interests include aerial platform based communications, cognitive green radio, particularly applying distributed artificial intelligence to resource and topology management to improve overall energy efficiency; 5G system architectures; dynamic spectrum access and interference management. He is currently a lead investigator on H2020 MCSA 5G-AURA and H2020 MCSA SPOTLIGHT. He was one of the lead investigators on FP7 ABSOLUTE and focussed on extending LTE-A for emergency/temporary events through application of cognitive techniques. He was a technical lead on the 14-partner FP6 CAPANINA project that dealt with broadband communications from high altitude platforms. He is an author of over 280 papers, and author/editor of 2 books. He is the former chair of IEEE Technical Committee on Cognitive Networks for the period 2013/4. He is a founding member of the IEEE Technical Committee on Green Communications and Computing. In 2000, he jointly founded SkyLARC Technologies Ltd, and was one of its directors.

Guoru Ding (S'10-M'14-SM'16) received the B.S. (Hons.) degree in electrical engineering from Xidian University, Xian, China, in 2008, and the Ph.D. (Hons.) degree in communications and information systems from the College of Communications Engineering, Nanjing, China, in 2014. He is currently an Associate Professor with the College of Communications Engineering, Army Engineering University, China. From 2015 to 2018, he was a Post-Doctoral Research Associate with the National Mobile Communications Research Laboratory, Southeast University, Nanjing. His research interests include cognitive radio networks, massive MIMO, machine learning, and big data analytics over wireless networks. He has received the Excellent Doctoral Thesis Award of the China Institute of Communications in 2016, the Alexander von Humboldt Fellowship in 2017, and the Excellent Young Scientist of Wuwenjun Artificial Intelligence in 2018. He is a Technical Editor and a Voting Member of the IEEE 1900.6 Standard Association Working Group. He was a recipient of several best paper awards from the IEEE WCSP 2009, the IEEE VTC 2014, and EAI MLICOM 2016. He has served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (special issue on spectrum sharing and aggregation in future wireless networks). He is currently an Associate Editor of the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

Junnan Yao received the B.S., M.S., and Ph.D. degrees in communications and information systems from PLA University of Science and Technology, Nanjing, China, in 2005, 2009 and 2013, respectively. He is currently a Postdoctoral Research Associate with College of Communications Engineering, Nanjing, China. His research interests include security issues in cognitive radio networks and wireless sensor networks.

Qihui Wu (SM'13) received the B.S. degree in communications engineering and the M.S. and Ph.D. degrees in communications and information systems from the Institute of Communications Engineering, Nanjing, China, in 1994, 1997, and 2000, respectively. From 2003 to 2005, he was a Postdoctoral Research Associate with Southeast University, Nanjing. From 2005 to 2007, he was an Associate Professor with the College of Communications Engineering, PLA University of Science and Technology, Nanjing, where he was a Full Professor from 2008 to 2016. Since May 2016, he has been a Full Professor with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China. From March 2011 to September 2011, he was an Advanced Visiting Scholar with the Stevens Institute of Technology, Hoboken, NJ, USA. His current research interests include the areas of wireless communications and statistical signal processing, with emphasis on system design of software defined radio, cognitive radio, and smart radio.