

Blockchain Empowered Decentralized Storage in Air-to-Ground Industrial Networks

Abstract—Blockchain has raised an evolution in the cyber network by using distributed storage, cryptography algorithms and smart contract. Many areas are benefiting from this technology, such as data integrity, security as well as authentication and authorization. Internet of Things network is often suffering from such security issues, obstructing its development in scales. In this paper, we employ blockchain technology to construct a decentralized platform for storing and trading information in the air-to-ground IoT heterogeneous network. To make both air and ground sensors trading in the decentralized network, we design a mutual benefit consensus process to the uneven equilibrium distribution of resources among the participators. We use the Cournot model to optimize the active density factor set in the heterogeneous air network and then employ Nash equilibrium to balance the number of ground supporters, which is subject to the achievable average downlink rate between the air sensors and the ground sensors. Finally, numerical results are provided to demonstrate the beneficial properties of the proposed consensus process for air-to-ground network, and show the maximum active sensors density utilization of air network to achieve a higher quality of service.

Index Terms—Blockchain, Industrial IoT, Stochastic Geometry, Cournot model, smart contract.

I. INTRODUCTION

In the past ten years, blockchain technology has found extensive use in various fields beyond Bitcoin. The largest use of blockchain platforms is still in public ledgers for cryptocurrencies. However, there are increasing uses in non-financial applications. A recent trend is the use of blockchain technology to strengthen the data security and model the decentralized and consensus mechanism structures such as Internet of Things (IoT) applications using the next generation of wireless communication networking [1, 2].

Use of IoT technologies in various industries has attracted huge attention from both academics and governments [3]. Some IoT applications are developed closely with other industrial applications such as agriculture, environmental monitoring and security surveillance. The designers of industrial applications are, in particular, required to make an effort to find a good, sometimes subtle, balance between expense with benefits. [4] To address this challenge, blockchains Peer-to-Peer (P2P) approach could play an important role in the development of IoT decentralized systems and data intensive applications running on billions of devices, preserving the privacy of the users. This could apply in many circumstances, for example:

- *Public Health*: Fake medicine and food traceability are urgent problems in public health. For example, on a farm, a tamper-proof system to record growth data for crops and aquacultures could remove some sources of insecurity in supply chains.

- *Smart Cities*: Smart cities are using blockchain as the foundation of systems to monitor city parameters such as temperature, humidity and PM 2.5 levels. The best current example is Dubai [5], which aims to cement its status as a global leader in the smart economy by becoming the first blockchain-powered government.
- *Data storage management*: Blockchain-based distributed data storage clouds can be applied to health, justice, legislation, safety, and business systems, to protect sensitive sensor data, contracts, private data, etc.

A. Related Works

1) *Blockchain Technology*: Blockchain uses public-key cryptography to create a ledger for published transactions which is suitable for use in a Peer-to-Peer (P2P) network [6]. Once a new block has been saved into the blockchain, the transactions of that block will be confirmed [7]. To guarantee the integrity and consistency of the consensus protocol when updating the blockchain, one specific mining technique in Bitcoin network called *Proof-of-Work* (PoW) has been proposed. [7]. According to [8], PoW requires miners to spend their computational power on a computationally-hard puzzle, i.e., to find a partial preimage satisfying certain conditions of a hash mapping based on the proposed blockchain state. To solve the PoW puzzle, the author in paper [9] proposed an optimized solution which involved a cooperative computing offloading decision and content caching. The optimized result shows that the scheme could achieve better performance than that with deterministic constraints, and it could solve PoW puzzles more efficiently.

Another method uses the replaceable decentralized consensus protocols commonly used for Blockchain IoT networks, named *Proof-of-stake* (PoS) [10]. In contrast to PoW, PoS demands much less CPU computation, energy, hardware, etc, in the mining process, and the opportunities for a node to mine the next block are related to the miners account to balance of stakes. The bigger the stake owned by a miner, the more mining power it has.

2) *IoT blockchain*: The central concept in IoT Blockchain is smart contracts, which allows the automation of complicated processes so that each participant benefits from and can trust such processes. The principles for applying blockchain technology to IoT network have been demonstrated [11]. The author points out that the purpose of sharing services and resources in decentralized IoT networks is to automate time-consuming workflows. In [12], the author describes a decentralized blockchain-based platform for data storage and trading in a wireless powered IoT crowd-sensing system. The data from RF-energy beacons are forwarded to the blockchain

network for distributed ledger services, which provides the analytical condition for a range of valuable results about the equilibrium strategies in the blockchain-based network.

In paper [13], the author examined an optimization problem for edge computing resource management to analyse the interaction effect between the computing service provider and miners in the blockchain. A blockchain solution for the energy industry has been studied in [14, 15]. In [15], the author designed a credit-based payment method to solve the problem of confirmation delays in the transaction and intermittent connectivity of energy nodes. This blockchain solution can be applied to various IoT scenarios, such as energy harvesting networks and vehicle-to-grid. A P2P electricity trading model for Plug-in Hybrid Electric Vehicles (PHEVs) in smart grids was studied in paper [14]. That mechanism requires no third party when trading charging and discharging of PHEVs using the shared ledger. The authors conclude that this auction mechanism could enhance the security of transactions.

3) *UAV-Based IoT Platforms*: Providing real-time data is a significant function of UAVs, which could make images or videos of damaged nuclear reactors or other disasters. UAVs can be connected to all kinds of IoT sensors and can be used to form a comprehensive P2P platform in the air [16].

A distributed trust system in an integrated unmanned aerial system was described in [17], whose ecosystem is made up of multi-tier partnerships, the human-robot trust between distributed entities. Paper [18] examined the secrecy performance of randomly deployed nodes to evaluate the UAV-enabled 3D antenna millimeter-wave based air-to-ground communication networks. However, for mechanical reasons, hovering UAVs suffer from high energy consumption; using traditional low-cost kites or balloons [19] could greatly reduce energy consumption, supporting more antennae or sending more information.

4) *Data storage management*: Data storage management is one of the most popular use cases of blockchain in IoT networks [20]. Combining blockchain and a P2P storage system to protect the sensitive data in IoT devices, data can be safely stored in different peers, and blockchain could guarantee their reliability and prevent tampering. A decentralized platform has been studied in [21], which protects personal private data using blockchain technology. Users of the platform can avoid the problem of the trustworthiness of any third party. It is also easy to collect and share sensitive data in legal and regulatory decisions. Paper [22] studies a decentralized cloud file storage platform named *Sia*, it uses cryptographic contracts to protect the storage agreements between clients and hosts. The host submits storage proofs to the network once a file is stored; the contracts are stored in a blockchain to provide a public audit.

5) *Security*: Blockchain depending on a distributed trust system could achieve high-security performance. However, blockchain technology still presents some potential security risks. For example, users in the system can suffer from the famous 51% attack that, anyone can forge the transaction if 51% of the computation power is accumulated in one place. Anyone can leverage the computation power to intercept,

modify and then rebroadcast the forged transaction where the system does not hold enough resource to validate.

The security of IoT systems is analysed in [23–25]. The author discusses a specific smart home system and proposes a blockchain-based framework to guarantee security, confidentiality, integrity, and availability. The security for information and energy interactions in the cloud as well as edge formed by electric vehicle nodes have been raised in [24]. Paper [25] proposed a secure P2P data sharing system in vehicular computing networks by utilising the concept of blockchain technologies. Paper [26] investigates a Mobi-Chain which applies blockchain technology to a novel m-commerce application to protect the security of data. It concludes that blockchain technology is valid for future m-commerce security applications.

B. Contributions and Organization

Motivated by existing developments, we describe a novel mutual-benefit treaty in a blockchain-based heterogeneous cellular air-to-ground network. This model not only balances the interests of both heterogeneous air and ground networks but also protects data integrity under the consensus mechanism. In contrast to existing work [22], it described a unilateral gain system in which the most benefit will directly accrue to the users. The advantage for decentralized storage air-to-ground network is of high-security performance, and it could achieve a closer connection link with two systems than the traditional centralized storage model. The main contributions of this paper are summarised as follows:

- We propose an innovative blockchain-based heterogeneous trading network. In the air-to-ground P2P jamming network, the GSs take out the caching space to support ASs to secure the collected data, in return, the ASs send back certain reward to the GSs, it will highly increase the air data security and the ability to resist jamming signal. We develop a Quality-of-Service (QoS) optimization of the active ASs' output by designing a Cournot game model.
- Through this trading process, we propose a novel dual user association strategy, the first user association aims to increase the average achievable rate, and the secondary user association not only balances the supply and demand in the air-to-ground market but also achieves the maximum benefit for both AS and GS networks.
- We establish two different reward allocation mechanisms in the P2P network, the numerical results demonstrate that the group reward scheme (GRS) always achieves higher spectral efficiency than the individual reward scheme (IRS) in blockchain empowered decentralized storage networks.

The rest of this paper is organized as follows. The system model is presented in Section II. The problem definition for trading contract for both the air and ground sides are provided in Section III. Simulation and numerical results, as well as discussions are given in Section V, followed by concluding remarks in Section VI.

II. SYSTEM MODEL

We consider a heterogeneous air-to-ground blockchain-based decentralized network. In this system, ASs collect the data in sky at different altitudes, then all the active ASs broadcast the data to the ground network due to limitation of caching space and computation in the ASs.

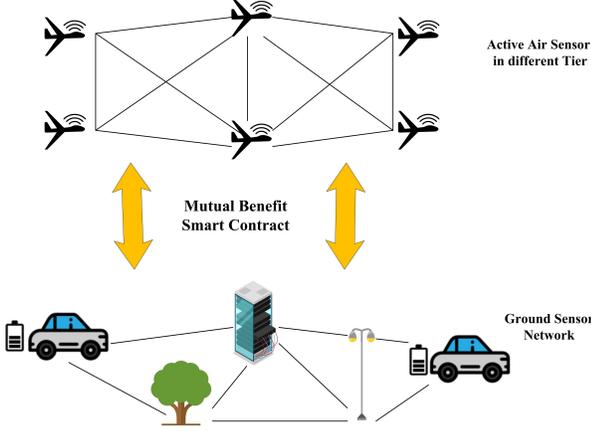


Fig. 1: Localized air-to-ground P2P Network. The GSs could be equipped with smart grid vehicles, server, trees or street lamp.

In Fig. 2, all the sensors work in air-to-ground network as a trusted trading node with the smart contract. The GSs provide storage space for the active ASs according to their QoS function, then the reward coins will be sent from the k -th tier ASs to the robust GS. The locations of the GSs are modelled using a homogeneous poisson point process (HPPP) Φ_G with density λ_G . The locations of the ASs in the k -th tier ($k = 1, \dots, K$) are modelled by an independent HPPP Φ_A^k with density λ_A^k . It is assumed that the density of GSs is much greater than ASs where $\lambda_G > \sum_{k=1}^K \lambda_A^k$, which can ensure that at least one GS could support the AS for the data storage process at each time slot T , the rest of ASs wait for the trading process in the following time slot. In the ASs set, the density decline with the altitude which is given by $\lambda_G \gg \lambda_A^1 > \dots > \lambda_A^k > \dots > \lambda_A^K$.

In addition, we call the active ASs who broadcast the collected data to the associated GSs in the present time slot in set $\tilde{\Phi}_A^k \in \Phi_A^k$, where $\tilde{\Phi}_A^k$ is the independent HPPP with density $a_k \lambda_A^k$. The rest AS who keep the data wait for spread in the next time slot are named quiet ASs with density $(1 - a_k) \lambda_A^k$ in set $\bar{\Phi}_A^k \in \Phi_A^k$, and we have $\tilde{\Phi}_A^k + \bar{\Phi}_A^k = \Phi_A^k$, where $a_k \in [0, 1]$, which means the active ASs output decision affects the QoS for each tier ASs.

More than that, the interpolators are unconscious of which AS generates new data until the transmission process starts. The ASs in the different tier has different susceptibility in the air environment, and the updated data will generate randomly around these sensors.

A. Consensus Process

The consensus process before transaction records forms the blockchain-based air-to-ground network as follows.

1) AS side-storage service requesting:

- Each tier of AS in Φ_A^k generates a serious of raw data from different altitudes. Then the active ASs who generate the data send a request to the contact centre. We assume that each active AS will request the service at one unit of time due to the massive information and information accuracy requirements.
- We define two types of incentive schemes. One is individual reward scheme (IRS), which means each active AS in k -th tier will take out b_k coin for robust GS. Another is group reward scheme (GRS), which means all the GSs who associated k -th tier UAV will share the sum coin b_k^I for reward.
- Based on the smart contract, each AS in tier takes out the given reward 'coin' to prove their ability to finish payments for data storage.
- We establish a benefit function which aims at each tier of ASs that will acquire maximum QoS in the trading market. Through the QoS function, the air network obtain the optimal active ASs set self-regulation via the reward of QoS in the market.

2) GS side-service support and coin payment:

- The typical GS \mathcal{G}_o forecast the achievable average rate for each tier of ASs which based on the current optimized active density.
- Then the typical GS \mathcal{G}_o do the secondary user association to make a decision the connection tier of AS, which aims to maximize the reward in unit time. The compensation depends on the units data reward 'coin' and the achievable average rate for each tier of ASs.
- The consensus protocol is implemented by authorized GSs and a robust GS \mathcal{G}_L who connect to k -th tier AS and achieve maximum data in the given time slot with a valid PoS, notice the gained by the data is depends on the instant achievable rate.
- Once all GSs agree on the block data and robust \mathcal{G}_L get the reward coin, GS \mathcal{G}_L in duty-bound to broadcast the block data and the corresponding signature to other GSs who did not participate in the competition for the same tier AS which guarantees the block data security. Notice PoS is a protocol between a Prover and a Verifier [27] that has two phases.
- After that the coin information issue to GS \mathcal{G}_L . At the same time, the ASs update the coin information and release temporary storage space for the new information storage.
- In return, the ASs will help the coin owner GSs to collect the required information in the air, which could help GSs predict the weather or route in the future.

3) *Blockchain Structure*: In our blockchain-enabled air-to-ground system, blockchain technology is utilized to enhance the IoT block data secure performance from different IoT sensors. We use the IoT security blockchain-based smart home framework [23] in our system, and each block incorporates a block header, a policy header and a group of block data.

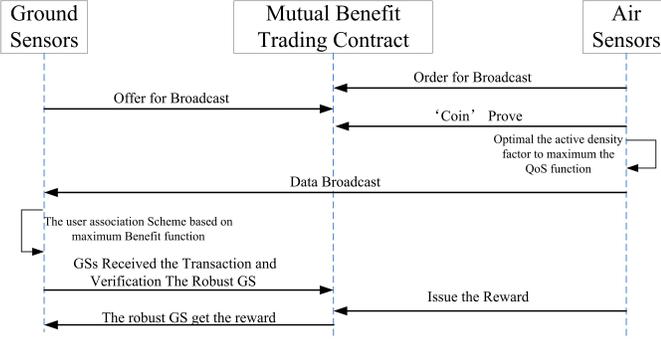


Fig. 2: Sequence diagram of the Air-to-Ground smart contract.

TABLE I: Notation and parameters.

Notation	Parameter
$\Phi_A^k, \tilde{\Phi}_A^k, \bar{\Phi}_A^k$	total AS PPP, active AS PPP and quite AS PPP
λ_A^k, a^k	AS density and active density factor
Φ_G, λ_G	GS PPP and density
Φ_e, λ_e	jamming PPP and density
T	duration time
\mathbf{P}, P_k	transmit power set and k -tier transmit power
\mathbf{h}, h_k	transmit power set and k -tier transmit power
α_L, α_N	LoS and NLoSpas loss exponent
g	small scale fading
β, δ^2	the frequency dependent constant parameter, noise power

B. Downlink Information Transfer

In the average rate predicted stage, AS transmits information signals to the serving GSs in the given duration time slot T with a specific transmit power power set $\mathbf{P} = [P_1, \dots, P_k, \dots, P_K]$, and the height set is $\mathbf{h} = [h_1, \dots, h_k, \dots, h_K]$ where $h_k < h_{k+1}$. Both ASs and GSs are equipped with a single antenna. We also consider the case of eavesdropping with jamming attacks to deteriorate the information transmission. The locations of eavesdroppers are modelled following an independent HPPP Φ_e with λ_e .

For a typical GS \mathcal{G}_o associated with the AS who belongs to a given k -th tier. All channels experience independent identically distributed (i.i.d.) quasistatic Rayleigh fading. We assume that for any typical GS who is located at the point of origin o that is associated with the nearest AS in the k -th tier that has support to save the instant data, the received signal-to-interference-plus-noise ratio (SINR) is shown below:

$$\text{SINR}_o^k = \frac{P_k g_{o,k} \beta |H_{o,k}|^{-\alpha_L}}{\mathcal{I}_k^A + \mathcal{I}_k^J + \delta^2}, \quad (1)$$

where P_k is the transmit power for the k -th tier AS, $g_{o,k}$ is the equivalent small-scale fading channel power gain between the typical GS \mathcal{G}_o and its nearest serving k -th tier AS. Notice when \mathcal{G}_o is associated to K -th tier, the path loss is $|H_{o,k}|^{-\alpha_L}$, where $H_{o,k} = \sqrt{X_{o,k}^2 + h_k^2}$ is the distance from the associated AS to the typical GS, β is the frequency dependent constant parameter and α_L is the line of sight (LoS) path loss exponent. Due to the building blockages around the terrestrial environment, the direct connection between GSs in the ground is weak. We consider the LoS link and same path loss exponent α_L between different tier of ASs to GSs, and the NLoS link between GSs [28]. δ^2 is the noise power.

The interference \mathcal{I}_k^A from the all the active ASs from k -th tier and other tiers which are given by

$$\mathcal{I}_k^A = \sum_{k'=1 \setminus k}^K \sum_{l \in \tilde{\Phi}_A^{k'}} P_{k'} g_{o,k'} \beta |H_{o,k'}|^{-\alpha_L} \quad (2a)$$

$$+ \sum_{j \in \tilde{\Phi}_A^k \setminus o} P_k g_{o,j} \beta |H_{o,j}|^{-\alpha_L}. \quad (2b)$$

(2a) and (2b) are the sum of interference from the interfering ASs in the k' -tier ($k' \neq k$) and the k -tier, $\Phi_A^{k'}$ and Φ_A^k are the point process with density $\lambda_A^{k'}$ and λ_A^k , where $g_{o,l} \sim \exp(1, 1)$ and $g_{o,k} \sim \exp(1, 1)$ are the small-scale fading interfering channel gain and $H_{o,k'} = \sqrt{X_{o,k'}^2 + h_{k'}^2}$ is the distance between a typical GS and the k' -th tier AS $l \in \tilde{\Phi}_A^{k'}$. The channel is authenticated to prevent eavesdropper from tampering with the messages. We assume that all the eavesdroppers transmit jamming signals to the GS, and $\mathcal{I}^J(k)$ is the interference from the jamming which is given by

$$\mathcal{I}_k^J = \sum_{e \in \Phi_e} P_e g_{o,e} \beta |X_{o,e}|^{-\alpha_N}, \quad (3)$$

where Φ_e is the locations of the ground eavesdroppers with density λ_e , where $g_{o,e} \sim \exp(1)$ is the small-scale fading interfering channel gain and $X_{o,e}$ is the distance between the \mathcal{G}_o and ground eavesdropper, and α_N is the none line of sight (NLoS) path loss exponent.

III. PROBLEM DEFINITION FOR TRADING CONTRACT

In this section, we present the trading process which includes the optimized QoS function for each tier of AS, and then we figure out the probability that a typical GS is associated with the AS in the k -th tier based on the achievable average k -th tier rate.

In the trading process, each AS collects useful information named raw data which needs to be protected, due to the limitation of storage space in the ASs and high demand for effective security. The AS generates the updated data then asks GS to help store the data and prevent the information has been tampered. Each GS will take out a certain amount of coin for reward, but only the most robust GS named \mathcal{G}_L will get the reward. In the future, the robust GS \mathcal{G}_L could use the reward 'coin' to request service for the air group to do the data ferry from the further area.

A. The Cournot-Nash equilibrium In Air Side

For the air side, each tier of AS will compete to attract more GSs to support the data storage. However, the more active ASs in the trading market will affect less associated service GSs for each AS at each time.

We assume the exact achievable rate for each tier is unknown where each UAV has incomplete information on other tiers of UAVs parameters, such as the height set \mathbf{h} and the transmit power set \mathbf{P} . The convergence to the Nash equilibrium in such a market is then analyzed using the well-known best response dynamics.

Based on that, we use the **Cournot-Nash equilibrium** to model the QoS function. The AS in k -th tier is a consensus group who expects the maximize profits, and its own active density decision will affect the results of its rivals (k' -tier of AS). The profit maximization problem of the IRS is simplified as follows:

$$\mathbb{P}_1 \quad \max_{\mathbf{a}^{(1)}} \quad Q_k^{\text{IRS}} = a_k \lambda_A^k (\rho_I - b_k), \quad (4a)$$

$$\text{s.t.} \quad \text{C1} : \rho_I = -\theta_1 \mathcal{N}_A + \theta_0, \quad (4b)$$

$$\text{C2} : 0 \leq a_k \leq 1, \quad (4c)$$

where in (4a), Q_k is the total QoS function in the k -tier, which means a high value could provide more support to the k -th tier AS. We assume that in all the ASs in k -th consensus tier are given the same QoS reward because they collect the same type of data in the air. Each tier of AS chooses its optimal active factor a_k independently, and the whole system determines how to achieve the benefit equilibrium for every participator.

Notice in this process, we assume the imperfect information ρ_k is unknown between different tier rivals, so the QoS function assume ρ_I denote the equilibrium service of storage by the competition among the ASs, and ρ_k is supposed to be equal here.

The inverse demand function in (4b), $\rho_I = -\theta_1 \mathcal{N}_A + \theta_0$ is subject to $\frac{d\rho_I}{d\mathcal{N}_A} < 0$, and the equilibrium is always inverse ratio with the number of request group \mathcal{N}_A , where $\mathcal{N}_A = \mathcal{A}_u \sum_{k=1}^K a_k \lambda_A^k$ is the total active density in the unit area market \mathcal{A}_u , θ_0 and θ_1 are the positive constant coefficients.

Because λ_k is fixed, we adjust a_k to decide how much active ASs broadcast the data in each slot and achieve the maximum QoS function Q_k , and the range for the active proportion is $a_k \in [0, 1]$. Notice although the QoS function Q_k is based on the imperfect information, and it could not predict the practical QoS for each tier, however, before the GS makes the final decision, AS could control the broadcast group to achieve the approximate optimal QoS.

Lemma 1: The optimal active density factor set \mathbf{a}_k in problem \mathbb{P}_1 can be expressed as follows

$$\mathbf{a}^{(1)*} = [a_1^{(1)*}, a_2^{(1)*}, \dots, a_K^{(1)*}] \quad (5)$$

where $a_k^{(1)*} = \min \left[\max \left[\frac{1}{\theta_1 \lambda_A^k} \left(\frac{\theta_0 + \sum_{k=1}^K b_k}{K+1} - b_k \right), 1 \right], 0 \right]$ is the active proportion for density of the k -th AS.

Proof 1: Substitute $\rho_I = -\theta_1 \mathcal{N}_A^{(1)} + \theta_0$ into $Q_k^{(1)}$, it can be expressed as:

$$Q_k^{(1)} = a_k \lambda_A^k (\theta_0 - \theta_1 \mathcal{A}_u \sum_{k=1}^K a_k \lambda_A^k - b_k) \quad (6)$$

$$= -\theta_1 (a_k \lambda_A^k)^2 + a_k \lambda_A^k (\theta_0 - \theta_1 \mathcal{A}_u \sum_{k'=1 \setminus k}^K a_{k'} \lambda_A^{k'} - b_k),$$

the first derivative equation can be expressed as:

$$\begin{aligned} \frac{dQ_k^{(1)}}{da_k} & \quad (7) \\ & = -2\theta_1 a_k (\lambda_A^k)^2 + \lambda_A^k (\theta_0 - \theta_1 \mathcal{A}_u \sum_{k'=1 \setminus k}^K a_{k'} \lambda_A^{k'} - b_k). \end{aligned}$$

From (14), $Q_k^{(1)}$ is the continuous quadratic function of $a_k^{(1)}$, and the second derivative of $Q_k^{(1)}$ with the respect to $a_k^{(1)}$ is

$$\frac{d^2 Q_k^{(1)}}{da_k^{(1)2}} = -2\theta (\lambda_A^k)^2 < 0, \quad (8)$$

then we can obtain that $Q_k^{(1)}$ is a concave function of $a_k^{(1)}$. Therefore, we can obtain the optimal output of $Q_k^{(1)}$ by setting the first derivative equal (14) to zero, then obtain $a_k^{(1)}$ as

$$a_k^{(1)} = -\frac{\mathcal{A}_u}{2\lambda_A^k} \sum_{k'=1 \setminus k}^K a_{k'}^{(1)} \lambda_A^{k'} + \frac{\theta_0 - b_k}{2\theta_1 \lambda_A^k}. \quad (9)$$

We can figure out the total active number of UAVs at one slot as follows:

$$\mathcal{N}_A^{(1)*} = \min \left[\max \left[\frac{K\theta_0 - \sum_{k=1}^K b_k}{\theta_1 (K+1)}, \mathcal{A}_u \sum_{k=1}^K \lambda_A^k \right], 0 \right], \quad (10)$$

after that, we can obtain the optimal a_k with (15) and (16) as follow

$$a_k^{(2)op} = \frac{1}{\theta_1 \lambda_A^k} \left(\frac{\theta_0 + \sum_{k=1}^K b_k}{K+1} - b_k \right), \quad (11)$$

based on $a_k^{(1)*} = \min \left[\max \left[a_k^{(1)op}, 0 \right], 1 \right]$, we completes the proof.

Consider the each k -th tier of UAV have been assigned with b_k^I coin, then we can given the profit maximization of the GRS as follow

$$\mathbb{P}_2 \quad \max_{\mathbf{a}} \quad Q_k^{(2)} = a_k \lambda_A^k (\rho_I - \frac{b_k^I}{a_k \lambda_A^k}), \quad (12a)$$

$$\text{s.t.} \quad \text{C1} : \rho_I = -\theta_1 \mathcal{N}_A^{(2)} + \theta_0, \quad (12b)$$

$$\text{C2} : 0 \leq a_k \leq 1, \quad (12c)$$

Lemma 2: The optimal active density factor set \mathbf{a}_k for maximum the problem \mathbb{P}_2 can be expressed as follows

$$\mathbf{a}^{(2)*} = [a_1^{(2)*}, a_2^{(2)*}, \dots, a_K^{(2)*}], \quad (13)$$

where $a_k^{(2)*} = \min \left[\max \left[\frac{1}{\lambda_A^k} \left(\frac{\theta_0}{\theta_1} - \frac{K}{K+1} \right), 0 \right], 1 \right]$.

Proof 2: Similar with \mathbb{P}_1 , we desired the first derivative equation for Q_k can be expressed as:

$$\frac{dQ_k^{(2)}}{da_k} = -2\theta a_k (\lambda_A^k)^2 + \lambda_A^k (\theta_0 - \sum_{k'=1 \setminus k}^K \theta_1 a_{k'} \lambda_A^{k'}). \quad (14)$$

Then we can derive that $Q_k^{(2)}$ is a concave continuous quadratic function of a_k , due to the second derivative of $\frac{d^2 Q_k^{(2)}}{da_k^2} < 0$. Therefore, we can obtain the optimal output of $\frac{dQ_k^{(2)}}{da_k} = 0$ to obtain a_k as

$$a_k^{(2)} = \frac{\theta_0 - \theta_1 \sum_{k'=1 \setminus k}^K a_{k'}^{(2)} \lambda_A^{k'}}{2\theta_1 \lambda_A^k}, \quad (15)$$

Substituting the optimal value in (15), we have the total active number of UAVs at one slot as follows:

$$\mathcal{N}_A^{(2)*} = \max \left[\frac{K\theta_0}{\theta_1(K+1)}, \sum_{k=1}^K \lambda_A^k \right], \quad (16)$$

after that, we can obtain the optimal a_k with (15) and (16) as follow

$$a_k^{(2)op} = \frac{1}{\lambda_A^k} \left\{ \frac{\theta_0}{\theta_1} - \frac{K}{K+1} \right\}, \quad (17)$$

based on $a_k^{(2)*} = \min \left[\max \left[a_k^{(2)op}, 0 \right], 1 \right]$, then we completes the proof.

B. Downlink Performance Evaluation In GS side

Before broadcasting the data, the typical GS \mathcal{G}_o figures out the achievable rate with every tier of AS with uncertain active proportion. Once the GS selects the given k -th tier AS, it will associated the closest AS according to data storage supporting, the connect probability for the k -tier is $f_k(x) = 2\pi a_k \lambda_k x e^{-x^2 \pi a_k \lambda_k}$.

Lemma 3: The achievable average downlink achievable rate between a typical GS \mathcal{G}_o and its serving the nearest AS in k -th tier is as follows:

$$\mathcal{R}_{DL}(k) = \frac{1}{\ln 2} \int_0^\infty \int_0^\infty \frac{\mathcal{P}_k^{cov}(x, \gamma_o)}{1 + \gamma_o} f_k(x) dx d\gamma_o \quad (18)$$

where $\mathcal{P}_k^{cov}(x, \gamma_o)$ is given in (19) shown at the top of the next page. The constant $\chi_N = \frac{2}{\alpha_N}$, $\chi_L = \frac{\alpha_L}{2}$, $\text{csc}(\cdot)$ is the cosecant-trigonometry function. For ease of notation, we define the following two functions O_k and $O_{k'}$, which are related to the interference from the AS s in the k -th tier and other tiers, respectively:

$$O_k = \int_{\sqrt{h_k^2+x^2}}^\infty \frac{1}{\left(\frac{r^2+h_k^2}{x^2+h_k^2} \right)^{\chi_L} / \gamma_o + 1} r dr, \quad (20)$$

$$O_{k'} = \int_{h_{k'}}^\infty \frac{1}{P_k \left(\frac{r^2+h_{k'}^2}{x^2+h_k^2} \right)^{\chi_L} / (\gamma_o P_{k'}) + 1} r dr. \quad (21)$$

Proof 3: The outage coverage probability is as follows

$$\mathcal{P}_k^{cov}(\gamma_o) = \Pr(\text{SINR}_{o,i}(k) \geq \gamma_o), \quad (22)$$

where $\mathcal{P}_k^{cov}(\gamma_o)$ is the CCDF of the received SINR from typical GS to the associated AS, denoted by $\text{SINR}_{o,i}(k)$, and is given by

$$\begin{aligned} \mathcal{P}_k^{cov}(\gamma_o) &= \int_0^\infty \mathcal{P}_{DL}(x, \gamma_o, k) f_k(x) dx \\ &= \int_0^\infty \Pr \left(\frac{P_k h_{o,i} \beta (x^2 + h_k^2)^{-\frac{\alpha_L}{2}}}{\mathcal{I}^A + \mathcal{I}^J + \delta^2} > \gamma_o \right) f_k(x) dx \\ &= \int_0^\infty e^{-\frac{\delta^2 (x^2 + h_k^2)^{\frac{\alpha_L}{2}} \gamma_o}{P_k \beta}} \\ &\quad \mathbb{E} \left\{ e^{-\frac{\mathcal{I}^A \delta^2 (x^2 + h_k^2)^{\frac{\alpha_L}{2}} \gamma_o}{P_k \beta}} \right\} \mathbb{E} \left\{ e^{-\frac{\mathcal{I}^J \delta^2 (x^2 + h_k^2)^{\frac{\alpha_L}{2}} \gamma_o}{P_k \beta}} \right\} f_k(x) dx \\ &= \int_0^\infty e^{-\frac{\delta^2 (x^2 + h_k^2)^{\frac{\alpha_L}{2}} \gamma_o}{P_k \beta}} \mathcal{L}_{\mathcal{I}^A}(s_k) \mathcal{L}_{\mathcal{I}^J}(s_k) f_k(x) dx, \end{aligned} \quad (23)$$

where $s_k = \frac{(x^2+h_k^2)^{\frac{\alpha_L}{2}} \gamma_o}{P_k \beta}$, and $\mathcal{L}_{\mathcal{I}^A}(s_k)$ and $\mathcal{L}_{\mathcal{I}^J}(s_k)$ are the Laplace transforms of the PDFs of \mathcal{I}^A and \mathcal{I}^J . By applying the stochastic geometry, we derive the Laplace transform of the PDF of \mathcal{I}^A :

$$\begin{aligned} \mathcal{L}_{\mathcal{I}^A}(s) &= \mathbb{E}_{\Phi_k^A} \left[\exp \left(-s_k \sum_{i \in \Phi_k^A} P_k h_{o,i} \beta H_{o,i}^{\alpha_L} \right) \right] \\ &+ \mathbb{E} \left\{ \sum_{k'=1 \setminus \{k\}}^K \exp \left(-s_k \sum_{l \in \Phi_{k'}^A} P_{k'} h_{o,l} \beta H_{o,l}^{\alpha_L} \right) \right\} \\ &= \exp \left\{ -2\pi a_k \lambda_k \times \right. \\ &\quad \left. \int_{\sqrt{h_k^2+x^2}}^\infty \left(1 - \frac{1}{1 + s_k P_k \beta (r^2 + h_k^2)^{-\chi_L}} \right) r dr \right\} \\ &\quad \times \prod_{k'=1 \setminus \{k\}}^K \exp \left\{ -2\pi a_{k'} \lambda_{k'} \times \right. \\ &\quad \left. \int_{h_{k'}}^\infty \left(1 - \frac{1}{1 + s_k P_{k'} \beta (r^2 + h_{k'}^2)^{-\chi_L}} \right) r dr \right\}. \end{aligned} \quad (24)$$

Using a similar approach in (24), we derive the interference coming from the jamming signal as follows

$$\begin{aligned} \mathcal{L}_{\mathcal{I}^J}(s_k) &= \mathbb{E}_{\Phi^J} \left[\exp \left(-s_k \sum_{j \in \Phi^J} P_e h_{o,e} \beta y_{o,e}^{\alpha_N} \right) \right] \\ &\stackrel{(a)}{=} \exp \left[-2\pi \lambda_e \int_0^\infty \left(1 - \frac{1}{1 + s_k P_e \beta r e^{-\alpha_N}} \right) r_e dr_e \right], \end{aligned} \quad (25)$$

where (a) is obtained by using the generating functional of PPP [29].

After that, we can obtain (24) and (25) of the SINR in (23), and this completes the proof.

Based on the predicted average achievable rate $\mathcal{R}_k(\mathbf{a}^{(1)*})$ which is associated to k -th tier AS, we can build the secondary user association scheme, which aims to maximize the benefit for the typical GS. The serving AS for a typical GS based on the IRS \mathbb{P}_1 is selected according to the following criterion:

$$\text{GS} : \arg \max_{k \in \{1, 2, \dots, K\}} \mathcal{F}_k^*, \quad (26)$$

where

$$\mathcal{F}_k^* = \mathcal{R}_k(\mathbf{a}^{(1)*}) \cdot b_k \cdot \Psi_k^{(1)}, \quad (27)$$

since each typical GS only associated to one UAV, and $\Psi_k^{(1)}$ is the success probability that the typical GS turn into the robust GS and obtain the reward b_k . Notice even a portion of GSs support the k -th tier ASs at each slot, but the block data will be copied to all the other GSs in the P2P network. Then we can see this is a Nash Equilibrium problem in which the typical GS will reward the same benefit \mathcal{F} from any tier of AS. Then we can formulate the secondary user association probability for the IRS \mathbb{P}_1 expression as:

$$\Psi_k^{(1)*} = \frac{1}{\mathcal{R}_k(\mathbf{a}^{(1)*}) b_k} \frac{1}{\sum_{k=1}^K \frac{1}{\mathcal{R}_k(\mathbf{a}^{(1)*}) b_k}}. \quad (28)$$

$$\mathcal{P}_k^{\text{cov}}(\gamma_o) = \exp \left\{ -\frac{\delta^2 \gamma_o}{P_k \beta} (x^2 + h_k^2)^{\chi_L} - \lambda_e \chi_N \pi \text{csc}(\chi_N \pi) (x^2 + h_k^2)^{\chi_N \chi_L} \left(\frac{\gamma_o P_e}{P_k} \right)^{\chi_N} - 2\pi a_k \lambda_k O_k - 2\pi \sum_{k'=1 \setminus \{k\}}^K a_{k'} \lambda_{k'} O_{k'} \right\} \quad (19)$$

Overall, for a typical GS in the heterogeneous UAV network with dual user association, the average achievable rate can be calculated as

$$\mathcal{R}_{\text{HetNet}}^{(1)} = \sum_{k=1}^K \Psi_k^{(1)} \mathcal{R}_k(\mathbf{a}^{(1)*}). \quad (29)$$

For the \mathbb{P}_2 bonus scheme, the secondary user association for the serving AS for a typical GS is selected according to the following criterion:

$$\text{GS} : \arg \max_{k \in \{1, 2, \dots, K\}} \mathcal{R}_k(\mathbf{a}^{(2)*}) \cdot \frac{b_k}{a^{(2)*} \lambda_k}, \quad (30)$$

where

$$\mathcal{F}_k^* = \mathcal{R}_k(\mathbf{a}^{(2)*}) \cdot \frac{b_k}{a^{(2)*} \lambda_k} \cdot \Psi_k^{(2)}, \quad (31)$$

the secondary user association probability for bonus scheme \mathbb{P}_2 expression as:

$$\Psi_k^{(2)*} = \frac{a_k^{(2)*} \lambda_k^A}{\mathcal{R}_k(\mathbf{a}^{(2)*}) b_k^I} \frac{1}{\sum_{k=1}^K \frac{a_k^{(2)*} \lambda_k^A}{\mathcal{R}_k(\mathbf{a}^{(2)*}) b_k^I}}. \quad (32)$$

Then we can obtain the average achievable rate for a typical GS in the heterogeneous UAV network with dual user association as

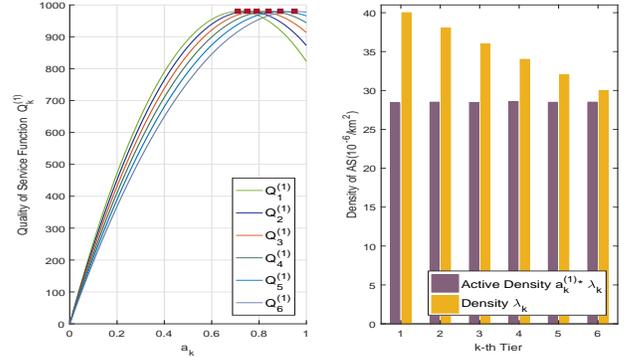
$$\mathcal{R}_{\text{HetNet}}^{(2)} = \sum_{k=1}^K \Psi_k^{(2)} \mathcal{R}_k(\mathbf{a}^{(2)*}). \quad (33)$$

IV. NUMERICAL RESULTS

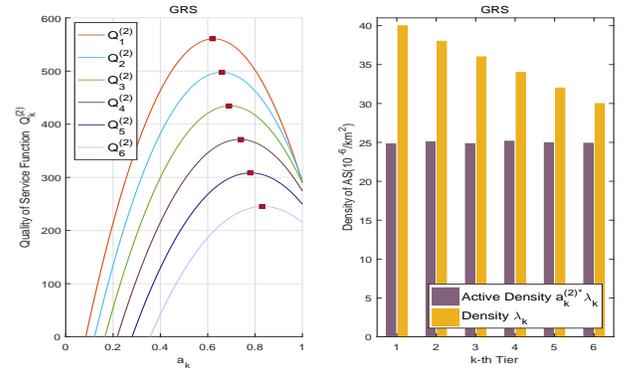
In this section, we present the numerical results to examine the impact of reward function of both the GS and AS network. We consider an air-to-ground blockchain based hybrid network, and there are six different tiers in the air system.

All the parameters used in the simulation are carefully selected and well referenced. The transmit power of different tier of AS are $\mathbf{P}_k = [20, 20, 23, 23, 30, 30]$ dBm, given the mobile-to-tower output power listed in the 3GPP channel model [30]. Also, considering the frequency requirement used in aircraft, we have $f_c = 2.43$ GHz. The Path loss exponent in urban micro-cellular for for LoS and NLoS are $\alpha_L=2$ and $\alpha_N=3.1$, respectively [31]. And finally, we design the heterogeneous ASs system work on altitude lower than 27 kilometers for information interaction and collection [32].

In the Fig. 3 we evaluate the optimal density in each tier in (5) for IRS and (13) for GRS which compare with original total density set $\lambda_k^A = [40, 38, 36, 34, 32, 30]/\text{km}^2$. We have constant $\theta_1 = 1.2 \times 10^{11}$ and $\theta_0 = 6 \times 10^7$, the unit area is $\mathcal{A}_u = 1$. We assume the reward 'coin' for IRS as $\mathbf{b}_k = [3, 4, 5, 6, 7, 8] \times 10^2$, and the reward 'coin' for GRS



(a) Individual reward scheme (IRS).



(b) Group reward scheme (GRS).

Fig. 3: The optimal active density $a_k \lambda_k^A$ and total density λ_k^A in different tier and the utility of QoS function Q_k in different tiers against active density factor a_k .

as $\mathbf{b}_k^I = [3, 4, 5, 6, 7, 8] \times 10^{1-8}$. Firstly, we observe that the optimal active density factors for both two schemes to obtain the maximum QoS function Q_k is existing. We are marking the optimal set \mathbf{a}^* are $\mathbf{a}^{(1)*} = [[0.71, 0.75, 0.79, 0.84, 0.89, 0.95]$ and $\mathbf{a}^{(2)*} = [0.62, 0.66, 0.69, 0.74, 0.78, 0.83]$ factor with red square from tier 1 to 6, respectively. We also observed that in both of these two schemes, the optimal active density are generally with similar value. In Fig. 3(a), we observe that the optimal $Q_k^{(1)}$ is almost in same lever, but the optimal $Q_k^{(2)}$ in Fig. 3(b) is decrease from tier one to tier six. Because in this market, even the upper tier with small density, the upper tier keeps higher active density to guarantee the balance of the trading market.

Fig. 4 shows the impact of the height set on the average heterogeneous achievable rates when the AS height set. In order to better analysis the performance of average rate, we assume the minimum height h_b and the actual height set is

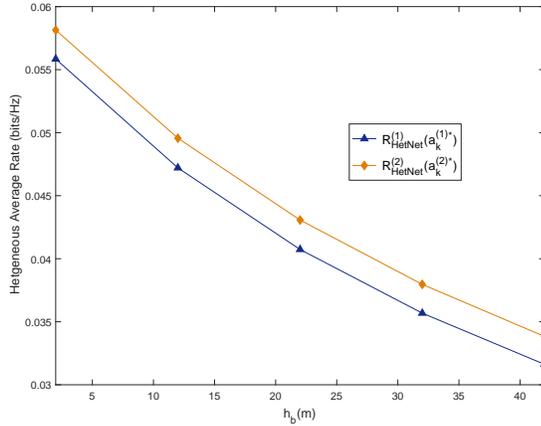


Fig. 4: Average heterogeneous rate via different height

$h_k = h_b + [20, 22, 24, 26, 28, 30]$ m. The analytical curves from (29) and (33) for IRS and GRS, respectively. We observe that the $\mathcal{R}_{\text{HetNet}}^{(2)}$ is always better than $\mathcal{R}_{\text{HetNet}}^{(1)}$, and GRS pay lower reward 'coin' than IRS. The result shows that dynamic allocation reward resource is more economical and achieve higher performance for the heterogeneous decentralized network.

V. CONCLUSION

In this paper, we proposed a blockchain based air to ground communication model that embraced the concept of distributed data storage and mutually beneficial transaction, to enable secure and efficient information transmission in industrial IoT network. While the security issues in data storage and transmission become more and more critical in the IoT network, the decentralized network can protect data integrity, as well as build up an eco-system among the heterogeneous networks. The simulation results show that the trading consensus process can be well adopted in the air-to-ground industrial IoT system, and the optimized active density could maximize the QoS for AS and increase the transmission rate for the information exchange system.

REFERENCES

- [1] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, Aug. 2017.
- [2] S. M. Z. C. Q. H. Y. Dai, D. Xu and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Network Magazine*, pp. 1–1, Jan. 2019.
- [3] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things," *Information Technology and Management*, vol. 13, no. 4, pp. 205–216, 2012.
- [4] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Infor.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
- [5] N. Lohade, "Dubai aims to be a city built on blockchain," *Wall Street Journal*, 2017.
- [6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system."
- [7] M. Conoscenti, A. Vetr, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, Nov. 2016, pp. 1–6.
- [8] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015, pp. 281–310.

- [9] M. Liu, R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, pp. 1–1, Aug. 2018.
- [10] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
- [11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, May 2016.
- [12] S. Feng, W. Wang, D. Niyato, D. I. Kim, and P. Wang, "Competitive data trading in wireless-powered internet of things (IoT) crowdsensing systems with blockchain," *arXiv preprint arXiv:1808.10217*, 2018.
- [13] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," *arXiv preprint arXiv:1711.01049*, 2017.
- [14] 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. Infor.*, vol. 13, no. 6, pp. 3154–3164, Dec 2017.
- [15] 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. Infor.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
- [16] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128–134, Feb. 2017.
- [17] K. E. Oleson, P. Hancock, D. R. Billings, and C. D. Schesser, "Trust in unmanned aerial systems: A synthetic, distributed trust model," in *GPaper presented at the 16th International Symposium on Aviation Psychology*, Dayton, OH, 2011.
- [18] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmwave networks Using Matérn hardcore point processes," *IEEE J. Sel. Areas Commun.*, pp. 1–1, Apr. 2018.
- [19] F. Nex and F. Remondino, "UAV for 3D mapping applications: a review," *Applied geomatics*, vol. 6, no. 1, pp. 1–15, Mar. 2014.
- [20] M. Conoscenti, A. Vetr, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. IEEE, 2016.
- [21] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, May 2015, pp. 180–184.
- [22] D. Vorick and L. Champine, "Sia: Simple decentralized storage," 2014.
- [23] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
- [24] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, May 2018.
- [25] 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 J. Inter. of Thi.*, pp. 1–1, Oct. 2018.
- [26] K. Suankaewmanee, D. T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, and Z. Han, "Performance analysis and application of mobile blockchain," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Mar. 2018, pp. 642–646.
- [27] S. Park, K. Pietrzak, J. Alwen, G. Fuchsbauer, and P. Gazi, "Spacecoin: A cryptocurrency based on proofs of space," IACR Cryptology ePrint Archive 2015, Tech. Rep., 2015.
- [28] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3074–3085, Sep. 2011.
- [29] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge University Press, 2013.
- [30] 3GPP TR 36.814, "Further advancements for E-UTRA physical layer aspects (V9.0.0)," Mar. 2010.
- [31] S. Sun, T. S. Rappaport, S. Rangan, T. A. Thomas, A. Ghosh, I. Z. Kovacs, I. Rodríguez, O. Koymen, A. Partyka, and J. Jarvelainen, "Propagation path loss models for 5g urban micro- and macro-cellular scenarios," in *Vehicular Technology Conference (VTC Spring)*, May 2016, pp. 1–6.
- [32] R. Weibel and R. J. Hansman, "Safety considerations for operation of different classes of UAVs in the nas," in *AIAA 4th Aviation Technology, Integration and Operations (ATIO) Forum*, p. 6244.