Incentivizing Resource Cooperation for Blockchain Empowered Wireless Power Transfer in UAV Networks

Li Jiang, Bin Chen, Shengli Xie, *Fellow, IEEE*, Sabita Maharjan, *Member, IEEE*, and Yan Zhang, *Fellow, IEEE*

***Abstract*—In unmanned aerial vehicle (UAV) networks, UAVs-assisted wireless power transfer is a promising approach to charge low-power smart devices for energy replenishment. However, security and privacy concerns associated with the energy micro-transactions in untrusted wireless trading environment present serious challenges. In this paper, we exploit Directed Acyclic Graph (DAG) and consortium blockchain to propose a new distributed and secure UAVs-assisted wireless power transfer framework named aerial-ground chain, where heterogeneous consensus is developed to verify the energy micro-transactions. Specifically, the UAVs verify energy micro-transactions simultaneously but asynchronously to form an aerial tangle. The smart devices also participate in maintaining the aerial tangle. We define timeout for the energy micro-transactions, and leverage a set of Access Points (APs) to cooperatively confirm the timeout energy micro-transaction by utilizing consortium blockchain, to form a ground main chain. Furthermore, a contract theory based resource cooperation scheme is designed to motivate the UAVs to participate in wireless power transfer, and to incentivize the APs to contribute their resources in cooperatively verifying the timeout energy micro-transactions. Security analysis and numerical results illustrate that the developed aerial-ground chain and the designed contract theory based resource cooperation scheme are secure and efficient for UAVs-assisted wireless power transfer.**

***Index Terms*—Unmanned aerial vehicle (UAV), wireless power transfer, directed acyclic graph (DAG), tangle, consortium blockchain, contract theory.**

Manuscript received June 6, 2020; revised September 23, 2020; accepted October 28, 2020. Date of publication November 6, 2020; date of current version January 22, 2021. This work was supported in part by the NSFC Programs under Grant 61701125, in part by the National Key R&D Program of China under Grants 2020YFB1807801 and 2020YFB1807800, in part by the Science and Technology Plan Project of Guangdong under Grants 2016A030313705 and 2017B010125002, in part by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Sklodowska-Curie Grant 824019. The review of this article was coordinated by Prof. Q. Song. *(Corresponding author: Dr. Li Jiang.)*

Li Jiang is with the Key Laboratory of Ministry of Education, School of Automation, Guangdong University of Technology, Guangzhou 510006, China, and also with the Guangdong Key Laboratory of IoT Information Processing, Guangzhou 510006, China (e-mail: jiangli@gdut.edu.cn).

Bin Chen is with the School of Automation, Guangdong University of Technology, Guangzhou 510006, China, and also with the Guangdong-HongKong-Macao Joint Laboratory for Smart Discrete Manufacturing, Guangzhou 510006, China (e-mail: bin.chen@mail2.gdut.edu.cn).

Shengli Xie is with the School of Automation, Guangdong University of Technology, Guangzhou 510006, China, and also with the State Key Laboratory of Precision Electronic Manufacturing Technology and Equipment, Guangzhou 510006, China (e-mail: shlxie@gdut.edu.cn).

Sabita Maharjan and Yan Zhang are with the University of Oslo, 0315 Oslo, Norway, and also with the Simula Metropolitan Center for Digital Engineering, 0315 Oslo, Norway (e-mail: sabita@ifi.uio.no; yanzhang@ieee.org).

Digital Object Identifier 10.1109/TVT.2020.3036056

I. Introduction

Due to the advantages of controllable mobility, flexible deployment and strong line-of-sight (LoS) channels, unmanned aerial vehicles (UAVs) can provide advanced services for edge-enabled Internet of Things (IoT) applications [1]–[5], such as acting as aerial base stations (BSs) or communication relays for ubiquitous connectivity to ground IoT smart devices. In this context, UAV networks, a new paradigm that integrates multiple coordinated UAVs to achieve autonomous aerial networks [6], emerges as a crucial area. In UAV networks, UAVs-assisted wireless power transfer has drawn significant research interest to enhance the efficiency of wireless power transfer for charging the ground low-power smart devices [7]. By exploiting their controllable mobility, UAVs mounted with energy transmitters can properly adjust their trajectory over time to reduce their distances with target ground smart devices, thus improving the efficiency of wireless power transfer. Although UAVs-assisted wireless power transfer has a potential to considerably improve energy replenishment for ground smart devices, new security and privacy issues arise due to the untrusted wireless trading environment: (i) The potential energy attacks from adversaries, such as energy repudiation of reception and energy state forgery [8], may lead to considerable amount of energy loss from UAVs; (ii) Conventional intermediary dependent management of energy micro-transactions may suffer scalability issues and problems like single point of failure. To this end, state of the art demands new approaches for enhancing security and privacy for UAVs-assisted wireless power transfer in UAV networks.

Blockchain is a promising solution to enable secure and privacy-preserved interactions between untrusted individuals without depending on a central authority [9]. With the characteristics of anonymity, tamper-proof and traceability, blockchain has gained much attention for addressing the security and privacy issues in areas such as in Internet of Things [10]–[12], vehicular networks [13], [14], mobile networks [15], [16] and UAV networks [17]–[19]. Therefore, we observe a close match between the features of a blockchain and the requirements of UAVs-assisted wireless power transfer in which UAVs and smart devices are distributed and do not trust each other. Nevertheless, the crypto-puzzle solving based Proof-of-Work (PoW) consensus protocol consumes a large amount of computation and energy resources, which is not suitable for the resource constrained UAVs and ground smart devices since they can not undertake heavy computation. Directed Acyclic Graph (DAG) has emerged as a new distributed ledger technology to enhance the efficiency of conventional blockchain [20]. In DAG, micro-transactions issued by users constitute site set instead of block based link list in traditional blockchain. There are no miners and no transaction fee. The confirmation of a micro-transaction depends on its increasing cumulative weight, which is determined by a Markov-Chain Monte Carlo method. The higher cumulative weight of a micro-transaction represents the higher probability that the micro-transaction will be accepted by the DAG. Therefore, the more micro-transactions are issued by the users, the more verification are executed, thus making the DAG faster and safer. The DAG with a tangle data structure has been used in IOTA to support frequent micro-transactions in a P2P network [22]. It is noteworthy that the distinct characteristics of DAG introduce unique challenges for UAVs-assisted wireless power transfer. In practice, the vast and growing scale of energy micro-transactions may not be successfully propagated among the nodes due to the limited bandwidth resource and the dynamic topology of UAVs. This can cause the energy micro-transactions confirmation procedure to fail. Besides, the confirmation delay of the energy micro-transactions is adversely affected by the uncertainty associated with the stochastic wireless transmission environment, making it difficult to find the range for the latency.

Heterogeneous blockchain is a concept developed to accommodate the different IoT use cases by integrating multiple blockchains [23], [24]. In a heterogeneous blockchain, multiple sub-blockchains are generated according to a set of rules that combine best practices in designing a sub-blockchain. Nodes in each sub-blockchain verify the local transactions using a certain consensus protocol, and do not have to verify transactions that occur in other sub-blockchains. Besides, an inter-connector framework, such as Polkadot [25] or Cosmos [26], is utilized to achieve inter-operability among sub-blockchains in order to form a unified public ledger. Motivated by the layered idea of heterogeneous blockchain, we utilize blockchain of DAG and consortium blockchain to develop a new distributed and secure UAVs-assisted wireless power transfer framework, which is named aerial-ground chain. Different from [27], where the authors developed a hybrid blockchain to protect the model parameters of federated learning in the Internet of vehicles, our work mainly focuses on developing a blockchain with heterogeneous consensus to secure the wireless power transfer in UAVs-assisted networks framework. Our main contributions are as follows:

- We exploit DAG and consortium blockchain to develop a new distributed and secure UAVs-assisted wireless power transfer framework named aerial-ground chain, where heterogeneous consensus is designed for UAVs to verify the energy micro-transactions to form an aerial tangle, and for the APs to verify the timeout energy micro-transactions to form the ground main chain.
- We investigate the interactions between the aerial tangle and the ground main chain to illustrate detailed operations of the proposed aerial-ground chain for UAVs-assisted wireless power transfer.
- We design a contract theory based resource cooperation scheme to find the optimal charging time for each UAV and the optimal verification rate for each AP.

The remainder of this paper is organized as follows. In Section II, we discuss the related works. In Section III, we present the proposed aerial-ground chain framework and introduce the main components. In Section IV, we present the detailed operations of the proposed aerial-ground chain. In Section V, we formulate a contract theory based resource cooperation scheme for *UAVs-assisted wireless power transfer* and *timeout energy micro-transactions verification*. In Section VI, we illustrate the performance of the resource cooperation scheme through extensive simulations. Section VII concludes this paper.

II. Related Works

A. Blockchain in Network Scenarios

Blockchain has been widely applied in IoT [10]–[12], vehicular networks [13], [14], and mobile networks [15], [16] to address the security and privacy issues associated with communications and resources trading. In [10], K. Zhang *et al.* designed a credit-differentiated edge transaction approval mechanism to achieve flexible and secure edge service management. In [11], Y. Li *et al.* investigated the impact of network load on the key performance metrics of DAG, which act as a guidance for practical deployment of DAG based IoT networks. In [12], O. Novo *et al.* exploited blockchain to develop a new and fully distributed access control system for IoT. In [13], V. Ortega *et al.* studied permissioned blockchain in vehicular communications to achieve the dynamic control of the integrity and validity of the information dissemination. In [14], H. Liu *et al.* studied blockchain during both information and energy interactions in electric vehicles hybrid cloud and edge computing to enhance security protection. In [15], Y. Dai *et al.* proposed a secure and intelligent architecture for next-generation wireless networks by integrating artificial intelligence and blockchain into wireless networks. In [16], L. Jiang *et al.* developed a D2D blockchain to enable security and privacy protection for data sharing between the proximity devices in 5G small cell networks.

B. Blockchain in UAV networks

With the high mobility and low cost, UAVs offer the potential to a wide range of applications to enhance the performance of terrestrial wireless networks. Nonetheless, the distributed UAV networks can make wireless resource transactions vulnerable to malicious nodes. Some recent works have leveraged blockchain into UAV networks for spectrum sharing [17], energy trading [18] and edge computing [19]. For instance, in [17], J. Qiu *et al.* utilized consortium blockchain to perform secure and distributed spectrum trading between mobile network operators and UAV operators. In [18], V. Hassijia *et al.* used advanced blockchain based on the DAG to create a distributed network

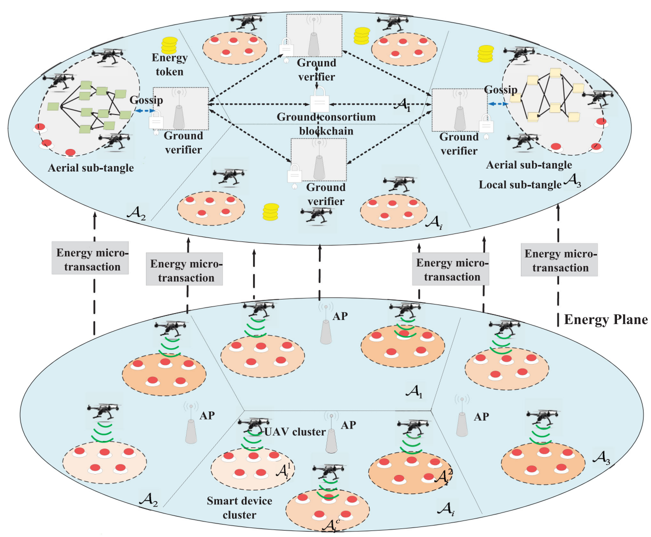


Fig. 1. System model of the proposed aerial-ground chain for UAVs-assisted wireless power transfer.

for secure energy trading between UAVs and charging stations. In [19], A. Asheralieva *et al.* considered UAVs as mobile-edge computing units to process some blockchain tasks from the IoT peers. However, the existing works have not specified any explicit framework to apply blockchain for UAVs-assisted wireless power transfer. Furthermore, the challenges associated with applying blockchain in UAVs-assisted wireless power transfer such as successful propagation of energy micro-transactions and fast confirmation of energy micro-transactions in dynamic wireless transmission environment have not been well studied. Motivated by such considerations, in this paper, we design a blockchain empowered UAVs-assisted wireless power transfer framework and optimize the energy micro-transactions confirmation procedure.

III. Blockchain Empowered Distributed and Secure UAVs-Assisted Wireless Power Tranfer Framework

The proposed blockchain empowered distributed and secure UAVs-assisted wireless power transfer framework is shown in Fig. 1, illustrating the energy plane, the blockchain plane and the interactions between these two planes. UAVs, APs and smart devices act as nodes in the proposed framework. Each node has a unique digital identity consisting of its public/private keys to ensure trust among the nodes during wireless power transfer.

A. Energy Plane

The energy plane is presented in the lower part of Fig. 1. The smart devices such as cameras or sensors are deployed in a geographical area $\mathcal{A}$ to monitor industrial machines and control systems. The collected data by the smart devices is sent to the near APs for analysis. We consider there are a set $\mathcal{I}$ of APs, and each AP $i \in \mathcal{I}$ covers an area $\mathcal{A}_i$, such that $\cup_{\forall i \in \mathcal{I}} \mathcal{A}_i = \mathcal{A}$, and $\mathcal{A}_i \cap \mathcal{A}_{i'} = \emptyset$ for any $i, i' \in \mathcal{I}$, and $i \neq i'$. In each coverage area $\mathcal{A}_i$, groups of smart devices are deployed to form a set $\mathcal{C}$ of clusters, $c \in \mathcal{C}$. We consider $\mathcal{U}_i^c$ smart devices uniformly distribute in each cluster and the amount of energy requirement is different among the clusters. As shown in Fig. 1, the cluster with darker color represents more energy demand from the smart devices in the cluster. A set $\mathcal{J}$ of UAVs mounted with energy transmitter are deployed in area $\mathcal{A}$ to wirelessly transfer power to the target smart device clusters. Besides, a docking station[1] is also placed so that the UAVs can charge their batteries. In order to enhance the efficiency of wireless power transfer, we consider an individual UAV only charges one smart device cluster at each time. By referring to [7], each UAV exploits a single-location hovering method for charging, the optimal charging location of each UAV can be designed to maximize the sum received energy for the corresponding smart device cluster.

At the beginning of wireless power transfer, the local AP broadcasts request including the charging locations and the energy requirement. Once receives the request, each UAV judges whether its current on-broad energy can meet the wireless power transfer requirement, such as the energy consumption for moving from its current location to the target charging location, hovering, charging, and flying from the target charging location to the docking station. If the UAVs satisfy the conditions, they fly from their current locations to the target charging locations with average flying speed V in m/s; otherwise, the UAVs fly back to the docking station and prepare for the next period of wireless power transfer. Thus, multiple UAVs can serve the local AP at each charging period and coordinate distributively with local information to form a UAV cluster. Denote P_p, P_h and P_c are constant propulsion power, hovering power and transmit power of the UAV, respectively. Since the UAV exploits single-location hovering method for charging, both the hovering time and the charging time are denoted as T_j^c.

During the wireless power transfer period, the jth UAV and the u_i^cth smart device have the fixed locations $\mathbf{y}_j = (x_j, y_j, H)$ and $\mathbf{x}_{u_i^c} = (x_{u_i^c}, y_{u_i^c}, 0)$ in a 3D Euclidean coordinate, respectively, where $j \in \mathcal{J}$, $c \in \mathcal{C}$, and each UAV is considered to fly at a fixed altitude H above the ground. The wireless channel between the jth UAV and the u_i^cth smart device is line-of-sight (LOS)-dominated, thus making the free-space path loss model reasonable to be captured [7]. Therefore, the channel power gain from the jth UAV to the u_i^cth smart device can be written as

$$h_{\mathbf{x}_{u_i^c}, \mathbf{y}_j} = \beta_0 d^{-2}_{\mathbf{x}_{u_i^c}, \mathbf{y}_j}, \tag{1}$$

where $d_{\mathbf{x}_{u_i^c}, \mathbf{y}_j} = \sqrt{(x_j - x_{u_i^c})^2 + (y_j - y_{u_i^c})^2 + H^2}$ is the distance between the jth UAV and the u_i^cth smart device, and β_0 denotes the channel power gain at a reference distance of $d_0 = 1$ m. The received energy by the u_i^cth smart device is thus given by

$$\begin{aligned} e_{\mathbf{x}_{u_i^c}, \mathbf{y}_j} &= \eta P_c h_{\mathbf{x}_{u_i^c}, \mathbf{y}_j} T_j^c \\ &= \frac{\eta \beta_0 P_c T_j^c}{(x_j - x_{u_i^c})^2 + (y_j - y_{u_i^c})^2 + H^2}, \end{aligned} \tag{2}$$

[1][Online]. Available: https://www.airoboticsdrones.com/

where $0 < \eta \leq 1$ denotes the RF-to-DC energy conversion efficiency of each smart device. It is noted that the RF-to-DC energy conversion efficiency is generally nonlinear. However, a generic model to accurately characterize the non-linear RF-to-DC conversion efficiency is not available yet[7]. Therefore, we consider a simplified RF-to-DC energy conversion efficiency by assuming that each smart device operates in the linear regime for RF-to-DC conversion. However, our design principles also can be extended to the scenario with non-linear energy harvesting model. The sum energy received by the cth smart device cluster is given by

$$\begin{aligned} E_i^c &= \sum_{u_i^c \in \mathcal{U}_i^c} e_{\mathbf{x}_{u_i^c}, \mathbf{y}_j} \\ &= \sum_{u_i^c \in \mathcal{U}_i^c} \frac{\eta \beta_0 P_c T_j^c}{\left(x_j - x_{u_i^c}\right)^2 + \left(y_j - y_{u_i^c}\right)^2 + H^2}, \end{aligned} \tag{3}$$

Given the energy that can be provided by the UAV in (3), the local AP needs to estimate a suitable UAV to charge the target smart device cluster. Since the APs and the UAVs belong to different operators, the local AP needs to pay each UAV the reward to compensate them for their energy consumption for wireless power transfer. In addition, the on-broad energy available with each UAV is different, which results in different energy cost for different UAVs in wireless power transfer.

B. Blockchain Plane

The UAVs-assisted wireless power transfer is vulnerable to unpredictable energy attacks, such as energy repudiation of reception and energy state forgery, that can result in considerable amount of energy loss from the UAVs. We exploit blockchain of DAG and consortium blockchain to develop an aerial-ground chain for protecting UAVs against energy attacks. In our developed aerial-ground chain as shown in the upper part in Fig. 1, we abstract three main components: 1) energy micro-transactions, 2) heterogeneous consensus and 3) energy token.

1) Energy Micro-Transactions: Considering the wireless power transfer frequently happens between the UAVs and the smart device clusters, and the transaction value is low, we define such wireless power transfer transaction as energy micro-transaction. When the UAV provides wireless power transfer to the smart device cluster, it first generates energy micro-transaction which records the information related to the wireless power transfer events. Then, the energy micro-transaction is digitally signed by using private key of both the UAV and the smart devices, and is confirmed by our developed aerial-ground chain.

2) Heterogeneous Consensus: The UAVs and the smart devices maintain the aerial tangle. To add an energy micro-transaction to the local sub-tangles, the UAV has to verify two previous energy micro-transactions by solving a simplified crypto-puzzle. After validation, the UAV appends the new energy micro-transaction to the local sub-tangle by attaching the hashes of the two validated energy micro-transactions to the new incoming energy micro-transaction. Then, the UAV broadcasts this new energy micro-transaction for verification. Besides, the smart devices act as lightweight nodes that can store the approval relationships of the energy micro-transactions (i.e., edges in sub-tangles).

The update of local sub-tangles needs to be interacted among the UAV clusters and the smart devices to synchronize the sub-tangles. In order to reduce the bandwidth and energy consumption, we select the UAV with sufficient resource in each cluster as *UAV cluster head* for coordinating the sub-tangles dissemination. The UAV cluster head disseminates the latest local sub-tangle to the smart devices and the other UAV clusters by utilizing gossip scheme. However, the gossip scheme can only maintain a relaxed consistency of the sub-tangles among the UAV clusters, which is less globally robust. The confirmation of the energy micro-transactions depends on their increasing cumulative weight, which is determined by a Markov-Chain Monte Carlo based tip selection algorithm [20]. Nevertheless, the confirmation delay of the energy micro-transactions is adversely affected by the uncertainty associated with the stochastic wireless transmission environment.

In order to improve the confirmation latency of energy micro-transactions, we define timeout for the energy micro-transactions which is a factor that the energy micro-transactions have not been confirmed by the aerial tangle within a time threshold τ_0. In this situation, the APs exploit consortium blockchain to cooperatively confirm the timeout energy micro-transactions by referring to a proof-based consensus protocol, so as to form a ground main chain.

3) Energy Token: A new digital cryptocurrency named energy token, which is similar to the token in IOTA [20], works as the digital asset for UAVs-assisted wireless power transfer. The energy token is stored and managed by the wallets associated with the nodes.

IV. Operation Process of the Aerial-Ground Chain

In this section, we model the interactions between the aerial tangle and the ground consortium blockchain to illustrate the more details about the key operations of the developed aerial-ground chain for UAVs- assisted wireless power transfer.

A. Initialization

The UAVs, the APs and the smart devices become legitimate entities after registration with a trusted authority. The legitimate entities receive their unique digital identity including public/privacy keys and the corresponding certificates for information encryption and decryption. In addition, the legitimate entities obtain their wallet addresses from the trusted authority for storing and managing the energy token. The elliptic curve digital signature algorithm and asymmetric cryptography are utilized to validate the authenticity of a transaction [21].

B. Energy Micro-Transactions Generation

When the batteries of the smart devices are at the low energy level, the local AP requests UAVs to provide wireless power transfer service for the target smart device clusters. To attribute

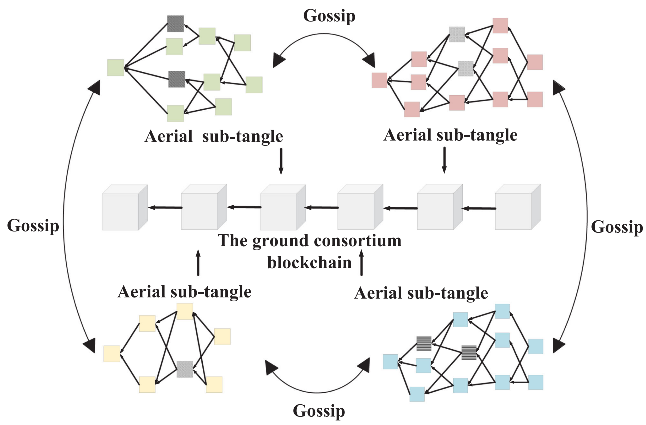


Fig. 2. Heterogeneous consensus of the aerial-ground chain.

credit to the smart devices, the UAVs generate energy micro-transactions that record identities of both the UAVs and the smart devices, timestamp, the amount of transferred energy and the rewards. Besides, the energy micro-transactions keeps the UAVs' data such as their onboard energy, current coordinate and path history, and also includes the opinion on the APs which is obtained according to their previous verification for the timeout energy micro-transactions.

C. Heterogeneous Consensus Process

In order to add the energy micro-transactions into the aerial-ground chain, the UAVs, the smart devices and the APs run a heterogeneous consensus process of a cumulative weight based consensus scheme in aerial tangle and a Delegated Proof-of-Stake (DPoS) based consensus scheme in ground consortium blockchain. The aerial tangle and the ground consortium blockchain work collaboratively to form a unified public ledger (i.e., aerial-ground chain). The operation details of the proposed heterogeneous consensus process is shown in Fig. 2.

1) Cumulative Weight Based Consensus Scheme in Aerial Tangle: Each energy micro-transaction has weight w, which is proportional to the amount of work that the issuing UAV invested into it. To ensure the reliability of the energy micro-transaction, the cumulative weight C_w is utilized to represent the authenticity of the energy micro-transaction, which is the sum of its own weight and the weights of all energy micro-transactions that directly or indirectly verify this energy micro-transaction, which is given by

$$C_w = w + \sum_{k=1}^{K} w(k), \tag{4}$$

where w is the energy micro-transaction's own weight, and $w(k)$ is the weight of the kth energy micro-transaction that directly or indirectly verifies this energy micro-transaction, $k \in \{1, \ldots, K\}$.

Unapproved energy micro-transactions in each sub-tangle is referred to as a tip. The process of a tip getting verified by new incoming energy micro-transactions is decided by Markov-Chain Monte Carlo based tip selection algorithm [20]. The probability that the tip is selected is modeled as

$$P_{xy} = \frac{\exp(\alpha(C_w(y) - C_w(x)))}{\sum_{z:z\to x} \exp(\alpha(C_w(z) - C_w(x)))}, \tag{5}$$

where P_{xy} denotes the transition probability that the walker walks towards the energy micro-transaction tip y, if energy micro-transaction tip y approves energy micro-transaction x, i.e., $y \to x$. $\alpha \in (0, 1)$ is a parameter to be chosen. z is the neighboring energy micro-transactions tips that approve x, and $y \in \{z : z \to x\}$. The cumulative weight of the energy micro-transaction gradually increases as the tips are validated by the new incoming energy micro-transactions. The higher cumulative weight of an energy micro-transaction represents higher probability that the micro-transaction will be accepted by the aerial tangle. Nonetheless, it is hard to find the range for the confirmation delay of an energy micro-transaction due to the dynamic and stochastic wireless transmission environment. The timeout energy micro-transactions which is shown in Fig. 2 as the shadowed energy micro-transactions.

2) DPoS Based Consensus Protocol in Ground Consortium Chain: In order to improve the confirmation latency of the timeout energy micro-transactions, we exploit consortium blockchain to develop a ground main chain. The local AP cooperatively verifies the integrity and correctness of the timeout energy micro-transactions, and processes the validated timeout energy micro-transactions into blocks. Then, a set $\mathcal{S}$ of APs are selected to act as verifiers and form a verification set. The local AP sends consensus requests to the verification set, which executes block verification and audit by using a proof-based consensus protocol. Due to the high efficiency and moderate cost, our previous works have applied DPoS consensus protocol in mobile charger assisted wireless power transfer networks [8] and device to device communication in 5G small cell networks [16]. Here, we utilize DPoS consensus protocol in our developed ground main chain for cooperatively verifying the *timeout energy micro-transactions*.

In each block verification sub-slot, the leader broadcasts the block to the verifiers for verification. Then, the verifiers reply the audit result with each other. Each verifier compares its audit result with those from other verifiers and sends a commit message to the leader. We denote the verification rate induced by the sth verifier is V_s^v, which can be expressed as

$$V_s^v = \frac{w_b}{\frac{C_b}{C_s} + \varphi w_b S}, \tag{6}$$

where w_b is the size of the unverified block, C_b is the required CPU cycles for verifying the block, C_s is the CPU cycles that the sth verifier is willing to contribute, φ is the average latency induced by each ground verifier in verification message broadcasting [16]. According to the Byzantine Fault Tolerance consensus condition, if the leader receives commit message from more than two third of the verifiers, the consensus of the current audited block is achieved [28]. Finally, the leader sends the audited block to the local AP and all the verifiers for appending the block to the ground main chain (i.e., the timeout energy micro-transactions are confirmed by the ground main-chain).

3) Interaction Between Aerial Tangle and Ground Main Chain: In our developed aerial-ground chain, the aerial tangle and the ground main chain interact with each other to collaboratively verify the energy micro-transactions. The aerial tangle first verify the energy micro-transactions through the coordination of the UAV cluster heads. Besides, the APs exploit consortium blockchain to verify the timeout energy micro-transactions, and append the verified timeout energy micro-transactions to the ground main chain. The APs act as the connector to combine the ground main chain with the aerial sub-tangles to form a unified public ledger.

D. Energy Token Payment

Once the energy micro-transactions are confirmed by the aerial-ground chain, the local AP pays UAVs reward to compensate for their on-broad energy consumption. In addition, the local AP also needs to pay the verifiers reward to compensate for their backhaul resource consumption (e.g., CPU cycles and bandwidth) in verifying the energy micro-transactions that have timed out. However, it is hard for the local AP to estimate the optimal reward to optimize its own payoffs while also paying sufficient to the UAVs and the ground verifiers. In particular, the available resources of both the UAVs and the ground verifiers vary with the time instances, and the local AP cannot obtain actual information about the resources that the UAVs and the verifiers are willing to contribute. Besides, rational UAVs and ground verifiers might not truthfully report their resources cost to cheat for higher reward, which will affect the benefit of the local AP. Thus, a proper incentive mechanism is essential for the local AP to determine the optimal reward for the UAVs to motivate them to contribute with wireless power transfer from their on-broad energy resources, and determine the optimal reward for the ground verifiers to incentivize them to contribute their backhaul resources in verifying the energy micro-transactions that have timed out.

V. Contract Theory Based Resource Cooperation Scheme for Wireless Power Transfer and Energy Micro-Transactions Verification

In this section, we propose a contract theory-based resource cooperation scheme for UAVs-assisted wireless power transfer and aerial-ground chain based timeout energy micro-transactions verification. Contract theory [29] is widely applied in economics in scenarios of information asymmetry to promote cooperation between two rational entities. Thus, we utilize contract theory in designing the best strategy for the local AP in employing UAVs to participate in wireless power transfer and in requesting the ground verifiers to verify the timeout energy micro-transactions.

In our designed contract theory based resource cooperation scheme, the local AP acts as employer, and a set $\mathcal{J}$ of UAVs and a set $\mathcal{S}$ of ground verifiers act as employees. The characteristics of the UAVs towards participating in wireless power transfer are different in terms of on-board energy, and the characteristics of the ground verifiers towards verifying the timeout energy micro-transactions are different in terms of CPU cycles and bandwidth. But due to their self interest, neither the UAVs nor the ground verifiers would provide information about their characteristics to the local AP. In the contract theory framework, J UAVs with different characteristics in wireless power transfer are classified into M types and are sorted in an ascending order: $\theta_1 < \cdots < \theta_m \cdots < \theta_M, m \in \{1, \ldots, M\}$. Meanwhile, S ground verifiers with different characteristics towards verifying the timeout energy micro-transactions are classified into N types and are sorted in an ascending order: $\phi_1 < \cdots < \phi_n \cdots < \phi_N$, $n \in \{1, \ldots, N\}$. The larger θ_m and ϕ_n imply that the UAVs and the ground verifiers are more eager to contribute their resources in wireless power transfer and in verifying the timeout energy micro-transactions, respectively.

Although the local AP cannot obtain the specific type of the UAVs and the ground verifiers, it can estimate the distribution probability λ_m with which a UAV belongs to type-m and the distribution probability λ_n with which a ground verifier belongs to type-n, via observations and statistics of the events of wireless power transfer and the energy micro-transactions verification in the aerial-ground chain [8]. By leveraging the estimated distribution probability λ_m and λ_n, the local AP designs contract item (T_m^c, R_m^c) for type-m UAV and designs contract item (V_n^v, R_n^v) for type-n ground verifier, where T_m^c is the required charging time for type-m UAV and R_m^c is the corresponding power transfer reward. V_n^v is the required verification rate for type-n ground verifier and R_n^v is the corresponding verification reward.

A. Utility of the Local AP

For the local AP that employs a type-m UAV for wireless power transfer, and requests a type-n ground verifier for verifying the timeout energy micro-transactions, proper utility functions can be respectively defined as

$$U_{AP}^C(m) = T_m^c - \rho_1 R_m^c, \tag{7a}$$

$$U_{AP}^V(n) = V_n^v - \rho_2 R_n^v, \tag{7b}$$

where T_m^c is the required charging time of the type-m UAV, and V_n^v is the required verification rate of the type-n ground verifier. R_m^c is the power transfer reward, and R_n^v is verification reward. ρ_1 and ρ_2 are the unit cost of the local AP for paying the power transfer reward R_m^c and the verification reward R_n^v, respectively.

As there are M types of UAVs with distribution probability λ_m, and N types of ground verifiers with distribution probability λ_n, the expected utility of the local AP is given by

$$U_{AP}^C = \sum_{m=1}^{M} \lambda_m J \left(T_m^c - \rho_1 R_m^c\right), \tag{8a}$$

$$U_{AP}^V = \sum_{n=1}^{N} \lambda_n S \left(V_n^v - \rho_2 R_n^v\right), \tag{8b}$$

B. Utility of the UAVs and the Ground Verifiers

The utility function of a type-m UAV employed based on a signed contract (T_m^c, R_m^c) during wireless power transfer is defined as

$$U_{UAV}^{C}(m) = \theta_m g_1\left(R_m^c\right) - c_1 T_m^c, \tag{9}$$

where $g_1(R_m^c)$ is the increasing and concave evaluation function of the power transfer reward R_m^c, c_1 is the unit energy cost on providing the required charging time. The utility of a type-m UAV is equal to the obtained power transfer reward minus the energy cost for wireless power transfer.

The utility function of a type-*n* ground verifier employed based on a signed contract (V_n^v, R_n^v) during verifying the timeout energy micro-transactions is defined as

$$U_{veri}^{V}(n) = \phi_n g_2\left(R_n^v\right) - c_2 V_n^v, \tag{10}$$

where $g_2(R_n^v)$ is the increasing and concave evaluation function of the verification reward R_n^v, c_2 is the unit cost of backhaul resources for providing the required verification rate. The utility of a type-*n* ground verifier is equal to the obtained verification reward minus the backhauling cost in verifying the timeout energy micro-transactions.

Given the utility functions in (9) and (10), the UAV and the ground verifier choose the contract that maximizes their own payoffs. Therefore, to ensure that the UAV and the ground verifier have a motivation to participate in the wireless power transfer and verifying timeout energy micro-transactions, the contract that the UAV and the ground verifiers select needs to satisfy the feasible conditions of *Individual Rationality (IR)* and *Incentive Compatibility (IC)* constraints [29]. In IR constraint, the UAV and the ground verifier need to select the contract that guarantees a non-negative utility for themselves (i.e., $U_{UAV}^{C}(m) \geq 0$ and $U_{Veri}^{V}(n) \geq 0$). In addition, according to the IC constraint, the UAV and the ground verifier prefer the contract that is designed for their own types rather than any other contracts, to obtain highest payoff. It is noted that both the IR and IC constraints are the basic conditions to incentivize the UAVs and the ground verifiers to participate in wireless power transfer and verifying timeout energy micro-transactions. Thus, the types of the UAVs and the verifiers will be truthfully revealed after their contract selection.

C. Contract Theory Based Resource Cooperation Optimization Problem Formulation

In the proposed contract theory based resource cooperation for wireless power transfer and timeout energy micro-transactions verification, our main goal is to maximize the expected utility of the local AP while meeting the IR and IC constraints for UAVs and ground verifiers contract selection. The optimization problem can be formulated as

$$\begin{aligned}
\max_{(T_m^c, R_m^c, V_n^v, R_n^v)} \quad & U_{AP} = U_{AP}^{C} + U_{AP}^{V} \\
\text{s.t.} \quad & C1: \theta_m g_1\left(R_m^c\right) - c_1 T_m^c \geq 0, \\
& C2: \phi_n g_2\left(R_n^v\right) - c_2 V_n^v \geq 0, \\
& C3: \theta_m g_1\left(R_m^c\right) - c_1 T_m^c \geq \theta_m g_1\left(R_{m'}^c\right) - c_1 T_{m'}^c, \\
& C4: \phi_n g_2\left(R_n^v\right) - c_2 V_n^v \geq \phi_n g_2\left(R_{n'}^v\right) - c_2 V_{n'}^v, \\
& C5: \sum_{n=1}^{N} \lambda_n S V_n^v \geq \frac{w_b}{\tau_0}, \\
& C6: \sum_{m=1}^{M} \lambda_m J R_m^c + \sum_{n=1}^{N} \lambda_n S R_n^v \leq R_{\max}^{AP}, \\
& \forall m, m' \in \{1, \ldots, M\}, m \neq m', \forall n, \\
& n' \in \{1, \ldots, N\}, n \neq n',
\end{aligned} \tag{11}$$

where *C*1 and *C*2 are the IR constraints for wireless power transfer and timeout energy micro-transactions verification, respectively. *C*3 and *C*4 are the IC constraints for wireless power transfer and timeout energy micro-transactions verification, respectively. *C*5 ensures that the average verification rate of the ground verifiers will not exceed the threshold of verification rate $\frac{w_b}{\tau_0}$. *C*6 ensures that the power transfer reward and the verification reward will not exceed the maximum reward of the local AP. Note that there are $M+N$ IR constraints and $M(M-1)+N(N-1)$ IC constraints, which are non-convex and indicate the coupling between the different types of UAVs and ground verifiers. Thus, it is difficult to solve the optimization problem in (11) directly.

D. Optimal Contract Solution

In this subsection, we will reduce the IR and the IC constraints in (11) to obtain a transformed optimization problem.

Definition 1: Monotonicity. For any feasible contract, $R_m^c \geq R_{m'}^c$ and $T_m^c \geq T_{m'}^c$ if and only if $\theta_m \geq \theta_{m'}, \forall m,\, m' \in \{1, \ldots, M\}, m \neq m'$. Meanwhile, $R_n^v \geq R_{n'}^v$ and $V_n^v \geq V_{n'}^v$ if and only if $\phi_n \geq \phi_{n'}, \forall n,\, n' \in \{1, \ldots, N\}, n \neq n'$.

Proof : The detailed proof of Definition 1 can be done similarly to Appendix A in [16]. □

Monotonicity implies that the UAV and the ground verifier with higher type should be paid a higher power transfer reward and verification reward, respectively. Meanwhile, the UAV and the ground verifier that obtain higher power transfer reward and verification reward should contribute more in wireless power transfer and verifying timeout energy micro-transactions, respectively. Next, we reduce the IR and the IC constraints, and have the following lemmas.

Lemma 1: IR Constraint Reduction. If IR constraints for type one UAV and type one ground verifier are satisfied, the IR constraints for other types of UAVs and ground verifiers will hold.

Proof: The detailed proof of Lemma 1 can be done similarly to Appendix B in [16]. □

Lemma 2: IC Constraint Reduction. We define the IC constraints between type-m and type-m' UAVs, and the IC constraints between type-n and type-n' ground verifiers, as downward incentive constraints (DIC), where $m \in \{2, \ldots, M\}$, $m' \in \{1, 2, \ldots, M-1\}$, $n \in \{2, \ldots, N\}$ and $n' \in \{1, 2, \ldots, N-1\}$. Moreover, we define the IC constraints between type-m and type-m'' UAVs, and the IC constraints between type-n and type-n'' ground verifiers, as upward incentive constraints (UIC), where $m'' \in \{m+1, \ldots, M\}$ and $n'' \in \{n+1, \ldots, N\}$. Both the DIC and the UIC for the UAVs and the ground verifiers can be respectively reduced as

$$\theta_m g_1\left(R_m^c\right) - c_1 T_m^c \geq \theta_m g_1\left(R_{m-1}^c\right) - c_1 T_{m-1}^c \quad \forall m \in \{2, \ldots, M\}, \tag{12}$$

$$\phi_n g_2\left(R_n^v\right) - c_2 V_n^v \geq \phi_n g_2\left(R_{n-1}^v\right) - c_2 V_{n-1}^v \quad \forall n \in \{2, \ldots, N\}, \tag{13}$$

Proof: The detailed proof of Lemma 2 can be done similar to Appendix C in [16]. □

Based on the Monotonicity and the Lemmas, the optimization problem in (11) can be transformed into a new optimization problem

$$\begin{aligned}
\max_{(T_m^c, R_m^c, V_n^v, R_n^v)} \; & U_{AP} = U_{AP}^C + U_{AP}^V \\
\text{s.t.} \; & C1: \theta_1 g_1\left(R_1^c\right) - c_1 T_1^c = 0, \\
& C2: \phi_1 g_2\left(R_1^v\right) - c_2 T_1^v = 0, \\
& C3: \theta_m g_1\left(R_m^c\right) - c_1 T_m^c = \theta_m g_1\left(R_{m-1}^c\right) \\
& \quad - c_1 T_{m-1}^c, \\
& C4: \phi_n g_2\left(R_n^v\right) - c_2 V_n^v = \phi_n g_2\left(R_{n-1}^v\right) \\
& \quad - c_2 V_{n-1}^v, \\
& C5: \sum_{n=1}^{N} \lambda_n S V_n^v \geq \frac{w_b}{\tau_0}, \\
& C6: \sum_{m=1}^{M} \lambda_m J R_m^c + \sum_{n=1}^{N} \lambda_n S R_n^v \leq R_{\max}^{AP}, \\
& C7: R_m^c \geq R_{m-1}^c \geq \cdots \geq R_1^c, \\
& C8: R_n^v \geq R_{n-1}^v \geq \cdots \geq R_1^v, \\
& \forall m \in \{1, \ldots, M\}, \forall n \in \{1, \ldots, N\},
\end{aligned} \tag{14}$$

where $C1$ and $C2$ are the reduced IR constraints for wireless power transfer and timeout energy micro-transactions verification, respectively. $C3$ and $C4$ are the reduced IC constraints for wireless power transfer and timeout energy micro-transactions verification, respectively. $C7$ and $C8$ are the monotonicity constraints. We now solve the transformed optimization problem in (14) to obtain the optimal contract items (T_m^{c*}, R_m^{c*}) and (V_n^{v*}, R_n^{v*}).

Based on constraints $C1-C4$, we can derive the charging time T_m^c and the verification rate V_n^v as

$$T_m^c = \frac{\sum_{l=1}^{m} \Delta_l + \theta_1 g_1\left(R_1^c\right)}{c_1}, \tag{15}$$

xd

$$V_n^v = \frac{\sum_{q=1}^{n} \Delta_q + \phi_1 g_2\left(R_1^v\right)}{c_2}, \tag{16}$$

where $\Delta_1 = 0, \Delta_l = \theta_l g_1(R_l^c) - \theta_l g_1(R_{l-1}^c), \forall l \in \{1, \ldots, m\}$, $\forall m \in \{1, \ldots, M\}$, and $\Delta_q = \phi_q g_2(R_q^v) - \phi_q g_2(R_{q-1}^v), \forall q \in \{1, \ldots, n\}, \forall n \in \{1, \ldots, N\}$.

By substituting (15) and (16) into optimization problem (14), we can obtain a transformed optimization problem

$$\begin{aligned}
\max_{(R_m^c, R_n^v)} U_{AP} = & \sum_{m=1}^{M-1} \left\{ \frac{J}{c_1} g_1\left(R_m^c\right) \zeta - \lambda_m J \rho_1 R_m^c \right\} \\
& + \frac{J}{c_1} \lambda_M \theta_M g_1\left(R_M^c\right) - \lambda_M J \rho_1 R_M^c \\
& + \sum_{n=1}^{N-1} \left\{ \frac{S}{c_2} g_2\left(R_n^v\right) \kappa - \lambda_n S \rho_2 R_n^v \right\} \\
& + \frac{S}{c_2} \lambda_N \phi_N g_2\left(R_N^v\right) - \lambda_N S \rho_2 R_N^v \\
\text{s.t.} \; & C5: \sum_{n=1}^{N} \lambda_n S V_n^v\left(R_n^v\right) \geq \frac{w_b}{\tau_0}, \\
& C6: \sum_{m=1}^{M} \lambda_m J R_m^c + \sum_{n=1}^{N} \lambda_n S R_n^v \leq R_{\max}^{AP}, \\
& C7: R_m^c \geq R_{m-1}^c \geq \cdots \geq R_1^c, \\
& C8: R_n^v \geq R_{n-1}^v \geq \cdots \geq R_1^v, \\
& \forall m \in \{1, \ldots, M\}, \forall n \in \{1, \ldots, N\},
\end{aligned} \tag{17}$$

where $\zeta = \theta_m \sum_{l=m}^{M-1} \lambda_l - \theta_{m+1} \sum_{l=m+1}^{M-1} \lambda_l, \kappa = \phi_n \sum_{q=n}^{N-1} \lambda_q - \phi_{n+1} \sum_{q=n+1}^{N-1} \lambda_q$, and $V_n^v(R_n^v)$ is given by (16). Since optimization problem (17) is convex, we can find the optimal R_m^{c*} and R_n^{v*} by applying KKT conditions. The Lagrangian dual function associated with problem (17) is given by

$$\begin{aligned}
& L\left(\{R_m^c\}, \{R_n^v\}, \alpha, \beta, \{\delta_m\}, \{\gamma_n\}\right) \\
& = U_{AP}\left(\{R_m^c\}, \{R_n^v\}\right) - \alpha \left(\frac{w_b}{\tau_0} - \sum_{n=1}^{N} \lambda_n S V_n^v\left(R_n^v\right) \right) \\
& + \beta \left(R_{\max}^{AP} - \sum_{m=1}^{M} \lambda_m J R_m^c - \sum_{n=1}^{N} \lambda_n S R_n^v \right) + \delta_1 R_1^c \\
& + \sum_{m=2}^{M} \delta_m \left(R_m^c - R_{m-1}^c\right) + \gamma_1 R_1^v + \sum_{n=2}^{N} \gamma_n \left(R_n^v - R_{n-1}^v\right),
\end{aligned} \tag{18}$$

where α and β are the Lagrange multipliers corresponding to constraints $C5$ and $C6$, respectively. $\{\delta_m, m \in \{1, ...M\}\}$ and $\{\gamma_n, n \in \{1, ...N\}\}$ are Lagrange multiplier vectors corresponding to constraints $C7$ and $C8$, respectively. KKT conditions can be given by

- Primary constraints: $R_1^{c*} \geq 0$, $R_1^{v*} \geq 0$, $R_m^{c*} \geq R_{m-1}^{c*}$ and $R_n^{v*} \geq R_{n-1}^{v*}, \forall m \in \{2, \ldots, M\}, \forall n \in \{2, \ldots, N\}$;
- Dual constraints: $\alpha^* \geq 0, \beta^* \geq 0, \delta_m^* \geq 0$, and $\gamma_n^* \geq 0$, $\forall m \in \{2, \ldots, M\}, \forall n \in \{2, \ldots, N\}$ and;
- Complementary slackness:

$$\alpha^* \left(\frac{w_b}{\tau_0} - \sum_{n=1}^{N} \lambda_n S V_n^v\left(R_n^{v*}\right) \right) = 0, \tag{19a}$$

$$\beta^* \left(R_{\max}^{AP} - \sum_{m=1}^{M} \lambda_m J R_m^{c*} - \sum_{n=1}^{N} \lambda_n S R_n^{v*} \right) = 0, \tag{19b}$$

$$\sum_{m=2}^{M} \delta_m^* \left(R_m^{c*} - R_{m-1}^{c*}\right) = 0, \tag{19c}$$

$$\sum_{n=2}^{N} \gamma_n^* \left(R_n^{v*} - R_{n-1}^{v*}\right) = 0, \tag{19d}$$

$$\begin{aligned} &\gamma_1^* R_1^{c*} = 0, \qquad \delta_1^* R_1^{v*} = 0, \\ &\forall m \in \{2, \ldots, M\}, \forall n \in \{2, \ldots, N\}, \end{aligned} \tag{19e}$$

- The first-order conditions of the Lagrange is deduced as

$$\begin{cases} \frac{\partial L}{R_m^c} = \frac{\partial U_{AP}(\{R_m^c\},\{R_n^v\})}{\partial R_m^c} - \beta\lambda_m J + \delta_m - \delta_{m+1} = 0, \\ \frac{\partial L}{R_M^c} = \frac{\partial U_{AP}\left(\{R_M^c\},\{R_N^v\}\right)}{\partial R_M^c} - \beta\lambda_M J + \delta_M = 0, \\ \frac{\partial L}{R_n^v} = \frac{\partial U_{AP}(\{R_m^c\},\{R_n^v\})}{\partial R_n^v} + \alpha\lambda_n S \frac{\partial V_n^v(R_n^v)}{R_n^v} - \\ \beta\lambda_n S + \gamma_n - \gamma_{n+1} = 0, \\ \frac{\partial L}{R_N^v} = \frac{\partial U_{AP}\left(\{R_M^c\},\{R_N^v\}\right)}{\partial R_N^v} + \alpha\lambda_N S \frac{\partial V_N^v\left(R_N^v\right)}{R_N^v} - \\ \beta\lambda_N S + \gamma_N = 0. \end{cases} \tag{20}$$

We can derive the optimal power transfer reward R_m^{c*} and the verification reward R_n^{v*} as follows

$$\begin{cases} R_m^{c*} = \frac{J\zeta}{c_1 \ln 2(\lambda_m J\rho_1 + \beta\lambda_m J - \delta_m + \delta_{m+1})}, \\ R_M^{c*} = \frac{J\lambda_M \theta_M}{c_1 \ln 2(\lambda_M J\rho_1 + \beta\lambda_M J - \delta_M)}, \\ R_n^{v*} = \frac{S\kappa + \alpha\lambda_n S\phi_n}{c_2 \ln 2(\lambda_n S\rho_2 + \beta\lambda_n S - \gamma_n + \gamma_{n+1})}, \\ R_N^{v*} = \frac{S\lambda_N \phi_N + c_2 \alpha\lambda_N S\phi_N}{c_2 \ln 2(\beta\lambda_N S - \gamma_N + \lambda_N S\rho_2)}. \end{cases} \tag{21}$$

After obtaining the optimal contract items (T_m^{c*}, R_m^{c*}) and (V_n^{v*}, R_n^{v*}), the local AP broadcasts the optimal contract to the UAVs and the ground verifiers, respectively. Each UAV evaluates whether its current on-broad energy can meet the wireless power transfer requirement, in the form of its utility according to (9). Besides, each ground verifier also evaluates its utility according to (10). Then, the UAV and the ground verifier feedback to the local AP to indicate whether they are willing to participate in wireless power transfer and verifying the timeout energy micro-transactions. After getting the feedback, the AP signs the contract with the wiling UAVs and the ground verifiers that accept the contract. Then, the UAVs move to the target charging location and transfer energy to the smart devices, and the ground verifiers participate in verifying the timeout energy micro-transactions. If the UAVs provide the required energy and the ground verifiers verify the timeout energy micro-transaction on time, the local AP rewards the UAVs and the ground verifiers according to the contract. The implementation process of contract theory based resource cooperation scheme for UAVs-assisted wireless power transfer and timeout energy micro-transactions verification can be illustrated in Algorithm 1.

Algorithm 1: Implementation Process of Contract Theory Based Resource Cooperation Scheme.

```
Input: θm, φn, λm, λn, c1, c2, ρ1 and ρ2;
Output: (Tm^c*, Rm^c*) and (Vn^v*, Rn^v*);
Solve problem (17) to obtain optimal contract items;
Local AP broadcasts the contract;
for each UAV do
    Judges whether its on-broad energy can meet the
    wireless power transfer requirement in the contract,
    in the form of its utility according to (9);
    if the UAV is willing to participate in wireless power
    transfer then
        It accepts the contract and prepares for flying to
        the target charging location to provide energy;
    end
    else
        It flies back to the docking station and prepares
        for the next period of wireless power transfer;
    end
end
for each ground verifier do
    Evaluates its utility according to (10);
    if the ground verifier is willing to participate in
    timeout energy micro-transaction verification then
        It accepts the contract and participates in DPoS
        based timeout energy micro-transaction
        verification;
    end
end
if The UAVs provide the required energy and the ground
verifiers verify the timeout energy micro-transaction on
time then
    The local AP rewards the UAVs and the ground
    verifiers according to the contract.
end
```

VI. Security Analysis and Numerical Results

A. Security Analysis

- *Get rid of single point of failure:* In the developed aerial-ground chain, the energy micro-transactions are audited and verified by the UAVs, the smart devices and the APs, which is unlike conventional intermediary dependent management of energy micro-transactions. Thus, the aerial-ground chain is robust in getting rid of single point of failure.
- *Energy non-repudiation of reception:* Once the energy micro-transactions are appended to the aerial-ground chain, the validated energy micro-transactions can be traced and retrieved by the users to defend against energy repudiation of reception.
- *Data unforgeability:* The decentralization characteristic of the developed aerial-ground chain with digitally signed energy micro-transactions guarantees that no adversary can pose as nodes to corrupt the aerial-ground chain, since the adversary cannot forge a digital signature of any legitimate node. Besides, the adversary cannot forge the audited and stored data in the aerial-ground chain which has been encrypted with keys of the nodes.
- *No double-spending:* Energy token depends on digital signature of the nodes to indicate ownership, and utilizes

TABLE I
PARAMETERS

Parameter	Value
Transmit power P_c of each UAV	10W
Propulsion power P_p of each UAV	1000W
Hovering power P_h of each UAV	10W
Channel power gain β_0	-30dB
Altitude H of each UAV	5m
Average flying speed V of each UAV	10m/s
The number of smart devices in the cluster	20
Energy conversion efficiency η	0.8
The number of UAVs	30
The number of ground verifiers	21
The size of block w_b	50KB
The threshold of verification time τ_0	0.5s
The threshold of verification rate $\frac{w_b}{\tau_0}$	100KB/s
The maximum reward $R_{\max}^{AP}$	500
The unit cost ρ_1 of local AP	0.2
The unit cost ρ_2 of local AP	0.2
The unit energy cost c_1 of UAV	0.3
The unit backhauling cost c_2 of verifier	0.2

the public ledger of aerial-ground chain to defend against double spending, in which the energy micro-transactions are agreed by using heterogeneous consensus.

B. Numerical Results

We evaluate the performance of our proposed contract theory based resource cooperation optimization for wireless power transfer and timeout energy micro-transactions verification. We consider UAVs-assisted wireless power transfer in IoT scenario consisting of 50 monitoring areas and each monitoring area is managed by an AP. The local AP covers 30 spatially-disjoint smart device clusters. The size of each cluster is 2m $\times$ 2m. The main simulation parameters are listed in Table I, where the UAVs-assisted wireless power transfer parameters are set according to [7] and the aerial-ground chain based verification parameters are set based on Tangle [20] and EoS [28]. We compare our proposed contract theory based resource cooperation scheme (RC-CA) with two other schemes: (i) contract theory based resource cooperation with complete information (RC-CC), in which the local AP knows the type of UAVs and the type of the ground verifiers; (ii) contract theory based resource cooperation with uniform contract (RC-UC), i.e., the local AP designs uniform contract based on a type-θ_{th} UAV and a type-ϕ_{th} ground verifier, respectively. The UAVs and the ground verifiers with types higher than θ_{th} and ϕ_{th} will accept the contract; otherwise, the UAVs and the ground verifiers will not choose the contract.

1) IR and IC Conditions Evaluation: Fig. 3 and Fig. 4 show the utilities of type-5, type-10, type-15 and type-20 UAVs, and the utilities of type-6, type-10, type-16 and type-20 ground verifiers, respectively. It is observed that each UAV and ground verifier can maximize their utilities if and only if they select the contract dedicated for their own types, which agrees with the IC condition. In addition, both the UAVs and the ground verifiers will not choose the contract that makes their utilities negative, which is consistent with the IR condition. It is also seen that the utilities of the UAVs and the ground verifiers increase with the increasing types of UAV and ground verifier, respectively. Therefore, the types of UAV and ground verifier will be truthfully revealed after the contract selection, which validates that our designed contract theory based resource cooperation optimization can overcome the information asymmetry between the local AP and the UAVs, and between the local AP and the ground verifiers.

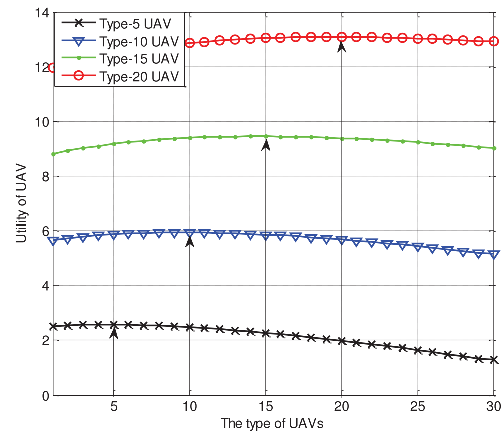


Fig. 3. Utility of UAV versus the type of UAVs.

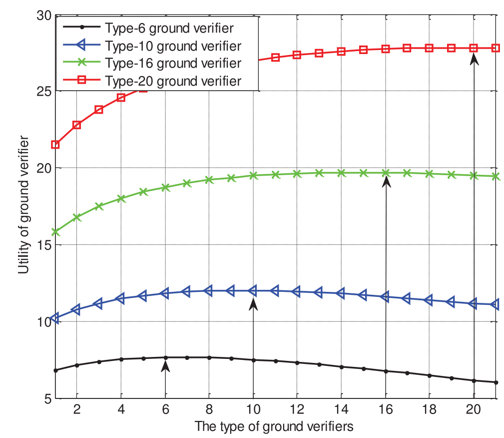
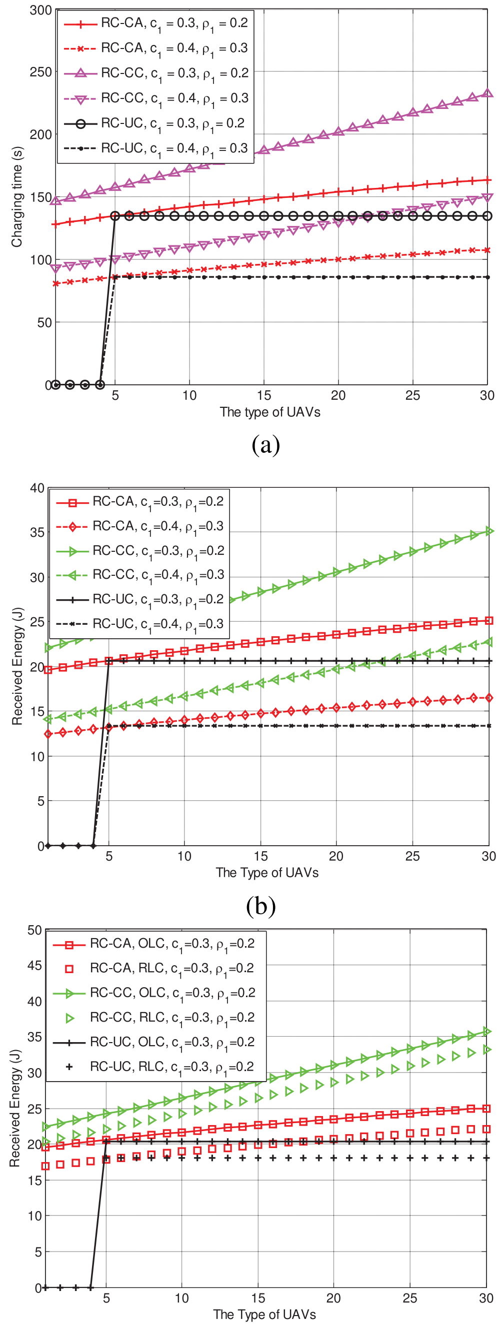


Fig. 4. Utility of ground verifier versus the type of verifiers.

2) Performance wrt Type of UAVs and Ground Verifiers: In this subsection, we illustrate the performance in terms of charging time of the UAVs, received energy by the local AP and the verification rate of the ground verifiers with respect to the type of UAVs and ground verifiers.

Charging Time: Fig. 5(a) shows the charging time of the UAVs versus the type of UAVs under different unit energy cost c_1 and unit cost ρ_1. Numerical results show that the charging time of the UAVs achieved by the RC-CC and our RC-CA schemes increases with the increasing type of UAVs, which proves that the UAVs with larger type are willing to contribute more in the wireless power transfer. Moreover, the charging time of the UAVs achieved by the RC-CC scheme is the longest, since the



(c)

Fig. 5. Performance of UAVs-assisted wireless power transfer versus the type of UAVs. (a) Charging time of the UAVs. (b) Received sum energy in each smart device cluster. (c) Received sum energy under different charging locations.

local AP knows the type of UAVs and it can design the contract to maximize its own utility while making the payoff for any UAV zero. In the RC-UC scheme, we set the type-θ_{th} is 5. We can see that the UAVs with type lower than θ_{th} reject the contract, which is indicated by zero charging time, while the UAVs with type higher than θ_{th} accept the contract, and thus have constant charging time.

Furthermore, it can be seen that the charging time of the UAVs achieved in the three schemes decreases with the increasing unit energy cost c_1 and unit cost ρ_1. The reason is that with the increasing unit energy cost c_1, the local AP needs to pay more power transfer reward to compensate for the energy consumption of UAVs in wireless power transfer. Meanwhile, the increase in the unit cost ρ_1 makes the local AP pay insufficient power transfer reward, and results in decreasing charging time of the UAVs.

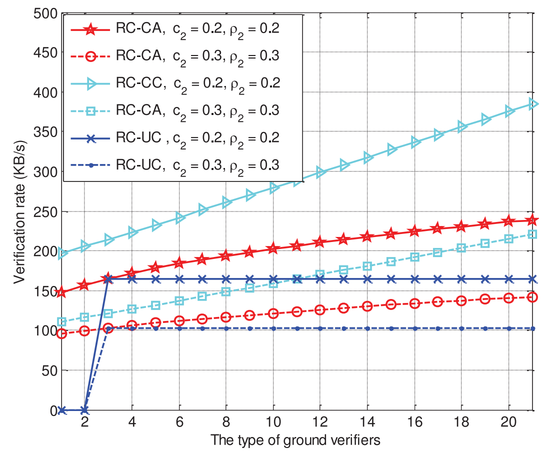


Fig. 6. Verification rate versus the type of ground verifiers.

Received Energy: Fig. 5(b) shows the received sum energy in each smart device cluster versus the type of UAVs under different unit energy cost c_1 and unit cost ρ_1. Numerical results show that the received energy achieved by the RC-CC and our RC-CA schemes increases with the increasing type of UAVs. The reason is that increasing the type of UAVs can increase the charging time of the UAVs, which corresponds to the increase in the received sum energy in each smart device cluster according to Eq. (3). It can be seen that the received energy achieved by the RC-CC scheme is the highest due to its longest charging time which has been proved in Fig. 5(a). Besides, increasing the unit energy cost c_1 and unit cost ρ_1 decreases the received energy in each smart device cluster.

Fig. 5(c) shows the received sum energy in each smart device cluster versus the type of UAVs under optimal location charging (OLC) method and random location charging (RLC) method. Numerical results show that the received energy achieved by the three schemes under the optimal location charging is higher than the one under the random location charging. The reason is that most of the smart devices are far away from the random charging location, thus making power decay with increasing distance.

Verification Rate: Fig. 6 shows the verification rate of the ground verifiers versus the type of ground verifiers under different unit backhauling cost c_2 and unit cost ρ_2. Numerical results show that the verification rate of the ground verifiers achieved by the RC-CC and our RC-CA schemes increases with the increasing type of ground verifiers. It can be seen that the verification rate of the ground verifiers in the RC-CC scheme is higher than our RC-CA scheme, since the local AP has the complete information of the type of the ground verifiers in the RC-CC scheme. In the RC-UC scheme, we set the type-ϕ_{th} of the ground verifiers as 3. Thus, any ground verifiers whose

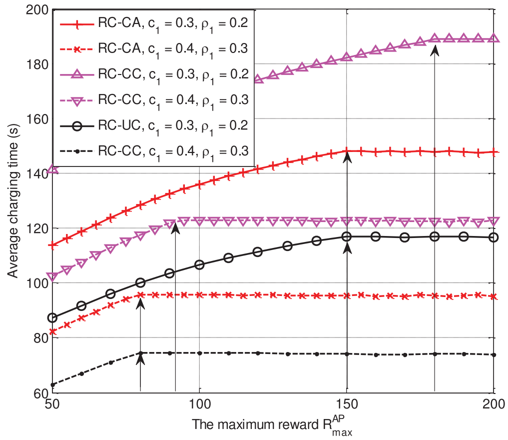


Fig. 7. Average charging time of UAVs-assisted wireless power transfer versus the maximum reward.

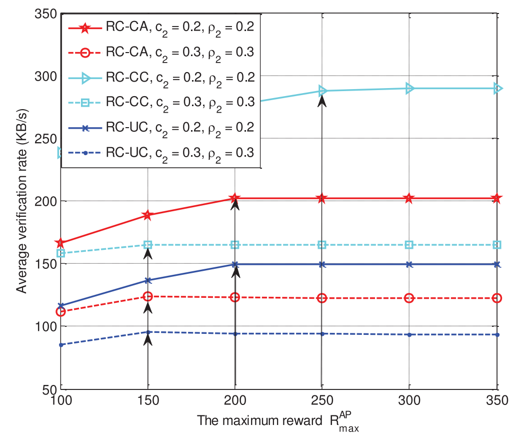


Fig. 8. Average verification rate versus maximum reward.

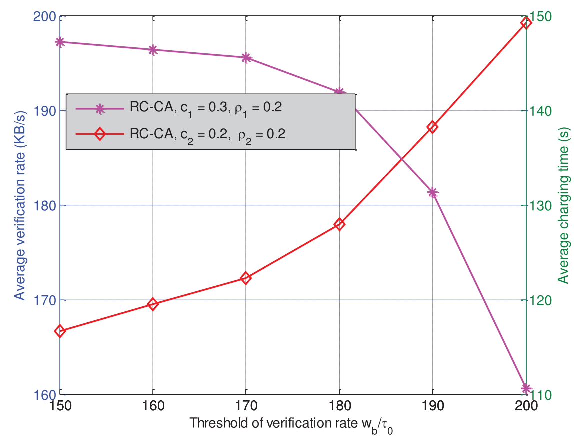


Fig. 9. Performance comparison of the average verification rate and the average charging time versus the threshold of verification rate.

type is lower than ϕ_{th}, does not choose the uniform contract, which makes the achieved verification rate zero. Only the ground verifiers whose types are higher than ϕ_{th} accept the uniform contract, and achieve the constant verification rate.

Besides, it can be observed that the verification rate achieved in the three scheme decreases with the increasing unit backhauling cost c_2 and unit cost ρ_2. With the increasing unit backhauling cost c_2, the local AP needs to pay a higher verification reward for the ground verifiers to compensate for their backhaul resource consumption in verifying timeout energy micro-transactions. However, increasing the unit cost ρ_2 of local AP leads insufficient verification reward for the ground verifiers, which in turn results in decrease in verification rate of the ground verifiers.

3) Performance wrt Maximum Reward of the Local AP: In this subsection, we illustrate the performance in terms of average charging time of the UAVs, average received energy by the smart devices clusters and the average verification rate of the ground verifiers versus the maximum reward $R^{AP}_{\max}$.

Average Charging Time: Fig. 7 shows the average charging time of the UAVs versus the maximum reward $R^{AP}_{\max}$. Numerical results show that the average charging time achieved by the three schemes increases with increasing $R^{AP}_{\max}$, and remains unchanged when $R^{AP}_{\max}$ increases up to a certain value. For example, when the $R^{AP}_{\max}$ increases to 150, the average charging time achieved by our RC-CA and the RC-UC schemes remains unchanged, and when the $R^{AP}_{\max}$ increases to 185, the average charging time of the RC-CC scheme remains unchanged. The reason is that the available charging time is constrained by the on-broad energy, the unit energy cost c_1 and the unit cost ρ_1. Once the available charging time achieves the maximum value, it will not change even if the local AP pays more power transfer reward. Moreover, increasing the unit energy cost c_1 and the unit cost ρ_1 decreases the average charging time of the UAVs.

Average Verification Rate: Fig. 8 shows the average verification rate of the ground verifiers versus the maximum reward $R^{AP}_{\max}$. It can be seen that the average verification rate achieved by the three schemes first increases with increasing $R^{V}_{\max}$, and keeps constant when $R^{V}_{\max}$ reaches a certain value. For instance, when the $R^{V}_{\max}$ increases to 200, the average verification rate achieved by our RC-CA and the RC-UC schemes remains unchanged, and when the $R^{V}_{\max}$ increases to 250, the average verification rate achieved by the RC-CC scheme remains constant. The reason is that the achieved verification rate is constrained by the backhaul resource of the ground verifiers, the unit backhauling cost c_2 and the unit cost ρ_2. Once the verification rate achieves the maximum value, it will not change even if the local AP increases the verification reward. Moreover, it can be observed that increasing the unit backhauling cost c_2 and the unit cost ρ_2 decreases the average verification rate of the ground verifiers.

4) Performance wrt the Threshold of Verification Rate: Fig. 9 shows the effect of the threshold of verification rate w_b/τ_0 on the average verification rate of the ground verifiers and the average charging time of the UAVs. It can be seen that as the threshold of verification rate increases, the average verification rate of the ground verifiers increases and the average charging time of the UAVs decreases. With the increasing threshold of verification rate, the local AP needs to pay more verification reward to motivate the ground verifiers to contribute with more backhaul resource in verifying timeout energy micro-transactions, to meet the increasing verification rate requirement. The power transfer reward paid to the UAVs decrease, which results in less average charging time.

VII. Conclusion

In this paper, we proposed a new distributed and secure UAVs-assisted wireless power transfer framework named aerial-ground chain, by exploiting blockchain of DAG and consortium blockchain. A heterogeneous consensus was developed for verifying the energy micro-transactions to form aerial sub-tangles and ground main chain. Besides, the interaction between the aerial sub-tangles and the ground main chain was modeled to illustrate the detailed operations of the proposed aerial-ground chain. Furthermore, we formulated a contract theory based resource cooperation scheme to motivate the UAVs to participate in wireless power transfer, and to incentivize the APs to contribute their resources in cooperatively verifying timeout energy micro-transactions. Security analysis proved that our developed aerial-ground chain is secure for the UAVs-assisted wireless power transfer. In addition, the numerical results indicated that our designed contract theory based resource cooperation scheme for wireless power transfer and timeout energy micro-transactions verification can improve the utility of local AP while ensuring the individual benefits of the UAVs and the ground verifiers under information asymmetry.

References

[1] B. Mao, Y. Kawamoto, and N. Kato, "AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7032–7042, Aug. 2020.
[2] K. Zhang, S. Leng, X. Peng, P. Li, S. Maharjan, and Y. Zhang, "Artificial intelligence inspired transmission scheduling in cognitive vehicular communications and networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1987–1997, Apr. 2019.
[3] T. Rodrigues, K. Suto, H. Nishiyama, J. Liu, and N. Kato, "Machine learning meets computation and communication control in evolving edge and cloud: Challenges and future perspective," *IEEE Commun. Surv. Tut.*, vol. 22, no. 1, pp. 38–67, Mar. 2020.
[4] T. Rodrigues, K. Suto, H. Nishiyama, N. Kato, and K. Temma, "Cloudlets activation scheme for scalable mobile edge computing with transmission power control and virtual machine migration," *IEEE Trans. Comput.*, vol. 67, no. 9, pp. 1287–1300, Sep. 2018.
[5] K. Zhang, Y. Zhu, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Deep learning empowered task offloading for mobile edge computing in urban informatics," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7635–7647, Oct. 2019.
[6] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surv. Tut.*, vol. 18, no. 4, pp. 2624–2661, Oct.–Dec. 2016.
[7] J. Xu, Y. Zeng, and R. Zhang, "UAV-enabled wireless power transfer: Trajectory design and energy optimization," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5092–5106, Aug. 2018.
[8] L. Jiang, S. Xie, S. Maharjan, and Y. Zhang, "Blockchain empowered wireless power transfer for green and secure Internet of Things," *IEEE Netw.*, vol. 33, no. 6, pp. 164–171, Dec. 2019.
[9] M. Conti, E. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tut.*, vol. 20, no. 4, pp. 3416–3452, May 2018.
[10] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for industrial Internet of Things," *IEEE Netw.*, vol. 33, no. 5, pp. 12–19, Sep./Oct. 2019.
[11] Y. Li *et al.*, "Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1643–1656, May 2020.
[12] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 1184–1195, Apr. 2018.
[13] V. Ortega, F. Bouchmal, and J. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.
[14] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, Jun. 2018.
[15] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Netw.*, vol. 33, no. 3, pp. 10–17, May 2019.
[16] L. Jiang, S. Xie, S. Maharjan, and Y. Zhang, "Joint transaction relaying and block verification optimization for blockchain empowered D2D communication," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 828–841, Oct. 2019.
[17] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-Based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operators perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.
[18] V. Hassijia, V. Chamola, D. Krishna, and M. Guizani, "A distributed framework for energy trading between UAVs and charging stations for critical applications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5391–5402, May 2020.
[19] A. Asheralieva and D. Niyato, "Distributed dynamic resource management and pricing in the IoT systems with blockchain-as-a-service and UAV-enabled mobile edge computing," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1974–1993, Mar. 2020.
[20] S. Popov, "The tangle," Version 1.4.3, Apr. 2018.
[21] N. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Oct. 2018.
[22] IOTA: A cryptocurrency for Internet-of-Things, 2020. [Online]. Available: http://www.iotatoken.com/
[23] WeCross, 2020. [Online]. Available: https://fintech.webank.com/en/
[24] G. Sagirlar, B. Carminati, E. Ferrari, J. Sheehan, and E. Ragnoli, "Hybrid-IoT: Hybrid blockchain architecture for Internet of Things - PoW sub-blockchains," in *Proc. IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, Jul. 2018, pp. 1007–1016.
[25] Polkadot, 2020. [Online]. Available: https://polkadot.network/
[26] Cosmos, 2020. [Online]. Available: https://cosmos.network/
[27] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020.
[28] EOS Block Producer Voting Guide, 2018. [Online]. Available: https://medium.com/coinmonks/eos-block-producer-voting-guide-fba3a5a6efe0
[29] P. Bolton and M. Dewatripont, *Contract Theory*," Cambridge, MA, USA: The MIT Press, 2004.

Li Jiang received the Ph.D. degree from the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, China, in 2017. She was also with the University of Oslo and Simula Metropolitan Center for Digital Engineering, Norway, as a Visiting Ph.D. Student from 2015 to 2016. She is currently a Lecturer with the School of Automation, Guangdong University of Technology, Guangzhou. Her current research interests include mobile blockchains, mobile edge computing, D2D communications, energy harvesting, and resource management for B5G and 6G networks.

Bin Chen is currently working toward the master's degree with the School of Automation, Guangdong University of Technology, Guangzhou, China. His current research interests include mobile blockchains, UAV networks, energy harvesting, and resource management for B5G and 6G networks.

Shengli Xie (Fellow, IEEE) received the Ph.D. degree in automatic control from the South China University of Technology (SCUT), in 1997. He was a Vice Dean with the School of Electronics and Information Engineering, SCUT, from 2006 to 2010. He is currently the Director of both the Institute of Intelligent Information Processing and Guangdong Key Laboratory of Information Technology for the Internet of Things, and also a Professor with the School of Automation, Guangdong University of Technology. He has authored or coauthored four monographs and more than 100 scientific papers published in journals and conference proceedings, and has been granted more than 30 patents. His research interests include broadly include statistical signal processing and wireless communications, with an emphasis on blind signal processing and the Internet of Things.

Sabita Maharjan (Senior Member, IEEE) received the Ph.D. degree in networks and distributed systems from the University of Oslo and Simula Research Laboratory, Norway, in 2013. She is currently an Associate Professor with the Department of Informatics, University of Oslo, Norway, and a Senior Research Scientist with Simula Metropolitan Center for Digital Engineering, Norway. She is currently the Vice Chair of the IEEE Communications Society Technical Committee on Green Communications and Computing (TCGCC) SIG on Green AI. She is an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL (IoT-J) and the IEEE OPEN COMPUTER SOCIETY JOURNAL. She was the Guest Editor for journals such as IEEE ACCESS, and in the technical program committee of top conferences like IEEE INFOCOM and IEEE IWQoS. Her current research interests include vehicular networks and 5G, network security, smart grid, Internet of Things, and computational intelligence.

Yan Zhang (Fellow, IEEE) received the B.S. degree from Beihang University, the M.S. degree from the Nanjing University of Post and Telecommunications, and the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. He is currently a Full Professor with the Department of Informatics, University of Oslo, Norway. His research interests include next-generation wireless networks leading to 5G beyond/6G, green and secure cyber-physical systems (e.g., smart grid and transport). Dr. Zhang is an Editor (or Area Editor, Senior Editor, Associate Editor) for several *IEEE transactions/magazine*, including *IEEE Communications Magazine*, *IEEE Network Magazine*, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, IEEE COMMUNICATIONS SURVEY AND TUTORIALS, IEEE INTERNET OF THINGS JOURNAL, IEEE SYSTEMS JOURNAL, *IEEE Vehicular Technology Magazine*, and IEEE BLOCKCHAIN TECHNICAL BRIEFS. He is a Symposium/Track Chair in a number of conferences, including IEEE ICC 2021, IEEE Globecom 2017, IEEE PIMRC 2016, IEEE SmartGridComm 2015. He is the Chair of IEEE Communications Society Technical Committee on Green Communications and Computing (TCGCC). He is an IEEE Vehicular Technology Society Distinguished Lecturer during 2016–2020. He is CCF Senior Member, an Elected Member of CCF Technical Committee of Blockchain, and 2019 CCF Distinguished Speaker. Since 2018, Dr. Zhang was the recipient of the global Highly Cited Researcher Award (Web of Science top 1% most cited worldwide). He is a Fellow of IET, Elected Member of Academia Europaea (MAE), and Elected Member of Norwegian Academy of Technological Sciences (NTVA).