Competitive Data Trading in Wireless-Powered Internet of Things (IoT) Crowdsensing Systems with Blockchain

Shaohan Feng*, Wenbo Wang*, Dusit Niyato*, Dong In Kim† and Ping Wang‡
*School of Computer Engineering, Nanyang Technological University, Singapore 639798
†School of Information and Communication Engineering, Sungkyunkwan University (SKKU), Suwon, Korea 16419
‡Department of Electrical Engineering & Computer Science, York University, Toronto, Canada ON M3J 1P3

***Abstract*—With the explosive growth of smart IoT devices at the edge of the Internet, embedding sensors on mobile devices for massive data collection and collective environment sensing has been envisioned as a cost-effective solution for IoT applications. However, existing IoT platforms and framework rely on dedicated middleware for (semi-) centralized task dispatching, data storage and incentive provision. Consequently, they are usually expensive to deploy, have limited adaptability to diverse requirements, and face a series of data security and privacy issues. In this paper, we employ permissionless blockchains to construct a purely decentralized platform for data storage and trading in a wireless-powered IoT crowdsensing system. In the system, IoT sensors use the power wirelessly transferred from RF-energy beacons for data sensing and transmission to an access point. The data is then forwarded to the blockchain for distributed ledger services, i.e., data/transaction verification, recording, and maintenance. Due to the coupled interference of wireless transmission and the transaction fee incurred by the blockchain's distributed ledger services, rational sensors have to decide on their transmission rates to maximize their individual payoff. Thus, we formulate a noncooperative game model to analyze this competitive situation among the sensors. We provide the analytical condition for the existence of the Nash equilibria as well as a series of insightful numerical results about the equilibrium strategies in the game.**

***Index Terms*—crowdsensing, blockchain, energy harvesting, concave games**

I. Introduction

At the dawn of 5G, the world has seen an enormous increase in the number of pervasively connected IoT devices, which are used in a plethora of scenarios such as vehicular networks, the logistics/manufacturing sectors, smart homes and e-health. With the trend of sensor miniaturization and the widespread adoption of IPv6, Cisco predicts that by 2021 an extraordinary amount of 847ZB data will be generated by IoT devices annually and about 7.2ZB will be finally stored worldwide [1]. Such technological development has created unprecedented opportunities of access to ubiquitous sensing data about the context in concern, e.g., smart city and urban environment, for both real-time use and big data-based analysis. However, it also imposes great challenges to network operation and data processing. Compared with the conventional Wireless Sensor Networks (WSNs), most of the IoT sensors are owned by users instead of operators. Meanwhile, the data generated by the same sensors may be consumed by different data services, which require various levels of data quality, timeliness and sampling frequency for different purposes. For this reason, conventional WSNs is limited in proliferation due to the cost of deployment and maintenance as well as the rigidness with task-specified data processing/dispatching structures.

To overcome the limitations of conventional WSNs in both network operation and data processing, a number of novel paradigms have been proposed at both the network side and the data processing side. In [2], a framework of wireless-powered sensing systems was proposed to address the issues of limited temporal-spatial coverage in urban crowdsensing over wearables. Therein, the mobile operator deploys ultra-dense charging stations using energy beamforming in small cells, which only require incremental upgrade of the protocols running on existing infrastructure. Such design enables the accommodation of the massive-scale, already-in-field IoT devices for Radio Frequency (RF)-powered pervasive sensing. Power transfer is used as incentiveness for IoT devices to execute tasks of crowdsensing applications. For involved parties, this framework helps to form the basis of an energy-data market at the data collection stage. At the operator side, data processing/aggregation is usually delegated to the cloud-based backend [3] or semi-centralized edge servers [4]. Under this paradigm, interconnections between the sensor cloud and the data processing backend rely on an intermediate layer provided by the operator for handling the tasks of data mediation, such as task association, data filtering, privacy preserving and data-integrity verification [3]. However, with the presence of such a middleware pre-designed and fully controlled by the operator, the IoT platforms and crowdsensing framework face the same problem of lacking adaptability and high installation cost as in WSNs. Also, the centralization of data processing, storage and trading inevitably causes the security risks such as data falsification and manipulation because of a single breach.

To overcome the flaws and vulnerability caused by centralization at the data processing stage, we resort to the emerging technology of permissionless blockchains [5]. Note that the functionalities of blockchains such as tamper-proof value transfer and smart contracts enables decentralized data-access control and transaction automation. Thus, a data trading platform based on permissionless blockchains is able to ensure that the task assignment, the data collection, storage and trading are all performed in a decentralized but trusted manner.

978-1-5386-7864-0/18/$31.00 ©2018 IEEE

Then, the centralized intermediate layer can be safely removed to enhance privacy and data security while the data integrity is still publicly verifiable. In brief, a permissionless blockchain system can be seen as a replicated database maintained by a number of pseudonymous nodes over peer-to-peer (P2P) connections. Blockchains use the public key infrastructure (PKI) mechanism and the data structure of hash linked list to ensure that the time order and the content of a data record (also known as a transaction) cannot be tampered without being noticed once it is confirmed on the chain [5]. The blockchain relies on Byzantine fault-tolerate mechanisms, e.g., Nakamoto protocol [6] or practical Byzantine Fault Tolerance (BFT) protocol [7], to coordinate the Byzantine agreement, i.e., peer consensus, about the state of the transaction storage among the consensus nodes. For permissionless blockchains, the messaging complexity for reaching the consensus among the P2P nodes are expected to be sufficiently low such that the size of the consensus network scales well.

In this paper, we propose a novel framework of an RF-powered IoT crowdsensing system. The IoT system under consideration involves three parties, i.e., the massive-scale IoT devices/sensors working as a sensing cloud, the wireless network operator, and the permissionless blockchain network as shown in Figure 1. The sensors operate by using wireless power transferred from RF-energy beacons. The power is consumed by the sensors for data sensing and for data transmission to the access point. The network operator provides wireless power transfer facility, i.e., RF-energy beacons, and data communication services, i.e., an access point, to the sensors. In exchange, the sensors are charged with a certain price for the transferred power by the network operator. The permissionless blockchain enables smart contracts in the form of programmable automata on the chain [8]. After the task schedulers (i.e., data consumers) deploy their own data trading contracts onto the blockchain, the sensors are able to autonomously choose a task to work for by responding to one of those smart contracts. By encapsulating the sensing data into transactions, the sensors send the data via virtual channels on the blockchain for ledger processing, e.g., data verification and ordering. The blockchain network adapts the scheme of Proof-of-Work (PoW) [6] for Sybil attack prevention [5]. As a result, the consensus nodes in the blockchain also charges a transaction fee for processing the data from sensors. After the data verification, the sensors trade the secured data on the blockchain with data consumers for revenue. Here, the data trading processes are completely self-organized with no middle layer controlled by the operator. From the perspective of the sensors and the data consumers, the blockchain can be regarded as a decentralized Platform as a Service (PaaS).

We investigate the self-organized data sensing process by focusing on the behaviors of data sensors. We consider that the sensors are rational and self-interested in maximizing their individual utility. The utility of a sensor can be defined as a function of the revenue from data trading, the payment made to the network operator and the transaction fee paid to the blockchain network. By choosing the data transmission rates,

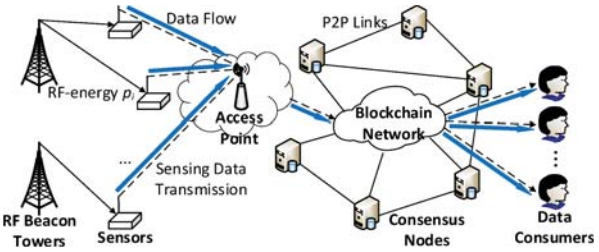

Figure 1: Schematics of the RF-powered IoT crowdsensing system.

the sensors are able to control the volume of traded data, and hence both the payment made to the blockchain and the operator and the revenue received from the task schedulers. However, when the sensors share the same wireless channel for data communication, this leads to a competitive situation due to co-channel interference. Also, we note that the transaction throughput at the blockchain side is a function of the sensors' transmission rates and depends on the consensus protocol adopted by the blockchain. Therefore, by considering the influence of the blockchain consensus protocol, we formulate the competition among sensors as a noncooperative game. Our analysis shows that by choosing the proper blockchain consensus protocol, the following key properties are guaranteed in the proposed IoT sensing system:

- The data, i.e., transaction, throughput of the blockchain scales well such that the massive data volume from the sensor cloud is handled smoothly.
- The rational and self-interested sensors noncooperatively decide on their own sensing/transferring data for individual utility optimization.
- The noncooperative sensors are able to reach a system equilibrium in a self-organized manner with limited coordination among themselves.

II. System Model

We consider an RF-powered IoT crowdsensing system as shown in Figure 1. Specifically, a cloud (i.e., set) of sensors denoted by $\mathcal{N}$ harvest energy from the beamforming-enabled RF-energy beacons to support data transfer from the sensors to the access point. Each sensor $i \in \mathcal{N}$ independently negotiates with the operator about the wirelessly received power level p_i within the range $\mathcal{D}_{p_i} = [0, p_i^{\mathrm{u}}]$. The data and payment transfer between the sensors and the data consumers is settled over virtual/logical (i.e., overlay peer-to-peer) links in the form of smart contracts in the blockchain network. The sensors upload their sensing data to the blockchain by sending them via the access points over a shared physical channel. Before investigating the behaviors of the decentralized sensors, we first describe the impact of the consensus protocol on the performance of the blockchain.

A. Scalable Consensus Protocol for Blockchains

The considered IoT sensing system requires that the data services, e.g., data storage, trading and task dispatching, are implemented on top of a permissionless blockchain. Namely,

the sensing data are encapsulated into blockchain transactions of fixed size, and the data trading process is performed in the form of smart contract execution. To enhance the storage efficiency, only the digest of each transaction is stored on the chain, and the content (i.e., payload data) of the transactions is stored off-chain by each consensus node. We note that as the number of transaction increases with the scale of the sensor cloud, it is necessary for the blockchain to provide scalable transaction throughput. However, since most of the popular Bitcoin-like blockchains rely on the Nakamoto protocol [6] for achieving probabilistic consensus, they are severely limited by their throughput bottleneck[1] [5].

To ensure that the blockchain's data processing capability matches the volume of data traffic from the sensor cloud, we adopt the scalable consensus protocol based on sharding [5] in the considered sensing system. Compared with the PoW-based Nakamoto protocol, which requires full data replication on each consensus node in the network, the sharding protocol dynamically partitions the consensus nodes into small groups of committees running BFT protocols. As a result, each committee only processes a subset (i.e., shard) of all the pending transactions, and the data replication is limited within each committee. Then, by increasing the number of the consensus nodes, the blockchain is able to form more BFT committees and process more transactions at the same time. In other words, sharding protocols parallelize data processing on the blockchain. Meanwhile, by allowing dynamical creation of shards out of the consensus nodes newly joining the blockchain network, the throughput constraint in Bitcoin-like blockchains can be completely lifted.

In this paper, we adopt the *ELASTICO* protocol from [9] to exemplify the approach of system analysis in the context of blockchains' sharding consensus. *ELASTICO* proceeds transactions in loosely-synchronized epochs, at the beginning of which the consensus nodes are required to provide solutions to their own PoW puzzles in order to join a BFT committee. More Specifically, *ELASTICO* is composed of two major stages, namely, the first stage of identity verification (i.e., PoW puzzle solution) for BFT committee formation and the second stage of BFT protocol execution for data processing. We assume that the consensus nodes are equipped with roughly the same computing power. Then, according to the analysis of *ELASTICO* [9], the transaction throughput increases almost linearly with the computational power admitted by the blockchain. Therefore, it is possible to scale the transaction throughput of the blockchain according to the total data transmission rate of the sensors, as long as the sensors are able to sustain the maintenance cost of the blockchain.

B. Sensor Interaction Model

After choosing the scalable consensus protocol for the blockchain, we are reedy to investigate the behaviors of the sensors in the decentralized IoT system. Let c_i be the fixed power level used by sensor i for circuit maintenance and data sensing. Then, the power used by sensor i to transmit data for storage and trading is $p_i - c_i$. We consider the path loss as a function of the distance d_i between sensor i and the access point connected to the blockchain. Let $\mathbf{r} = [r_i]^\top_{i\in\mathcal{N}}$ be the vector of the transmission rates, $\mathbf{p} = [p_i]^\top_{i\in\mathcal{N}}$ be the vector of received powers, i.e., the power transferred from the RF-energy beacons received by a sensor. Likewise, let $\mathbf{p}_{-i}$ be the vector of the received powers except sensor i. Then, the transmission rate of sensor i can be derived as follows $\forall i \in \mathcal{N}$:

$$r_i = R_i\left(p_i, \mathbf{p}_{-i}\right) = b_i \log_2\left(1 + \frac{g_i \frac{p_i - c_i}{(d_i)^{\alpha_i}}}{\sum\limits_{j\neq i} g_j \frac{p_j - c_j}{(d_j)^{\alpha_j}} + \sigma^2}\right), \quad (1)$$

where σ^2 is the variance of the additive white Gaussian noise, g_i is the channel gain of sensor i, and b_i is the corresponding bandwidth. We define $\mathbf{R}\left(\mathbf{p}\right) = \left[R_i\left(p_i, \mathbf{p}_{-i}\right)\right]^\top_{i\in\mathcal{N}}$, where $\mathbf{R}\left(\mathbf{p}\right): \mathcal{D}_{\mathbf{p}} = \times_{i\in\mathcal{N}} \mathcal{D}_{p_i} \mapsto \mathcal{D}_{\mathbf{r}}$ is a continuous closed mapping.

We consider that the maintenance cost of the blockchain is measured in the supplied computational power. Based on the linear relationship between the computational power and the transaction throughput in *ELASTICO*, we can further express the required computational power as $m\sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)$, where $m > 0$ is the computational power coefficient and $\sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)$ is the total data rate of the sensor cloud. Furthermore, it is well-known that the power consumption in modern computer architecture can be modeled as a quadratic function of the corresponding computational frequency [10]. Therefore, the power consumption of the sharded blockchain network can be derived as

$$p_{\mathrm{b}} = a\left[m\sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)\right]^2 + b\left[m\sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)\right] + c, \quad (2)$$

where a, b and c are the power consumption coefficients.

To enjoy the data service (e.g., smart contracts and transaction recording) provided by the sharded blockchain, sensor i needs to pay the transaction fee to compensate the cost of the consensus nodes incurred by energy consumption. We assume that the sensors proportionally share the blockchain maintenance cost among themselves according to the volume of data that they propose to the blockchain. Then, the rate of payment by sensor i depends on its fraction of the total transmit rate as follows:

$$C_i = \frac{R_i\left(p_i, \mathbf{p}_{-i}\right)}{\sum_{j\in\mathcal{N}} R_j(p_j, \mathbf{p}_{-j})}\left\{a\left[m\sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)\right]^2 + b\left[m\sum_{j\in\mathcal{N}} R_j(p_j, \mathbf{p}_{-j})\right] + c\right\}. \quad (3)$$

The revenue of a sensor is a function of the volume of its sensing data recorded by the blockchain. Let λ_i denote the price of unit bitrate of sensor i and ϕ denote the price of unit power transferred from the RF-energy beacons. To support the wirelessly received power level p_i for sensor i, the

[1]For example, the Bitcoin network supports a maximum throughput of 7 transactions per second.

wirelessly transferred power level of the RF-energy beacons i is $P^{\mathrm{t}}\left(p_i, d_i^{\mathrm{t}}\right) = p_i \left(d_i^{\mathrm{t}}\right)^{\eta}$ based on the Slivnyak-Mecke's theorem [11], where η is the path-loss exponent of wirelessly power transfer and d_i^{t} is the distance between the RF-energy beacons and sensor i. Based on (1)-(3), the utility of sensor i can be expressed as follows:

$$u_i\left(p_i, \mathbf{p}_{-i}\right) = \lambda_i R_i\left(p_i, \mathbf{p}_{-i}\right) - \phi P^{\mathrm{t}}\left(p_i, d_i^{\mathrm{t}}\right) - \frac{R_i\left(p_i, \mathbf{p}_{-i}\right)}{\sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)} \times \left\{ a\left[m \sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)\right]^2 + b\left[m \sum_{j\in\mathcal{N}} R_j\left(p_j, \mathbf{p}_{-j}\right)\right] + c \right\}. \tag{4}$$

In (4), a larger λ_i indicates a higher quality (hence a higher value) of the data generated by sensor i.

Each sensor aims to maximize its individual utility, i.e., $\max_{p_i\in\mathcal{D}_{p_i}} u_i\left(p_i, \mathbf{p}_{-i}\right)$, given the interference from other sensors. Therefore, the sensors' strategy are coupled, and a noncooperative game can be formulated as a four-tuple $\mathcal{G}_{\mathrm{s}} = \{\mathcal{N}, \mathbf{p}, \mathcal{D}_{\mathbf{p}}, \mathbf{u}\}$, where

- $\mathcal{N}$ is the set of active sensors, i.e., the players;
- $\mathcal{D}_{\mathbf{p}} \subset \mathbb{R}^{|\mathcal{N}|}$ is the domain of $\mathbf{p}$, i.e., strategy, and an $|\mathcal{N}|$-polyhedron;
- $\mathbf{p} \in \mathcal{D}_{\mathbf{p}}$ is the sensor-determined received power vector;
- $\mathbf{u} = [u_i]_{i\in\mathcal{N}}$ is the vector of sensors' utilities as a function of $\mathbf{p}$, where u_i is given by (4).

Based on the game formulation, we consider the Nash equilibrium to be the solution for the sensors.

III. Equilibrium Analysis

To ease the analysis of the Nash Equilibrium (NE) in game $\mathcal{G}_{\mathrm{s}}$, we consider that the sensors optimize their utilities by deciding on their transmission rates instead of on their power strategies $\mathbf{p}$. This is owning to the fact that the vector of the functions describing the relationship between $\mathbf{r}$ and $\mathbf{p}$, i.e., $\mathbf{r} = \mathbf{R}\left(\mathbf{p}\right)$, is a continuous, closed injective operator as shown in Theorem 1. Then, there exists an inverse operator of $\mathbf{R}\left(\mathbf{p}\right)$, denoted by $\mathbf{R}^{-1}\left(\mathbf{r}\right) : \mathcal{D}_{\mathbf{r}} \mapsto \mathcal{D}_{\mathbf{p}}$, such that the sensors' received power vector $\mathbf{p}$ is uniquely determined given their transmission rates $\mathbf{r}$.

Theorem 1. *There exists an inverse operator of* $\mathbf{R}\left(\mathbf{p}\right)$*, i.e.,* $\mathbf{R}^{-1}\left(\mathbf{r}\right) : \mathcal{D}_{\mathbf{r}} \mapsto \mathcal{D}_{\mathbf{p}}$*, such that* $\mathbf{p} = \mathbf{R}^{-1}\left(\mathbf{r}\right)$.

Proof. Let $\gamma_i\left(r_i\right) = e^{\frac{r_i \ln 2}{b_i}} - 1$, $\beta_i\left(p_i\right) = g_i \frac{p_i - c_i}{\left(d_i\right)^{\alpha_i}}$, and $\boldsymbol{\beta}\left(\boldsymbol{p}\right) = \left[\beta_i\left(p_i\right)\right]_{i\in\mathcal{N}}^{\top}$. According to (1), we have

$$\gamma_i\left(r_i\right) = \Lambda_i\left(\boldsymbol{\beta}\left(\boldsymbol{p}\right)\right) = \frac{\beta_i\left(p_i\right)}{\sum\limits_{j\neq i} \beta_j\left(p_j\right) + \sigma^2}. \tag{5}$$

Since $\forall i \in \mathcal{N}$ both $\gamma_i\left(r_i\right)$ and $\beta_i\left(p_i\right)$ are continuous, closed injective operators, the injective properties of $\mathbf{R}\left(\mathbf{p}\right)$ can be ensured iff $\boldsymbol{\Lambda}\left(\boldsymbol{\beta}\left(\boldsymbol{p}\right)\right) = \left[\Lambda_i\left(\boldsymbol{\beta}\left(\boldsymbol{p}\right)\right)\right]_{i\in\mathcal{N}}$ is injective.

We prove by contradiction that $\boldsymbol{\Lambda}\left(\boldsymbol{\beta}\left(\boldsymbol{p}\right)\right)$ is injective. Assume that $\boldsymbol{\Lambda}\left(\boldsymbol{\beta}\left(\boldsymbol{p}\right)\right)$ is not injective. Then, there exist $\mathbf{p}'$, $\mathbf{p} \in \mathcal{D}_{\mathbf{p}}$ and $\mathbf{p}' \neq \mathbf{p}$ such that $\mathbf{r}' = \mathbf{r}$. Without loss of generality, we assume $p_i' > p_i$. To ensure $r_i' = r_i$, $\mathbf{p}'$ should satisfy

$$\frac{\beta_i\left(p_i'\right)}{\sum\limits_{j\neq i} \beta_j\left(p_j'\right) + \sigma^2} = \frac{\beta_i\left(p_i\right)}{\sum\limits_{j\neq i} \beta_j\left(p_j\right) + \sigma^2}, \tag{6}$$

and hence

$$\sum_{j\neq i} \beta_j\left(p'_j\right) = \frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} \sum_{j\neq i} \beta_j\left(p_j\right) + \left[\frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} - 1\right] \sigma^2. \tag{7}$$

By (7), for $\forall l \in \mathcal{N}$, we have the following equality:

$$\begin{aligned} \frac{\beta_l\left(p'_l\right)}{\sum\limits_{j\neq l} \beta_j\left(p'_j\right) + \sigma^2} &= \frac{\beta_l\left(p'_l\right)}{\beta_i\left(p'_i\right) + \sum\limits_{j\neq i} \beta_j\left(p'_j\right) - \beta_l\left(p'_l\right) + \sigma^2} \\ &\overset{(7)}{=} \frac{\beta_l\left(p'_l\right)}{\beta_i\left(p'_i\right) + \frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} \sum\limits_{j\neq i} \beta_j\left(p_j\right) + \left[\frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} - 1\right] \sigma^2 - \beta_l\left(p'_l\right) + \sigma^2} \\ &= \frac{\beta_l\left(p'_l\right)}{\frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} \left[\sum\limits_{j\in\mathcal{N}} \beta_j\left(p_j\right) + \sigma^2\right] - \beta_l\left(p'_l\right)}. \end{aligned} \tag{8}$$

With $\mathbf{r}' = \mathbf{r}$, we have $r_l' = r_l$, $\forall l \in \mathcal{N}$. Then, according to (8), we have the following equality condition:

$$\begin{aligned} &\frac{\beta_l\left(p_l\right)}{\sum\limits_{j\neq l} \beta_j\left(p_j\right) + \sigma^2} \\ &= \frac{\beta_l\left(p'_l\right)}{\sum\limits_{j\neq l} \beta_j\left(p'_j\right) + \sigma^2} = \frac{\beta_l\left(p'_l\right)}{\frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} \left[\sum\limits_{j\in\mathcal{N}} \beta_j\left(p_j\right) + \sigma^2\right] - \beta_l\left(p'_l\right)} \\ &\Leftrightarrow \beta_l\left(p'_l\right) = \frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} \beta_l\left(p_l\right). \end{aligned} \tag{9}$$

Summing $\beta_l\left(p'_l\right)$ with respect to l over $\mathcal{N}$ leads to $\sum\limits_{l\in\mathcal{N}} \beta_l\left(p'_l\right) = \sum\limits_{l\in\mathcal{N}} \frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} \beta_l\left(p_l\right)$. This contradicts with the result derived from (7), i.e., $\beta_i\left(p'_i\right) + \sum\limits_{j\neq i} \beta_j\left(p'_j\right) = \sum\limits_{j\in\mathcal{N}} \beta_j\left(p'_j\right) = \frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} \sum\limits_{j\in\mathcal{N}} \beta_j\left(p_j\right) + \left[\frac{\beta_i\left(p'_i\right)}{\beta_i\left(p_i\right)} - 1\right] \sigma^2$. Therefore, the assumption that $\boldsymbol{\Lambda}\left(\boldsymbol{\beta}\left(\boldsymbol{p}\right)\right)$ is not injective cannot be true, and $\boldsymbol{\Lambda}\left(\boldsymbol{\beta}\left(\boldsymbol{p}\right)\right)$ is injective. With the injective property of $\gamma_i\left(r_i\right)$ and $\beta_i\left(p_i\right)$, $\forall i \in \mathcal{N}$, $\mathbf{R}\left(\mathbf{p}\right)$ is an injective operator. Since $\mathbf{R}\left(\mathbf{p}\right)$ is a continuous, closed operator, its inverse operator, i.e., $\mathbf{R}^{-1}\left(\mathbf{r}\right)$, exists and the proof is completed. □

By Theorem 1, the utility of sensor i in the form of (4) can be rewritten as in (10). It is now possible for each sensor to optimize the individual utility by deciding on its transmission rate instead of the received powers from the RF-energy beacons. Then, we can obtain the following condition for the existence of the NE in game $\mathcal{G}_{\mathrm{s}}$:

Theorem 2. *The NE to the noncooperative game* $\mathcal{G}_{\mathrm{s}}$ *exists if* $am^2 - c \geq 0$ *and* $\sum\limits_{j\in\mathcal{N}} r_j \geq 1$.

$$u_i\left(r_i, \mathbf{r}_{-i}\right) = \lambda_i r_i - \phi P^{\mathrm{t}}\left(R_i^{-1}\left(\mathbf{r}\right), d_i^{\mathrm{t}}\right) - \frac{r_i}{\sum\limits_{j\in\mathcal{N}} r_j}\left[a\left(m\sum_{j\in\mathcal{N}} r_j\right)^2 + b\left(m\sum_{j\in\mathcal{N}} r_j\right) + c\right]. \tag{10}$$

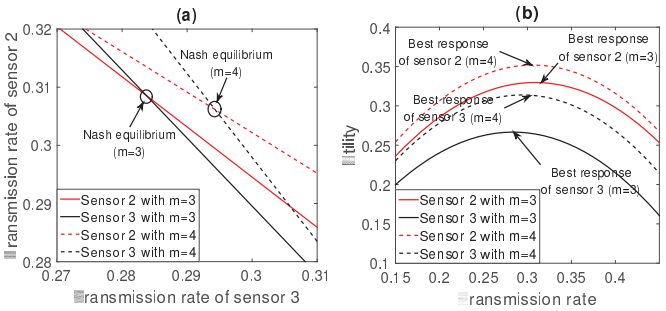

Figure 2: (a) The Nash equilibrium and (b) the best response.

Proof. By (10), $u_i\left(r_i, \mathbf{r}_{-i}\right)$ is continuous and differentiable on r_i, $\forall i \in \mathcal{N}$. Now, we examine the second derivatives of $u_i\left(r_i, \mathbf{r}_{-i}\right)$ with respect to r_i as shown in (11), $\forall i \in \mathcal{N}$:

$$\frac{\partial^2 u_i\left(r_i, \mathbf{r}_{-i}\right)}{\partial {r_i}^2} = -\phi\frac{\partial^2 P^{\mathrm{t}}\left(R_i^{-1}\left(\mathbf{r}\right), d_i^{\mathrm{t}}\right)}{\partial {r_i}^2} - 2am^2 + 2c\sum_{j\neq i} r_j \Bigg/ \left(\sum_{j\in\mathcal{N}} r_j\right)^3. \tag{11}$$

By Theorem 2, the sum of the last two terms in (11), i.e., $-2am^2 + 2c\sum\limits_{j\neq i} r_j \Big/ \left(\sum\limits_{j\in\mathcal{N}} r_j\right)^3$, is smaller than 0. Moreover, since $r_i = R_i\left(p_i, \mathbf{p}_{-i}\right)$ defined in (1) is concave with respect to p_i, its inverse operator, i.e., $p_i = R_i^{-1}\left(\mathbf{r}\right)$, is correspondingly convex with respect to r_i according to the injective property. Since $P^{\mathrm{t}}\left(R_i^{-1}\left(\mathbf{r}\right), d_i^{\mathrm{t}}\right)$ is a linear function of $R_i^{-1}\left(\mathbf{r}\right)$, $-\phi\frac{\partial^2 P^{\mathrm{t}}\left(R_i^{-1}\left(\mathbf{r}\right), d_i^{\mathrm{t}}\right)}{\partial {r_i}^2}$ is smaller than 0, and $\frac{\partial^2}{\partial {r_i}^2} u_i\left(r_i, \mathbf{r}_{-i}\right)$ is therefore smaller than 0. According to Theorem 1 in [12], the solution to the noncooperative game $\mathcal{G}_{\mathrm{s}}$ exists, and the proof is completed. □

It is well-known that following the concavity condition in Theorem 2, the continuous better-reply in the form of simultaneous gradient ascent admits an equilibrium point (see [12, Theorem 7]). Due to the space limit, we omit the presentation of the equilibrium searching algorithm and the discussion on the globally asymptotic stability of the equilibrium. Interested readers are referred to [12] for more details.

IV. Performance Evaluation

In this section, we present numerical studies to evaluate the performance of the IoT crowdsensing system. For ease of illustration, we consider 10 sensors, i.e, $|\mathcal{N}| = 10$, working as a sensing cloud. The bandwidth of a sensor is $b_i = 2$, $\forall i \in \mathcal{N}$, and the noise σ is 1. The vector of the distances between the sensors and the access point connected to the blockchain, i.e., $\mathbf{d} = [d_i]_{i\in\mathcal{N}}$, is set to be $[0.25, 0.2, 0.15, 0.25, 0.2, 0.15, 0.25, 0.2, 0.15, 0.25]$, and $\boldsymbol{\alpha} = [\alpha_i]_{i\in\mathcal{N}} = [3.5, 3, 2.5, 3.5, 3, 2.5, 3.5, 3, 2.5, 3.5]$. The channel gain $\mathbf{g} = [g_i]_{i\in\mathcal{N}}$ is set to be $[1.95, 2, 2.18, 1.95, 2, 2.18, 1.95, 2, 2.18, 1.95]$. The price of unit received power ϕ is set to be 0.01, and the circuit and sensing power vector for the sensors $\mathbf{c} = [c_i]_{i\in\mathcal{N}}$, is $[1, 2, 3, 1, 2, 3, 1, 2, 3, 1]$. The coefficients in the blockchain power consumption model are $a = 0.1$, $b = 0.1$, $c = 0.1$ and the computational power coefficient is $m = 3$. The distance between the sensors and RF-energy beacons $\mathbf{d}^{\mathrm{t}} = [d_i^{\mathrm{t}}]_{i\in\mathcal{N}}$ is $[1, 2, 3, 1, 2, 3, 1, 2, 3, 1] \times 10^{-3} + 1$ and $\eta = 2$. The price of unit bitrate of sensors is $\lambda_i = 20$, $\forall i \in \mathcal{N}$.

A. Numerical Result

Figures 2(a) and 2(b) show the NE and best responses, respectively. Figure 2(a) illustrates the NE of the transmission rates for sensors 2 and 3. The NE is the point at which the best responses for sensors 2 and 3 intersect. We observe that the transmission rate of sensor 3 increase as the computational power coefficient m increases. The reason is that when m increases, the computational power increases more quickly, resulting in high energy consumption of the blockchain. Consequently, the transaction fee rises sharply, and hence the less cost-effective transaction fees that sensor 3 will be charged. In this case, sensor 3 increase its transmission rate. In contrast, the transmission rate of sensor 2 decreases as the value of the computational power coefficient m increases. The reason is that the transmission rate of sensor 2 is higher than that of sensor 3, which means that the transaction fee of sensor 2 increases more rapidly than that of sensor 3. Accordingly, sensor 2 decreases its transmission rate.

We then evaluate the utilities of sensors 2 and 3. In Figure 2(b), the utility of sensor 2 changes because of the different transmission rates for transferring the data to the blockchain. From Figure 2(b), there is a point where the utility of sensor 2 is maximized, which is pointed by the arrowhead of "Best response". This point indicates the NE for sensor 2. As is evident from Figure 2(b), this utility, which is a function of the transmission rate, is unimodal, and the optimal solution can be obtained analytically.

We next investigate the sensors' states, i.e., the transmission rates, ratio of the total transaction fee, and utilities in Figures 3(a), 3(b), and 3(c), respectively. As shown in Figure 3, the transmission rates of sensors 1, 4, 7, and 10 are among the highest ones because of their shortest distance to the RF-energy beacons. Specifically for sensors 1 and 2, the gap between sensors 1 and 2 in the utility is even larger than that in the transmission rate, i.e., $\frac{u_1}{u_2} \approx \frac{0.35}{0.33} > \frac{r_1}{r_2} \approx \frac{0.31}{0.3}$. The reason is that each sensor needs to pay the transaction fee according

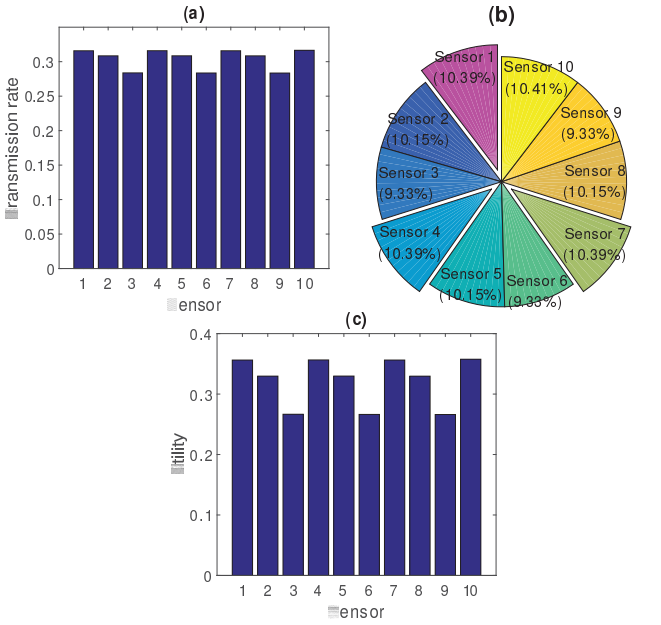

Figure 3: (a) Transmission rates, (b) ratio of transaction fee, and (c) utilities for each sensor.

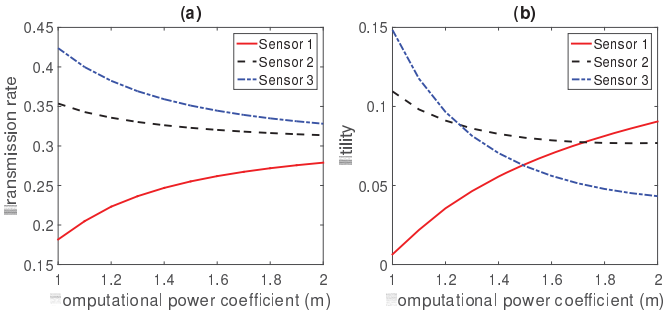

Figure 4: Transmission rates and utilities under varied m

to its fraction of the sum of all the sensors' transmission rates while the total transaction fee is increasing rapidly, i.e., as a convex function, with respect to the total transmission rates. This means that the less the sensor's fraction of the sum of all the sensors' transmission rates is, the less cost-effective transaction fee that it will be charged. This is consistent with the result shown in Figure 2.

Finally, we study the impact of the computational power coefficient m on the achievable transmission rates of each sensor at the equilibrium. In Figure 4(a), we observe that the transmission rate of sensor 1 increases as m increases. This is due to the fact that the transaction fee charged to sensor 1 will be less cost-effective as m increases if it operates with a small transmission rate. Then, sensor 1 tends to increase its transmission rate. In contrast, due to the large fraction of the sum of all the sensors' transmission rates, the transaction fees for sensors 2 and 3 will increase rapidly as m increases. In this case, both sensors 2 and 3 will decrease their transmission rates. Then, the utility of sensor 1 increases as m increases while those of sensors 2 and 3 decrease (see Figure 4(b)).

V. Conclusion

In this paper, we have presented a noncooperative-game model to analyze the transmission strategy in the self-organized wireless-powered IoT crowdsensing system built upon permissionless blockchains. We have focused on the interactions of the sensors and considered the impact of both the interference and the blockchain maintenance cost on the sensors' utilities. Analytically, we have established a joint model describing the impact of the sensors' transmission strategies on their transmission rate and the needed transaction fee on the blockchain side. We have studied the equilibrium strategies of the sensors in the wireless-powered IoT crowdsensing system by using best response. We have analytically examined the conditions for the solution, i.e., the Nash equilibrium, of the game to exist. Our future work will extend to the study in the impact of user-demands on the sensors' strategies.

VI. Acknowledgement

This work was supported in part by WASP/NTU M4082187 (4080), Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17, MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15, NRF2015-NRF-ISF001-2277, EMA Energy Resilience under Grant NRF2017EWT-EP003-041, and in part by the National Research Foundation of Korea (NRF) Grant funded by the Korean Government under Grant 2014R1A5A1011478.

References

[1] C. V. Networking, "Cisco global cloud index: Forecast and methodology, 2016-2021. white paper," *Cisco Public, San Jose*, Feb. 2018.

[2] O. Galinina, K. Mikhaylov, K. Huang, S. Andreev and Y. Koucheryavy, "Wirelessly powered urban crowd sensing over wearables: Trading energy for data," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 140–149, Apr. 2018.

[3] R. K. Ganti, F. Ye and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 32–39, Nov. 2011.

[4] M. Marjanovi, A. Antoni and I. P. arko, "Edge computing architecture for mobile crowdsensing," *IEEE Access*, vol. 6, pp. 10662–10674, Jan. 2018.

[5] W. Wang, D. T. Hoang, Z. Xiong, D. Niyato, P. Wang, P. Hu and Y. Wen, "A survey on consensus mechanisms and mining management in blockchain networks," *arXiv preprint arXiv:1805.02707*, 2018.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Self-published Paper*, May 2008.

[7] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[8] C. D. Clack, V. A. Bakshi and L. Braine, "Smart contract templates: foundations, design landscape and research directions," *arXiv preprint arXiv:1608.00771*, 2016.

[9] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert and P. Saxena, "A secure sharding protocol for open blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, Oct. 2016, ACM, pp. 17–30.

[10] R. Teodorescu and J. Torrellas, "Variation-aware application scheduling and power management for chip multiprocessors," in *ACM SIGARCH computer architecture news*, 2008, vol. 36, pp. 363–374.

[11] F. Baccelli, B. Błaszczyszyn et al., "Stochastic geometry and wireless networks: Volume ii applications," *Foundations and Trends® in Networking*, vol. 4, no. 1–2, pp. 1–312, 2010.

[12] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.