Blockchain-Based Mobile Crowd Sensing in Industrial Systems

Junqin Huang, Linghe Kong, *Senior Member, IEEE*, Hong-Ning Dai, *Senior Member, IEEE*, Weiping Ding, *Senior Member, IEEE*, Long Cheng, Guihai Chen, Xi Jin, and Peng Zeng

***Abstract*—The smart factory is a representative element reshaping conventional computer-aided industry to data-driven smart industry, while it is nontrivial to achieve cost effectiveness, reliability, mobility, and scalability of smart industrial systems. Data-driven industrial systems mainly rely on sensory data collected from statically deployed sensors. However, the spatial coverage of industrial sensor networks is constrained due to the high deployment and maintenance cost. Recently, mobile crowd sensing (MCS) has become a new sensing paradigm owing to its merits, such as cost effectiveness, mobility, and scalability. Nevertheless, traditional MCS systems are vulnerable to malicious attacks and single point of failure due to the centralized architecture. To this end, in this article we integrate MCS with industrial systems without introducing any additional dedicated devices. To overcome the drawbacks of traditional MCS systems, we propose a blockchain-based MCS system (BMCS). In particular, we exploit miners to verify the sensory data and design a dynamic reward ranking incentive mechanism to mitigate the imbalance of multiple sensing tasks. Meanwhile, we also develop a sensory data quality detection scheme to identify and mitigate the data anomaly. We implement a prototype of the BMCS on top of Ethereum and conduct extensive experiments on a realistic factory workroom. Both experimental results and security analysis demonstrate that the BMCS can secure industrial systems and improve the system reliability.**

***Index Terms*—Blockchain, mobile crowd sensing (MCS), mobility, scalability, security, smart factory.**

Manuscript received August 31, 2019; revised December 1, 2019; accepted December 21, 2019. Date of publication January 3, 2020; date of current version June 22, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 61972253, Grant 61672349, Grant U190820096, Grant 61672353, Grant 61672348, and Grant 61976120, in part by the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning, in part by the Macao's key R&D Funding Program under Grant 0025/2019/AKP, in part by the Macao Science and Technology Development Fund under Grant 0026/2018/A1, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20191445, in part by the Six Talent Peaks Project of Jiangsu Province under Grant XYDXXJS-048, and in part by the Qing Lan Project of Jiangsu Province. Paper no. TII-19-4042. *(Corresponding author: Linghe Kong.)*

J. Huang, L. Kong, and G. Chen are with Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: junqin.huang@sjtu.edu.cn; linghe.kong@sjtu.edu.cn; gchen@cs.sjtu.edu.cn).

H.-N. Dai is with the Macau University of Science and Technology, Taipa, Macau (e-mail: hndai@ieee.org).

W. Ding is with the School of Information Science and Technology, Nantong University, Nantong 226019, China (e-mail: dwp9988@163.com).

L. Cheng is with the School of Computing, Clemson University, Clemson, SC 29634 USA (e-mail: lcheng2@clemson.edu).

X. Jin and P. Zeng are with the Laboratory of Networked Control Systems, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China (e-mail: jinxi@sia.cn; zp@sia.cn).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2963728

I. Introduction

WITH the upcoming era of Industry 4.0, it becomes a trend to converge the physical world and the cyberspace in industrial sectors. A smart factory is the representative during the evolution from traditional computer-aided industry to data-driven smart industry, which is featured with the improved productivity and operational efficiency [1]. Typically, industrial systems make decisions depending on environmental information collected from ambient sensors distributed across the whole factory. However, the spatial coverage of industrial sensor networks is often constrained due to the high cost of deployment and maintenance [1]. In addition, industrial sensor networks are suffering from insufficiency in mobility and scalability [2].

Mobile crowd sensing (MCS) has received considerable interest recently [3]–[7]. MCS has become a leading paradigm to collect sensory data with powerful sensors embedded at mobile devices, such as mobile phones. Attributing to the merits like cost effectiveness, mobility, and scalability, there are many MCS applications or systems proposed in academia community, such as *SmartRoad* [8], *TransitLabel* [9], and *Map++* [10]. MCS provides a possible solution to the aforementioned industrial issues. In particular, MCS can extend existing industrial sensing systems in a smart factory without introducing additional dedicated devices. For example, factory staffs can use mobile phones to collect environmental information (e.g., the abnormal machinery noise) so as to monitor operating status of machines. The integration of MCS with existing static sensing methods can achieve a wide spatial coverage with a scalable and cost-effective solution.

A. Motivation

However, there are three main challenges when introducing MCS into a factory:

1) *Reliability:* For an industrial system, the provision of reliable services is one major concern. Most of the existing MCS systems are based on the centralized architecture, where all devices need to communicate with each other through the central server. Such centralized systems that

are fragile to the single point of failure cannot provide highly reliable services, which is not acceptable in modern industries. For example, it was reported in April 2015 that Uber China [11] failed to provide services due to the hardware failure. As a result, passengers cannot cease the order at the end of services, consequently incurring economic loss.

2) *Security:* Because of the traditional centralized architecture, MCS is exposed to the risk of malicious attacks, such as distributed-denial-of-service (DDoS) attack and man-in-the-middle attack. Besides the system safety issues, data security issues cannot be negligible. For the traditional MCS system, massive sensory data are stored in the centralized datacenter. The collected sensory data may be tampered after malicious attacks such as SQL injection attack, even if these attacks are initiated from insiders.

3) *Sensory data quality:* Moreover, different from the fixed sensors, mobile sensors in MCS are typically carried by human staffs who may behave unreliably or maliciously during data collection process. Thus, it is crucial to assess and guarantee the quality of collected data [12]. However, few existing MCS systems perform data quality verification. Motivated by the above three open issues in MCS, this article aims at answering this question: *Can we design a reliable, secure, and quality-guaranteed MCS for industrial systems?*

The past few years have witnessed the emergence and development of blockchain and its applications [13]–[16]. Featured with tamper-proof, integrity, and fault tolerance, blockchain brings an opportunity to solve the above three issues of MCS systems. First, blockchain can improve the system reliability due to the decentralization of MCS, thereby reducing the risk of single point failure. Second, blockchain can secure MCS via tamper-proof data storage and consensus mechanisms. Third, integrating data detection schemes with incentive mechanism, blockchain can guarantee the data quality.

B. Contributions

In this article, we propose a blockchain-based mobile crowd sensing system (BMCS) for industrial systems. There are three roles in traditional MCS systems: requesters, workers, and centralized platform; they essentially construct the triangular architecture. The BMCS breaks the triangular architecture in traditional MCS systems via exploiting decentralized feature of blockchain. In particular, the BMCS adopts the decentralized blockchain to replace the traditional centralized server. Meanwhile, we introduce *miners* who are responsible for generating blocks and validating transactions into the BMCS to help requesters verify the quality of large amount data collected by workers. The verification rules are embedded in smart contracts. Different sensing tasks have different verification rules. Miners can obtain extra rewards according to their proof-of-data. Since smart contracts are immutable codes running on top of the blockchain, under the guarantee of the trusted mechanism, requesters and workers can commit secure transactions without the trust of each other, consequently mitigating false-reporting and free-riding threats.

In addition, there exists an imbalance among different data collection spots in a factory. For example, data are often collected redundantly at popular locations while sparsely at unpopular locations. Therefore, we design a dynamic reward ranking (DRR) incentive mechanism specialized for the BMCS to solve the imbalance of sensory data. Owing to the trust fabric provided by the blockchain (i.e., no false-reporting and free-riding threats), this incentive mechanism can motivate more workers to participate in sensing tasks at unpopular sites, thereby achieving the balance of data collection.

Attributing to benefits of decentralized transparent blockchain and tamper-proof smart contracts, the BMCS improves the reliability and security for MCS systems. Without relying on any third-party arbiter, the BMCS guarantees the secure execution of transactions in a trustless environment.

The main contributions of this article are listed as follows.

1) To the best of our knowledge, this is the first study in incorporating MCS into smart factories. Leveraging the sensing capabilities offered by mobile phones of staffs in a factory, we can improve the mobility, scalability, and cost effectiveness of sensory data collection without introducing any additional dedicated devices.
2) We propose a BMCS, which breaks the triangular architecture of traditional MCS systems and improves the system reliability and security. Moreover, we design a sensory data quality detection scheme to exploit miners to verify the data quality. We also design a DRR incentive mechanism specialized for the BMCS to mitigate the issue of imbalanced data collection.
3) We implement a prototype of BMCS on top of Ethereum and conduct a case study of sound sensing in a public blockchain network. Both theoretical analysis and experimental results demonstrate the reliability, security, and efficiency of the BMCS.

The rest of this article is organized as follows. Section II presents related studies. Section III introduces preliminaries. Overview and detailed design of the BMCS are presented in Section IV. Section V introduces the implementation of a prototype of the BMCS and gives experimental evaluation. Security analysis is presented in Section VI. Finally, Section VII concludes this article.

II. Related Work

In this section, we briefly review related work in MCS from three aspects: system reliability and security, incentive mechanism, and data quality.

System reliability and security: In the aspect of services reliability of MCS, Zhou *et al.* [17] designed a robust mobile crowd sensing (RMCS) architecture based on edge computing to ensure reliable service provisioning. To improve the antiattack capability of MCS, Ni *et al.* [18] focused on studying the security requirements in fog-based vehicular crowd sensing and describing the possible solutions to achieve security assurance. Lin *et al.* [19] designed the Sybil-proof auction-based incentive mechanism (SPIM) to deter the Sybil attack. Gisdakis *et al.* [20] proposed a comprehensive security and privacy-preserving architecture in MCS, which is resilient to abusive users and guarantees privacy protection. Nevertheless, these proposed schemes are based on centralized servers, which are fragile to malicious attacks. There are also some general blockchain-based methods to strengthen the security of MCS, for example, Li *et al.* [11] conceptualized a framework, CrowdBC, for crowd sourcing based on blockchain. However, CrowdBC failed to consider the sensing quality issue, which is not practical in industrial spaces.

Incentive mechanism: There are several surveys [21], [22] reviewing a variety of incentive mechanisms that motivate people to contribute to MCS efforts. Jin *et al.* [23] proposed a differentially private incentive mechanism that preserves the privacy of each worker's bid against other honest-but-curious workers. Ota *et al.* [24] proposed a new incentive mechanism called QUOIN, which simultaneously ensures quality and usability of information for crowd sensing application requirements. Xu *et al.* [25] designed truthful incentive mechanisms to minimize the social cost such that each of the cooperative tasks can be completed by a group of compatible users.

Data quality: There are a number of studies contributing to the improvement of data quality in MCS. In particular, Restuccia *et al.* [12] focused on defining and enforcing the quality of information in crowd sensing. Jin *et al.* [26] proposed INCEPTION, which integrates an incentive, a data aggregation, and a data perturbation mechanism in the crowd sensing system, to ensure high quality of sensory data. Cheng *et al.* [27] proposed a compressive-sensing-based data quality improvement method, DECO, to detect false values for crowd sensing in the presence of missing data. RMCS [17] also provides a deep-learning-based method to verify the data quality. Peng *et al.* [28] incorporated the consideration of data quality into the design of incentive mechanism for crowd sensing to motivate the rational participants to perform data sensing efficiently. Kong *et al.* [29] proposed a novel approach based on compressive sensing to reconstruct massive missing data.

III. Preliminaries

A. Background

1) Mobile Crowd Sensing: MCS has become a new paradigm, which takes advantages of pervasive mobile devices and sensors to collect data efficiently, thereby enabling numerous industrial applications. Different from traditional sensing techniques, which rely on specialized equipment (such as sensors, radio frequency identification tags, and smart meters), MCS unburdens data collection tasks to ordinary people. MCS adopts off-the-shelf mobile devices (like mobile phones, pads, and tablets) that are easily carried by people. These massive mobile devices constitute a large-scale sensing system, which can rapidly accomplish large-scale sensing tasks through collecting data from mobile devices.

2) Blockchain: Blockchains are essentially distributed ledgers or databases that enable parties, which do not fully trust each other to reach a consensus about the existence, status, and evolution of a set of shared facts. Blockchains are enabled by complex cryptographic technologies and consensus models. Data stored in blockchain cannot be tampered, because it is easy to verify the data integrity through digital signatures and hash values. These benefits of blockchain have gained considerable research interests from both industry and academia.

B. Why Blockchain in MCS

Most MCS systems rely on centralized data centers to store massive sensory data. Due to the inability to verify whether data were not manipulated, those sensory data stored in centralized servers cannot be fully trusted. We know that the basic feature of blockchain is the decentralized trust, i.e., the nontamperable source of data. By leveraging this feature, we can guarantee the integrity of sensory data in MCS systems. Also, the decentralized architecture of blockchains can improve the reliability of MCS systems. As a result, MCS systems are resilient to the single point of failure and can provide reliable services. The combination of blockchain and MCS can strengthen the security of MCS systems from the perspective of the architecture. Moreover, smart contracts running on the top of blockchain can prevent free-riding and false-reporting phenomena in MCS systems effectively. Thus, we adopt blockchain-based methods to solve aforementioned open issues in MCS systems.

C. Threat Models

To demonstrate the advantages of the BMCS in reliability and security, we first analyze several possible threats as follows.

1) Single Point of Failure: The single point of failure means that a part of system's failure will prevent the entire system from working, which is undesirable in any system with a goal of high availability or reliability.

2) Sybil Attack: In a peer-to-peer network, each node has a unique identity generally. However, there may exist some evil nodes pretending multiple identities illegitimately and attempting to control most nodes in the network, which aims at eliminating the function of redundant replicated nodes, or defrauding multiple rewards. This malicious behavior is known as Sybil attack.

3) Free-Riding and False-Reporting: If the payment is made before a worker completes the sensing task, the worker always has the instinct to cease to work while taking the remuneration; this behavior is known as *free-riding*. If the payment is made after the worker completes the sensing task, the requester always has the instinct to refuse to pay for this task by lying about the status of this task; this behavior is known as *false-reporting* [30].

We assume that sensory data (like industrial sounds) in a smart factory are nonprivacy sensitive. So, we do not consider privacy preservation of data in this article, while other papers such as [7] offer the privacy-preserved solution. To address the above threats, the BMCS has three security and reliability goals: *1) Service availability*: The BMCS can handle the single point failure and enhance the system availability of services. *2) Antiattack capability*: The BMCS can mitigate the effects of Sybil attack, free-riding and false-reporting, DDoS attack, etc. *3) Data integrity*: The BMCS can guarantee the integrity of sensory data and protect collected data from being tampered.

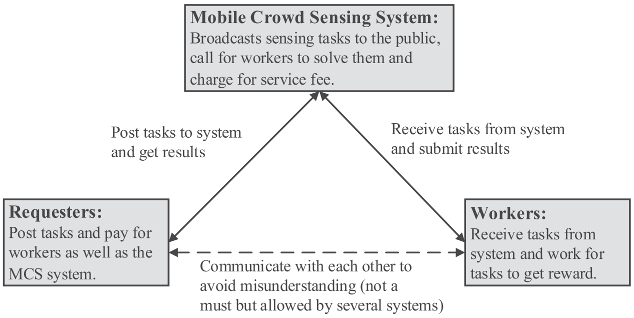

Mobile Crowd Sensing System:
Broadcasts sensing tasks to the public, call for workers to solve them and charge for service fee.
Post tasks to system and get results
Receive tasks from system and submit results
Requesters:
Post tasks and pay for workers as well as the MCS system.
Workers:
Receive tasks from system and work for tasks to get reward.
Communicate with each other to avoid misunderstanding (not a must but allowed by several systems)

Fig. 1. Traditional MCS triangular architecture.

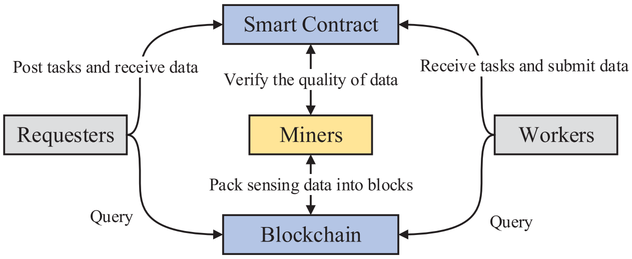

Smart Contract
Post tasks and receive data
Verify the quality of data
Receive tasks and submit data
Requesters
Miners
Workers
Pack sensing data into blocks
Query
Blockchain
Query

Fig. 2. Overall architecture design of the BMCS.

IV. BMCS: Blockchain-Based MCS in Smart Factory

In this section, we first present the architecture and workflow of the BMCS and then introduce the design of the DRR incentive mechanism and the sensory data quality detection scheme specialized for the BMCS.

A. Architecture Overview

As shown in Fig. 1, a traditional crowd sensing system consists of three groups of roles: requesters, workers, and centralized server. Requesters post tasks to the server and receive sensing results from the server. Workers receive tasks from the server, then accept tasks that they are interested in, and later submit the collected data to the server. The centralized server deals with requests from requesters and workers and then responds to them respectively. In this architecture, we can observe that the centralized server is a middleman, who needs to handle all of operations in the system. Nevertheless, the centralized server is vulnerable to various failures or attacks, such as DDoS, Sybil attack, and single point failure. The poor reliability due to the centralized architecture is not acceptable especially in industrial sectors.

In contrast, the BMCS consists of four groups of roles, as shown in Fig. 2. A decentralized blockchain is adopted as the system infrastructure instead of the traditional centralized server. In particular, smart contracts in blockchain can replace the server to handle operations of various sensing tasks. Meanwhile, in this architecture, we introduce a new role, *miners*, which are responsible for verifying data quality and maintaining the whole blockchain system. It is worth noting that requesters in smart factories can be factory owners or managers, and workers are those employees who work in factories. Requesters can publish sensing tasks in the form of smart contracts, and workers can use their mobile phones to collect ambient information, such as industrial sounds, so as to fulfill the demands of the requesters. In this way, the BMCS can extend the industrial sensor network without any additional dedicated device in a flexible manner.

Due to the decentralized architecture of blockchains, the BMCS eliminates the centralized server consequently achieving the decentralization. The BMCS adopts replicated nodes to store blockchain data, thereby improving blockchain data reliability. In spite of the failure of several nodes due to hardware faults or malicious attacks, the BMCS can provide reliable services due to the duplication of nodes. Thus, the BMCS is resilient to attacks like DDoS, single point of failure, etc. Blockchains are actually kind of distributed databases, so we may consider that we can store the collected data in blockchains. Also, by leveraging the characteristics of blockchains, we can guarantee data stored in blockchains not being tampered.

In the BMCS, we use smart contracts to handle requests from users instead of the centralized server. Smart contracts are immutable codes running on blockchain, and the mechanism of autoexecution by reaching preset conditions guarantees the fairness and trust fabric of the system. Since the crowd sensing process does not depend on any central third party, the single point of failure has been mitigated. Requesters can publish their sensing tasks through deploying specific smart contracts. Workers can participate in sensing tasks through posting sensory data to corresponding smart contracts. Stipulating that each identity must make a deposit before participation in smart contract protocols, we can efficiently prevent various malicious attacks (e.g., DDoS, Sybil, free-riding, and false-reporting attacks [30]).

We introduce the new role, *miner*, to verify the sensory data quality and store the data into blocks. The miner in the blockchain system plays a role in verifying and broadcasting received transactions, mining new blocks, and running smart contracts. However, miners in blockchains waste substantial computation resources to solve *useless* proof-of-work (PoW) puzzles. Moreover, how to guarantee the sensory data quality becomes a problem in crowd sensing systems. To this end, we propose the concept of *proof of data*, i.e., utilizing miners to verify the data quality. The verification rules are set by the requesters. Miners can obtain the rewards from requesters for their efforts in the proof of data.

We next illustrate the crowd sensing workflow in the BMCS as shown in Fig. 3.

1) Requesters Publish Sensing Task Contracts: Requesters publish their sensing tasks by writing and deploying specific smart contracts. They set up some necessary parameters in smart contracts, such as data type, data quantity required, and task rewards. Requesters formulate different data quality verification rules for different sensing tasks by creating functions in smart contracts. For example, in a factory, there may be a sensing task to collect industrial sounds to detect the operating status of machines, and the system makes judgment if the machines work normally by analyzing collected sensory data. The requester can set the upper bound or the lower bound in the smart contract to define the qualified range of the sensory data, and then, miners verify the data quality through sensory data quality detection scheme with the rules set by the requester.

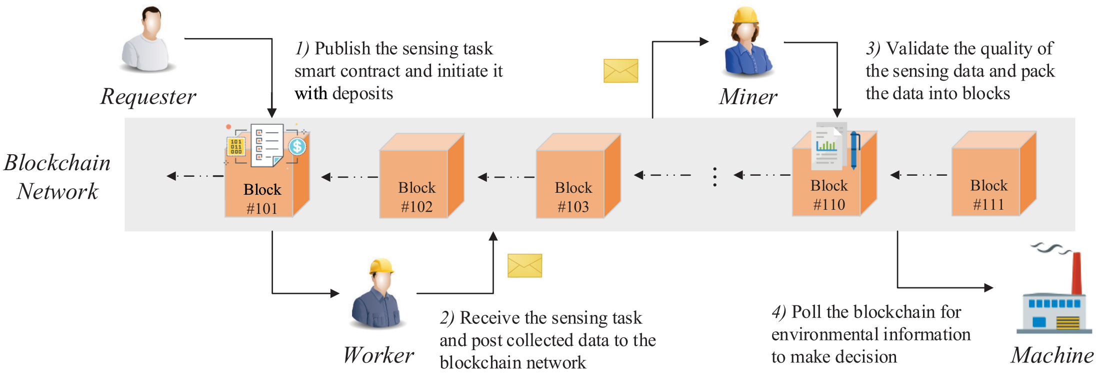

Requester
1) Publish the sensing task smart contract and initiate it with deposits
Miner
3) Validate the quality of the sensing data and pack the data into blocks
Blockchain Network
Block #101
Block #102
Block #103
Block #110
Block #111
Worker
2) Receive the sensing task and post collected data to the blockchain network
4) Poll the blockchain for environmental information to make decision
Machine

Fig. 3. Crowd sensing process in the BMCS.

2) Workers Receive Tasks and Upload Sensory Data: Workers query published task contracts in blockchain and accept interested sensing tasks according to the task information. They conduct sensing tasks by submitting collected data as transactions through calling specific functions in corresponding contracts. The submission of collected data will cost workers a certain amount of transaction fees. In fact, it is tantamount for workers to make the security deposits before participating in a crowd sensing task; this mechanism can efficiently mitigate attacks such as DDoS, Sybil, free-riding, and false-reporting attacks [30] from evil workers.

3) Miners Validate Data Quality and Transactions: Miners fetch unsubstantiated transactions and verify the quality of sensory data through the data-quality scheme with the rules predetermined by requesters. After substantiating the quality of sensory data, miners pack the verified sensory data into new mined blocks. Then, miners and workers will obtain corresponding rewards from requesters. In general, miners obtain rewards for executing smart contracts, and workers obtain rewards due to the efforts of uploading high quality sensory data. On one hand, through this incentive mechanism provided by the blockchain, we can establish the reputation of the system and raise the enthusiasm of both miners and workers in a short time. On the other hand, since rewarding deposits have been made in task contracts before publishing, the rules of completing tasks and getting rewards are *printed* in smart contracts, which cannot be denied. Thus, both requesters and workers can trust the immutable codes, i.e., smart contracts, as a credible administrator. This incentive mechanism not only satisfies the requirements of trustfulness and efficiency, but also eliminates the security vulnerability caused by the failure at a trustful center.

4) Convergence of Information Technology (IT) and Operational Technology (OT): After collecting sensory data and storing them in the blockchain, the machines in the factory poll the blockchain for ambient information to make adjustments in industrial operations; this process is known as IT/OT convergence. This step is to integrate IT systems used for data-centric computing with OT systems used to monitor devices in the factory.

5) Requesters Abort Sensing Tasks: Requesters can poll the status of sensing tasks periodically. Once they are satisfied with the received sensory data or decide not to continue collecting data for some reasons, they can abort the sensing task and get the remaining rewarding deposits from the smart contract. As this abort signal will be broadcasted in the blockchain network, then miners and workers will cease to work on this task.

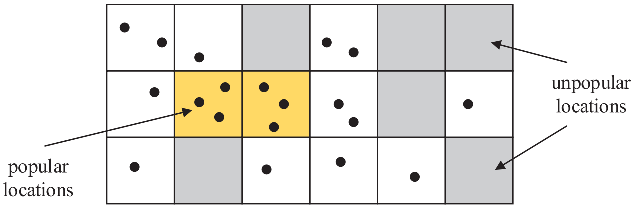


Fig. 4. Sensing squares division in the DRR incentive mechanism.

B. DRR Incentive Mechanism

In industrial systems, there is an imbalance among sensing tasks at different sensing regions. For example, redundant data are collected at some popular locations, while sparse data (even no data) are collected at some unpopular locations. In this section, we design a DRR incentive mechanism for the BMCS to mitigate this phenomenon.

We assume that all sensory data have location labels. We divide the whole sensing area into n small squares, and each piece of sensory data belongs to a specific square based on the location label. We define square i contains k_i pieces of sensory data. We consider that the square is small enough so that sensory data belong to the same square have similar values. If there are redundant sensory data in the square, this region is named as the *popular location*. If there are sparse data (even no data) in the square, this region is named as the *unpopular* location.

Fig. 4 presents an example consisting of 18 squares. The yellow squares represent popular locations and the gray squares represent unpopular locations. For popular locations, we may not need to collect too much sensory data. For unpopular locations, more workers are expected to collect sensory data here. Thus, the basic idea of the DRR incentive mechanism is to provide different task rewards in different regions. For example, the task reward in unpopular locations is higher than that in popular locations, which can motivate workers to collect data in those unpopular locations to earn more rewards. Meanwhile, we update the rewards allocation after each round of data submission based on the data density in the square. In this way, we can attract more workers to collect sensory data in those unpopular locations and finally achieve the sensing balance in different regions.

Suppose that the requester expects that there are at least d pieces of sensory data in each square, and the remaining rewards are w. We then give the definition of the reward r_i of square i as follows:

$$r_i = \begin{cases} w \times (d - k_i)/\sum_{i=1}^{n} \max(d - k_i, 0), & \text{if } k_i < d \\ 0, & \text{if } k_i \geq d \end{cases}. \quad (1)$$

As shown in (1), if square i has collected enough data, i.e., $k_i \geq d$, then we set the reward r_i to 0 in this square. If the amount of collected data have not reached d in square i, we allocate the remaining task rewards based on the data density in those squares. Once the system receives a new qualified data and confirms this submission, the task rewards will be reallocated based on the current data density in the squares. The reward r_i of square i is not equally distributed. We adopt the *dichotomy* to distribute the reward r_i according to the coming-first principle. It means that the sooner workers complete the sensing task, the more rewards they can gain. So, the reward paid for the worker is $r_i/2$; r_i is calculated according to the current sensing progress. Consequently, in this manner, we can motivate workers to collect sensory data in unpopular locations for higher rewards, and it can alleviate the imbalanced sensing situation. Thus, the DRR incentive mechanism can lead to a more uniform sensory data distribution, which contributes to making a higher sensing quality.

C. Sensory Data Quality Detection Scheme

In order to guarantee the higher data quality, it is necessary to have a clear idea of how to build the trust between requesters and workers, and how to validate the quality of submitted data. In the BMCS, users do not need to trust each other due to decentralized consensus mechanisms supported in blockchains. They can make secure deals without a trusted third-party. Thus, how to estimate the usefulness of collected data is crucial. To evaluate the quality of collected data, we define two types of low quality data: abnormal data and redundant data.

Abnormal data: Due to the hardware faults or the fake data submitted by dishonest users, there may exist outliers in the collected data. This kind of data should be detected and eliminated.

Redundant data: For the low time-dependent data, we do not need redundant data in the geographically approximated locations. Thus, this kind of redundant data should also be eliminated to improve the data quality.

Regarding these two types of low-quality data, we have different strategies. Because all sensory data have location labels, it is easy to filter illegal data that are out of expected geographic locations through location labels. Also, combining with the region squares division, it is apparent to find which square has redundant data. With respect to abnormal data, we can mitigate the outliers through analyzing hidden structural information from sensory data. Here, we take sound sensory data as an example to reveal its inherent properties. We collected the sound sensory data through MI 4 mobile phones for more than 10 min (more details will be given in Section V-A). The sampling frequency is 1 Hz. We chose 600 consecutive samples of the whole dataset to mine the hidden structures in the sound sensory data. This subset contains 3600 pieces of sound data. We show a sample of sound data as follows, and we can calculate the size of each piece of sound data is about 94 bytes.

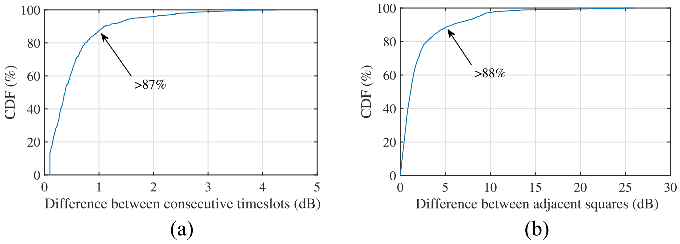


Fig. 5. Inherent properties in the sound sensory data. (a) Temporal stability feature. (b) Spatial correlation feature.

```
{
″timestamp″:1559196237390,
 ″decibel″:49.431602,
 ″longitude″:121.4368860,
 ″latitude″:31.02717034
} // a sample of sound data
```

We first investigate the temporal stability of the sound sensory data, which represents the degree of difference between two consecutive data points in one data trace. Thus, it is defined as $|x(t) - x(t-1)|$, where $x(t)$ denotes the tth piece of sound sensory data in the data trace x. According to the definition of temporal stability, we plot the cumulative distribution function (CDF) result in Fig. 5(a). We can observe that more than 87% sound data have less than 1-dB difference between consecutive data points. If we normalize the difference value as

$$\nabla_{x,t} = \frac{|x(t) - x(t-1)|}{x(t-1)} \quad (2)$$

we can observe that more than 91% consecutive sound data points have less than 0.02 difference, which shows a strong temporal stability feature [29]. Thus, the above analysis demonstrates that the sound sensory data have a good temporal stability.

We then explore the spatial correlation of the sound sensory data. The spatial correlation has a similar definition to the temporal stability. It denotes the degree of difference among data points in adjacent squares at the same time slot. It can be defined as $|x(t) - y(t)|$, where x and y represent two adjacent region squares. Fig. 5(b) plots the CDF result of the spatial correlation. We can observe that more than 88% sound data have less than 5-dB difference between adjacent squares at the same time slot. Similarly, we calculate the normalized value as follows:

$$\nabla_{x,y,t} = \frac{|x(t) - y(t)|}{x(t)} \quad (3)$$

and we can observe that more than 80% adjacent data points have less than 0.05 difference. So, we also can conclude that the sound sensory data also have a good spatial correlation feature [29].

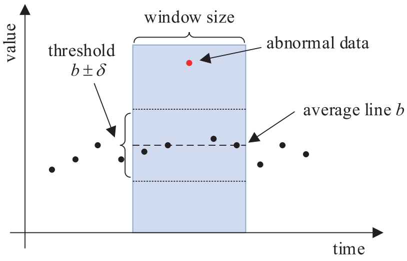


Fig. 6. Local average detection method.

Through leveraging the temporal stability and the spatial correlation features, we divide the sensory data quality detection scheme into two phases.

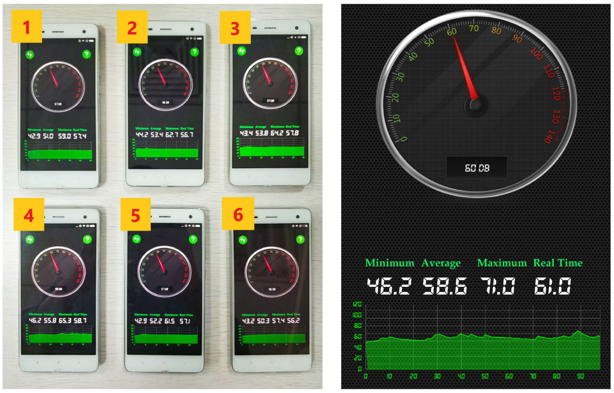
In the first phase, we utilize the temporal stability to detect if the sensory data distribution is qualified. The main idea of the first phase detection method is illustrated in Fig. 6. For given a time-series sensory data, we detect the data quality in a sliding window, where the window size is s. We put the data point to be detected in the middle of the window. We then calculate the average line of other data points in the current window, which is denoted by b. We define that the threshold for normal data is $b \pm \delta$. Thus, the red point in Fig. 6 is out of the threshold, which is considered as an abnormal data point.

In the second phase, we utilize the spatial correlation to judge if the sensory data lie in a reasonable range. Since the sound sensory data have a good spatial correlation, it implies that the detected data point should have a similar value to those of its neighbors at the same time slot. So, we calculate the average value of all of its neighbors, which is denoted by a. Then, we compare the average value with this data point. If the data point is in the range of $a \pm \beta$, we consider it as a normal data point. Only if the data point passes both phases' detection, we consider it as a qualified data point. Otherwise, we classify it as an abnormal data point.

V. Experimental Evaluation

A. Implementation

We implemented a prototype of the BMCS on Ethereum and conducted the sound sensing task in the public blockchain test network. We used a commercial PC to construct the public blockchain test network and multiple processes running on this PC acted as miners and requesters (i.e., Ethereum nodes). These nodes provide the blockchain Application Programming Interface (API) over the JSON-Remote procedure call (RPC) interface for workers who use mobile phones. Also, we adopted the PoW as the consensus mechanism of the BMCS and maintained the difficulty of the blockchain network as the default value,[1] i.e., 0 × 20 000. For workers, we used six MI-4 mobile phones, numbered from 1 to 6, to act as six workers to conduct the sound sensing task, which is shown in Fig. 7(a). Workers also have their own blockchain accounts, but different from miners and requesters, they do not run Ethereum nodes and just store part of blockchain data, for reasons of limited computing capacities. Workers submit sensory data and retrieve blockchain data over the JSON-RPC interface provided by Ethereum nodes.



(a) (b)

Fig. 7. Prototype of the BMCS implemented in the sound sensing task. (a) MI-4 mobile phones. (b) Sound sensing screenshot.

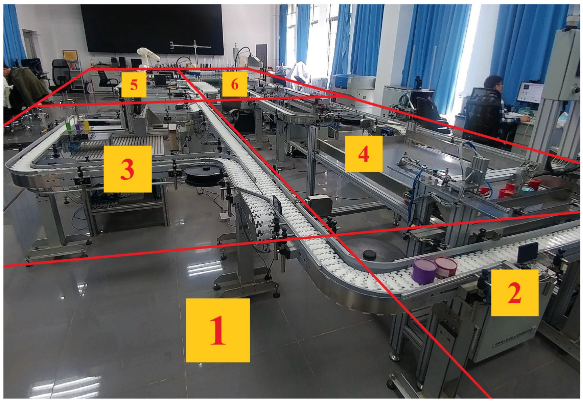


Fig. 8. Test scenario of sound sensing tasks.

We conducted experiments in a factory workroom, as shown as Fig. 8. This factory workroom has a logistics prototype, which can simulate the workflow of a real logistics distribution system. We evaluated the BMCS in the workroom in order to be as close as possible to the real application scenario. The area of the experimental testbed is about 150 m^2. We divide the testbed area into six squares, each of which is 5 × 5 m^2. Each mobile phone was placed in the corresponding numbered square, as shown in Fig. 8. The sampling frequency is 1 s. We collected the sound data lasting for more than 10 min, and the collected dataset contains more than 4000 pieces of sensory data. Fig. 10(a) plots the partial sound data trace we collected; the x-axis represents time series and the y-axis represents the decibel of sound. This case study demonstrates that the BMCS is feasible in the prototype of a smart factory.

B. Ethereum Blockchain Efficiency Concerns

According to Decker and Wattenhofer's research [31], they measured Bitcoin network latency and determined that 12.6 s is the time that it takes for a new block to propagate to 95%

[1] [Online]. Available: https://github.com/ethereum/go-ethereum

of nodes. Thus, the Ethereum network is designed to produce a block every 12 s[2] (but indeed it is around 14 s) in order not to generate too many stale blocks. Miners collect unspent transaction outputs from the transaction pool and verify and pack them into a new block. Because the number of transactions contained in one block is not fixed, the transaction per second (TPS) of Ethereum network fluctuates from 15 to 25 TPS.

The TPS of Ethereum blockchain is much lower than that of traditional centralized servers; there may be some efficiency concerns about blockchains, but we consider that the BMCS is delay tolerant. We know that the TPS of Ethereum means the number of transactions *confirmed* per second, but not the number of transaction *submitted* per second. The task rewards are transferred to workers after transactions confirmed; we think this step is totally delay tolerant. There is no need for workers to wait the previous transaction to be confirmed before submitting a new transaction, so the process of consensus mechanism does not impact workers collecting sensory data and submitting new transactions. Workers just wait for their transactions to be confirmed and then get their task rewards.

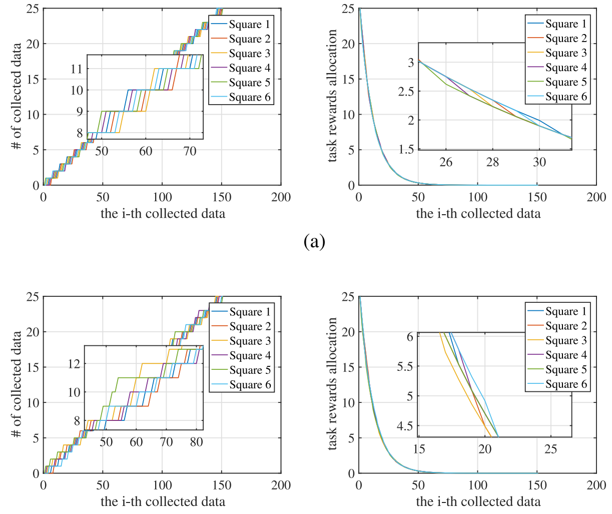
C. DRR Incentive Mechanism

We first evaluated the performance of dynamic reward-incentive mechanism. We adopted the following parameters in the simulations: 1) the number of region squares is $n = 6$; 2) it is expected to collect $d = 25$ pieces of sensory data in each square; and 3) the initial total reward is $w = 150$. In addition, we conducted two groups of experiments. The first group of experiments has the assumption that workers always prefer to collect sensory data in the locations, where higher rewards can be obtained. The second group of experiments assumes that only 50% workers will follow this preference.

As shown in Fig. 9(a), we can observe that workers always choose the highest rewards after each round of reward updation, and the number of collected data is increasing uniformly in each square. It mitigates the imbalance of multiple sensing tasks between popular locations and unpopular locations. Thus, the DRR incentive mechanism can motivate workers to collect sensory data uniformly.

In Fig. 9(b), when only 50% workers follow this mechanism, we can observe that workers may not obtain the highest rewards in each round of reward updating. According to (1), if the number of collected data pieces in a certain square is more than those in other squares, the rewards in this square will be lower than those in others. In general, workers tend to conduct the tasks, which can bring more rewards. Consequently, this mechanism can mitigate the imbalance of multiple sensing tasks.

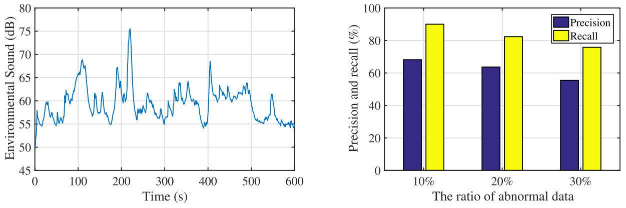
Equilibrium or not? Above experiments demonstrate that this mechanism can balance the sensing opportunities between popular locations and unpopular locations. However, will the mechanism result in fairness among workers? As illustrated in Section IV-B, the mechanism adopts the coming-first principle; workers who gather the required sensory data earlier can get more rewards. But how to guarantee this principle to be carried out strictly? We know that the task rewards are deposited in smart contracts by requesters when initializing sensing tasks; the rewards will be transferred to workers automatically after the submitted data verified, so workers have no need to concern about the false-reporting issue. Thus, by leveraging irresistible smart contracts, we can guarantee the rewarding fairness among workers under the coming-first principle.



(a)

(b)

Fig. 9. Performance of the DRR incentive mechanism. (a) Workers always choose the highest rewards. (b) 50% workers always choose the highest rewards.



(a)

(b)

Fig. 10. Performance of sensory data quality detection. (a) Sound sensory data samples. (b) Precision and recall.

D. Sensory Data Quality Detection Scheme

Based on the observation in Fig. 5(a) and (b), we set the threshold in the first phase $\delta = 1$ dB, and the threshold in the second phase $\beta = 5$ dB. We used the collected sound sensory data to evaluate the performance of the detection scheme. The sound dataset contains six traces, and we chose the subset of 600 data points for each trace in this experiment. We choose the first data trace to be the tested dataset and randomly select a fraction of data points in the trace as abnormal data. We generate anomaly data through adding random biases to the original data, and we set the ratio of anomaly data as 10%, 20%, and 30%, respectively, in this experiment.

Fig. 10(b) plots evaluation results. We observe that the precision and recall of data quality detection decrease with the

[2] [Online]. Available: https://docs.ethhub.io/using-ethereum/mining/

increased ratio of anomaly data. When the ratio of anomaly data is 10%, the detection scheme has the best performance, i.e., about 70% precision and 90% recall. When the ratio is 30%, the detection scheme has about 55% precision and 75% recall. These results imply that the proposed data quality detection scheme achieves an excellent performance via leveraging the temporal and spatial features of sensory data.

VI. Security Analysis

We first analyze the BMCS security concerns in four aspects: single point of failure, Sybil attack, DDoS attack, and free-riding and false-reporting. Then, we give some discussion on blockchain security and make some comparison between the BMCS and other MCS systems.

Prevention of single point of failure: The BMCS is built on a blockchain, which is essentially a distributed ledger consisting of a group of replicated database nodes. The data are duplicated by all nodes, so the BMCS is resilient to the failure of one or several nodes. More exactly, for PoW-based blockchain systems, if the system contains $2n + 1$ blockchain nodes, then it can tolerate up to n failures, where $n \in N^+$.

Prevention of Sybil attack: Each node in a blockchain must solve complex puzzles to verify a transaction; this mechanism increases the costs of Sybil attack. Moreover, workers actually need to make security deposits, i.e., pay transaction fees to miners, before participation in a crowd sensing task; it also efficiently prevents Sybil attack. We assume that the attacker has the computing capacity of c. If the attacker wants to launch a Sybil attack, he needs to divide his computing capacity c into several subparts $c_1, c_2, \ldots, c_n$ to pretend different identities. However, this will weaken the total computing capacity of the attacker because of some extra computing costs brought by process scheduling, which makes $c_1 + c_2 + \cdots + c_n \leq c$. Also, n fake identities need to pay n-fold transaction fees, which induces large extra costs. Thus, from either computation costs or transaction costs, the BMCS can mitigate the Sybil attack well.

Prevention of DDoS attack: The BMCS can prevent DDoS attacks well because it is decentralized, while DDoS attacks rely on centralized systems. By leveraging the decentralized nature of blockchains, the BMCS can allocate data and bandwidth to absorb DDoS attacks as they happen. Also, in the BMCS, malicious attackers need to pay transaction fees to miners before sending transactions, which are much costly to launch DDoS attacks.

Prevention of free-riding and false-reporting: The BMCS adopts smart contracts, which are immutable codes running on a blockchain, in which both requesters and workers trust this incentive mechanism. In particular, requesters must make deposits in smart contracts before publishing a sensing task. The status of a task will be automatically judged by a smart contract, thereby efficiently preventing the false-reporting attack. Workers must upload qualified sensory data and complete the task according to requirements written in the smart contract. After that, they will get rewards transferred from the smart contract without relying on any central trust. This mechanism can essentially prevent the free-riding attack.

TABLE I
Comparison Between the BMCS and Some Other MCS Systems

	BMCS	SPIM [19]	CrowdBuy [34]	CrowdBC [11]
Single Point Failure	√	×	×	√
Sybil Attack	√	○	×	√
DDoS Attack	√	×	×	√
Free-riding and False-reporting	√	×	×	√
Data Quality	√	×	√	×

Note: √ denotes the challenge being tackled without using any central trust model; × denotes the challenge still existing; ○ denotes the challenge being (partially) tackled based on a central trust or third-party arbiter; and − denotes this issue does not exist.

In the BMCS, we adopt the public blockchain as the underlying technology, so users who want to participate in the system do not need to be authorized. They can join it freely, while the openness of the public blockchain system may also attract some malicious users, whose existence threatens the security of blockchains. The major security issues of public blockchains which we focus on are *51% attack* and *double-spending attack* [32]. For PoW-based blockchains, the premise of the success of 51% attacks is that attackers must own more than half computation capability of the whole system. It is almost impossible to achieve especially when the number of users is larger and larger. Double-spending attacks can cause the fork of the blockchain because of the inconsistent transactions. The attackers attempt to spend the same token twice to defraud services or rewards. However, this issue can be mitigated by the consensus mechanism, which can make the status of blockchains consistent across the network finally. And according to the theory of six-blocks-security [33] in bitcoin, we consider that six confirmed blocks are enough to defend double-spending attacks.

Table I compares the BMCS with other representative MCS systems from the security perspectives. We observe that the BMCS outperforms other MCS systems in addressing various threads. For example, SPIM [19] and CrowdBuy [34] built on the central architecture are vulnerable to secure threats. Meanwhile, SPIM does not consider the data quality in MCS systems. Though CrowdBC [11], which is a blockchain-based crowd sensing system, can mitigate malicious attacks via exploiting the benefits of blockchains and smart contracts, it has no mechanism to guarantee the data quality.

VII. Conclusion

In this article, we proposed a BMCS and conducted realistic experiments in a prototype of a factory. We exploited MCS to extend the traditional industrial sensor network in the smart factory to achieve an enhanced scalability, mobility, and cost effectiveness. Harnessing benefits of blockchains, the BMCS compensated for the paucity of MCS with enhanced security and reliability. We also presented a novel concept of proof of data, through which miners conduct the *useful* work, i.e., verifying the sensory data quality. Moreover, we designed a simple incentive mechanism to mitigate the imbalance of multiple sensing tasks in MCS systems. Furthermore, we proposed a temporal and spatial feature-based data quality detection scheme to check whether the sensory data were normal.

However, there are still some deficiencies in the BMCS, for example, in this article, we failed to consider some privacy-preserving methods for sensory data. In future research directions, we can focus on how to protect data privacy in public blockchains. We believe that the BMCS has a wide spectrum of industrial applications, such as smart cities, intelligent transportation systems, and logistics in the future.

References

[1] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[2] H.-N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, "Big data analytics for manufacturing Internet of Things: Opportunities, challenges and enabling technologies," *Enterprise Inf. Syst.*, 2019, doi:10.1080/17517575.2019.1633689.

[3] Y. Liu, L. Kong, and G. Chen, "Data-oriented mobile crowdsensing: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2849–2885, Third Quarter 2019.

[4] H. Ma, D. Zhao, and P. Yuan, "Opportunities in mobile crowd sensing," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 29–35, Aug. 2014.

[5] L. He, L. Kong, Y. Gu, J. Pan, and T. Zhu, "Evaluating the on-demand mobile charging in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 14, no. 9, pp. 1861–1875, Sep. 2015.

[6] L. Kong, M. K. Khan, F. Wu, G. Chen, and P. Zeng, "Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: Overview, design, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 62–68, Jan. 2017.

[7] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[8] S. Hu, L. Su, H. Liu, H. Wang, and T. F. Abdelzaher, "SmartRoad: Smartphone-based crowd sensing for traffic regulator detection and identification," *ACM Trans. Sens. Netw.*, vol. 11, no. 4, 2015, Art. no. 55.

[9] M. Elhamshary, M. Youssef, A. Uchiyama, H. Yamaguchi, and T. Higashino, "TransitLabel: A crowd-sensing system for automatic labeling of transit stations semantics," in *Proc. 14th Annu. Int. Conf. Mobile Syst., Appl. Services*, 2016, pp. 193–206.

[10] S. J. Sheikh, A. Basalamah, H. Aly, and M. Youssef, "Demonstrating map++: A crowd-sensing system for automatic map semantics identification," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun. Netw.*, 2014, pp. 152–154.

[11] M. Li *et al.*, "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1251–1266, Jun. 2019.

[12] F. Restuccia, N. Ghosh, S. Bhattacharjee, S. Das, and T. Melodia, "Quality of information in mobile crowdsensing: Survey and research challenges," *ACM Trans. Sensor Netw.*, vol. 13, no. 4, 2017, Art. no. 34.

[13] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[14] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: A lightweight blockchain system for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019.

[15] W. Feng and Z. Yan, "MCS-chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain," *Future Gener. Comput. Syst.*, vol. 95, pp. 649–666, 2019.

[16] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[17] Z. Zhou, H. Liao, B. Gu, K. M. S. Huq, S. Mumtaz, and J. Rodriguez, "Robust mobile crowd sensing: When deep learning meets edge computing," *IEEE Netw.*, vol. 32, no. 4, pp. 54–60, Jul. 2018.

[18] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.

[19] J. Lin, M. Li, D. Yang, G. Xue, and J. Tang, "Sybil-proof incentive mechanisms for crowdsensing," in *Proc. IEEE Conf. Comput. Commun.*, 2017, pp. 1–9.

[20] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "Security, privacy, and incentive provision for mobile crowd sensing systems," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 839–853, Oct. 2016.

[21] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 370–380, Oct. 2015.

[22] X. Zhang *et al.*, "Incentives for mobile crowd sensing: A survey," *IEEE Commun. Surv. Tut.*, vol. 18, no. 1, pp. 54–67, First Quarter 2016.

[23] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling privacy-preserving incentives for mobile crowd sensing systems," in *Proc. IEEE 36th Int. Conf. Distrib. Comput. Syst.*, 2016, pp. 344–353.

[24] K. Ota, M. Dong, J. Gui, and A. Liu, "QUOIN: Incentive mechanisms for crowd sensing networks," *IEEE Netw.*, vol. 32, no. 2, pp. 114–119, Mar. 2018.

[25] J. Xu, Z. Rao, L. Xu, D. Yang, and T. Li, "Incentive mechanism for multiple cooperative tasks with compatible users in mobile crowd sensing via online communities," *IEEE Trans. Mobile Comput.*, to be published, doi:10.1109/TMC.2019.2911512.

[26] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "INCEPTION: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proc. 17th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2016, pp. 341–350.

[27] L. Cheng *et al.*, "Compressive sensing based data quality improvement for crowd-sensing applications," *J. Netw. Comput. Appl.*, vol. 77, pp. 123–134, 2017.

[28] D. Peng, F. Wu, and G. Chen, "Pay as how well you do: A quality based incentive mechanism for crowdsensing," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 177–186.

[29] L. Kong *et al.*, "Data loss and reconstruction in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 2818–2828, Nov. 2014.

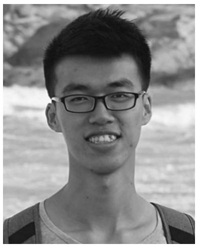
[30] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "Keep your promise: Mechanism design against free-riding and false-reporting in crowdsourcing," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 562–572, Dec. 2015.

[31] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *Proc. IEEE P2P Conf.*, Sep. 2013, pp. 1–10.

[32] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, to be published, doi:10.1016/j.future.2017.08.020.

[33] R. Bhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *J. Econ. Perspectives*, vol. 29, no. 2, pp. 213–238, May 2015.

[34] L. Zhang *et al.*, "CrowdBuy: Privacy-friendly image dataset purchasing via crowdsourcing," in *Proc. IEEE Conf. Comput. Commun.*, 2018, pp. 2735–2743.



Junqin Huang received the B.E. degree in computer science and technology from the University of Electronic Science and Technology of China, Chengdu, China, in 2018. He is currently working toward the master's degree in computer technology with Shanghai Jiao Tong University, Shanghai, China.

His research interests include crowdsensing, cybersecurity, mobile computing, Internet of Things, and blockchain.

Linghe Kong (Senior Member, IEEE) received the bachelor's degree in automation from Xidian University, Xi'an, China, in 2005, the master's degree in telecommunication from TELECOM SudParis (ex. INT), Essonne, France, in 2007, and the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2012.

He is currently a Tenure-track Research Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai. He was a Postdoctoral Researcher with Columbia University, McGill University, and the Singapore University of Technology and Design. His research interests include wireless networks, big data, mobile computing, Internet of Things, and smart energy systems.

Hong-Ning Dai (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Chinese University of Hong Kong, Hong Kong, in 2008.

He was with the Department of Information Engineering, Chinese University of Hong Kong, and the Hong Kong Applied Science and Technology Research Institute after his Ph.D. study. He is currently an Associate Professor with the Faculty of Information Technology, Macau University of Science and Technology, Taipa, Macau. His research interests include Internet of Things, big data analytics, and blockchains.

Weiping Ding (Senior Member, IEEE) received the Ph.D. degree in computation application from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2013.

He was a Visiting Scholar with the University of Lethbridge, Lethbridge, AB, Canada, in 2011. From 2014 to 2015, he was a Postdoctoral Researcher with the Brain Research Center, National Chiao Tung University, Hsinchu, Taiwan. In 2016, he was a Visiting Scholar with the National University of Singapore, Singapore. From 2017 to 2018, he was a Visiting Professor with the University of Technology Sydney, Ultimo, NSW, Australia. His main research interests include data mining, machine learning, granular computing, evolutionary computing, and big data analytics.

Long Cheng received the Ph.D. degree in computer science from the Beijing University of Posts and Telecommunications China, Beijing, China, in 2012, and the second Ph.D. degree in computer science (with a focus on cyber security) from the Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, in 2018.

From 2012 to 2015, he was a Research Fellow with the Singapore University of Technology and Design, and then a Research Scientist with the A*STAR Institute for Infocomm Research, Singapore. From 2009 to 2011, he was a Research Assistant with Hong Kong Polytechnic University, Hong Kong, and the University of Texas at Arlington, Arlington, TX, USA. He is currently an Assistant Professor with the School of Computing, Clemson University, Clemson, SC, USA. His research interests include cyber security and wireless networking.

Guihai Chen received the B.E. degree in computer software from Nanjing University, Nanjing, China, in 1984, the M.E. degree in computer science from Southeast University, Nanjing, in 1987, and the Ph.D. degree in computer science from the University of Hong Kong, Hong Kong, in 1997.

He is currently a Distinguished Professor of Department of Computer Science and Engineering with Shanghai Jiaotong University, Shanghai, China. He has been invited as a Visiting Professor by many universities, including Kyushu Institute of Technology, Kitakyushu, Japan, in 1998, the University of Queensland, Brisbane, QLD, Australia, in 2000, and Wayne State University, Detroit, MI, USA, from September 2001 to August 2003. He has a wide range of research interests with a focus on sensor networks, peer-to-peer computing, high-performance computer architecture, and combinatorics.

Xi Jin received the Ph.D. degree in automation from Northeastern University, Shenyang, China, in 2013.

She is currently an Associate Professor of Industrial Control Network and System Department with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang. Her research interests include wireless sensor networks and real-time systems, especially the real-time scheduling algorithms and worst-case end-to-end delay analysis.

Peng Zeng received the B.S. degree in computer science from Shandong University, Shandong, China, in 1998, and the Ph.D. degree in mechatronic engineering from the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China, in 2005.

From 2005 to 2007, he was an Associate Professor of Industrial Control Network and System Department with the Shenyang Institute of Automation, Chinese Academy of Sciences, where he was involved in research on wireless sensor networks. He is currently a Professor with the Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang. His current research interests include wireless sensor networks for industrial automation, smart grids, and demand response.