Received 30 July 2023; revised 28 August 2023; accepted 8 September 2023. Date of publication 18 September 2023; date of current version 13 October 2023.

Digital Object Identifier 10.1109/OJCOMS.2023.3316118

Data Quality in Human-Centric Sensing-Based Next-Generation IoT Systems: A Comprehensive Survey of Models, Issues, and Challenges

KONSTANTINA BANTI[1], MALAMATI LOUTA[1] (Senior Member, IEEE), AND PERISTERA BAZIANA[2]

[1]Department of Electrical and Computer Engineering, University of Western Macedonia, 50100 Kozani, Greece
[2]Department of Informatics and Telecommunications, University of Thessaly, 351 00 Lamia, Greece

CORRESPONDING AUTHOR: M. LOUTA (e-mail: louta@uowm.gr)

This work was supported by the Project “AGROTOUR—New Technologies and Innovative Approaches to Agri-Food and Tourism to Boost Regional Excellence in Western Macedonia” under Grant MIS 5047196, which is implemented under the Action “Reinforcement of the Research and Innovation Infrastructure,” supported by the “Operational Program Competitiveness, Entrepreneurship and Innovation” (NSRF 2014–2020), and co-financed by Greece and the European Union (European Regional Development Fund).

ABSTRACT Human-Centric Sensing (HCS), a novel approach in the evolution of the Next Generation Internet of Things (NG-IoT), exploits the ubiquity of diverse smart devices, including smartphones or wearable devices, in conjunction with their enhanced sensing capabilities to collect information, leveraging human intelligence for the common benefit of the crowd. The main feature of HCS is the involvement of mobile users in data collection, processing, analysis and sharing. Thus, the main challenge in HCS systems is to ensure users’ participation and trustworthiness as well as data quality. The aim of this work is, as a first step, to identify and discuss the factors that affect data quality in HCS-based NG-IoT systems, as well as elaborate on their interrelation. Furthermore, potential solutions that could be adopted to ensure the highest possible degree of data quality are highlighted, in conjunction with critical aspects that should be considered, proposing a novel classification with three major categories: task assignment, reputation mechanisms and blockchain technology. Finally, a trust-aware task assignment model is proposed to effectively address the data quality challenge in HCS-based IoT systems, reflecting users’ trustworthiness, willingness, experience, and ability to collect and share high-quality data contributions. The proposed trust-aware task assignment model exploits a reputation mechanism and is designed using blockchain and smart contract technologies to enable the decentralized provision of trustworthy services among entities and preserve users’ privacy, harnessing the decentralization, transparency and immutability offered by blockchain. Trust-based task assignment offers an effective solution for trustworthy users’ selection while ensuring high-quality contributions and users’ privacy.

INDEX TERMS Blockchain, data quality, Internet of Things (IoT), human centric sensing (HCS), reputation mechanism, task assignment.

I. INTRODUCTION

THE NEXT Generation Internet of Things (NG-IoT) stands as an emerging technology aimed to effectively incorporate, manage, and analyze an extensive volume of data gathered by diverse devices at an unprecedented scale and analysis. Core NG-IoT enabling technologies including edge computing, advanced mobile communication systems like 5G and beyond, blockchain, virtual/augmented reality and tactile Internet are anticipated to deliver effective approaches for addressing diverse challenges stemming from the proliferation of interconnected devices and the massive volume of data produced. These challenges include availability, latency, scalability, energy efficiency, security and privacy, interoperability, and reliability [1]. Despite the fact that humans are an integral part of IoT, their involvement continues to be largely overlooked by modern IoT systems. Incorporating humans into the loop and elevating their role in a reliable and sustainable manner holds paramount significance for NG-IoT systems [2]. This transformation has the potential to impact society and economy across diverse domains such as energy, agriculture, smart cities, mobility, healthcare, and more.

The wide adoption of smart devices (like smartphones, smartwatches, tablets) with various embedded powerful sensors (e.g., Global Positioning System (GPS), accelerometer, gyroscope, microphone, camera) has become an integral part of people's everyday life, enabling a broad spectrum of applications. The emergence of the IoT coupled with the widespread use of social media and the human mobility and ubiquity has led to the emergence of a new sensing paradigm known as Mobile Crowd Sensing (MCS) or People/Human Centric Sensing (HCS) [3], [4], are two terms often used interchangeably to stress the pivotal role of human involvement in establishing and operating large-scale sensing networks. MCS/HCS enhances the NG-IoT paradigm by incorporating human presence, involving a large number of individuals equipped with sensing and computing devices into the loop of data collection-analysis-sharing for the benefit of society. MCS/HCS is a promising technology for NG-IoT, interconnecting things with things, things with people, and people with people [5]. In our work, we adopt HCS term to emphasize the active role of humans in the data collection-analysis-sharing loop, as we place a significant emphasis on the role of users' trustworthiness, willingness, experience and social aspects in gathering and sharing high-quality data contributions.

HCS leverages the ubiquity of mobile devices in conjunction with the inherent mobility and intelligence of their owners, empowering sensing, analysis and sharing of information about their surroundings to accomplish specific tasks. In this respect, HCS enables the cost-effective and timely monitoring of extensive-scale phenomena that cannot be otherwise easily measured. This way, in HCS-based NG-IoT systems, humans are not only passive recipients of IoT applications; they actively participate as data or service providers, strengthening the effectiveness of IoT. A wide range of applications have been developed leveraging HCS, including environmental monitoring (e.g., air quality [6], water management [7], [8]), smart parking [9], healthcare, and smart agriculture [10], [11], [12].

The success of HCS-based NG-IoT systems heavily relies on the capabilities offered by emerging technologies in the 5G/6G context. These advanced communication technologies provide ultra-reliable and low-latency communication, ultra-high bandwidth and ultra-large throughput, and enhanced connectivity, which are crucial for the efficient operation of HCS [13]. As we move towards the 6G era, these technologies will play an even more crucial role, with 6G networks designed to meet higher global coverage requirements, enhanced spectral efficiency, and a minimized carbon footprint, promoting sustainability, equity, trust, and security [13]. Additionally, edge computing is expected to play a pivotal role in HCS-based NG-IoT systems by enabling data processing closer to the data source, thus reducing latency, improving energy efficiency in IoT devices, and facilitating large-scale, continuous data collection in the cloud. By minimizing the need for data transmission, edge computing also enhances data security and privacy. Virtual and augmented reality technologies, in combination with the Tactile IoT, offer powerful capabilities for enhancing user interaction in HCS-based NG-IoT systems. By providing immersive and intuitive experiences, virtual and augmented reality enable users to contribute data in engaging ways, resulting in increased user involvement. Moreover, the Tactile IoT introduces a human-centric perspective and sensing/actuating capabilities, eliminating the need for physical proximity between people and the systems they interact with. This allows for remote control and operation, creating new possibilities for seamless user engagement and interaction within HCS-based systems. Machine learning and artificial intelligence techniques are essential in efficiently managing the increased complexity of HCS-based NG-IoT systems. By analyzing the vast amounts of collected data, these technologies provide valuable insights and predictions, enhancing the overall value of the data. The robustness, explainability, and interpretability of the adopted mechanisms are crucial for building end-users' trust and overcoming potential barriers to the acceptance of new applications. The decentralized and secure nature of blockchain technology, gaining traction in the 5G/6G era, serves as a robust framework for ensuring data integrity and user privacy in HCS-based NG-IoT systems but also offers interoperability across the IoT. By providing a unified authentication and authorization system, as well as supporting traceability and reliability of IoT data, distributed ledger technology, such as blockchain, enhances the overall trustworthiness and transparency of HCS-based systems. Thus, these advancements contribute to more accurate, timely, and valuable data, enhancing the overall effectiveness and reliability of HCS-based systems.

HCS presents several unique characteristics, with the most significant being the active involvement of humans in data collection, processing, analysis and sharing, bringing forth both opportunities and challenges that must be effectively addressed for HCS to reach its full potentials. The growing popularity of HCS has led to the publication of numerous comprehensive surveys in recent years, focusing on challenging issues such as user recruitment, task allocation and scheduling, privacy, incentives, and data quality problems. However, most studies are limited to solving a certain challenge (or a subgroup of identified challenges), without taking into account the effect and the interrelation with other challenges as well.

Focusing on the data quality challenge, ensuring accuracy and trustworthiness of the user's contributed data is a paramount concern in HCS-based NG-IoT systems. In these systems, the crowd participates in solving complex problems through open calls, where the aggregation of information often leads to better decisions compared to those made by any single member of the crowd [25].

However, due to the inherently open nature of HCS systems, there is a risk of noisy, obsolete, incomplete and inaccurate data. Additionally, security and privacy concerns arise, as personal information such as daily routines and activity patterns could be easily disclosed [26]. Simultaneously, incentive mechanisms ought to be established to foster cooperation, bolster users' trust in data sharing, thereby ensuring substantial human participation [23]. The success of HCS systems heavily relies on acquiring sufficient and reliable data from participants [27], who should be appropriately compensated for their time, effort and cost incurred [28].

In the light of the aforementioned in [24], the authors propose a framework that outlines the concept of data quality in terms of information quantity and accuracy and highlight the importance of truth discovery and trust frameworks to assess and guarantee data quality in HCS. However, it's important to mention that the survey on the data quality challenge lacks an exploration of the interrelation and the role of each challenge in influencing the data quality issue. In [16], the authors examine data quality from two facets: coverage and fault tolerance, highlighting that task allocation is a critical issue that impacts data quality. The [21] highlights that data quality can be influenced by the number of participants, the sensor quality, and redundant sensing. Moreover, the [23] discusses on the potential impact of environmental factors and malicious users on data quality. The paper proposes incentive and task allocation mechanisms to address data quality concerns. In [5], the authors state that resource limitations can impact data quality and highlight as future work that trust preservation and abnormal detection technologies are necessary to ensure data quality. Similarly, in many approaches (e.g., [29], [30], [31], [32], [33]), data quality challenge is addressed without considering the interrelation among all the distinct issues, failing to address them collectively, to optimize HCS-based NG-IoT system's operation. The major contributions of recent related research literature surveys concerning data quality, task assignment, incentives, privacy and security (selected considering their relevance to the topic, timeliness and number of citations) are summarized in Table 1 and Table 2. However, the existing literature lacks a comprehensive survey that explores the main aspects of data quality, considering all interrelated aspects and challenges from a holistic perspective in the context of human centric sensing NG-IoT systems. To bridge this gap, different from the previous works, we provide an in-depth analysis of the factors affecting data quality in HCS-based NG-IoT systems. We explore unintentional and intentional low-quality data provisioning, data completeness, and area coverage, and examine the interdependencies between data quality and other challenges such as task assignment, energy efficiency, privacy-security, incentives, and interoperability. Following, a novel taxonomy of factors and critical issues to be considered when designing potential solutions for the data quality challenge is proposed. These factors are classified into three categories: task assignment problem, reputation mechanisms for incentive provisioning to promote users' cooperation and blockchain technology for alleviating security concerns. Finally, to the best of our knowledge, such a comprehensive and detailed analysis of data quality challenge in HCS-based NG-IoT systems, along with the proposed solutions, has not been presented in previous survey papers. Moreover, the focus on the human aspect present in this work is not as prominent in the previous papers.

Specifically, emphasis is laid on the task assignment problem complemented with reputation mechanisms, which have been successfully utilized in various domains and contexts (e.g., [34], [35], [36], [37], [38], [39], [40]), providing a softer security layer compared to Trusted Third Parties to ensure a minimum level of trust self-interested entities. Reputation mechanisms encourage collaboration and act as a motivator for positive conduct by rewarding those who exhibit good behavior and imposing penalties on those who engage in undesirable actions, leading to improved data quality in the context of HCS-based NG-IoT systems. Our main objective is to provide a comprehensive overview of the aspects and issues that need to be taken into account when designing a trust-aware reputation mechanism to complement a task assignment strategy, ultimately aiming to achieve optimal data quality. Blockchain technology has emerged as a highly reliable and secure platform for various applications beyond cryptocurrencies, including healthcare, e-commerce, supply chain among others. The possibilities for utilizing blockchain technology are extensive and continue to broaden as the technology advances and matures. Integrating blockchain into HCS systems offers a promising solution to address several issues. The combination of blockchain and HCS introduces a new paradigm that harnesses the advantages of blockchain characteristics including decentralization, traceability and immutability, enhances the security of HCS systems, eliminates the weaknesses of a centralized platform [31], guarantees the integrity of sensory data and improves the system's reliability [41]. However, there are still open challenges that need to be effectively addressed to fully unlock its potential. In this study, after elaborating on the characteristics of blockchain technology that align with the challenges and benefits of HCS-based NG-IoT systems, critical issues and open challenges are identified and discussed. Additionally, we propose the use of incentive mechanisms that can effectively and efficiently motivate users to report high quality information.

In the light of the aforementioned, in this work a trust-aware reputation model is proposed that exploits the synergies of technologies and solutions proposed in three categories, namely task assignment strategies, reputation mechanisms, and blockchain technology to effectively address the data quality challenge in HCS-based IoT systems, while alleviating security and privacy concerns.

The main contributions of this paper can be summarized as:

TABLE 1. Summary of state-of-the-art surveys on MCS.

Work	Major Contribution	Main Topic
[5]	Survey MCS strategies to reduce resource cost and achieve high quality of service, present strategies for application domains and describe the challenges of MCS and future research directions.	Resource limitations and quality of service (QoS)
[14]	Survey the research status of MCS task allocation and incentive methods.	Task allocation and incentives
[15]	Provide a comprehensive review for task allocation methods in MCS and highlight future research directions.	Task allocation
[16]	Survey task allocation methods in terms of data quality and sensing cost, review unique issues of task allocation and highlight future research opportunities.	Task allocation
[17]	Categorize mechanisms for preserving the location privacy of Workers and highlight future research directions.	Location privacy
[18]	Survey and evaluate existing solutions on privacy protection and privacy-preserving incentive solutions as well as highlight open issues and future research challenges.	Privacy protection
[19]	Survey applications, methodologies, simulators and architectures and present future research directions.	Categorization on many aspects of MCS solutions
[20]	Present the existing MCS frameworks, applications and discuss about MCS challenges and research findings.	Address MCS applications
[21]	Discuss about task assignment models and attacks on them, incentive and privacy-preserving mechanisms and highlight future research directions to design a privacy-preserving incentive-based task management mechanism without analyzing in-depth the impact of data quality factor.	Privacy preservation
[22]	Survey MCS challenges and present blockchain-based MCS solutions to address the MCS challenges as well as discuss about challenges and opportunities in blockchain-based MCS. However, it does not analyze the factors that affect the data quality challenge or the interrelationship between MCS challenges.	Blockchain-integrated MCS solutions
[23]	Present MCS applications, testbeds and architectures, and survey incentive, security and privacy-preserving mechanisms as well as resource optimization and data analysis techniques focusing on how to evaluate the quality of gathered data without taking into the interrelation of the other challenges on data quality.	Incentive mechanisms, security protection and privacy preserving, resource optimization
[24]	Analyze the state-of-the-art works on quality of information and truth discovery as well as propose a new framework for defining and ensuring the quality of information without addressing other MCS challenges.	Quality of information (QoI)
This work	Survey HCS challenges with emphasis on data quality, investigate the interrelation between HCS challenges and data quality and provide an in-depth analysis and discussion of factors that affect data quality. It provides a novel taxonomy of critical issues that should be considered when designing solutions to the data quality challenge, classified upon three major categories: task assignment problem, reputation mechanisms promoting users' cooperation and persistent good behavior and blockchain technology. Finally, it proposes a blockchain enabled trust-aware reputation mechanism complementing task assignment to efficiently address the data quality challenge, exploiting in combination proposed solutions in each distinct category.	Data Quality

- We provide an overview of the challenges faced by HCS-based NG-IoT systems and elaborate further on the factors that affect the data quality challenge on a holistic perspective.
- We conduct a comprehensive analysis of the state-of-the-art solutions and key techniques utilized to efficiently address the data quality challenge in HCS-based NG-IoT systems.
- We present the key elements and critical aspects to be considered when designing solutions for the data quality challenge.
- We propose a novel taxonomy of the aforementioned aspects upon three major categories: task assignment, reputation mechanism, and blockchain technology.
- We explore the integration of blockchain into HCS-based NG-IoT systems, highlighting the benefits it

TABLE 2. Comprehensive overview: vision, technology, and solution in the state-of-the-art surveys on MCS.

Work	Vision	Technology	Solution
[5]	A cost-efficient MCS system capable of cost reduction through optimal resource utilization and enhanced QoS for users	Analyze strategies for reducing resource cost and achieving good QoS	
[14]	Solving large-scale and uncertain sensing environments	Analyze task allocation and incentive methods from different aspects	
[15]	Address the gap between ideal problem setting and real-world applications	Analyze problem formulation approaches within task allocation and corresponding algorithms	
[16]		Analyze task allocation strategies in wireless sensor networks and MCS	
[17]	Extensive integration of location privacy protection mechanisms in MCS	Categorize and compare location protection mechanisms	
[18]	A holistic scheme to preserve the privacy of identity, data, attribute and task	Classify privacy protection schemes and survey privacy-preserving incentives	
[19]		Propose a detailed taxonomy and classification of MCS works based on four-layered architecture	Introduce a four-layered architecture
[20]	Attractive MCS systems while taking into account the privacy of the participants	Identify the application areas emphasizing on the participatory and opportunistic sensing	Propose an infrastructure for the MCS framework
[21]	An efficient privacy-preserving incentive-based task management mechanism	Classify privacy-preserving and incentive mechanisms, and task management models	
[22]		Review blockchain-based MCS approaches	
[23]		Survey incentive mechanisms, security protection and privacy preservation techniques, and resource optimization strategies	
[24]		Analyze truth discovery and trust frameworks to estimate and enforce QoI	Propose a unified framework for defining and enforcing the QoI
This work	Implementation and evaluation of the blockchain enabled trust-aware reputation mechanism complementing task assignment to efficiently address the data quality challenge	Analyze task assignment strategy, reputation mechanism, and blockchain technology	Propose a blockchain-based trust-aware HCS-based NG-IoT platform

brings and identifying critical challenges that remain to be addressed.

- We propose a blockchain-based trust-aware HCS-based NG-IoT platform, paving the way towards efficiently addressing the data quality challenge.

The structure of the paper is presented in Fig. 1. Section II presents the HCS based NG-IoT architecture and models. Section III overviews the challenges that arise in HCS systems and discusses in detail upon the challenge of data quality. Section IV focuses on the task assignment challenge and particularly explores the interdependencies between task assignment and data quality. Section V elaborates on the design of a reputation mechanism to address the data quality challenge, highlighting various aspects and issues that should be considered. Section VI presents in detail the benefits introduced by blockchain technology in HCS-based NG-IoT systems, while highlighting critical aspects that need to be addressed to mitigate security concerns. Section VII proposes a blockchain-based trust-aware HCS-based NG-IoT platform, discussing its main constituent elements and their role in efficiently addressing the data quality challenge. Finally, in Section VIII, we conclude the paper and provide directions for future research.

II. HCS-BASED NG-IOT ARCHITECTURE & SYSTEM MODELS

In an HCS-based IoT ecosystem, data originating from diverse sources, such as sensors and smart devices is collected, analyzed and processed to deliver intelligent services. Additionally, by harnessing the power of the crowd, human's intelligence, knowledge, and mobility heterogeneous information about phenomena of common interest is collected for supporting a variety of IoT applications. In this sense, IoT is being extended beyond the sole reliance on smart devices [42].

A general Human centric IoT system is illustrated in Fig. 2. It consists of the following main entities:

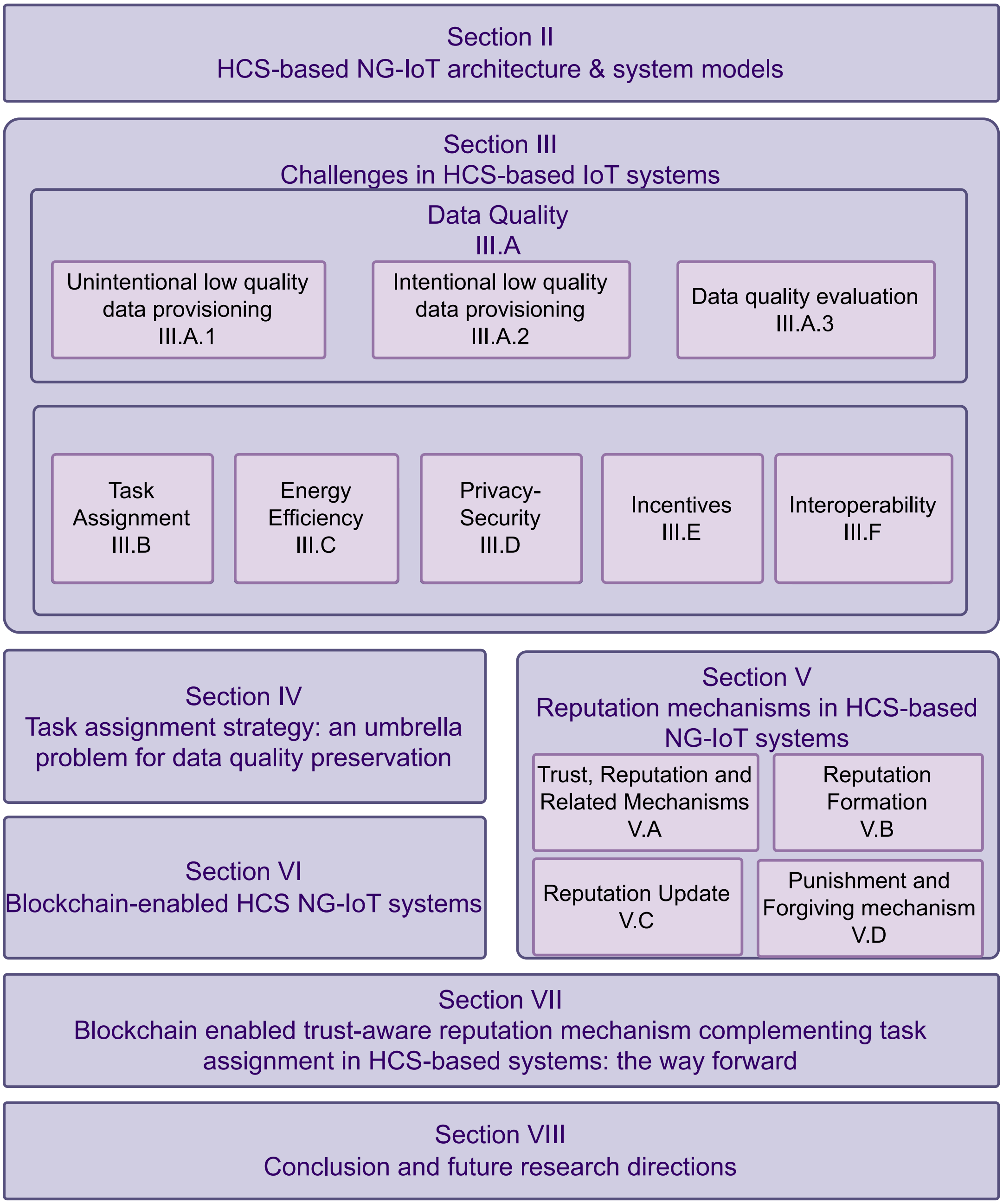
Section II
HCS-based NG-IoT architecture & system models
Section III
Challenges in HCS-based IoT systems
Data Quality
III.A
Unintentional low quality data provisioning III.A.1
Intentional low quality data provisioning III.A.2
Data quality evaluation III.A.3
Task Assignment III.B
Energy Efficiency III.C
Privacy-Security III.D
Incentives III.E
Interoperability III.F
Section IV
Task assignment strategy: an umbrella problem for data quality preservation
Section V
Reputation mechanisms in HCS-based NG-IoT systems
Trust, Reputation and Related Mechanisms V.A
Reputation Formation V.B
Reputation Update V.C
Punishment and Forgiving mechanism V.D
Section VI
Blockchain-enabled HCS NG-IoT systems
Section VII
Blockchain enabled trust-aware reputation mechanism complementing task assignment in HCS-based systems: the way forward
Section VIII
Conclusion and future research directions

FIGURE 1. Data Quality in Human-Centric Sensing based NG-IoT systems: the structure of this work.

a) the Requestors: These are the entities that initiate the targeted data collection process. They submit sensing tasks relevant to their interests to the Crowdsensing platform and have access to the knowledge acquired when Workers send the collected data to the platform.

b) the Workers or Participants: They play a critical role as the primary source of information in the data collection process. They utilize their smart devices to collect the relevant information. Also, sensors / IoT devices deployed in the environment provide additional information that complements the data collected by Workers using their smart devices.

c) the Crowdsensing Platform: It serves as the main communication link between Requestors and Workers. It stores, processes, and analyzes data contributed by Workers and Requestors. Additionally, it integrates this data with information collected from established sensor networks and other IoT devices. The platform collectively analyzes the data to extract knowledge and insights, which is then made available to users through IoT applications and services.

Specifically, the centralized HCS platform handles and manages all relevant processes, including user recruitment, data aggregation, task creation and execution as well as incentive schemes. Also, energy-efficiency and

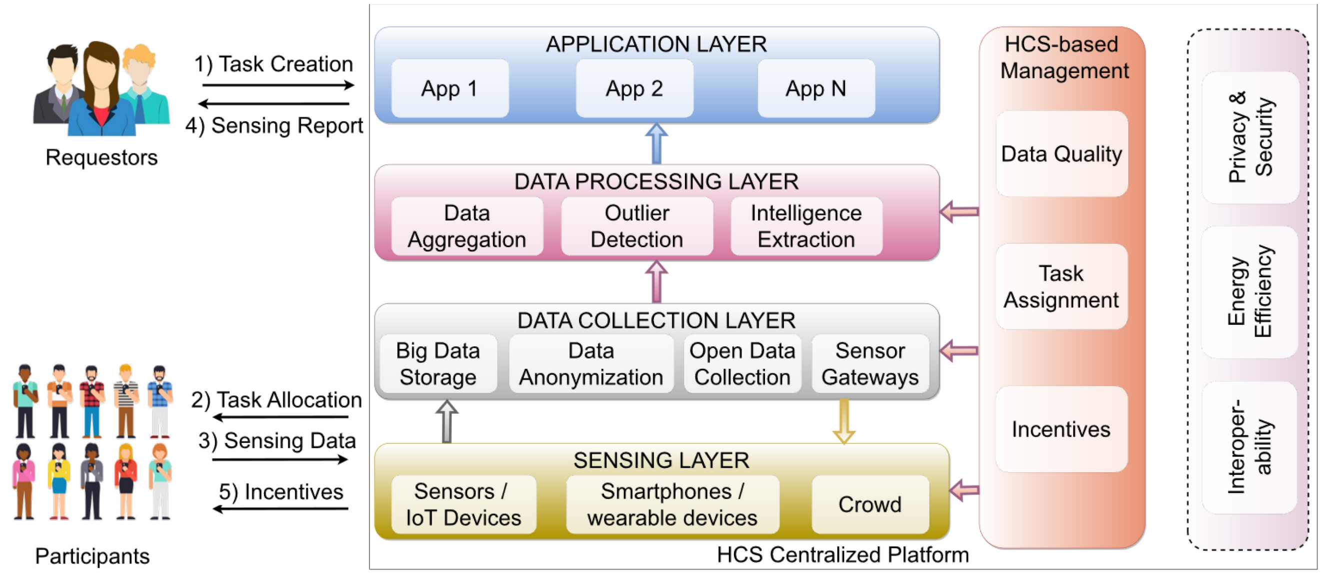

FIGURE 2. **HCS-based NG-IoT System Architecture.**

privacy-preserving mechanisms as well as interoperability issues, should also be considered in the HCS platform, as we discuss in the following section.

It consists of four layers: *sensing layer*, *data collection layer*, *data processing layer* and *application layer*. In the Sensing Layer, raw data is collected through the crowd and sensors or sensing devices, including user devices like mobile/smartphones, wearable devices, smart vehicles, and more. The Data Collection Layer consists of sensors gateways that facilitate data gathering from various sources such as IoT objects, sensing devices, and the crowd [43]. This layer modifies and represents data in a unified manner using big data storage, collects open data, and supports privacy protection through methods like data anonymization. The processed data is then sent to the Data Processing Layer. In the Data Processing Layer, data from sensors/mobiles, and the crowd are processed, aggregated and analyzed. This layer identifies and removes outliers in sensing data, eliminates potential low-quality contributions, and extracts useful knowledge and intelligence to deliver smart services. Finally, in the Application Layer, IoT applications and services are provided to users.

Especially, the life cycle of a HCS task consists of five stages: *Task Creation*, *Task Assignment*, *Task Execution*, *Data Aggregation* and optionally *Reward Payment*.

1. *Task Creation*

Firstly, the Requestor creates a task based on his/her interests/requirements and submits it to the platform.

2. *Task Assignment*

The HCS platform assigns the task to specific Workers in order to perform it. The task assignment process can be categorized based on how the task is allocated to the Workers. Two task assignment models could be adopted, namely the *pull model* and *the push model*.

- In the *pull model*, Workers access active tasks through the platform and choose the ones they want to participate in.
- In the *push model*, Workers provide their interests, preferences, and availability to the platform. The platform then pushes tasks to their mobile devices solely when the declared specific requirements and criteria are fulfilled [21]. In this model, the procedure mostly occurs outside the user's control.

3. *Task Execution*

Workers utilize their smart devices to complete assigned tasks within a predefined period of time. They collect and forward the required data to the platform. Also, based on the desired degree of user involvement in the sensing process, which can be explicit or implicit, there are two different sensing execution models: participatory sensing (active sensing mode) and opportunistic sensing (passive sensing mode).

- *Participatory Sensing* requires explicit user actions to contribute sensor data.
- *Opportunistic Sensing*, the task is executed in the background without the active involvement of users [19].

However, a hybrid model has also been introduced, which combines the benefits of both methods [44]. In this model, participants apply both active and passive sensing modes in the platform. In this way, the accuracy of the collected data is improved as certain information that users might be unable to share can be effectively collected opportunistically [45].

Regarding data transmission, users might embrace the *opportunistic transmission model,* following a store-carry-forward behavior, transmitting information to other users when better forwarding opportunities arise or the *infrastructure-based* transmission, utilizing deployed communication systems [46], [47].

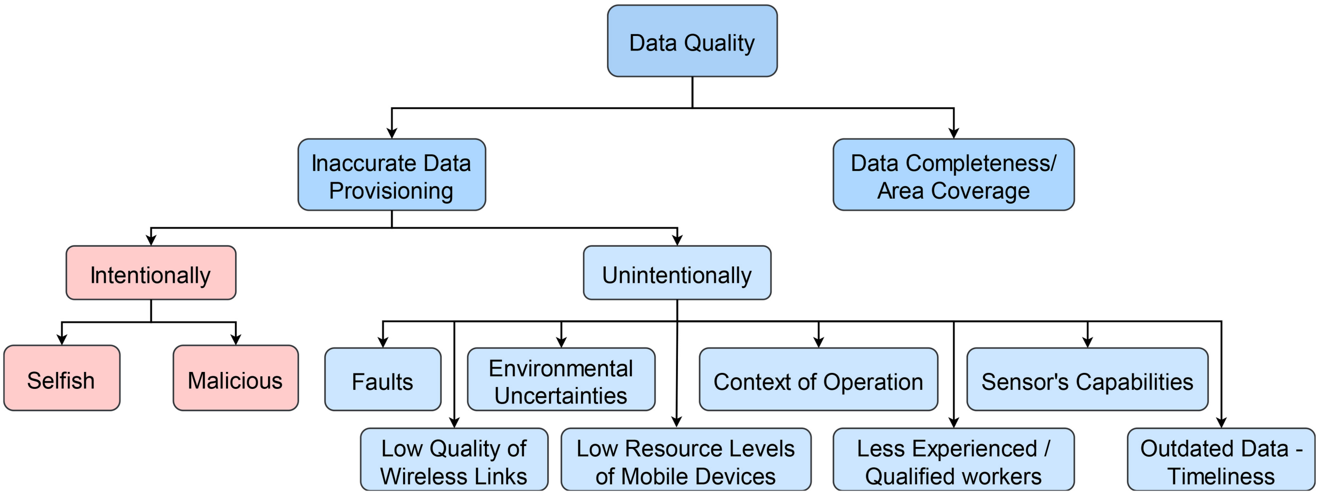
Data Quality
Inaccurate Data Provisioning
Data Completeness/ Area Coverage
Intentionally
Unintentionally
Selfish
Malicious
Faults
Environmental Uncertainties
Context of Operation
Sensor's Capabilities
Low Quality of Wireless Links
Low Resource Levels of Mobile Devices
Less Experienced / Qualified workers
Outdated Data - Timeliness

FIGURE 3. Factors influencing Data Quality of HCS-based NG-IoT Systems.

4. *Data Aggregation*

The platform aggregates data from all participants, along with data collected from sensor networks and IoT devices. It evaluates their quality and processes them to provide the required information to the Requestors in the desired format. In case of a *delay-sensitive task*, where Requestors require prompt data delivery, the platform immediately processes the responses from Workers and sends the outcomes to the Requestor. On the other hand, in the event of a *delay-tolerant task*, the platform waits until all participants have contributed their data before sending it to the Requestor.

5. *Reward Payment*

Finally, the platform or the Requestor provides rewards to the participants for their contributions. The reward can be determined by the platform (platform-centric), where the Workers have no control over the payment, or it can be user-centric, where the Workers have control by announcing a price that corresponds to the minimum estimated reward for their participation. However, the reward is optional; as there are HCS systems where Workers contribute voluntarily [19].

III. CHALLENGES IN HCS-BASED IOT SYSTEMS

As highlighted above, in the context of HCS-based IoT, the active participation of humans in the loop for data collection, processing, analysis and sharing, introduces both opportunities and challenges. To fully realize the potential of HCS-based IoT applications, it is crucial to address several critical issues. Aspects that merit meticulous consideration mainly pertain to ensuring data integrity and quality coupled with security, privacy and incentives that should be in place. Given the human involvement, the selection of participants to execute the required tasks should be carefully considered. Additionally, the conditions experienced by mobile devices along with the constraints imposed by factors such as energy, bandwidth, computing resources, considering also the current context of operation should be taken into account. Next, we will provide a comprehensive overview of the data quality challenge. Also, we present the challenges of task assignment, energy efficiency, privacy and security, incentives, and interoperability.

A. DATA QUALITY

The data quality issue arises as a result of the open nature inherent in HCS systems that rely on users' contributions to provide intelligent services and applications. On one hand, HCS-based IoT systems enable the monitoring of large-scale phenomena in a cost and time efficient manner, which would not be possible otherwise. On the other hand, given the fact participant is a potential threat source [48] and user participation may introduce data of poor quality into the system. Data quality is associated with accuracy, trustworthiness, completeness, consistency, timeliness, uniqueness, and validity [49]. Area coverage quantifies how uniformly and completely the Workers cover the area of interest. Also, low quality data can result from various factors such as device faults, low resource levels of the mobile device (energy, computational), poor communication channel conditions, the current context of operation, less qualified and/or experienced Workers, multiple tasks that a user performs simultaneously, and outdated data due to the time elapsed before uploading data to the platform (referred to hereafter as *unintentional low quality data provisioning*). On the other side, participants seeking to maximize their welfare may act selfishly and even maliciously by providing low quality and even falsified data, leading thus to a significant deterioration of HCS systems' performance (referred to hereafter as *intentional low quality data provisioning*). Both cases lead to low quality data provisioning, which should be identified and eliminated to prevent adverse impacts on the whole system's performance. Fig. 3 depicts the aforementioned factors that influence data quality, which will be further analyzed in the following subsections.

1) UNINTENTIONAL LOW QUALITY DATA PROVISIONING

As aforementioned, participants may inadvertently contribute poor-quality data. Referring to cases users do not deliberately provide inaccurate data, the data quality could potentially be influenced by users who are unfamiliar with the target area or topic of interest and/or have to make a special effort because of an absence of prior experience and knowledge how to perform their assigned task [50]. Additionally, Workers might inadvertently place their mobile devices in an undesirable position while collecting sensor readings, thereby reducing the quality of the data being submitted [25], [51]. Specifying levels of difficulty for sensing tasks announced and providing instructions consistently and clearly can influence the quality of sensed data [52]. Moreover, low-quality data can be produced when a user performs multiple tasks simultaneously, increasing thus the latency and potentially degrading the quality of sensor readings by lowering the duty cycle or defining a different set of sensors according to the available energy levels. Furthermore, if the Requestor require data pertaining to specific time and specific location or area and participants provide inconsistent data and/or send outdated data, poor quality contributions have been provided that may lead to an inadvertently incorrect result. Finally, sensed data quality (in terms of accuracy and latency) can vary significantly due to faults, low quality of the wireless link, device mobility, current resources' availability, sensor capabilities, the operational context of mobile device, and environmental uncertainties [53].

2) INTENTIONAL LOW QUALITY DATA PROVISIONING

Intentional inaccurate information provisioning corresponds to cases of selfish and/or malicious entities that purposely offer low quality and/or erroneous data.

- Selfish users

Selfish users aim to minimize their effort and resource consumption while maximizing their own utility and/or preserving their privacy when performing the assigned sensing tasks. Their actions can lead to low-quality data provisioning, such as non-fresh or random sensor readings. Despite this, they still expect to receive the specified reward for task execution. For instance, in real-time traffic monitoring, selfish users may submit false traffic congestion warnings with the intention of diverting traffic away from their own routes [54].

- Malicious users

On the other hand, malicious users contribute false/erroneous data in order to harm the HCS systems and the usefulness of the extracted knowledge/information. For instance, a malicious participant can spoof a GPS location [55] and provide falsified location data. At this point, it should be pointed out that participants may collude and provide similar contributions, making it challenging to identify falsified data [48]. Another issue arises when malicious users accept sensing requests but deliberately abstain from providing responses, thereby preventing other honest users from being chosen.

3) DATA QUALITY EVALUATION

Data quality evaluation is a crucial task as in the most systems there is no knowledge of the ground truth or gold answers. For this reason, mechanisms for validating collected data should be in place so as to ensure the usefulness and the integrity of collected information. Certain methods have been proposed, including data selection and comparison techniques, to filter out low-quality or irrelevant data and generate a high-quality dataset [56]. In comparison techniques, reliable IoT data can be used to evaluate the data submitted by users. It is also important to assess the reliability of IoT sensors by comparing data from similar sensors and/or open data sources in order to identify faulty and inconsistent data [57]. Estimating and predicting sensing data, coupled with statistical analysis to identify and remove outliers in sensed values [43], can also be utilized. Considering location-based tasks, location validation can be enforced to eliminate potential contributions received from users who are not at the specified location of interest (within a certain acceptable distance) or the requested period time [55]. Finally, selecting trustworthy users to complete sensing tasks is expected to improve data quality [34]. Several performance metrics can be used to evaluate the performance of the proposed solutions, such as the distance between the submitted sensing data and the ground truth [58], [59], the similarity between submitted answers [27], the accuracy of correctly detecting false/normal data [48], the accuracy of location [50], the ratio of the area coverage [60], while also exploring the impact of residual battery level, the distance to the point of interest, and sensors' quality on quality score [29], the impact of users' experience and device context on the achieved quality score [60], the impact of the number of recruited Workers and allocated budget [33], percentage of task completion over time [50], reputation values of trustworthy users [27], [61], reputation values of selfish/malicious users [27], and the total payment [27], since the total payment for each user is proportional to the quality of user's contribution.

B. TASK ASSIGNMENT

The participant selection problem stands as a significant challenge within the HCS paradigm, which has an impact on task efficiency and quality. Finding appropriate participants is a core issue to attain diverse optimization objectives, like ensuring area coverage and data quality, minimizing task completion time, while maintaining a low number of participants involved in task execution. Prediction models [62] can be exploited to select the minimum number of participants required capable of delivering high-quality data to achieve the required sensing coverage. Providing proper incentives and selecting trustworthy participants are related subproblems that should be efficiently addressed in this context [34], [63], [64], [65].

C. ENERGY EFFICIENCY

Energy efficiency is another significant parameter for HCS-based NG-IoT systems, as Workers want to save smart device resources for other purposes as well. Energy efficiency can be achieved in various ways. For example, processing of the sensed data locally on mobile devices and exploitation of edge computing could yield intermediate results that require less energy, resources and bandwidth for transmission [66]. Additionally, optimized task assignment approaches that determine the right type of data and the required number of participants will minimize the volume of data that needs to be sensed and transmitted, thereby reducing total energy consumption.

D. PRIVACY-SECURITY

HCS goals are accomplished based on users' contributions, which can lead to many privacy breaches. Sensed data, combined with spatio-temporal information, can potentially reveal users' location, daily habits, routines and personal activities [26]. Users desire access to HCS-based IoT services but are generally reluctant to disclose sensitive information. Therefore, the challenge arises is preserving users' privacy and the security of the sensed data. Ensuring privacy preservation in HCS systems encourage users' participation in sensing and data collection tasks, promoting the usage of relevant IoT applications. Given the paramount importance of preserving individual privacy, it becomes crucial to establish a comprehensive privacy and security framework that applies to all HCS applications and data types, regardless of their nature. Finally, identity privacy and location privacy are two performance metrics that can be used to evaluate the privacy preservation of the system [66].

E. INCENTIVES

Data collection in HCS relies on the willingness of participants to collect data using their smart devices. Users may incur energy and computational resource consumption, monetary cost, traffic cost or need to invest their time and effort to effectively accomplish their tasks. In crowdsensing systems, incentive mechanisms are necessitated so as to encourage user's cooperation and sustain their involvement in accurate data collection/generation and sharing. User incentives may be financial, interest and entertainment or social and ethical (like users' recognition, socialization) or service-based [68].

F. INTEROPERABILITY

Data interoperability remains a key challenge, as there is a need for data reuse across different applications in HCS NG-IoT systems, leading to minimization of time, effort, cost, and resource consumption, is an aspect of outmost importance. Currently, HCS architectures lack sufficient inter-architecture interoperability. Each HCS application is associated with a specific platform, limiting or lacking support for data/results sharing across different applications. Data interoperability enables sharing of user-generated data between HCS tasks, services and applications, using it in a meaningful way, it is critical to identify the common data requirements among these tasks, services and applications and ensure that the data collected is relevant and accurate. Multiple advantages related to data interoperability support in HCS based systems have been noted in [68]. Firstly, data can be reused without additional cost. Secondly, reusing sensory data reduces or eliminates duplicated sensing and processing, thus, the overall system efficiency is improved. Thirdly, tasks can collectively utilize many mobile users through the platform. Achieving interoperability between different HCS platforms can be accomplished by providing a unified ecosystem that serves as a framework for crowdsensing services [70].

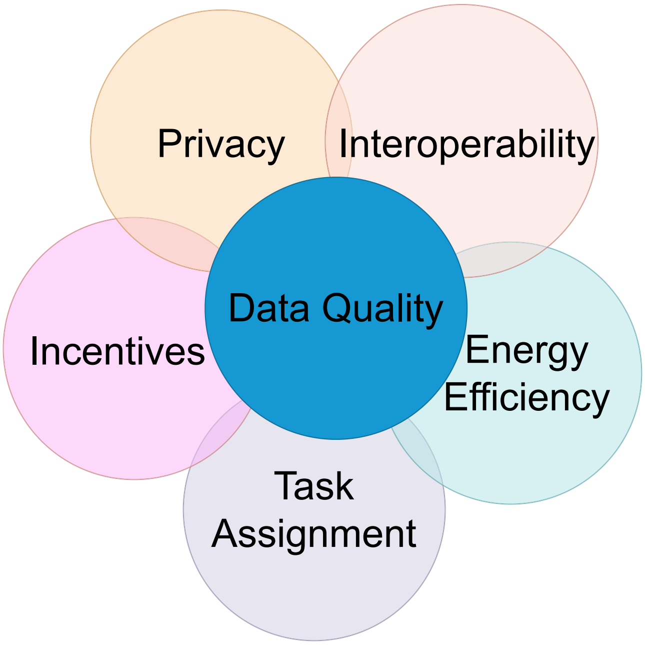

FIGURE 4. HCS challenges interdependencies with Data Quality.

IV. TASK ASSIGNMENT STRATEGY: AN UMBRELLA PROBLEM FOR DATA QUALITY PRESERVATION

Ensuring data quality and integrity is a vital and complex open concern that needs to be effectively tackled to facilitate the unimpeded advancement of HCS-based IoT systems. Data quality is a key factor for various HCS challenges including task assignment, energy-efficiency, user privacy, interoperability and incentive mechanisms, as shown in Fig. 4. Efficiently addressing these challenges is a prerequisite for HCS adoption, but trade-offs between different aspects should not be overlooked. In this section, we particularly focus on the interdependencies between HCS task assignment and data quality challenges, discussing on their interrelations and effects on the other challenges as well.

First, the data quality challenge in HCS-based systems is closely related to the task assignment process, which aims to identify the most suitable users, devices, and sensors capable of providing high-quality data. However, this process is complex as it requires selecting the appropriate participants to achieve diverse optimization objectives, encompassing maximum area coverage and high sensing quality, minimizing costs and/or ensuring a limited number of participants engaged in task execution.

The absence of sensing reports in specific sub-areas can diminish the overall data quality, and even potential report redundancy in other areas might not offset this deficiency, jeopardizing the knowledge extracted by HCS systems. While data collected from a small number of users may not be highly accurate, multiple sensing results for the same task provide more valid data. However, increasing the number of participants, does not inherently guarantee an improvement in the overall data quality [71]. In addition, data redundancy and diversity should be considered in optimizing task allocation taking into account users' behavior. For instance, users in close proximity might provide similar data, leading to data redundancy, or devices at the same location may possess varying sensing capacities, resulting in data diversity. Therefore, the behavior and the experience of mobile users have a significant impact on the quality of the data [24]. As the data quality of participants is initially unknown, some systems employ a learning approach, where Workers execute tasks for a few rounds and their gathered data is evaluated to determine their quality. The platform then recruits Workers based on the acquired knowledge of their qualities to enhance the overall quality [72].

Furthermore, task assignment and scheduling across multiple devices with varying sensing capabilities, resource availability and limitations imposed as well as the operational context may lead to higher or lower data quality. Enhancing data quality while concurrently minimizing the utilization of essential resources poses a challenging concern to address. Different types of sensed data can be generated for the same purpose, each with varying data quality and necessitating different resource consumption levels. Current energy efficiency solutions adopt low duty cycling for sensors that produce high quality data (requiring significant energy) and activate different set of sensors according to the devices' available energy levels to produce data with lower quality, so as to preserve energy consumption levels [73]. Specifically, many tasks necessitate specific device sensors to collect the required data. In such situations, users with devices lacking the required capabilities may be excluded from participating in the data collection process [74]. Many systems [74], [75] pre-define a required energy threshold and respectively check the energy levels of the participants' smart devices. If the energy levels exceed the pre-specified threshold, the user can participate in the data collection; otherwise, the participation is declined. Therefore, techniques that achieve an optimal balance between data accuracy and energy consumption are necessitated.

Also, to ensure data quality, HCS systems should consider users' experience and qualifications, preferences, trustworthiness in contributing valid and high-quality data, their current location and mobility, travel distance, current context of operation, dynamic conditions experienced by the mobile devices and the number of tasks each participant is currently handling. Specifically, different users may participate in various types of tasks that necessitate different domain-specific knowledge or expertise.

However, most of the HCS systems often overlook the manner in which a user executes a task and the sequence of steps taken to sense data, which can significantly impact data quality [60]. As a result, in an attempt to eliminate the impact of non-familiar participants and select the most suitable participants, some systems create user profiles based on personal information such as preferences, interests, and activities or data retrieved from social networking applications such as interests, expertise and education [76]. Also, the task assignment mechanism may constrain the assignment of tasks to users that have already reached a maximum workload set so as to minimize the delay resulting from the execution of multiple tasks at the same time [77]. Moreover, users located outside the specified area may excluded from the task assignment process [78].

As users' contributions may be intentionally inaccurate/falsified so as to either save their own resources and/or degrade the usefulness of the extracted knowledge, task assignment can help reduce vulnerabilities, risks and potential attacks in HCS systems by considering users' trustworthiness based on their past task completion history [33].

Once the reward is involved, participants become susceptible to manipulate the system by submitting false information. Therefore, truthful incentive mechanisms should be designed and complement task assignment not only to promote users' participation and ensure the quality of the collected sensing data, but, also, to avoid mobile users manipulating the HCS system [53]. It should be noted that, considering the design of the incentive mechanism, HCS systems should maximize data quality under budget constraints or minimize the total budget, while ensuring data quality. Thus, incentive mechanisms should balance both the requirements of the participants and the platform budget constraints [83], [84].

Lately, reputation mechanisms have been proposed in the context of HCS systems so as to a) identify the most reliable users to be involved in specific sensing tasks (e.g., [34]) and b) weigh the significance of collected data according to the reputation of each participating entity, waiving thus the effect of incorrect data and improving the overall trustworthiness of data contributed by the crowd [59], [85]. This way the overall data quality / integrity is enhanced. Also, systems have been proposed (e.g., [86]) estimating the reputation score for each device used, which in essence quantifies the accuracy and functionality that is expected from the smart device (sensor's accuracy).

As shown in Table 3, most systems relate data quality to task assignment to select participants who will produce high quality data. Therefore, they consider factors such as the user experience, willingness, reputation, as well as his/her location and travel mode, which are also important to consider when allocating tasks, as many location-based HCS tasks

TABLE 3. Summary of data quality related literature.

	Experience	User assignment	Reputation	Quality Evaluation	Device context	Travel mode	Incentives	Contextual factors	Performance Metrics
[27]			✓	Similarity score			✓		Impact of user behavior
[29]		✓		Battery level, distance, sensors' quality	✓			✓	Impact of residual battery level, distance, sensors' quality
[31]		✓	✓	Similarity score				✓	Time of aggregation process, reputation
[33]		✓		Distance between data and ground truth			✓		Impact of number of Workers, budget
[48]			✓	Distance between data and real data				✓	Accuracy of correctly detecting false/normal data
[50]		✓		Distance between data and real data			✓		Impact of Workers number, human behavior, Workers' cost
[58]		✓	✓	Distance between data and ground truth			✓		Impact of the historical performance of the Worker
[59]	✓		✓	Similarity score					Impact of Worker kind (trustworthy, inexperienced, malicious)
[60]	✓	✓		User experience, device context, coverage, sensed time	✓				Impact of user experience, device context, coverage, sensed time
[61]		✓	✓	Distance between data and ground truth					Impact of error, number of Workers
[79]	✓	✓	✓	Based on application					Social welfare
[80]				Distance between data and ground truth	✓		✓		Error
[81]		✓		Distance between data and ground truth	✓	✓			Impact of the selected points of interests
[82]				User willingness, regional preferences	✓				Impact of the coverage

require sensing data with different attributes, e.g., travel mode. In addition, they consider the device context, such as resource availability and sensor capabilities, in order to achieve data accuracy. Lastly, most systems measure data quality by comparing the answers to the same task from different Workers to filter out irrelevant data and reward users for contributing according to data quality.

Preserving data quality and ensuring user privacy are crucial objectives in HCS systems. As already mentioned, through data submitted by users, information about the routines and daily habits of users can be extracted. This fact negatively affects the participation of users, leading, thus, to the degradation of the quality of the collected data. A commonly adopted solution for privacy preservation is to provide anonymity to participants, linking users to their actions; in such a case though trustworthiness evaluation is constituted a very difficult process [87]. Thereby, anonymous users may send submit quality or even fake data to the platform. Recently, blockchain has been proposed to be integrated into HCS systems, enabling users who do not fully trust each other to make transactions [88], [89], allowing for data sharing and storing between a large number of nodes in a cryptographic manner.

An optimal participant selection promotes data quality prior to data collection, aggregation, and analysis. However, HCS systems must consider the challenge of data quality at every stage of their lifecycle to provide a high level of information and services. During data aggregation and processing, systems should efficiently handle noisy, obsolete and/or inconsistent data [59]. At the data processing stage, machine learning and data mining techniques can be used to filter data and improve accuracy. Local processing could undertake partly this task so that the data transmitted and uploaded to the HCS-based system is only of improved quality. Additionally, provided data quality could be enhanced after its comparison/integration with reliable related data collected from already deployed sensor networks in the area [57], while the effect of inaccurate data or data originating from untrustworthy participants should be mitigated. Finally, data should be reused, while its quality is guaranteed. One of the most common definitions of data quality is its fitness for the purpose of use [24]. As sensory data has both multiple uses and users, data for one use or user may be or not be of sufficient quality. Thus, sustaining the desired level of data quality for the considered scope is of utmost importance.

V. REPUTATION MECHANISMS IN HCS-BASED NG-IOT SYSTEMS

In this section, we define trust and reputation, elaborating thereafter on the factors that should be considered when designing a reputation mechanism for the HCS-based NG-IoT systems.

A. TRUST, REPUTATION AND RELATED MECHANISMS

Trust refers to the belief that one entity has in the competence and benevolence of another entity to act honestly, reliably, correctly, and dependably [90]. Trust is generally considered to enhance data quality/integrity in the presence of misbehaving entities [91]. Trust mechanisms help establish trust relationships among the parties, allowing them to automatically adapt their behavior based on different levels of cooperation. In the literature, the most common soft approach introduced for building trust is reputation mechanisms. Reputation constitutes a metric to evaluate the trustworthiness of participants and predict their future behaviors.

In the context of HCS-based NG-IoT systems, reputation mechanisms are crucial for establishing trust among participants. The reputation of a Worker is dynamically updated based on the quality of their contribution. When Workers provide high quality data, their contribution is deemed more valuable, resulting in a positive impact on their reputation within the system. Conversely, low data quality negatively affects Worker's reputation, reinforcing the importance of maintaining high quality data provisioning to foster trust among participants. Trust of the participating Worker in HCS systems may be a combination of personal, sensing, and social factors as shown in Fig. 5. Personal factors include the user's expertise [92], frequency of contribution [59], willingness to participate [74], and experience [34] in task execution. Users with higher expertise, more frequent contributions, greater willingness, and substantial experience are more likely to make valuable contributions. Sensing factors encompass attributes such as sensing cost [86], [93], sensor type and capabilities, and travel mode/profile [94]. These factors significantly impact the quality of user contribution. For instance, a picture or a video clip may provide better information compared to a text-only description. Additionally, the capabilities of sensors, along with the mode and the speed of travel, influence the quality of the submitted data, thereby affecting user contribution. Finally, social relations can be leveraged to enhance trust evaluation, mirroring human behavior in establishing trustworthy social communications [85]. The trust system can consider social relations between participants, such as friendship ties and their duration (long lasting friendship relations normally translate to a greater trust degree between two friends), the number / frequency of interactions and the interaction time interval (number of interactions and the time that has elapsed between two consecutive interactions among participants is a good indicator of the strength of friendship ties).

Trust and reputation have been well-studied terms in a multi-disciplinary context, while various models and systems have been developed in many information and communication technologies related research areas. Indicatively, reputation mechanisms have been implemented in various domains, including e-commerce systems (such as eBay, Amazon, etc.) [95], [96], supply chains [97], ad-hoc networks, mobile ad-hoc networks (MANETs) & vehicular ad-hoc networks (VANETs) [98], [99], [100], peer-to-peer networks [101], [102], wireless sensor networks (WSN) [103] and IoT [104], [105], [106], among others. These mechanisms highly depend on the underlying model and related mechanisms for collecting and analyzing trust-related information, forming reputation ratings and taking actions when misbehaving entity is identified. Concerning the information collection, there are schemes that utilize only information collected based on the participants' personal observations and experiences with participants in the system in order to evaluate their behavior, while some schemes exploit also feedback acquired from other participants in the system concerning their own experiences with the target participants under evaluation in the past (e.g., [40], [107]). The latter subcategory should cater for trustworthy feedback propagation/acquisition aspects (e.g., only entities with

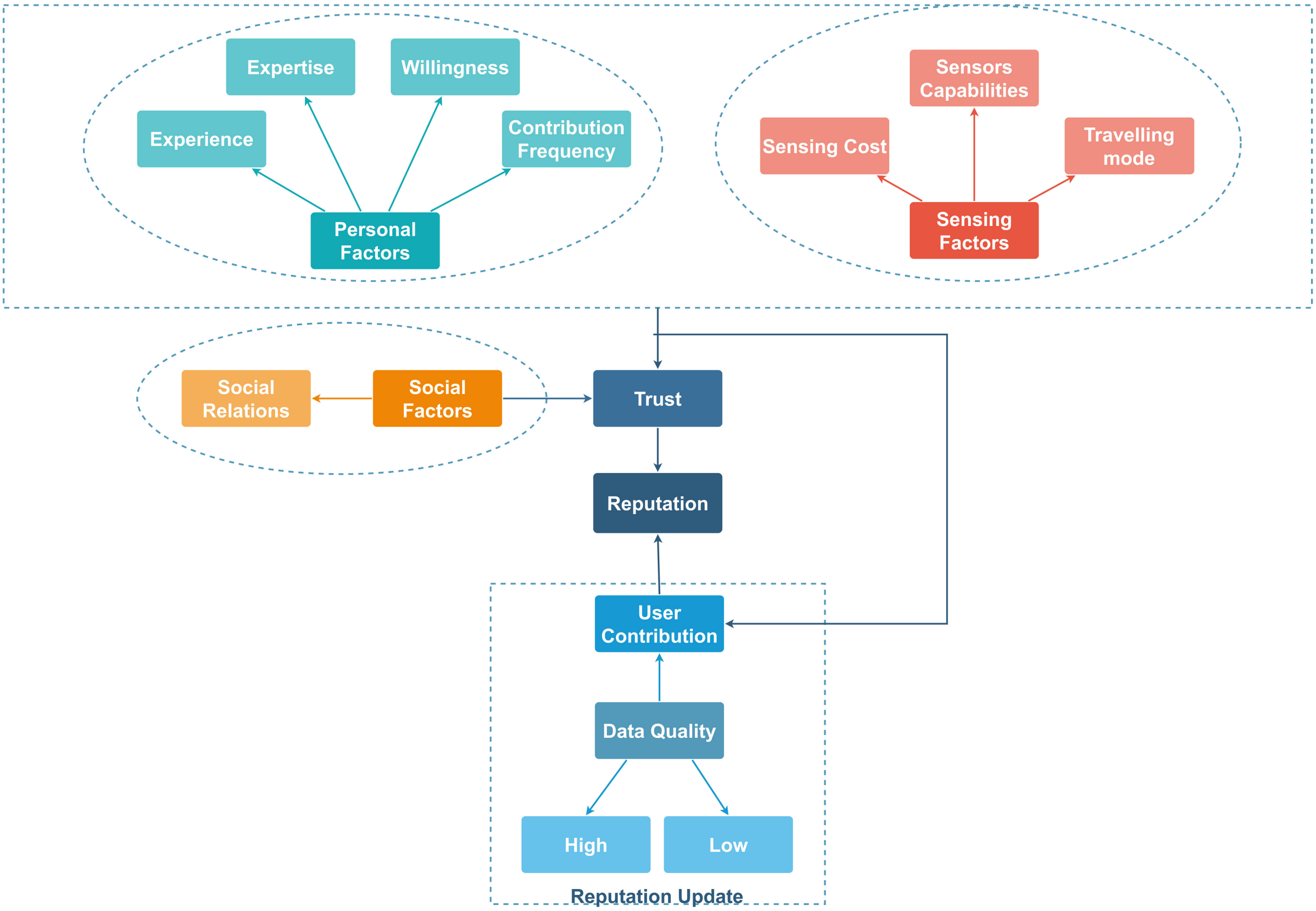

FIGURE 5. Factors Influencing Trust and Reputation.

good reputation scores can rate others in [108]). The formation of reputation rating component should cater for defining a simple, yet effective model to quantify the reliability of each system's participant [109]. Different aspects could be considered in this regard (e.g., the initial reputation value attributed to each system participant that may be increased / decreased following his/her behavior in the system, his/her willingness to cooperate / provide services to others system's participants, the interaction timeliness so that recent events have a greater significance on the reputation value estimation [110]). Furthermore, some related research works integrate techniques to isolate misbehaving participants, i.e., those that show a low reputation value. Depending on the system, misbehaving participants may be permanently excluded or given the opportunity to re-access the system if they exhibit good behavior in the future. In any case, reputation mechanisms are effective in detecting selfish / malicious users in a fast ad effective manner, especially when reputations are formed based on collaborative manner; thus, they enhance system security and the quality of services. However, a common weakness of the proposed systems is that reputation computation focuses on service quality assessment and may not consider malicious / selfish behavior of otherwise competent / qualified participant [59]. In some systems, reputation ratings are utilized to define proper economic incentives, where participants with high reputation values receive higher rewards. This helps increase participants' enthusiasm for offering high-quality services to the system [40]. In general, reputation systems play a substantial role in systems where limited knowledge about users could potentially lead to undesirable situations regarding the reliability of the information they provide [111].

B. REPUTATION FORMATION

Reputation estimation is primarily based on observations, past experiences and other entities' views/opinions [113]. Thus, reputation information may be based on the direct experiences of the Requestor, who acts as the evaluator entity, regarding the behavior of the Worker (the target entity under evaluation). This factor is referred to hereafter as first-hand information. Reputation information concerning the behavior of the target Worker can be provided to interested Requestors from other parties (Witnesses) who have past experience with the target Worker, to be taken into account during reputation rating formation. This factor is referred to hereafter as second-hand information. The reputation estimation may be based on a combination of both types of reputation information collected.

In this way, the Requestor would consider his/her personal trust perception of the participant and the reputation score(s) of the participant calculated and shared by the Witnesses (and/or by the platform) according to the quality of his/her contributions. However, when direct experience is sufficient, the effect of second-hand information may be less [53]. Reputation estimation exclusively based on direct experiences and observations increases the time required for identifying a misbehaving participant. On the contrary, considering truthful second-hand information, the rating estimation process will be faster; thus, allowing for earlier identification of malicious and selfish participants. Nevertheless, honest behavior cannot always be ascertained. Thus, the reputation of the witnesses regarding their contributions / reports given on their experiences with other entities must be considered, so that reports originating from honest witnesses have a greater impact on the formation of the target Worker's reputation rating, while reports disseminated from untrustworthy witnesses have a smaller impact. Also, reputation estimation exclusively based on second-hand information may prove useless if the propagated information is inaccurate. In the light of the aforementioned, the selection of truthful witnesses is considered of utmost importance. At this point it should be noted that a truthful Requestor or Worker does not necessarily lead to a truthful Witness, considering that trust is context specific.

Furthermore, when dealing with second-hand information regarding the propagation of reputation ratings, the following considerations merit attention; a) to which Requestors should participants' reputation be propagated, b) when and how often participants' reputation should be propagated (e.g., upon detecting a misbehaving entity, at predefined time intervals, or after a certain number of tasks have been completed) and c) what kind of reputation related information should be shared (e.g., positive and/or negative reputation information, reputation scores derived from Requestors' experiences, aggregated reputation scores corresponding to specific time-periods or tasks, an alert message identifying a misbehaving entity).

A reputation system can be centralized, decentralized, or hybrid. In a centralized system [48], the platform will undertake the responsibility of estimating and updating reputations for all its members. The platform receives and evaluates the participants' contributions to estimate a reputation score for each participant. As a first step, the platform checks if the Worker has completed the task or if the task remains unsolved [75], and if data is sent within the required response time; subsequently, it checks and evaluates the quality of the data submitted. One of the most commonly adopted solutions in this respect is by comparing the user's response with the majority of responses received [75]. Other techniques could also be exploited as shown in Section III-A.3 (Data Quality Evaluation).

Most reputation mechanisms aggregate the responses of all users assigned with the same sensing task, using a majority rule, comparing the data with the most frequent and popular answers from the participants with a similarity score to detect and filter out inaccurate data as well as to detect "anomalous" users, whose sensory readings deviate significantly from the group consensus [27], [48], [59]. Also, users' locations can be taken into account as users in close proximity may have similar sensing data [112]. The quality of a submitted answer is considered proportional to its similarity to other answers submitted for the same task, assuming that honest Workers will have similar submissions. Also, the Requestor will be more inclined to believe the truthfulness of an answer if multiple participants submit the same response [114].

In a decentralized system, each Requestor runs a local instance of the reputation system [53]. The Requestor receives participants' contributions, evaluates them, and calculates reputation scores for each participant. When requested, each Requestor shares the calculated participants' reputation scores while also considering the other Requestors' reputation scores for the target participant, acting as Witnesses. Hybrid systems have also been suggested, combining elements and characteristics of both centralized and distributed reputation systems, allowing the platform and each Requestor to individually calculate/vote on the participant's reputation value and share reputation-related information [86], [93].

One important issue in reputation rating formation is the initial reputation value assigned to new users who wish to participate and are unknown to the system, which is known as the cold start problem [91]. Specifically, initial reputation value should be carefully chosen to give new participants a chance to be selected as Workers and not be rejected by the system. However, it will not constitute an incentive for bad behavior, adopting new identities and whitewashing thus previous misbehavior [91].

A commonly used approach is to assign neutral / default reputation values to new users when enter the system. Mostly the reputation value range is between 0 and 1, and the default value is usually within the range of 0 to 0.5. For example, in [92], every user is associated with a reputation score that is initialized to a default value for new users. Similarly, in [74], the initial reputation value of each participant is set to neutral to provide them with an opportunity to be selected for their first task. In [48], the authors suggest an initialization phase for reputation training aimed at acquiring basic insights into participants' reputation. Within this phase, the distance between each sensory data piece and real-world measurement is computed.

C. REPUTATION UPDATE

Once participants are selected for the sensing campaign, they contribute sensing data and their reputation is updated after the completion of each task based on the behavior they have exhibited as shown in Fig. 6. The Workers' reputation needs to be updated many times so as to make the estimated reputation more precise. In a centralized architecture, the platform checks the quality of the contributed data to update the reputation of each Worker. In a decentralized architecture, the requestor assesses the quality of the provided answer, while a hybrid architecture combines both approaches.

According to perceived data quality, the user's reputation increases in case of a high quality data contribution and decreases if the user contributed low quality data [48], [55]. The calculation formula for reputation can be relatively simple, involving the aggregation of the new outcome expressed as a standard (upwards or downwards) reputation value modification with the most recent reputation value available. More complex formulations can also be exploited to discourage intentional misbehavior. For example, reputation may be slightly increased after receiving a high quality contribution, while, at the same time, largely decreased after receiving a low data quality contribution [74] (e.g., by using logistic function [27]) promotes a consistent truthful data sharing behavior. Additionally, it is important that reputation updates are primarily based on recent events to ensure that a user's behavior is accurately reflected in their reputation score; in order to consider the time effects, assigning greater weight to the most recent users' interactions is imperative. This has been implemented in some of the proposed systems (e.g., [27]).

The newly attained reputation value will replace the old one in the next update process. A high reputation score signifies that the user has consistently contributed high-quality data in the past, which consequently implies that their data is likely to remain accurate and trustworthy in the future. Workers' trustworthiness should be taken into account, besides the task assignment process for the selection of the most suitable set of participants for each sensing task, in the data collection and evaluation process, so as to outweigh the effect of a report originating from an untrustworthy Worker [115].

D. PUNISHMENT AND FORGIVING MECHANISM

Most systems do not discriminate between inaccurate data, intentionally or unintentionally provided. However, a user who unintentionally contributes low quality data due to factors like faulty sensor or poor communication channel conditions should not be severely punished (i.e., the reputation value should not be largely decreased). Similarly, high reputation participants may not always contribute high quality data [59]. In [48], an algorithm is used to a) identify and filter out false data and b) identify dishonest users who deliberately contribute low quality or incorrect data, decreasing thus their reputation value. In [59], the authors choose the density-based outlier detection algorithm to identify corrupted data from abnormal participants (inexperienced or malicious) with respect to normal one's accounting for the majority of total participants.

Identifying users who intentionally provide inaccurate information may constitute a very difficult process. Malicious users may strategically alter their behavior over time to maximize their benefit while covering their true behavior. For example, a participant may first submit correct data to build a high reputation and then randomly submit false sensing data or exhibits an oscillating pattern (contributing high data quality for a period of time and low data quality for the next period and so on, or even adopting a random pattern) to bypass reputation-based detection techniques [116]. Attacks such as "On-off" attacks, Sybil, and collusion attacks are possible [117]. The number of the transactions (tasks) the participants are involved in and their respective value could be taken into account for potential misbehavior identification, considering that the user is inclined to strategically misbehave a few times when the respective transactional value (and therefore his/her own benefit) is big [93], [118]. Users identified as deliberately providing false / inaccurate information should be severely punished based on the frequency and severity of erroneous data [53], excluded and isolated from the system if they have reached a certain threshold of misbehavior [114]. However, a forgiving mechanism should be in place to allow misbehaving entities to re-enter in the system if they exhibit good behavior [55]. According to the information discussed above, two summarized tables provide a comparison of the related papers in Table 4 and Table 5.

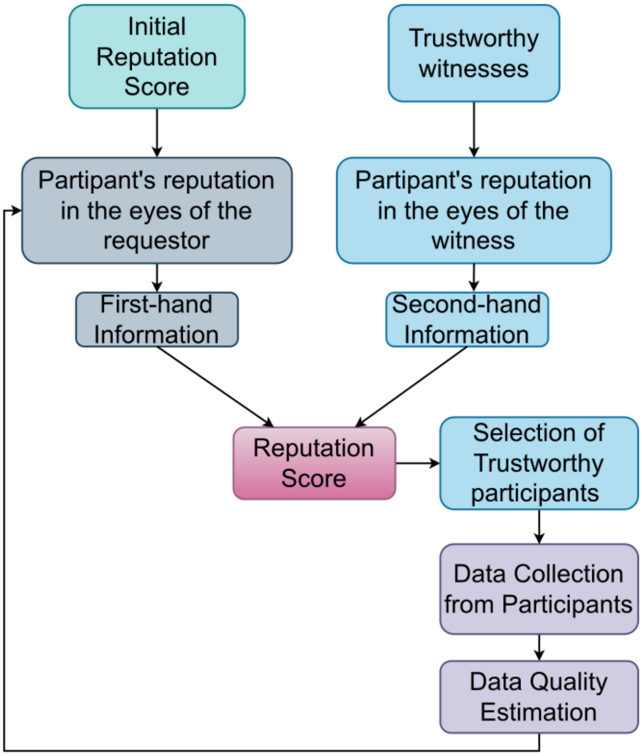
Initial Reputation Score
Trustworthy witnesses
Partipant's reputation in the eyes of the requestor
Partipant's reputation in the eyes of the witness
First-hand Information
Second-hand Information
Reputation Score
Selection of Trustworthy participants
Data Collection from Participants
Data Quality Estimation

FIGURE 6. Reputation Formation & Update.

VI. BLOCKCHAIN-ENABLED HCS-BASED NG-IOT SYSTEMS

Recently, blockchain has gained popularity as a distributed, transparent and robust technology that secures, verifies, and records transactions in a safe, transparent, and timely manner [119]. Blockchain offers highly secured, authenticated and trusted services in various applications such as healthcare [120], e-commerce [121], finance [122], supply chain [123], military [124], transportation [125], VANETs [114], unmanned aerial vehicles (UAVs) [126] and

TABLE 4. Comparison of reputation systems.

	Data quality / Historical behavior	Initial reputation	User Experience	Voted reputation	Response Time	Unfinished Task	Reward
[27]	✓						✓
[48]	✓	✓					
[55]	✓	✓					✓
[59]	✓		✓				
[74]	✓	✓			✓		
[75]	✓					✓	✓
[85]	✓	✓	✓	✓	✓		
[86]	✓	✓		✓			
[92]	✓	✓					✓
[93]	✓	✓		✓			✓
[112]							✓

TABLE 5. Comparison of reputation systems.

	Recent Interactions	Similarity Score	Malicious Users	Unintentionally low quality	Reward / Penalty Policy	Participation Frequency
[27]	✓	✓			✓	
[48]		✓	✓		✓	
[55]			✓		✓	
[59]		✓	✓	✓	✓	✓
[74]					✓	
[75]		✓			✓	
[85]					✓	
[86]			✓			
[92]			✓		✓	
[93]			✓			
[112]		✓			✓	

IoT [137]. The decentralized nature of blockchain technology makes it a reliable platform for replacing centralized servers in different applications. Blockchain technology ensures that user data is encrypted and secure, and only authorized users can access it. Moreover, the use of blockchain technology offers improved security by preventing the leakage of users' identities and data, which is a major concern in traditional centralized systems [22], [58]. Furthermore, the use of blockchain technology prevents unfair incentives, as all transactions are transparent, and any suspicious activity can be easily detected and prevented. On the whole, blockchain technology offers highly secure, authenticated and trusted services in various applications, making it a popular choice for businesses and organizations looking to improve their security and transparency. As presented above, a key feature of HCS-based systems is the centralized platform, which is used as a bridge for the communication between Requestors and Workers as well as for collecting, storing and analyzing the data sent, while also being responsible for the determination and payment of rewards. However, centralized architecture design suffers from failures and attacks and may lead to privacy leakage, as various malicious users may seek access to the platform for the purpose of stealing, processing, replacing data and harming the benefit and privacy of HCS users.

By integrating blockchain into HCS-based systems' architecture, security is improved; the centralized platform is replaced with a distributed and reliable blockchain platform [31], thereby reducing the risk of single point failure, privacy breaches and data tampering, easily verifying data integrity through digital signatures and hash values [88] and guaranteeing the trustworthiness of the data [114].

The main parties involved in a blockchain-enabled HCS-based NG-IoT system are Requestors, Workers, Blockchain Network and Miners. Miners a new role introduced in support of the blockchain and are responsible for the validation of transactions and potentially for the verification of the quality of the large amount data collected by Workers, followed subsequently by the block generation process [30]. Blocks are a continuously growing sequence of transaction records that are interconnected through the cryptographic hash of the preceding block. Once a block is written to a blockchain, the information cannot be changed. Blockchain-based applications use consensus mechanisms to verify new transactions and add them to the blockchain. The consensus mechanism establishes the conditions for reaching agreement on the validity of new blocks between participating nodes. The most used consensus mechanisms are namely Proof of Work (PoW) and Proof of Stake (PoS) [138]. PoW wastes a large amount of computational power as it requires all miners to attempt to validate transactions.

On the other hand, Proof-of-stake (PoS) is a scalable and lightweight alternative to PoW. PoS uses randomly selected miners to validate transactions. Proposed blockchain-based HCS applications perform a miner recruitment process to select random miners [139] or exploit all active Miners or the Miners who are closest to the Workers and Requestors [127]. All the selected miners verify every transaction. Also, there are many other consensus mechanisms that can be used, such as Practical Byzantine Fault Tolerance (PBFT), Proof of Capacity (PoC), Proof of Authority (PoA), Proof of Elapsed Time (PoET), Proof of Activity (PoAc), RAFT and Proof of Burn (PoB) [140].

The main workflow of a blockchain enabled HCS system is as follows. Initially, the Requestor publishes a task that contains explicit evaluation criteria for sensing data quality (such as the type, range and accuracy of data necessitated) and broadcasts the task information through the blockchain. Subsequently, the Requestor and the Worker(s) selected by the related *Task Assignment Strategy* reach an agreement by signing a smart contract on the blockchain, which includes a set of agreed-upon rules. Also, the task requirements and verification rules are embedded in smart contracts.

Thereafter, the Workers and Miners receive their rewards automatically and mandatorily through smart contracts. In general, Miners receive rewards for executing smart contracts. Also, the Miners can verify the payment transactions to the Workers to avoid potentially unfair treatment [30], relieving Workers from the fear of receiving unfair rewards if the sensing data meet the requirements set. In these systems, usually only the Requestor makes a deposit to determine the rewards; however, recent proposals involve Workers also making a deposit to participate in tasks, aiming to prevent the system from many attacks such as denial-of-service (DoS), Sybil, "free-riding" and "false-reporting" attacks [138] as well as from malicious users who quit their tasks [136]. The deposit is returned to Workers who are not selected for specific tasks. If the selected Worker fails to contribute data on time or provide unsatisfactory data that does not adhere to the terms and conditions set in the smart contract, the Worker loses his deposit [114].

Based on the aforementioned, blockchain can tackle various HCS related problems and challenges, as shown in Fig. 7. Blockchain includes several attractive characteristics, such as decentralization, traceability, immutability, transparency, trust and auditability [140]. First, decentralized blockchain and tamper-proof smart contracts improve the reliability and security of HCS systems. Since no central authority exists, blockchain eliminates central servers, single point of failure and potential performance bottlenecks, thereby improving security, reliability and scalability [140]. As aforementioned, a blockchain network is based on nodes, where each node has its own copy of the ledger and can validate transactions before adding them to a new block. A majority of nodes must agree to approve a transaction before it can be added to the blockchain. In this way, control and decision-making are distributed evenly throughout a network so that bias and misjudgment are eliminated.

Furthermore, a smart contract promotes transaction security, enhancing the decentralized nature of blockchain applications. Specifically, smart contracts, as immutable codes, can permit and establish trusted transactions to be carried out among Requestors and Workers without the need for explicit trust connections with each other. A smart contract authenticates users and enables secure data sharing between them [141]. Moreover, there is no way to modify or alter the data in any block of information; data provided by a device can be identified, constituting data more accurate, reliable and transparent to store in a blockchain. The blockchain technology offers a reliable approach to trace transactions, therefore, nodes can easily verify and trace the origin of historical blocks. Also, this will allow all illegal and unauthorized actions to be traced [142]. Thus, blockchains' immutability ensures the high quality of data [143], auditability and the reliability of HCS.

Lately, blockchain technology has been integrated with reputation mechanisms [144], [145], [146], [147], [148], [149], [150] for the decentralized management and storage of reputation values [151]. In this way the security of the systems is enhanced, as reputation values cannot be modified [152], and any updates to the reputation values can be tracked and viewed by all entities [153]. Additionally, the integration of reputation mechanisms with blockchain technology ensures that reputation values cannot be manipulated by a single entity, making them fairer and trustworthy.

In addition, blockchain supports anonymity; this way, participants' private information can be protected when participating in the sensing task, ensuring that the user's identity and privacy are not compromised. Therefore, the blockchain will provide a secure platform for HCS systems. A blockchain-enabled crowdsensing system can evaluate sensing data quality based on the Requestors' requirements, utilizing smart contracts for the verification process. Furthermore, a deposit-based mechanism ensures fair transactions between Workers and Requestors and

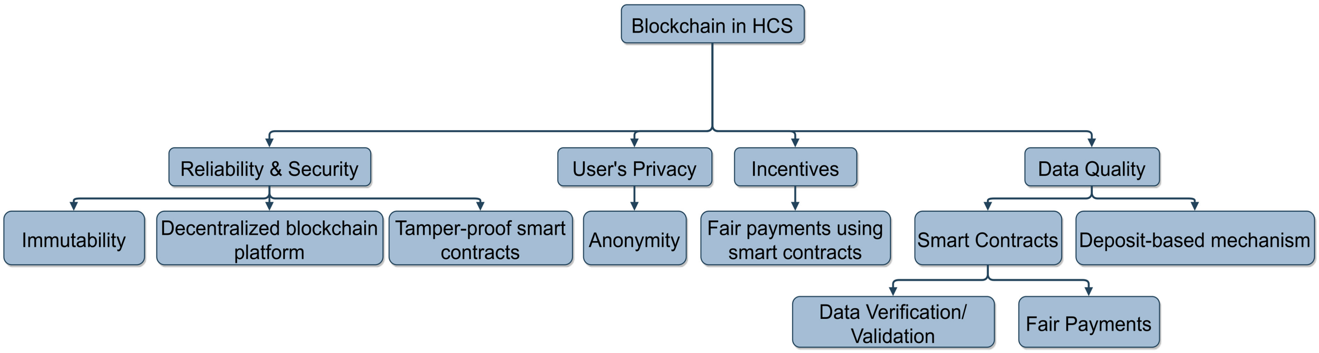

FIGURE 7. **Blockchain benefits in HCS.**

addresses adequately the problem associated with selfish and/or malicious Workers who do not submit qualified data or even leave the task uncompleted. Finally, the blockchain-based incentive mechanism encourages users to submit high quality data, raises their enthusiasm and satisfies the requirements for truthfulness and fairness.

Several existing studies have proposed blockchain-based human centric systems to improve data reliability and enhance privacy and security. Specifically, in [128], the authors propose a Blockchain architecture that validates participants' contributions by considering their historical data quality scores and a behavioral analysis based on the reliability scores of participants for the detection and prevention of fake sensing activities in HCS. This architecture leverages miners to ensure the validation of the collected information. In [134], a blockchain-based crowd-sensing trust management mechanism is proposed to evaluate the credibility of reports and the trust of participants, while preventing the tampering of trust values by malicious users. In [136], the authors propose a decentralized blockchain-based crowdsensing framework to achieve trustworthy data trading and fair rewards according to the data quality of the Workers. In [129], the authors present a reputation management scheme enhanced by blockchain to identify malicious users, preserve users' privacy and eliminate single point of failure in crowdsensing technology. Reference [130] proposes a blockchain privacy-preservation crowdsensing system, to protect the privacy of Worker locations and the identity of Workers. Also, in [89], robust crowdsensing model leveraging blockchain for preserving location privacy is proposed to avoid repudiation and tampering of information and protect the privacy of Workers' locations. In [131], the authors propose a blockchain-based location privacy protection incentive mechanism to ensure that data is not tampered with by others and protect the user's privacy information, offering specific incentives to encourage user engagement in sensing tasks. In [135], the authors propose a blockchain-based secure, interactive and fair HCS to alleviate centralized issues, prevent location privacy leakage, select qualified participants and achieve fair reward.

In [127], the authors propose a blockchain-based HCS framework that preserves participants' privacy and enhances the security of both the sensing process and the reward allocation through the utilization of miners and smart contracts. In [30], the authors propose a privacy-preserving blockchain incentive mechanism wherein verifiable data quality evaluation by miner can eliminate the security and privacy issues caused by a central authority and to encourage users to submit high quality sensing data. Also, they use a signcryption technique to prevent miners and other adversaries from violating users' privacy. In [132], a decentralized blockchain-based HCS framework with smart contracts is proposed to solve the single point of failure problem and the trust issue. In [61], the authors propose a trustworthy and privacy-preserving scheme for selecting Workers in blockchain-based crowdsensing while guaranteeing reputation privacy. In [133], the authors propose a decentralized crowdsensing architecture built upon blockchain technology which will help improve the attack resistance and protect individuals' privacy. In [31], the authors integrate the blockchain and edge computing in the HCS scenario to construct a privacy-preserving reputation management scheme in order to resist malicious users. Additionally, they use a novel consensus algorithm, Proof of Elapsed Time (PoET), that is Central Processing Unit (CPU)-efficient and efficient in dealing with large networks.

Based on the analysis provided, Table 6 and Table 7 summarize the key features of the related papers in Blockchain-based HCS systems. Most works address security issues associated with centralized servers in traditional HCS applications [132], [133], protecting privacy [30], [31], [61], [89], [127], [129], [130], [131], [133], [135] (including sensor data, personal information, location, and reputation scores), as well as ensuring fair incentive systems [30], [127] and trustworthy Worker selection [61]. Specifically, numerous techniques are proposed to protect user privacy such as anonymity [30], [89], [127], [130], encryption [61], [129], [133] and digital signature [133] as well as verifiable [129] and additive secret sharing [31]. Many works utilize the reputation score of a participant as a screening indicator of reliability for trustworthy Worker selection, where only participants with high reputation score are assigned tasks [31], [61], [127], [129], [133], [134]. Furthermore, some proposed schemes, in order to

TABLE 6. Comparison of blockchain-based HCS systems.

	Main Goal	User Privacy	Location Privacy	Blockchain	Distributed	Consensus	Reputation
[30]	Privacy-preserving incentive mechanism	Anonymity		Public	✓		
[31]	Privacy-preserving reputation management	Additive secret sharing		Public	✓	PoET	✓
[61]	Privacy-preserving Worker selection	Encryption		Consortium	✓		✓
[89]	Location privacy-preserving	Anonymity	✓	Public	✓	PoW	
[127]	User privacy/secure reward allocation	Anonymity		Public	✓	PoW	✓
[128]	Detection of fake sensing			Not Defined	Not Defined		
[129]	Privacy-preserving reputation management	Encryption & verifiable secret sharing		Public	✓		✓
[130]	Location privacy-preserving	Anonymity	✓	Public/Private	✓		
[131]	Location privacy-preserving incentive mechanism		✓	Public	✓		
[132]	Decentralization, incentive mechanism			Public	✓	PoW	
[133]	Decentralization, user privacy, incentive mechanism	Encryption & digital signature		Consortium	✓		✓
[134]	Trust management			Not Defined	✓	PoW & PBFT	✓
[135]	Location privacy-preserving, fair reward		✓	Private	✓		✓
[136]	Trust management, avoid malicious users, support large number of users			Public	✓		

encourage Workers to contribute their own sensing data, offer appropriate incentive mechanisms that comprehensively consider factors including data quality [30], [61], [89], [127], [128], [130], [132], [133], [135], participant's reputation [127], [133], location [130], participation level [135] and bidding [133]. However, most studies rewards or penalties based on the quality of the data provided by participants. Few works include users' reputation to reward estimation process. Lastly, many systems endeavor to resist to malicious users, such as Requestors and Workers. Only one system, however, takes into account that not all miners are trustworthy [30], but there are also malicious miners who attempt to steal data, imitate participants or maximize profits, as miners may verify and validate participants' identities, the sensing task, the sensing procedure, and the reward allocation. Also, a group of malicious miners may conspire to insert fake blocks of data into the blockchain [114]. This aspect should be properly addressed in blockchain-based HCS frameworks.

The main parties involved in a blockchain-based HCS system are Requestors, Workers, Blockchain Network and Miners. However, other entities are also considered in many works including *Task Distribution Center* [31],

TABLE 7. Comparison of blockchain-based HCS systems.

	Entities	Quality Evaluation	Malicious Users	Incentive Mechanism	Edge
[30]	Server, Participants, Miners, Blockchain	Miners	Miners	Quality-aware	
[31]	Requestor, Participants, Task Distribution Center, Key Distribution Center, Edge Computing Node	Requestor	Participants		✓
[61]	Requestor, Participants, Blockchain, Computing Servers	Computing Server	Participants	Quality-aware	
[89]	Requestor, Participants, Miners	Requestor	Participants	Quality-aware	
[127]	Requestor, Participants, Miners	Miners	Requestors/ Participants	Quality-aware and reputation-based	
[128]	Requestor, Participants, Miners, Reward Server	Miners	Participants	Quality-aware and Reliability-based	
[129]	Requestor, Participants, Blockchain, Key Distribution Authority	Blockchain	Participants		
[130]	Requestor, Participants, Miners, Agents	Miners	Participants	Quality-aware and location-based	
[131]	Server, Blockchain, Miners		Participants		
[132]	Requestor, Participants, Computing Oracles, Blockchain	Blockchain		Quality-aware	
[133]	Requestor, Participants	Requestor	Participants	Quality-aware, Reputation-based and bid-based	
[134]	Requestor, Participants, Blockchain, Evacuation Perception Unit	Evacuation Perception Unit	Participants		
[135]	Requestor, Service provider, miners, participants	Requestor	Requestor/ Participants	Quality-aware and participation-based	
[136]	Requestor, Participant, Blockchain	Blockchain	Requestor/ Participants	Quality-aware	

responsible for selecting participants for sensing tasks, *Reward server* [128], responsible for assigning rewards to participants, *Server* [30], [131], responsible for issuing sensing tasks and distributing rewards, *Computing servers* [61] and *Evacuation Perception Unit (EPU)* [134], responsible for calculating participant trust/reputation values, *Computing oracles* [132], trusted third-party entities that can perform computing tasks for smart contracts to avoid the high computational cost in blockchain, *Agents* [130] who work as miners in the private blockchain, *Key distribution authority / center* [31], [129], primarily responsible for distributing keys to preserve the privacy of users, *Edge computing nodes* [31] responsible for data aggregation and reputation update, *Service provider* [135], responsible for distributing keys and assigning rewards. In the related research literature, different entities have been proposed to undertake the task of data quality evaluation. Specifically, the Requestor, when receiving the Workers' response / sensing data, proceeds to data quality evaluation [31], [89], [133], [135]. The data quality evaluation process is handled by the Requestors in order to reduce pressure and computational cost in the blockchain nodes [135]. Alternatively, miners validate data quality based on the criteria uploaded by the Requestor [30], [127], [128], [130] or the Server / the blockchain evaluate data quality [61], [129], [132] according to specific criteria such as timeliness [132] or calculating the distance between observed data and estimated ground truth [61].

However, blockchain has not yet been fully exploited in HCS systems, and there are still challenges to overcome [154]. As a first note, related research literature aims at providing solutions to different sub-problems, not addressing systematically all interdependent to the data quality challenges. We believe that a blockchain enabled architecture should consider Worker selection, incentive mechanism provisioning, and data quality estimation. The most trustworthy and appropriate participants (as determined by means of their associated reputation score) should contribute to task execution, while data quality estimation should provide positive or negative feedback taken into account for reputation update, discriminating between intentional and unintentional misbehavior by Workers.

Additionally, as the requirements of sensing data are defined by Requestors, they can maliciously create abnormal smart contracts of requirements. Furthermore, since miners' opinion are used to verify the quality of sensing data, a

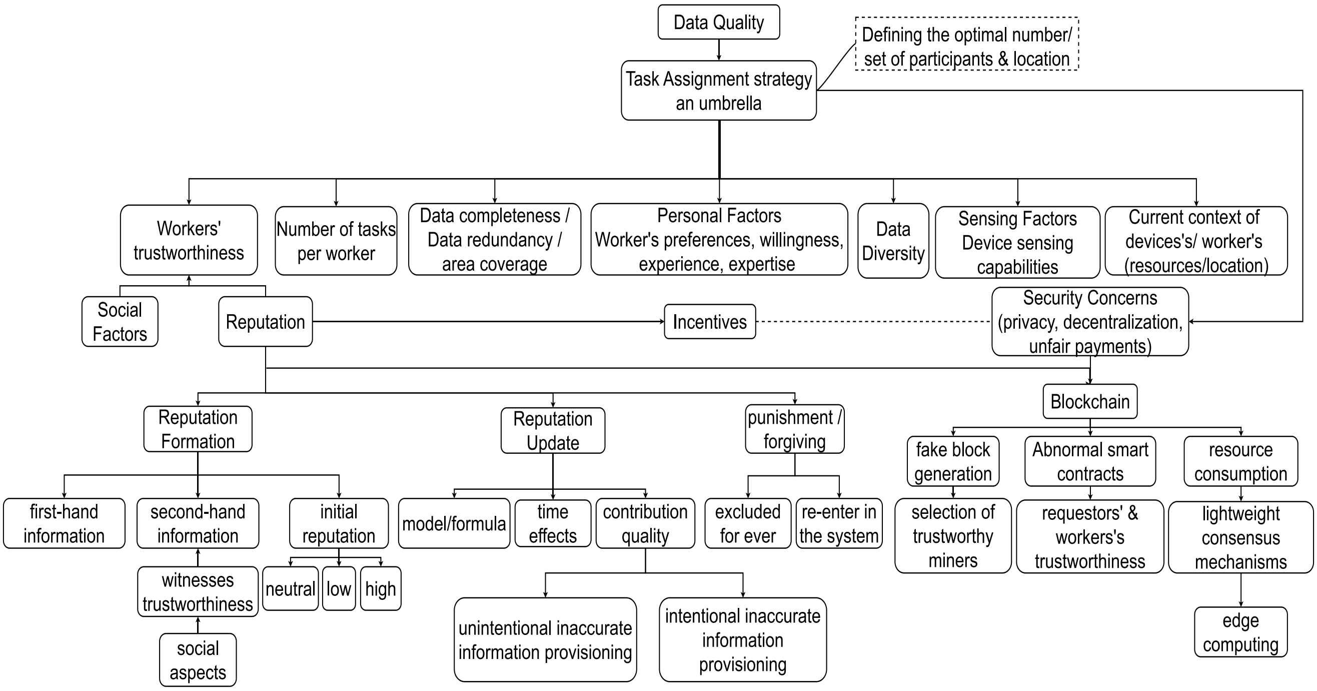
Data Quality
Task Assignment strategy an umbrella
Defining the optimal number/ set of participants & location
Workers' trustworthiness
Number of tasks per worker
Data completeness / Data redundancy / area coverage
Personal Factors Worker's preferences, willingness, experience, expertise
Data Diversity
Sensing Factors Device sensing capabilities
Current context of devices's/ worker's (resources/location)
Social Factors
Reputation
Incentives
Security Concerns (privacy, decentralization, unfair payments)
Blockchain
Reputation Formation
Reputation Update
punishment / forgiving
fake block generation
Abnormal smart contracts
resource consumption
first-hand information
second-hand information
initial reputation
model/formula
time effects
contribution quality
excluded for ever
re-enter in the system
selection of trustworthy miners
requestors' & workers's trustworthiness
lightweight consensus mechanisms
witnesses trustworthiness
neutral
low
high
unintentional inaccurate information provisioning
intentional inaccurate information provisioning
edge computing
social aspects

FIGURE 8. Taxonomy diagram of critical aspects of proposed solutions.

Miner may maliciously misrepresent the quality of the contributions. Usually, systems focus on participants' reliability, while neglecting miners' reliability. This challenge can be efficiently addressed by using a reputation mechanism to classify miners as reliable or unreliable. Both miners and Workers may provide incorrect data or not perform their task in order to disrupt the system intentionally or gain undeserved rewards. Therefore, the problem of unfair payment must be solved. Thus, an efficient solution should consider both current sensing data quality and the reputation of Workers/miners to promote consistent good behavior. Finally, due to the limited storage space and computing resources of mobile devices, applying blockchain directly to HCS-based NG-IoT systems is challenging. Blockchain consensus mechanisms have limited throughput and high resource consumption, and all the nodes must have a copy of all transactions [140]. In the light of the aforementioned, the authors in [155] propose the integration of edge computing and blockchain as a potential solution.

VII. BLOCKCHAIN ENABLED TRUST-AWARE REPUTATION MECHANISM COMPLEMENTING TASK ASSIGNMENT IN HCS-BASED SYSTEMS: THE WAY FORWARD

We believe that in order to efficiently tackle the challenge of data quality and ensure the quality of the collected data the solutions presented above should be exploited in combination as shown in the Fig. 8 in which all critical aspects of each solution are presented. The task assignment decision-making process in HCS plays a crucial in ensuring the quality of collected data. Several factors need to be considered when assigning tasks, to ensure that the collected data is accurate and reliable, including sensing factors (i.e., device / sensor capabilities, such as its computing and communication capabilities as well as maximum range and resolution), data completeness, data redundancy and data diversity, area coverage, context of operation, and number of tasks per Worker. Personal factors like user experience and willingness to participate are also important, as they can impact Worker efficiency and motivation. However, the trustworthiness of Workers is a critical factor that significantly affects the accuracy and reliability of collected data. Reputation is commonly used as a metric to assess Worker trustworthiness. In this context, reputation mechanisms play an important role in establishing and quantifying trust relations between Requestors and Workers, using reputation scores to assess the trustworthiness of Workers. Workers with higher reputation scores are generally considered to be more trustworthy. Using reputation scores, when assigning tasks in HCS, it is possible to improve the quality of the collected data, as the Workers selected for the task are considered more trustworthy and reliable. However, accurate reputation rating formation and updating are crucial to ensure that reputation values reflect a Worker's actual performance. The formation of reputation ratings can be impacted by several issues related to the collection of accurate and relevant information about a Worker's performance and the initial reputation value considered. Proper feedback mechanisms should be exploited, such as ratings and reviews, to gather information from the task Requestor and other trustworthy Requestors who have worked with the Worker in the past. Another issue with reputation rating formation is the initial reputation of a Worker.

When a Worker is new to a platform and lacks reputation or feedback, a neutral reputation score can be assumed initially and updated based on the Worker's performance over time. Also, reputation update can be influenced by factors such as time effects, reputation calculation models or formulas, and the impact of a Worker's contribution quality on the reputation value, properly discriminating between intentional or unintentional inaccurate information provisioning. In addition, it is important to have mechanisms in place that allow for punishment and forgiveness in HCS to ensure that Workers are held accountable for their actions. Punishment mechanisms can include lowering a Worker's reputation score when consistently providing inaccurate or unreliable data, excluded from the task assignment and/or excluded from accessing services provided. Forgiving mechanisms, on the other hand, can allow Workers to re-enter the system, being reconsidered in the task assignment process and allow them to improve their performance over time. Reputation and social factors are closely linked in HCS, as Requestors may tend to trust Workers with whom they have social connections, either in the physical or online world. Reputation mechanisms can be employed in synergy with social aspects and can help to mitigate the impact of social biases by providing an objective measure of trustworthiness. For example, Requestors may assign tasks to Workers with whom they have a social connection, even if there are other Workers who are more qualified or experienced. By using reputation scores as an impartial measure, requestors can make more informed and unbiased decisions when assigning tasks.

The integration of blockchain technology in HCS offers several solutions related to trustworthiness and security, as the decentralized and distributed network architecture of blockchain combined with cryptographic techniques for securing transactions and data has the potential to minimize the risk of a single point of failure and ensure the integrity and validity of information; however, several aspects should be considered in order to provide efficient solutions. Ensuring the trustworthiness of miners, detecting abnormal behavior of Workers and Requestors, preventing the generation of fake blocks, and designing effective consensus mechanisms. By utilizing a decentralized blockchain network, miners can be selected based on their reputation and performance, ensuring that only trustworthy miners are selected to participate in the network. Reputation scores can be recorded on the blockchain in a decentralized manner [156], creating an immutable record of a miner's performance and trustworthiness. This helps to prevent the participation of untrustworthy miners and reduces the risk of fake block generation. At this point, it should be noted that consensus mechanisms require a significant amount of computational resources. Effective consensus mechanisms are also vital in blockchain-based HCS. These mechanisms should be designed to be lightweight and efficient, considering the limitations of computational resources. Scalability and performance can be improved by leveraging edge computing, which offloads computational tasks to edge devices, reducing the burden on the blockchain network and enhancing its overall efficiency. Finally, Workers' and trustworthiness as quantified by reputation ratings, can play a role in preventing abnormal smart contracts in blockchain-based HCS.

This study proposes the integration of a reputation mechanism into the task assignment process to select the most reliable Workers for executing sensing tasks. Reputation information allows the classification and sorting of potential Workers based on their past performance in providing high-quality data. Additionally, an incentive mechanism is essential to motivate users to cooperate and contribute high quality data. The platform should appropriate reward each user with a proper payment, considering their contribution and reputation, in order to promote consistent good behavior. Furthermore, the integration of blockchain technology is recommended, as its advanced features (e.g., anonymity, immutability) provide a solution to the HCS privacy challenges and security concerns. By leveraging blockchain technology, security is improved in terms of ensuring data and reputation values' reliability [53], [143], preventing the disclosure of users' identities and data, and guaranteeing fair incentives to Workers.

In this section, we present the proposed architecture and provide details about the data quality calculation and Workers' reputation determination approaches utilized in our architecture. Fig. 9 illustrates our architecture, which includes the following main parties:

- *Requestors:* Each node can become a Requestor that publishes sensing tasks for the purpose of collecting related information; it broadcasts them through blockchain network.
- *Workers:* Workers utilize their smart devices (such as smartphones, tablets, wearables) to collect data related to specific sensing tasks. They submit sensing data to the blockchain. Since Workers may exhibit malicious behavior, their reputation is taken into consideration when selecting the appropriate set of Workers for executing each task. They receive rewards according to the quality of their sensing data.
- *Witness:* Witness was a Requestor in the past and provides her/his opinion based on her/his experience about a specific Worker, so as to be taken into account from Reputation Manager during the reputation calculation.
- *Miners:* Miners are responsible for verifying and validating each transaction (such as the sensing task, the sensing procedure and the reward allocation) and recording them on the blockchain.
- *Blockchain Network:* The blockchain network serves as a trusted crowdsensing platform where users' identities, sensing data, reputation and rewards are stored. Finally, smart contract automatically executes the reward process.

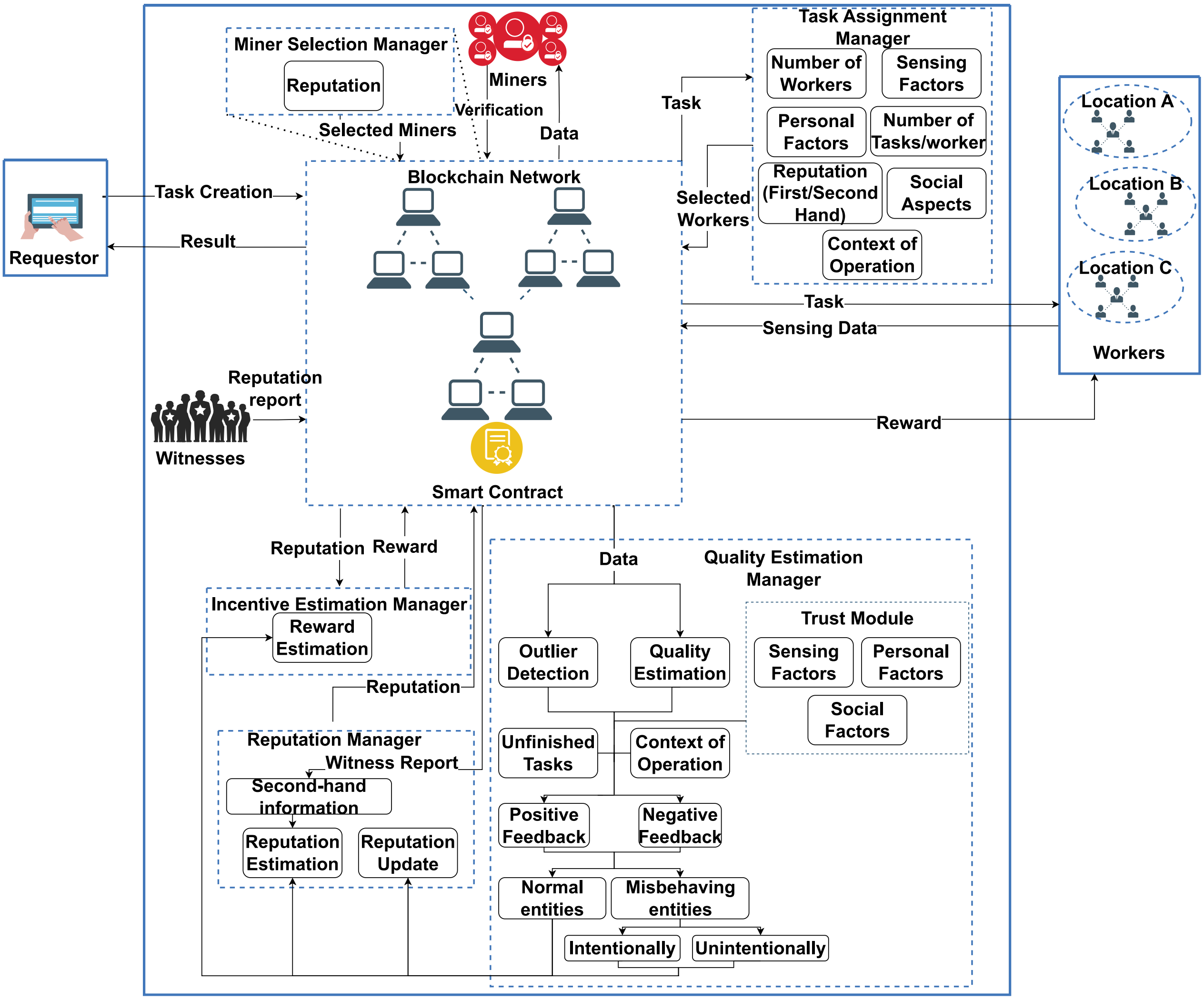

FIGURE 9. Blockchain-HCS architecture.

- *Task Assignment Manager:* Task assignment manager recruits an appropriate number of trustworthy Workers based on multiple factors including number of simultaneous tasks, Workers' reputation, social ties, Workers' experience, Workers' willingness, Workers' contribution frequency, sensor capabilities. This ensures the collection of high-quality data.
- *Quality Estimation Manager:* Quality estimation manager is responsible for evaluating the data submitted by Workers. It provides positive or negative feedback to the Workers based on the estimated data quality and discriminates between intentionally or unintentionally inaccurate data. This enables the allocation of high rewards to trustworthy Workers and impose severe penalties on malicious Workers.
- *Reputation Manager:* Reputation manager calculates the reputation of Workers based on the feedback from the Quality Estimation Manager. The calculated reputation scores are then submitted to the blockchain.
- *Incentive Estimation Manager:* Incentive estimation manager calculates rewards for participants based on the quality of the data they provide and their reputation scores. The resulting rewards are sent to the blockchain for distribution.
- *Miner Selection Manager:* Miners may be malicious; thereby miner selection manager selects miners based on their reputation which is evaluated by the set of miners.

The Unified Modeling Language (UML) sequence diagram in Fig. 10 shows the flow of operations and interactions between entities in the system [157]. Firstly, Requestors and Workers Requestors need to register to the blockchain. Requestors upload their sensing tasks to the blockchain, creating a smart contract that includes task criteria such as time deadline / task duration, location and budget. Then, the *Task Assignment Manager* receives the task data, estimates the optimal number of Workers required to execute the sensing tasks and selects the most suitable Workers to ensure

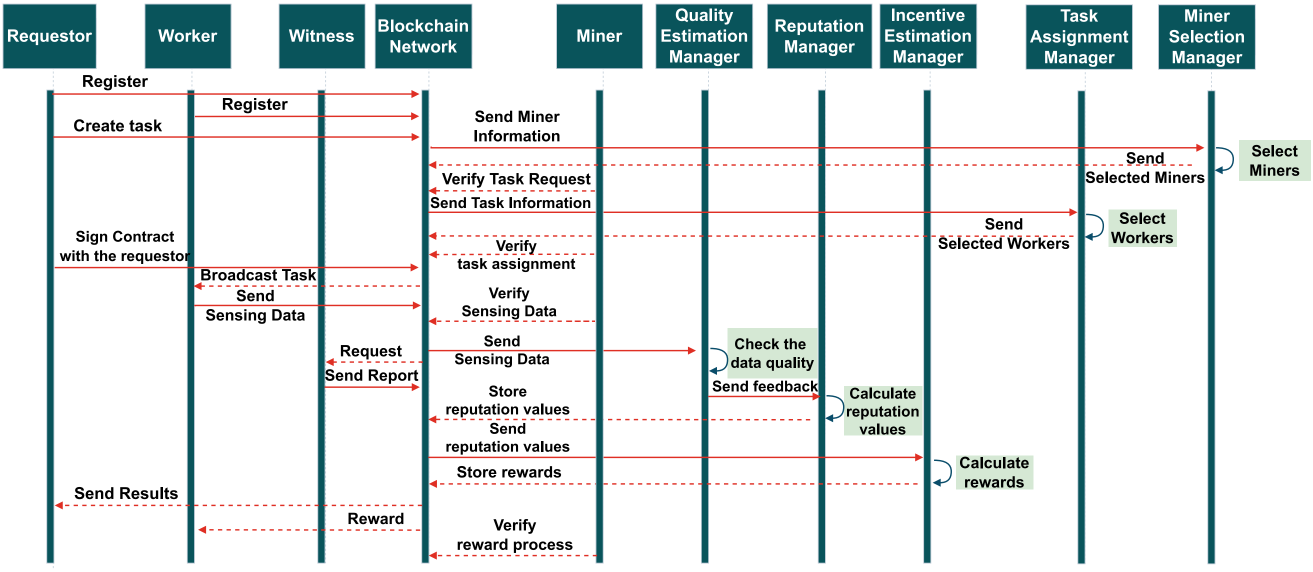

FIGURE 10. UML sequence diagram for proposed HCS-based system.

maximum coverage and high-quality data collection. The task assignment mechanism considers multiple factors for selecting Workers such as *sensing performance related factor* (dependent on the Workers' capabilities and their current context in conjunction with the smart device used, and task requirements) complemented with a *trust related facto*r, dependent on the reputation of each Worker in accomplishing successfully assigned tasks and providing high quality data. Furthermore, since Requestors tend to trust more the Workers they know and Workers tend to provide better quality data on their friends' task, a *social related factor* will favor Workers with explicit and/or implicit positive connections / relationships with the Requestor in the physical and/or online world. Specifically, the sensing related factor considers user expertise, qualifications, willingness, sensor capabilities, resource availability, and current context to eliminate non-relevant Workers and select the most capable device. Additionally, the location of each potential Worker is taken into account, as increased distance results in additional time, effort, and cost to reach the workplace, leading to extra delays in data collection. It is worth noticing that the proposed mechanism will also set a maximum number of concurrent tasks per Worker. The reputation of each Worker is considered during the assignment process in order to select the most trustworthy Workers based on their past performance in task execution. The *Reputation Manager* forms the reputation value of each Worker based on Requestors' past experiences with the Workers. Additionally, second-hand information from a trustworthy set of Workers (witnesses) who recently interacted with the Worker is gathered. This approach aims to form an accurate reputation value in a time-efficient manner, leveraging not only personal experiences but also input from witnesses. Also, social factors play a pivotal role in selecting the witnesses from the trust circle of the Requestor (friends, friends of friends etc.) for their opinion on the performance of the Worker. The witnesses' opinion is weighted based on their trustworthiness in the eyes of the Requestor. Even though trust is context specific (thus, reputation may be different for different undertaken tasks), we address reputation as a behavioral related aspect, while sensing related performance parameters are considered in the first factor.

In the proposed system, the selection result of Workers is recorded in the blockchain, and a smart contract is created to ensure fair trading between the Requestor and the Worker.

Regarding reputation formation and update, an initial neutral reputation value is considered for all Workers to give them an equal chance of being selected. During a training phase, the reputation value is not considered for the task assignment process. This phase is necessary for the system to acquire an accurate value of the Workers' reputation scores. The Workers' reputation is updated each time that a task is completed, according to the following process. After the selected Workers collect the sensing data and upload it to the blockchain, the data is forwarded to the *Quality Estimation Manager*. The user's response is compared with the majority of responses received from other Workers and related IoT data from the sensors/devices (if available). The scheme discriminates between inaccurate data intentionally or unintentionally provided by Workers. Thus, in order not to severely punish an inexperienced Worker or those with devices equipped with lower-capability sensors, the quality estimation takes into account other aspects such as personal factors (user's willingness and experience), location and time of the sensing data, as well as sensing and social factors as Workers tend to provide better quality data on their friends' tasks. The quality estimation also considers if the Worker has completed the assigned task within the specified deadlines or if the task remains unsolved. An outlier detection technique is applied to classify the Workers into two categories: normal Workers and misbehaving Workers, depending on whether one's sensing data is far away from the group consensus, with the latter category consisting of intentionally and unintentionally misbehaving Workers' subcategories. The outlier detection process runs parallel to the quality estimation process, and the results can be used to update users' reputation scores. Thus, according to the positive or negative feedback, the *Reputation Manager* increases or decreases the reputation of every Worker, with the unintentionally misbehaving Workers not being severely punished for the lower quality of data provided. Thus, the user's reputation may decrease linearly if a user unintentionally contributes low-quality data but decrease exponentially if the user intentionally contributes low-quality data.

The Worker's reputation value is accumulated based on his/her historical behaviors. When updating the reputation value. the old reputation value is taken into account along with the reputation feedback gained in the current task. At this point it should be noted that the reputation calculation should be based mostly on recent events. Thus, misbehaving entities have the opportunity to re-enter the system if they exhibit good behavior. Nevertheless, consistent high-quality data contribution should be required to improve the reputation of a misbehaving entity. The updated reputation value is stored to the blockchain, ensuring the system's reliability. Unlike previous reputation management systems, our proposed framework operates on a distributed system without a centralized server, which mitigates the single point of failure problem. Additionally, by utilizing blockchain's traceability, openness, and transparency, the reputation values of users, as well as data collected and uploaded by Workers are ensured to be trustworthy and accessible to all participants in the network.

Finally, in the proposed architecture, the incentive mechanism takes into account the reputation and quality of data returned by each participating entity to determine the reward for their contributions. Data quality is important to determine the payment and reputation value of Workers. However, users' consistent good behavior should be rewarded as malicious nodes may strategically alter their behavior for maximizing their benefit; thus, the system should punish users that strategically change their behavior with time. As a result, this solution encourages users to contribute high quality of data to receive higher payments. Finally, the reward calculated by the *Incentive Estimation Manager* is stored to the blockchain and then distributed to the Workers. The smart contract automatically executes the reward allocation process, ensuring transparency and fairness. The proposed architecture uses miners to verify and validate every transaction such as the sensing task, the sensing procedure and the reward allocation. Miners are selected according to their reputation by the *Miner Selection Manager* as the miners are not always trustworthy. Each miner is supervised by an implicit and randomly selected group of miners, responsible for assigning a reputation score based on each miner's performance following each transaction in order to calculate a public reputation value. In fact, reputation is a measure of the mining performance and behavior (i.e., honest or malicious activities). Therefore, the design of the proposed mechanism requires careful consideration of various aspects in order to promote cooperation and enhance the quality of data provisioning in HCS systems.

Lastly, in order to describe the proposed architecture, the 1+5 architectural views model, as proposed in [157], is utilized. The UML deployment diagram is used to illustrate the physical nodes in the system. As a new type of modeling element, stereotypes extend the semantics of existing elements in the UML metamodel. Nodes have been labeled with proper stereotypes (such as ≪RequestorNode≫, ≪WorkerNode≫, ≪ReputationManagerNode≫, ≪MinerNode≫), as shown in Fig. 11.

VIII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Ensuring the quality of contributed data is an issue of utmost importance in Human-Centric Systems and the broader IoT domain. In this article, after presenting the main challenges that need to be addressed in HCS systems, the data quality challenge in HCS has been extensively discussed, identifying and elaborating on the factors that affect data quality, either unintentionally or intentionally. The solutions proposed in related research literature are categorized and analyzed under three main categories: task assignment mechanisms, reputation mechanisms, and blockchain. Subsequently, a comprehensive list of critical aspects that should be considered when designing such mechanisms is formed. We propose a blockchain-enabled data quality control model that incorporates a trust-aware task assignment mechanism, a hybrid reputation mechanism and the utilization of social connections for selecting trustworthy Workers, witnesses and miners. The proposed architecture involves various entities and roles, considering multiple factors that influence the reputation of the participants. It discriminates on intentional and unintentional misbehaving entities and leverages blockchain technology to protect participants' privacy while avoiding the limitations associated with a centralized platform.

Our future plans include conducting extensive performance evaluation experiments (lab-based and in pilot scale) of the proposed HCS-based system. Additionally, as shown in Table 8, high data storage and computing requirements can drain the device's limited resources, lightweight processing algorithms and consensus mechanisms should be designed. Furthermore, the integration of the edge technology in blockchain-based HCS systems presents opportunities for improved performance. We will explore the inclusion of trusted edge nodes in the proposed architecture to satisfy strict latency constraints. The edge layer, built between the users and the HCS platform will perform

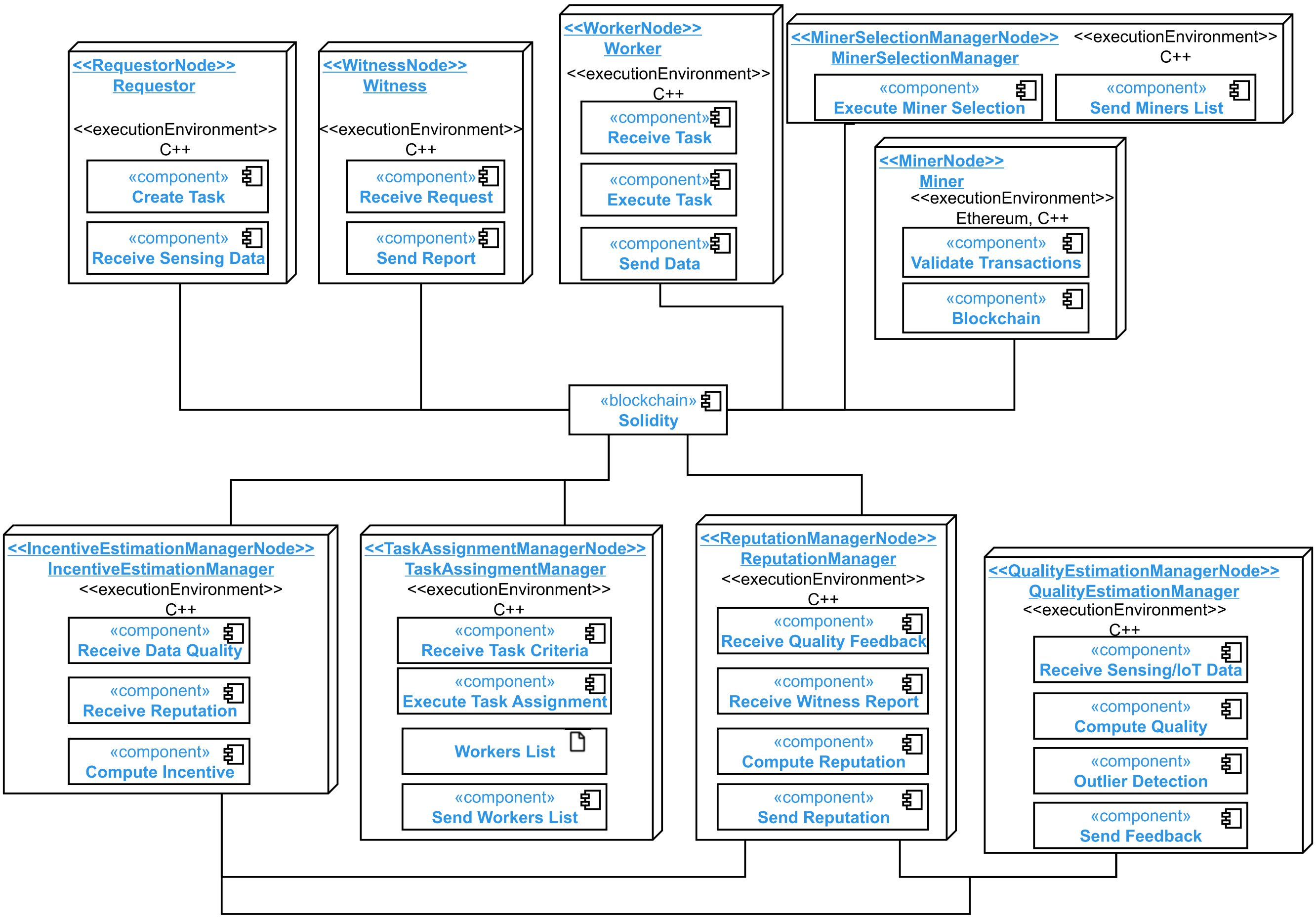

FIGURE 11. UML deployment diagram for proposed HCS-based system.

necessary processes for blockchain services, minimizing data transmission and processing, and enhancing fault tolerance, energy consumption and security of the system, and improving the overall system performance [158]. Moreover, we will work towards identifying the common data requirements across different tasks and applications to enable data sharing and correlation, resulting in energy resource savings.

Additionally, emerging technologies such as Metaverse and Digital Twins can offer significant advancements to HCS systems [159]. Digital Twins is a virtual replica of a physical system capable of simulating, monitoring, integrating, and testing physical objects in different what if scenarios through their virtual representation. By connecting the physical and digital aspects, digital twins enable a deeper understanding, control, and optimization of real-world systems, leading to improved performance, efficiency, and sustainability, exploiting data collected from humans and IoT devices. The Metaverse is a virtual realm where users can immerse themselves through digital avatars. By leveraging augmented reality, artificial intelligence, and blockchain, the Metaverse is becoming a tangible reality. Its immersive and hyper-spatiotemporal nature, coupled with features like scalability and interoperability, make it an ideal solution for promoting user involvement, increasing their trustability, and handling vast amounts of data from sensors and Workers in HCS-based systems. Integrating the Metaverse and Digital Twins with HCS enhances decision-making, offers a deeper understanding and acceptance of collected data, and enables more sophisticated data analysis, contributing to the advancement of HCS capabilities. Integrating these technologies can enhance the overall quality and effectiveness of HCS-based systems.

Lastly, as continuous delivery and continuous deployment practices speed up the development and delivery software process without compromising on the quality, they are considered crucial to the quick and easy creation and management of distributed ledger systems, such as blockchain, and have been investigated by excellent works (such as [160]) in order to automate the entire process of delivery and development of a blockchain-based software. Specifically, a continuous delivery strategy automates each stage of the process of delivering changes made by a developer to the code repository or container registry, and the changes are automatically tested before being pushed [161]. Testing is very useful for detecting failures and guaranteeing that the software being tested has been developed correctly [162]. Continuous delivery ensures that the new code process is expedited and requires minimal effort

TABLE 8. Future research directions.

Challenging Direction	Expected Solution
Resource optimization	Design lightweight processing algorithms and consensus mechanisms, integration of edge technology
Low latency systems	Integration of edge technology in blockchain-based HCS systems to satisfy strict latency constraints
Data sharing and correlation for energy efficient systems	Identify common data requirements of different tasks and applications, and develop mechanisms for data sharing and correlation
Automation of software delivery and development	Utilize continuous delivery and continuous deployment practices, incorporating smart contracts

to deploy new changes. Continuous deployment refers to the automated procedure of deploying changes to the production as soon as they are ready, devoid of the need for human intervention. Thus, any changes made to the proposed architecture and pushed to the code repository are automatically deployed from the repository to production. Continuous delivery and continuous development practices can be used for fast and secure delivery and development of software releases. Our future plans concerning continuous delivery and deployment include the utilization of the Ethereum blockchain to run smart contracts to manage interactions between Requestors and Workers easily.

REFERENCES

[1] O. Vermesan et al., "The next generation Internet of Things—Hyperconnectivity and embedded intelligence at the edge," in *Next Generation Internet of Things–Distributed Intelligence at the Edge and Human–Machine Interactions*. New York, NY, USA: River, 2022, pp. 19–102.

[2] V. Petrov et al., "When IoT keeps people in the loop: A path towards a new global utility," *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 114–121, Jan. 2019, doi: 10.1109/MCOM.2018.1700018.

[3] H. Ma, D. Zhao, and P. Yuan, "Opportunities in mobile crowd sensing," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 29–35, Aug. 2014, doi: 10.1109/MCOM.2014.6871666.

[4] F. A. Santos, T. H. Silva, T. Braun, A. A. Loureiro, and L. A. Villas, "Towards a sustainable people-centric sensing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.

[5] J. Liu, H. Shen, H. S. Narman, W. Chung, and Z. Lin, "A survey of mobile crowdsensing techniques: A critical component for the Internet of Things," *ACM Trans. Cyber Phys. Syst.*, vol. 2, no. 3, pp. 1–26, Jun. 2018, doi: 10.1145/3185504.

[6] C. Leonardi, A. Cappellotto, M. Caraviello, B. Lepri and F. Antonelli, "SecondNose: An air quality mobile crowdsensing system," in *Proc. 8th Nordic Conf. Human–Comput. Interact. Fun Fast, Found.*, Helsinki, Finland, 2014, pp. 1051–1054.

[7] C. Mloza-Banda and B. Scholtz, "Crowdsensing for successful water resource monitoring: An analysis of citizens' intentions and motivations," in *Proc. Annu. Conf. South African Inst. Comput. Sci. Inf. Technol.*, Port Elizabeth South Africa, 2018, pp. 55–64.

[8] M. Rutten, E. Minkman, and M. van der Sanden, "How to get and keep citizens involved in mobile crowd sensing for water management? A review of key success factors and motivational aspects," *Interdiscipl. Rev. Water*, vol. 4, no. 4, pp. 1–10, Apr. 2017, doi: 10.1002/wat2.1218.

[9] R. Salpietro, L. Bedogni, M. Di Felice, and L. Bononi, "Park here! A smart parking system based on smartphones' embedded sensors and short range communication technologies," in *Proc. IEEE 2nd World Forum Internet Things*, Milan, Italy, 2015, pp. 18–23.

[10] Y. Sun et al., "When mobile crowd sensing meets smart agriculture: Poster," in *Proc. ACM Turing Celebration Conf.*, Chengdu, China, 2019, pp. 1–2.

[11] A. Ginige and J. Sivagnanasundaram, "Enhancing agricultural sustainability through crowdsensing: A smart computing approach," *J. Adv. Agricult. Technol.*, vol. 6, no. 3, pp. 161–165, Sep. 2019, doi: 10.18178/joaat.6.3.161-165.

[12] J. Sivagnanasundaram, A. Ginige, and J. Goonetillake, "Farmers as sensors: A crowdsensing platform to generate agricultural pest incidence reports," in *Proc. Int. Conf. Internet Things Res. Practice (iCIOTRP)*, Sydney, NSW, Australia, 2019, pp. 13–18.

[13] Q. V. Khanh, A. Chehri, N. M. Quy, N. D. Han, and N. T. Ban, "Innovative trends in the 6G era: A comprehensive survey of architecture, applications, technologies, and challenges," *IEEE Access*, vol. 11, pp. 39824–39844, 2023, doi: 10.1109/ACCESS.2023.3269297.

[14] H. Wang, "A survey of application and key techniques for mobile crowdsensing," *Wireless Commun. Mobile Comput.*, vol. 2022, Nov. 2022, Art. no. 3693537, doi: 10.1155/2022/3693537.

[15] J. Wang, L. Wang, Y. Wang, D. Zhang, and L. Kong, "Task allocation in mobile crowd sensing: State-of-the-art and future opportunities," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3747–3757, Oct. 2018, doi: 10.1109/JIOT.2018.2864341.

[16] W. Guo, W. Zhu, Z. Yu, J. Wang, and B. Guo, "A survey of task allocation: Contrastive perspectives from wireless sensor networks and mobile crowdsensing," *IEEE Access*, vol. 7, pp. 78406–78420, 2019, doi: 10.1109/ACCESS.2019.2896226.

[17] J. W. Kim, K. Edemacu, and B. Jang, "Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey," *J. Netw. Comput. Appl.*, vol. 200, Apr. 2022, Art. no. 103315, doi: 10.1016/j.jnca.2021.103315.

[18] Y. Wang, Z. Yan, W. Feng, and S. Liu, "Privacy protection in mobile crowd sensing: A survey," *World Wide Web*, vol. 23, no. 1, pp. 421–452, Jan. 2020, doi: 10.1007/s11280-019-00745-2.

[19] A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich, and P. Bouvry, "A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2419–2465, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2914030.

[20] K. Abualsaud et al., "A survey on mobile crowd-sensing and its applications in the IoT era," *IEEE Access*, vol. 7, pp. 3855–3881, 2018, doi: 10.1109/ACCESS.2018.2885918.

[21] F. Khan, A. U. Rehman, J. Zheng, M. A. Jan, and M. Alam, "Mobile crowdsensing: A survey on privacy-preservation, task management, assignment models, and incentives mechanisms," *Future Gener. Comput. Syst.*, vol. 100, pp. 456–472, Nov. 2019, doi: 10.1016/j.future.2019.02.014

[22] Z. Chen, C. Fiandrino, and B. Kantarci, "On blockchain integration into mobile crowdsensing via smart embedded devices: A comprehensive survey," *J. Syst. Architect.*, vol. 115, pp. 102011–102019, May 2021, doi: 10.1016/j.sysarc.2021.102011.

[23] Y. Liu, L. Kong, and G. Chen, "Data-oriented mobile crowdsensing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2849–2885, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2910855.

[24] F. Restuccia, N. Ghosh, S. Bhattacharjee, S. K. Das, and T. Melodia, "Quality of information in mobile crowdsensing: Survey and research challenges," *ACM Trans. Sensor Netw.)*, vol. 13, no. 4, pp. 1–43, Nov. 2017, doi: 10.1145/3139256.

[25] B. Guo, Z. Yu, D. Zhang, and X. Zhou, "From participatory sensing to mobile crowd sensing," in *Proc. 12th IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshop)*, Budapest, Hungary, 2014, pp. 593–598.

[26] F. Hou, Y. Pei, and J. Sun, *Mobile Crowd Sensing: Incentive Mechanism Design*. Cham, Switzerland: Springer Int., 2019.

[27] S. Yang, F. Wu, S. Tang, X. Gao, B. Yang, and G. Chen, "On designing data quality-aware truth estimation and surplus sharing method for mobile crowdsensing," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 4, pp. 832–847, Apr. 2017, doi: 10.1109/JSAC.2017.2676898.

[28] V. S. Dasari, B. Kantarci, M. Pouryazdan, L. Foschini, and M. Girolami, "Game theory in mobile crowdsensing: A comprehensive survey," *Sensors*, vol. 20, no. 7, p. 2055, Apr. 2020, doi: 10.3390/s20072055.

[29] M. E. Barachi, A. Lo, S. S. Mathew, and K. Afsari, "A novel quality and reliability-based approach for participants' selection in mobile crowdsensing," *IEEE Access*, vol. 7, pp. 30768–30791, 2019, doi: 10.1109/ACCESS.2019.2902727.

[30] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17545–17556, 2018, doi: 10.1109/ACCESS.2018.2805837.

[31] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing," *IEEE Access*, vol. 7, pp. 74694–74710, 2019, doi: 10.1109/ACCESS.2019.2920922.

[32] H. Jin, L. Su, D. Chen, H. Guo, K. Nahrstedt, and J. Xu, "Thanos: Incentive mechanism with quality awareness for mobile crowd sensing," *IEEE Trans. Mobile Comput.*, vol. 18, no. 8, pp. 1951–1964, Aug. 2019, doi: 10.1109/TMC.2018.2868106.

[33] X. Wei, Y. Wang, J. Tan, and S. Gao, "Data quality aware task allocation with budget constraint in mobile crowdsensing," *IEEE Access*, vol. 6, pp. 48010–48020, 2018, doi: 10.1109/ACCESS.2018.2865095.

[34] N. B. Truong, G. M. Lee, T. W. Um, and M. Mackay, "Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2705–2719, Oct. 2019, doi: 10.1109/TIFS.2019.2903659.

[35] E. Zupančič and B. Žalik, "Data trustworthiness evaluation in mobile crowdsensing systems with users' trust dispositions' consideration," *Sensors*, vol. 19, no. 6, p. 1326, Mar. 2019, doi: 10.3390/s19061326.

[36] Z. Wang, L. Liu, L. Wang, X. Wen, and W. Jing, "Privacy-protecting and reputation-based participant recruitment scheme for IoV-based MCS," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22490–22500, Dec. 2021, doi: 10.1109/JIOT.2021.3138131.

[37] M. M. Rahman and N. A. Abdullah, "A trustworthiness-aware spatial task allocation using a fuzzy-based trust and reputation system approach," *Exp. Syst. Appl.*, vol. 211, Jan. 2023, Art. no. 118592, doi: 10.1016/j.eswa.2022.118592.

[38] E. Chiejina, H. Xiao, B. Christianson, A. Mylonas, and C. Chiejina, "A robust Dirichlet reputation and trust evaluation of nodes in mobile ad hoc networks," *Sensors*, vol. 22, no. 2, p. 571, Jan. 2022, doi: 10.3390/s22020571.

[39] Z. Hu, X. Li, J. Wang, C. Xia, Z. Wang, and M. Perc, "Adaptive reputation promotes trust in social networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 4, pp. 3087–3098, Aug. 2021, doi: 10.1109/TNSE.2021.3103771.

[40] L. Sun, Q. Yang, X. Chen, and Z. Chen, "RC-chain: Reputation-based crowdsourcing blockchain for vehicular networks," *J. Netw. Comput. Appl.*, vol. 176, pp. 102956–103017, Feb. 2021, doi: 10.1016/j.jnca.2020.102956.

[41] Z. Noshad et al., "An incentive and reputation mechanism based on blockchain for crowd sensing network," *J. Sensors*, vol. 2021, pp. 1–14, Jul. 2021, doi: 10.1155/2021/1798256.

[42] J. Domaszewicz and D. Parzych, "Intra-company crowdsensing: Datafication with human-in-the-loop," *Sensors*, vol. 22, no. 3, p. 943, Jan. 2022, doi: 10.3390/s22030943.

[43] B. Guo et al., "Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm," *ACM Comput. Surveys*, vol. 48, no. 1, pp. 1–31, Aug. 2015, doi: 10.1145/2794400.

[44] H. Vahdat-Nejad, E. Asani, Z. Mahmoodian, and M. H. Mohseni, "Context-aware computing for mobile crowd sensing: A survey," *Future Gener. Comput. Syst.*, vol. 99, pp. 321–332, Oct. 2019, doi: 10.1016/j.future.2019.04.052.

[45] D. M. Kalui, D. Zhang, G. M. Muketha, and J. O. Onsomu, "Simulation of trust-based mechanism for enhancing user confidence in mobile crowdsensing systems," *IEEE Access*, vol. 8, pp. 20870–20883, 2020, doi: 10.1109/ACCESS.2020.2968797.

[46] X. He, M. Liu, and G. Yang, "Spatiotemporal opportunistic transmission for mobile crowd sensing networks," *Pers. Ubiquitous Comput.*, vol. 27, pp. 551–561, Aug. 2020, doi: 10.1007/s00779-020-01439-7.

[47] Y. Al Sawafi, A. Touzene, K. Day, and N. Alzeidi, "Mobile crowd sensing RPL-based routing protocol for smart city," *Int. J. Comput. Netw. Commun. (IJCNC)*, vol. 12, no. 2, pp. 1–20, Mar. 2020, doi: 10.5121/ijcnc.2020.12203.

[48] T. Zhou, Z. Cai, M. Xu, and Y. Chen, "Leveraging crowd to improve data credibility for mobile crowdsensing," in *Proc. 21th IEEE Symp. Comput. Commun. (ISCC)*, 2016, pp. 561–568.

[49] M. T. Wynn and S. Sadiq, "Responsible process mining—A data quality perspective," in *Proc. 17th Int. Conf. Bus. Process Manag. (BPM)*, Vienna, Austria, 2019, pp. 10–15.

[50] B. Guo et al., "TaskMe: Toward a dynamic and quality-enhanced incentive mechanism for mobile crowd sensing," *Int. J. Human–Comput. Stud.*, vol. 102, pp. 14–26, Jun. 2017, doi: 10.1016/j.ijhcs.2016.09.002.

[51] M. Louta, K. Banti, G. Karetsos, and T. Lagkas, "Mobile crowd sensing architectural frameworks: A comprehensive survey," in *Proc. 7th IEEE Int. Conf. Inf. Intell. Syst. Appl. (IISA)*, Chalkidiki, Greece, 2016, pp. 1–7.

[52] D. Peng, F. Wu, and G. Chen, "Data quality guided incentive mechanism design for crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 307–319, Feb. 2018, doi: 10.1109/TMC.2017.2714668.

[53] L. Wei, Y. Yang, J. Wu, C. Long, and B. Li, "Trust management for Internet of Things: A comprehensive study," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7664–7679, May 2022, doi: 10.1109/JIOT.2021.3139989.

[54] L. Cheng et al., "Compressive sensing based data quality improvement for crowd-sensing applications," *J. Netw. Comput. Appl.*, vol. 77, pp. 123–134, Jan. 2017, doi: 10.1016/j.jnca.2016.10.004.

[55] M. Talasila, R. Curtmola, and C. Borcea, "Mobile crowd sensing," in *Sensor Networking: Advanced Technologies and Applications*. Boca Raton, FL, USA: CRC Press, 2015, pp. 1–10.

[56] G. Ding et al., "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014, doi: 10.1109/TCOMM.2014.2346775.

[57] K. Banti et al., "Intelligent mechanisms for irrigation optimization via treated wastewater management in precision agriculture—The AUGEIAS example," *Environ. Sci.*, vol. 21, no. 1, p. 50, Oct. 2022, doi: 10.3390/environsciproc2022021050.

[58] J. An et al., "A lightweight blockchain-based model for data quality assessment in crowdsensing," *IEEE Trans. Comput. Soc. Syst.*, vol. 7, no. 1, pp. 84–97, Feb. 2020, doi: 10.1109/TCSS.2019.2956481.

[59] R. Yu, R. Liu, X. Wang, and J. Cao, "Improving data quality with an accumulated reputation model in participatory sensing systems," *Sensors*, vol. 14, no. 3, pp. 5573–5594, Mar. 2014, doi: 10.3390/s140305573.

[60] A. A. Gad-ElRab and A. S. Alsharkawy, "Statistical-based data quality model for mobile crowd sensing systems," *Arab. J. Sci. Eng.*, vol. 43, no. 12, pp. 8195–8207, Jun. 2018, doi: 10.1007/s13369-018-3374-0.

[61] S. Gao, X. Chen, J. Zhu, X. Dong, and J. Ma, "TrustWorker: A trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing," *IEEE Trans. Services Comput.*, vol. 15, no. 6, pp. 3577–3590, Nov./Dec. 2022, doi: 10.1109/TSC.2021.3103938.

[62] Y. Gao, X. Li, J. Li, and Y. Gao, "A dynamic-trust-based recruitment framework for mobile crowd sensing," in *Proc. Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.

[63] D. Zhang, H. Xiong, L. Wang, and G. Chen, "CrowdRecruiter: Selecting participants for piggyback crowdsensing under probabilistic coverage constraint," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2014, pp. 703–714.

[64] M. Dai, Z. Su, Q. Xu, Y. Wang, and N. Lu, "A trust-driven contract incentive scheme for mobile crowd-sensing networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1794–1806, Feb. 2022, doi: 10.1109/TVT.2021.3117696.

[65] W. Jiang, P. Chen, W. Zhang, Y. Sun, C. Junpeng, and Q. Wen, "User recruitment algorithm for maximizing quality under limited budget in mobile crowdsensing," *Discr. Dyn. Nat. Soc.*, vol. 2022, pp. 1–13, Jan. 2022, doi: 10.1155/2022/4804231.

[66] W. Yu et al., "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017, doi: 10.1109/ACCESS.2017.2778504.

[67] H. Li, D. Liao, G. Sun, M. Zhang, D. Xu, and Z. Han, "Two-stage privacy-preserving mechanism for a crowdsensing-based VSN," *IEEE Access*, vol. 6, pp. 40682–40695, 2018, doi: 10.1109/ACCESS.2018.2854236.

[68] R. I. Ogie, "Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: From literature review to a conceptual framework," *Human Centric Comput. Inf. Sci.*, vol. 6, no. 1, pp. 1–31, Dec. 2016, doi: 10.1186/s13673-016-0080-3.

[69] C. Jiang, L. Gao, L. Duan, and J. Huang, "Exploiting data reuse in mobile crowdsensing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–6.

[70] A. Antonic, K. Roankovic, M. Marjanovic, K. Pripuic, and I. P. Zarko, "A mobile crowdsensing ecosystem enabled by a cloud-based publish/subscribe middleware," in *Proc. IEEE Int. Conf. Future Internet Things Cloud*, 2014, pp. 107–114.

[71] R. Azzam, R. Mizouni, H. Otrok, A. Ouali, and S. Singh, "GRS: A group-based recruitment system for mobile crowd sensing," *J. Netw. Comput. Appl.*, vol. 72, pp. 38–50, Sep. 2016, doi: 10.1016/j.jnca.2016.06.015.

[72] M. Xiao, B. An, J. Wang, G. Gao, S. Zhang, and J. Wu, "CMAB-based reverse auction for unknown worker recruitment in mobile crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 21, no. 10, pp. 3502–3518, Oct. 2022, doi: 10.1109/TMC.2021.3059346.

[73] M. Marjanović, L. Skorin-Kapov, K. Pripužić, A. Antonić, and I. Žarko, "Energy-aware and quality-driven sensor management for green mobile crowd sensing," *J. Netw. Comput. Appl.*, vol. 59, pp. 95–108, Jan. 2016, doi: 10.1016/j.jnca.2015.06.023.

[74] W. Wang, H. Gao, C. H. Liu, and K. K. Leung, "Credible and energy-aware participant selection with limited task budget for mobile crowd sensing," *Ad Hoc Netw.*, vol. 43, pp. 56–70, Jun. 2016, doi: 10.1016/j.adhoc.2016.02.007.

[75] R. Estrada, R. Mizouni, H. Otrok, A. Ouali, and J. Bentahar, "A crowd-sensing framework for allocation of time-constrained and location-based tasks," *IEEE Trans. Services Comput.*, vol. 13, no. 5, pp. 769–785, Sep./Oct. 2020, doi: 10.1109/TSC.2017.2725835.

[76] M. Girolami, D. Belli, S. Chessa, and L. Foschini, "How mobility and sociality reshape the context: A decade of experience in mobile crowdsensing," *Sensors*, vol. 21, no. 19, pp. 6397, Sep. 2021, doi: 10.3390/s21196397.

[77] J. Wang, Y. Wang, D. Zhang, F. Wang, Y. He, and L. Ma, "PSAllocator: Multi-task allocation for participatory sensing with sensing capability constraints," in *Proc. ACM Conf. Comput. Supported Cooper. Work Soc. Comput.*, Portland, OR, USA, 2017, pp. 1139–1151.

[78] C. Fiandrino, B. Kantarci, F. Anjomshoa, D. Kliazovich, P. Bouvry, and J. Matthews, "Sociability-driven user recruitment in mobile crowdsensing Internet of Things platforms," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.

[79] H. Jin, L. Su, D. Chen, K. Nahrstedt, and J. Xu, "Quality of information aware incentive mechanisms for mobile crowd sensing systems," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Hangzhou, China, 2015, pp. 167–176

[80] H. Jin, L. Su, and K. Nahrstedt, "THESEUS: Incentivizing truth discovery in mobile crowd sensing systems," in *Proc. 18th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Chennai, India, 2017, pp. 1–10.

[81] S. Liu, Z. Zheng, F. Wu, S. Tang, and G. Chen, "Context-aware data quality estimation in mobile crowdsensing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Atlanta, GA, USA, 2017, pp. 1–9.

[82] J. Yang, L. Fu, B. Yang, and J. Xu, "Participant service quality aware data collecting mechanism with high coverage for mobile crowdsensing," *IEEE Access*, vol. 8, pp. 10628–10639, 2020, doi: 10.1109/ACCESS.2020.2965734.

[83] H. Gao et al., "A survey of incentive mechanisms for participatory sensing," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 918–943, 2nd Quart., 2015, doi: 10.1109/COMST.2014.2387836.

[84] Z. Wang, Y. Huang, X. Wang, J. Ren, Q. Wang, and L. Wu, "SocialRecruiter: Dynamic incentive mechanism for mobile crowdsourcing worker recruitment with social networks," *IEEE Trans. Mobile Comput.*, vol. 20, no. 5, pp. 2055–2066, Feb. 2020, doi: 10.1109/TMC.2020.2973958.

[85] H. Amintoosi and S. S. Kanhere, "A reputation framework for social participatory sensing systems," *Mobile Netw. Appl.*, vol. 19, no. 1, pp. 88–100, Feb. 2014, doi: 10.1007/s11036-013-0455-x.

[86] M. Pouryazdan, B. Kantarci, T. Soyata, L. Foschini, and H. Song, "Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing," *IEEE Access*, vol. 5, pp. 1382–1397, 2017, doi: 10.1109/ACCESS.2017.2660461.

[87] D. He, S. Chan, and M. Guizani, "User privacy and data trustworthiness in mobile crowd sensing," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 28–34, Feb. 2015, doi: 10.1109/MWC.2015.7054716.

[88] J. Huang et al., "Blockchain-based mobile crowd sensing in industrial systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6553–6563, Oct. 2020, doi: 10.1109/TII.2019.2963728.

[89] S. Zou, J. Xi, H. Wang, and G. Xu, "CrowdBLPS: A blockchain-based location-privacy-preserving mobile crowdsensing system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4206–4218, Dec. 2019, doi: 10.1109/TII.2019.2957791.

[90] D. Gambetta, *Trust: Making and Breaking Cooperative Relations*. New York, NY, USA: Basil Blackwell, 1988.

[91] N. Mantas, M. Louta, E. Karapistoli, G. T. Karetsos, S. Kraounakis, and M. S. Obaidat, "Towards an incentive-compatible, reputation-based framework for stimulating cooperation in opportunistic networks: A survey," *IET Netw.*, vol. 6, no. 6, pp. 169–178, Nov. 2017, doi: 10.1049/iet-net.2017.0079.

[92] T. Luo, J. Huang, S. S. Kanhere, J. Zhang, and S. K. Das, "Improving IoT data quality in mobile crowd sensing: A cross validation approach," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5651–5664, Jun. 2019, doi: 10.1109/JIOT.2019.2904704.

[93] B. Kantarci, P. M. Glasser, and L. Foschini, "Crowdsensing with social network-aided collaborative trust scores," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, 2015, pp. 1–6.

[94] X. Liu, J. Fu, Y. Chen, W. Luo, and Z. Tang, "Trust-aware sensing quality estimation for team crowdsourcing in social IoT," *Comput. Netw.*, vol. 184, Jan. 2021, Art. no. 107695, doi: 10.1016/j.comnet.2020.107695.

[95] M. Aparicio, C. J. Costa, and R. Moises, "Gamification and reputation: key determinants of e-commerce usage and repurchase intention," *Heliyon*, vol. 7, no. 3, pp. 1–14, Mar. 2021, doi: 10.1016/j.heliyon.2021.e06383.

[96] S. Qi, Y. Li, W. Wei, Q. Li, K. Qiao, and Y. Qi, "Truth: A blockchain-aided secure reputation system with genuine feedbacks," *IEEE Trans. Eng. Manag.*, early access, Feb. 24, 2022, doi: 10.1109/TEM.2021.3128930.

[97] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020, doi: 10.1109/ACCESS.2020.2986257.

[98] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021, doi: 10.1109/TITS.2020.2973715.

[99] Y. Liu et al., "VRepChain: A decentralized and privacy-preserving reputation system for social Internet of Vehicles based on blockchain," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13242–13253, Dec. 2022, doi: 10.1109/TVT.2022.3198004.

[100] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, M. Fayaz, and J. Gwak, "Counteracting selfish nodes using reputation based system in mobile ad hoc networks," *Electronics*, vol. 11, no. 2, pp. 1–22, 2022, doi: 10.3390/electronics11020185.

[101] R. Gupta, Y. N. Singh, and A. Goswami, "Trust estimation in peer-to-peer network using blue," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 888–897, Jan. 2021, doi: 10.1007/s12083-020-01049-3.

[102] N. Al-Otaiby, A. Alhindi, and H. Kurdi, "AntTrust: An ant-inspired trust management system for peer-to-peer networks," *Sensors*, vol. 22, no. 2, p. 533, Jan. 2022, doi: 10.3390/s22020533.

[103] H. Alrahhal, R. Jamous, R. Ramadan, A. M. Alayba, and K. Yadav, "Utilising acknowledge for the trust in wireless sensor networks," *Appl. Sci.*, vol. 12, no. 4, p. 2045, Feb. 2022, doi: 10.3390/app12042045.

[104] A. A. Battah, Y. Iraqi, and E. Damiani, "A trust and reputation system for IoT service interactions," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 3, pp. 2987–3005, Sep. 2022, doi: 10.1109/TNSM.2022.3179875.

[105] Z. Liao and S. Cheng, "RVC: A reputation and voting based blockchain consensus mechanism for edge computing-enabled IoT systems," *J. Netw. Comput. Appl.*, vol. 209, Jan. 2023, Art. no. 103510, doi: 10.1016/j.jnca.2022.103510.

[106] A. Patel and D. Jinwala, "A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things," *Int. J. Commun. Syst.*, vol. 35, no. 1, Jan. 2022, Art. no. e5007, doi: 10.1002/dac.5007.

[107] J. Zhang, Y. Wu, and R. Pan, "Incentive mechanism for horizontal federated learning based on reputation and reverse auction," in *Proc. Web Conf.*, Ljubljana, Slovenia, 2021, pp. 947–956.

[108] K. Mrabet, F. E. Bouanani, and H. Ben-Azza, "Generalized secure and dynamic decentralized reputation system with a dishonest majority," *IEEE Access*, vol. 11, pp. 9368–9388, 2023, doi: 10.1109/ACCESS.2023.3239394.

[109] F. Zeng, Y. Chen, L. Yao, and J. Wu, "A novel reputation incentive mechanism and game theory analysis for service caching in software-defined vehicle edge computing," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 467–481, Sep. 2021, doi: 10.1007/s12083-020-00985-4.

[110] Y. Zou, F. Shen, F. Yan, J. Lin, and Y. Qiu, "Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IoV," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Nanjing, China, 2021, pp. 1–6.

[111] C. Tanas and J. Herrera-Joancomarti, "When users become sensors: can we trust their readings?" *Int. J. Commun. Syst.*, vol. 28, no. 4, pp. 601–614, Mar. 2015, doi: 10.1002/dac.2689.

[112] S. Chen, B. Li, L. Rui, J. Wang, and X. Chen, "A blockchain-based creditable and distributed incentive mechanism for participant mobile crowdsensing in edge computing," *Math. Biosci. Eng.*, vol. 19, no. 4, pp. 3285–3312, Jan. 2022, doi: 10.3934/mbe.2022152.

[113] S. Kraounakis, I. Demetropoulos, A. Michalas, M. Obaidat, P. Sarigiannidis, and M. Louta, "A robust reputation-based computational model for trust establishment in pervasive systems," *IEEE Syst. J.*, vol. 9, no. 3, pp. 878–891, Sep. 2015, doi: 10.1109/JSYST.2014.2345912.

[114] W. Ahmed, W. Di, and D. Mukathe, "A blockchain-enabled incentive trust management with threshold ring signature scheme for traffic event validation in VANETs," *Sensors*, vol. 22, no.17, p. 6715, Sep. 2022, doi: 10.3390/s22176715.

[115] K. Banti, F. Katsimpoura, M. Louta, and G. Karetsos, "Data quality in mobile crowd sensing systems: Challenges and perspectives," in *Proc. IEEE 9th Int. Conf. Inf. Intell. Syst. Appl. (IISA)*, Zakynthos, Greece, 2018, pp. 1–8.

[116] Y. Chae, L. C. DiPippo, and Y. L. Sun, "Trust management for defending on-off attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 1178–1191, Apr. 2015, doi: 10.1109/TPDS.2014.2317719.

[117] T. Zhou, Z. Cai, K. Wu, Y. Chen, and M. Xu, "FIDC: A framework for improving data credibility in mobile crowdsensing," *Comput. Netw.*, vol. 120, pp. 157–169, Jun. 2017, doi: 10.1016/j.comnet.2017.04.015.

[118] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," *IEEE Access*, vol. 4, pp. 529–541, 2016, doi: 10.1109/ACCESS.2016.2519820.

[119] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, "Hybrid blockchain platforms for the Internet of Things (IoT): A systematic literature review," *Sensors*, vol. 22, no. 4, p. 1304, Feb. 2022, doi: 10.3390/s22041304.

[120] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Netw.*, vol. 200, Dec. 2021, Art. no. 108500, doi: 10.1016/j.comnet.2021.108500.

[121] H. Treiblmaier and C. Sillaber, "The impact of blockchain on e-commerce: A framework for salient research topics," *Electron. Commerce Res. Appl.*, vol. 48, Jul./Aug. 2021, Art. no. 101054, doi: 10.1016/j.elerap.2021.101054.

[122] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *J. Bus. Venturing Insights*, vol. 13, Jun. 2020, Art. no. e00151, doi: 10.1016/j.jbvi.2019.e00151.

[123] D. Shakhbulatov, J. Medina, Z. Dong, and R. Rojas-Cessa, "How blockchain enhances supply chain management: A survey," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 230–249, 2020, doi: 10.1109/OJCS.2020.3025313.

[124] Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, "A study of blockchain technology development and military application prospects," *J. Phys. Conf.*, vol. 1507, no. 5, Apr. 2020, Art. no. 52018, doi: 10.1088/1742-6596/1507/5/052018.

[125] N. Khoshavi, G. Tristani, and A. Sargolzaei, "Blockchain applications to improve operation and security of transportation systems: A survey," *Electronics*, vol. 10, no. 5, p. 629, Mar. 2021, doi: 10.3390/electronics10050629.

[126] P. Han, A. Sui, and J. Wu, "Identity management and authentication of a UAV swarm based on a blockchain," *Appl. Sci.*, vol. 12, no. 20, Oct. 2022, Art. no. 10524, doi: 10.3390/app122010524.

[127] J. Hu, K. Yang, K. Wang, and K. Zhang, "A blockchain-based reward mechanism for mobile crowdsensing," *IEEE Trans. Comput. Soc. Syst.*, vol. 7, no. 1, pp. 178–191, Feb. 2020, doi: 10.1109/TCSS.2019.2956629.

[128] M. Arafeh, M. E. Barachi, A. Mourad, and F. Belqasmi, "A blockchain based architecture for the detection of fake sensing in mobile crowdsensing," in *Proc. IEEE 4th Int. Conf. Smart Sustain. Technol. (SpliTech)*, Split, Croatia, 2019, pp. 1–6.

[129] W. Zhang, Y. Luo, S. Fu, and T. Xie, "Privacy-preserving reputation management for blockchain-based mobile crowdsensing," in *Proc. 17th Annu. IEEE Int. Conf. Sens. Commun. Netw. (SECON)*, Como, Italy, 2020, pp. 1–9.

[130] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019, doi: 10.1016/j.future.2018.11.046.

[131] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors*, vol. 18, no. 11, p. 3894, Nov. 2018, doi: 10.3390/s18113894.

[132] X. Tao and A. S. Hafid, "ChainSensing: A novel mobile crowdsensing framework with blockchain," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2999–3010, Feb. 2022, doi: 10.1109/JIOT.2021.3094670.

[133] L. Wei, J. Wu, and C. Long, "A blockchain-based hybrid incentive model for crowdsensing," *Electronics*, vol. 9, no. 2, p. 215, Jan. 2020, doi: 10.3390/electronics9020215.

[134] J. Yu, G. Zhang, D. Lu, and H. Liu, "Blockchain-based crowdsensing trust management mechanism for crowd evacuation," in *Proc. 25th Int. Conf. Comput. Support. Cooper. Work Design (CSCWD)*, Hangzhou, China, 2022, pp. 1179–1184.

[135] W. Wang et al., "BSIF: Blockchain-based secure, interactive, and fair mobile crowdsensing," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3452–3469, Oct. 2022, doi: 10.1109/JSAC.2022.3213306.

[136] E. Wang et al., "Trustworthy and efficient crowdsensed data trading on sharding blockchain," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3547–3561, Dec. 2022, doi: 10.1109/JSAC.2022.3213331.

[137] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100006, doi: 10.1016/j.bcra.2021.100006.

[138] 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 doi: 10.1109/TPDS.2018.2881735.

[139] C. Li, X. Qu, and Y. Guo, "TFCrowd: A blockchain-based crowdsourcing framework with enhanced trustworthiness and fairness," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–20, Aug. 2021, doi: 10.1186/s13638-021-02040-z.

[140] D. Stefanescu, L. Montalvillo, P. Galán-García, J. Unzilla, and A. Urbieta, "A systematic literature review of lightweight blockchain for IoT," *IEEE Access*, vol. 10, pp. 123138–123159, 2022, doi: 10.1109/ACCESS.2022.3224222.

[141] F. Alkhabbas, M. Alsadi, S. Alawadi, F. M. Awaysheh, V. R. Kebande, and M. T. Moghaddam, "ASSERT: A blockchain-based architectural approach for engineering secure self-adaptive IoT systems," *Sensors*, vol. 22, no. 18, p. 6842, Sep. 2022, doi: 10.3390/s22186842.

[142] J. Han et al., "A blockchain-based and SGX-enabled access control framework for IoT," *Electronics*, vol. 11, no. 17, p. 2710, Aug. 2022, doi: 10.3390/electronics11172710.

[143] L. Ting, M. Khan, A. Sharma, and M. D. Ansari, "A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing," *J. Intell. Syst.*, vol. 31, no. 1, pp. 221–236, Feb. 2022, doi: 10.1515/jisys-2022-0012s.

[144] S. Khezr, A. Yassine, R. Benlamri, and M. S. Hossain, "An edge intelligent blockchain-based reputation system for IIoT data ecosystem," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8346–8355, May 2022, doi: 10.1109/TII.2022.3174065.

[145] G. D. Putra, C. Kang, S. S. Kanhere, and J. W. K. Hong, "DeTRM: Decentralised trust and reputation management for blockchain-based supply chains,," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Shanghai, China, 2022, pp. 1–5.

[146] Z. Chen, H. Cui, E. Wu, and X. Yu, "Dynamic asynchronous anti poisoning federated deep learning with blockchain-based reputation-aware solutions," *Sensors*, vol. 22, no. 2, p. 684, Jan. 2022, doi: 10.3390/s22020684.

[147] Z. Wang, R. Xiong, J. Jin, and C. Liang, "AirBC: A lightweight reputation-based blockchain scheme for resource-constrained UANET," in *Proc. 25th IEEE Int. Conf. Comput. Support. Cooper. Work Design (CSCWD)*, Hangzhou, China, 2022, pp. 1378–1383.

[148] S. Fu, X. Huang, L. Liu, and Y. Luo, "BFCRI: A blockchain-based framework for crowdsourcing with reputation and incentive," *IEEE Trans. Cloud Comput.*, vol. 11, no. 2, pp. 2158–2174, Apr.–Jun. 2023, doi: 10.1109/TCC.2022.3190275.

[149] C. P. Fernandes, C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham, "A blockchain-based reputation system for trusted VANET nodes," *Ad Hoc Netw.*, vol. 140, Mar. 2023, Art. no. 103071, doi: 10.1016/j.adhoc.2022.103071.

[150] L. E. Wang, S. Ma, and Z. Sun, "Blockchain-based reputation sharing for high-quality participant selection of MCS," *Security Commun. Netw.*, vol. 2023, Jan. 2023, Art. no. 6120860, doi: 10.1155/2023/6120860.

[151] Z. Zhou, M. Wang, C. N. Yang, Z. Fu, X. Sun, and Q. J. Wu, "Blockchain-based decentralized reputation system in E-commerce environment," *Future Gener. Comput. Syst.*, vol. 124, pp. 155–167, Nov. 2021, doi: 10.1016/j.future.2021.05.035.

[152] Q. Zhang, Q. Ding, J. Zhu, and D. Li, "Blockchain empowered reliable federated learning by worker selection: A trustworthy reputation evaluation method," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Nanjing, China, 2021, pp. 1–6.

[153] T. Wang, J. Guo, S. Ai, and J. Cao, "RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," *Appl. Energy*, vol. 295, Aug. 2021, Art. no. 117056, doi: 10.1016/j.apenergy.2021.117056.

[154] Y. Liang, Y. Li, and B. S. Shin, "FairCs—Blockchain-based fair crowdsensing scheme using trusted execution environment," *Sensors*, vol. 20, no. 11, p. 3172, Jun. 2020, doi: 10.3390/s20113172.

[155] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018, doi: 10.1109/MCOM.2018.1701095.

[156] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "IoT public fog nodes reputation system: A decentralized solution using Ethereum blockchain," *IEEE Access*, vol. 7, pp. 178082–178093, 2019, doi: 10.1109/ACCESS.2019.2958355.

[157] T. Górski, "The 1+5 architectural views model in designing blockchain and IT system integration solutions," *Symmetry*, vol. 13, no. 11, p. 2000, Oct. 2021, doi: 10.3390/sym13112000.

[158] Q. V. Khanh, V.-H. Nguyen, Q. N. Minh, A. D. Van, N. L. Anh, and A. Chehri, "An efficient edge computing management mechanism for sustainable smart cities," *Sustain. Comput. Informat. Syst.*, vol. 38, Apr. 2023, Art. no. 100867, doi: 10.1016/j.suscom.2023.100867.

[159] V. A. Dang, Q. V. Khanh, V. H. Nguyen, T. Nguyen, and D. C. Nguyen, "Intelligent healthcare: Integration of emerging technologies and Internet of Things for humanity," *Sensors*, vol. 23, no. 9, p. 4200, Apr. 2023, doi: 10.3390/s23094200.

[160] T. Górski, "Continuous delivery of blockchain distributed applications," *Sensors*, vol. 22, no. 1, p. 128, Dec. 2021, doi: 10.3390/s22010128.

[161] I. C. Donca, O. P. Stan, M. Misaros, D. Gota, and L. Miclea, "Method for continuous integration and deployment using a pipeline generator for agile software projects," *Sensors*, vol. 22, no. 12, p. 4637, Jun. 2022, doi: 10.3390/s22124637.

[162] S. Zardari et al., "A comprehensive bibliometric assessment on software testing (2016–2021)," *Electronics*, vol. 11, no. 13, p. 1984, Jun. 2022, doi: 10.3390/electronics11131984.

KONSTANTINA BANTI received the M.Eng. degree in informatics and telecommunications engineering from the University of Western Macedonia, Greece, in 2016, where she is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering. Her research interests focus on the areas of mobile crowdsensing, data quality, trust management, blockchain, and next-generation Internet of Things.

MALAMATI LOUTA (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees in electrical and computer engineering in 1997 and 2000, respectively, and the M.B.A. degree from the National Technical University of Athens in 2004. She is the Director of Telecommunication Networks and Advanced Services Laboratory and an Associate Professor with the Electrical and Computer Engineering Department, School of Engineering, University of Western Macedonia, Greece. Her research interests include telecommunication networks and advanced services engineering. She serves as an associate editor, the general chair, the technical program committee chair and member, a session organizer, and a reviewer for a number of international conferences and journals. She is a member of ACM and the Technical Chamber of Greece.

PERISTERA BAZIANA is currently serving as an Assistant Professor with the Department of Informatics and Telecommunications, University of Thessaly, Greece. Since 2017, she has been a Visiting Professor with the Beijing University of Posts and Telecommunications, China. Her research interests include optical communications, optical networks architectures and protocols, and analytical modeling and optimization. She has several publications in international journals and proceedings of conferences with reviewers, related to these fields. She is a member of the Technical Chamber of Greece.