"Worth One Minute": An Anonymous Rewarding Platform for Crowd-Sensing Systems

Lorenz Cuno Klopfenstein, Saverio Delpriori, Alessandro Aldini and Alessandro Bogliolo

Abstract: **Readily available and affordable consumer-grade electronics, with ever-increasing sensing, computing, and communication capabilities, have provided the ground for distributed computation and data collection systems. Crowd-sensing applications rely on volunteers providing access to their personal devices—a category encompassing smartphones, wearables, vehicles, and a wide range of 'Internet of Things' appliances—and using them as sensors. These systems rely on the willingness of participants to invest in a common cause, which often entails explicit efforts from users, occupation of hardware resources, and risks of sharing private data. Incentives and rewarding schemes are adopted to encourage user participation. This paper introduces the "Worth One Minute" (WOM) platform: an implementation of a general-purpose rewarding system based on anonymous vouchers. The platform is designed to reward user efforts towards the common good, rewarding their contributions and the intrinsic social value they provide, while preserving their anonymity.**

Index Terms: **Anonymized data, crowd-sensing, incentive mechanisms, participatory sensing, privacy, rewarding stratigies.**

I. INTRODUCTION

TECHNOLOGICAL developments over the last decade have transformed consumer electronics available to everybody into powerful instruments with always increasing sensing capabilities, computational power, and communication means. These devices include smart vehicles, wearable devices, health or fitness aids, home appliances, and smartphones, each of which has the capability of collecting, processing, and transmitting data. Applications and services that rely on these capabilities being distributed to the edge of the Internet, instead of residing on centralized servers, have been classified under the novel "edge computing" label. In particular, the near ubiquitous nature of the modern smartphone—readily available to the majority of the world population—has given life to a vision in which crowds of citizens equipped with "edge" devices perform tasks such as collecting and sharing data sensed from their near environment.

This edge-focused data collection paradigm, similar in principle to that of wireless sensor networks, benefits from many advantages: It provides access to a variety of sensing capabilities (provided by cameras, microphones, GNSS receivers, gyroscopes, accelerometers, and more) and information provided by users or their context, it leverages existing infrastructure, it has low deployment and development costs, and it exploits the inherent distribution and mobility of users and their devices, which may opportunistically reach massive coverage.

Data collection systems adopting this paradigm have been grouped under the terms *people-centric sensing* [1], *participatory sensing*, *citizen sensing*, *community sensing* [2], or *crowd-sensing* [3]. In this respect, these systems take the "wisdom of crowds" approach from *crowdsourcing* and apply it to data collection tasks [4]. Guo et al. give a specific definition of mobile crowd-sensing and computing (MCSC) as a large-scale sensing paradigm based on user-provided smart devices and envision additional data aggregation and fusion capabilities that allow to tap into the crowd's collective intelligence [5].

Incentive and rewarding mechanisms are critical to the utilization and success of crowd-sensing systems. Individuals owning the collection devices must be singularly encouraged to participate in sensing activities, which (a) require long-term commitment but do not bring any direct benefits to the contributor; (b) incur in non-trivial costs, in terms of time, effort, and mobile device resources (e.g., energy and data usage) [6]. When collecting user location data or sensible information, users must also be convinced to overcome their privacy concerns [7].

A. Contribution

Crowd sensing and computing systems can unleash the exceptional potential of mobile and edge devices. In doing so, they stimulate active citizenship and generate intrinsic social value thanks to the cooperation of a large number of volunteers. Data and results from crowd sensing can be of direct interest not only to the crowd-sensing provider and its participants but also to third-party stakeholders, which can be interested in the results of the data collection process without being directly involved in it [8].

In this work, we present an **anonymous monetization platform** that, instead of being bound to a single crowd-based initiative, provides an *open participative infrastructure* that serves as an interface between volunteers and the stakeholders that wish to support their efforts.

The incentives provided by stakeholders reinforce the motivation of volunteers across all crowd-based initiatives adopting the system, thus leveraging positive externalities (i.e., the "network effect") on the entire platform and its participants [9]. Decoupling crowd-based initiatives from the rewarding system they adopt allows applying the platform economy paradigm, multiplying the impact of each participating initiative and each reward provider [10]. Also, the platform allows reward providers to target their incentives towards specific causes or locations, in order to implement cross-platform policies and incentivization

Manuscript received February 6, 2019.

This project received funding from the European Union's Horizon 2020 research and innovation program under grant agreement № 687959 and has also received funding from a DiSPeA department grant.

L. C. Klopfenstein, S. Delepriori, A. Aldini, and A. Bogliolo are with DiSPeA, University of Urbino Carlo Bo, Italy and DIGIT Srl, Urbino, Italy. email: cuno.klopfenstein, saverio.delpriori, alessandro.aldini, alessandro.bogliolo@uniurb.it

L. C. Klopfenstein is a corresponding author.

Digital Object Identifier: 10.1109/JCN.2019.000051

strategies.

The presented platform is based on a revised version of voucher-exchange protocols from previous work [11], introducing updated in order to strengthen both security and privacy aspects. In Section III we introduce the design goals, sample use-cases, the adopted terminology, the architecture, and the main entities involved in the platform, named worth one minute (WOM). Section IV details the platform's implementation and expands the exchange protocols with further detail and additional privacy and security discussions. Release and integration of the platform are discussed in Section V.

II. RELATED WORK

A. Crowdsourced Sensing and Citizen Science

According to Campbell et al., sensing platforms can be classified as *personal sensing applications* (aimed at monitoring and archiving an individual's activity, such as smart pedometers or personal carbon footprint trackers), *social sensing* (collecting information shared within a social circle and aimed at special interest groups), and *public sensing* (collecting and sharing data, for the public good, such as congestion or pollution in cities) [1]. Sensing applications in the latter categories capture information about the surroundings of participants, which is exploited publicly or at a community scale. Personal, social, and public sensing platforms are employed to gather data in order to achieve aims pertaining to the common interest [12].

A survey by Christin et al. cites many different examples of "environment-centric sensing applications", which may help to monitor environmental parameters of public interest such as air quality, noise, traffic conditions, or information of social nature [2]. Sensing applications limited to the personal realm may also contribute to improving public well-being directly or indirectly [13]. A trivial example could be a fitness tracking app which encourages users to reach fitness goals based on averaged statistics, thus increasing awareness of the user's conditions and possibly reducing the public cost of health care. Many projects similar in scope have been presented in the context of personal health monitoring [14]–[16]. Collection of air quality data from cheap embedded sensing devices has a direct utility for volunteers, who are informed about pollution in their cities, but has also been shown to be a useful source of information to generate realistic air quality models which can be frequently updated [17], [18]. Similarly, a study based on noise level detection using do-it-yourself sensors found that participatory sensing had a positive impact on citizen awareness and campaigns against noise pollution at city-level [19].

Active participation of citizens to these data collection campaigns can foster a symbiotic relationship between the crowd-sensing system, the community, and individual volunteers. Knowledge about public policies in effect and their repercussions on day-to-day life creates awareness and stimulates active citizenship. People are directly involved "in the loop", gaining a greater collective perception of monitored parameters and their significance, as observed in many *citizen science* studies [20].

B. Crowd-Sensing and Incentive Schemes

Without strong incentives, mobile crowd-sensing systems may suffer from insufficient user participation, which reduces the amount of data they are able to collect and thus their usefulness. Performing work or providing data for the collective good is not always an effective motivation on the long term. In many scenarios users prefer a "free ride" approach, waiting for others to volunteer and work towards their own goals [21].

A user incentives study by Zhang et al. divides user incentives into three major categories: a) **Entertainment incentives**, whereby the crowd sensing task is turned into a game, such that users can contribute to the initiative while playing; b) **Service provision in exchange for work**, which requires that sensing platform and users are able to provide mutual benefits to each other; c) **Monetary incentives**, whereby the sensing service pays a given amount of money (or an equivalent) in exchange for work [22]. Guo et al. include additional incentive types, such as **social** reasons (i.e., the ability to socializing with others or gaining recognition) or purely **ethical** reasons. Crowd-sensing systems may also indirectly enhance user participation by providing energy conservation or privacy protection mechanisms [5].

In a study by Gao et al. a further distinction is made between rewards for *server-initiated* and *user-initiated* sensing. Server-initiated sensing allows the service provider to select the user who will perform the sensing task. The provider thus retains all control over how tasks are scheduled and how they are rewarded. User-initiated sensing instead is based on users actively deciding when and where to collect data [23]. A survey by Ogie provides a similar distinction, based on whether the provider or the user is able to set the level of monetary rewards. Furthermore, rewards are divided into *static* and *dynamic* mechanisms: the first kind establishes the price of a sensing task in advance, while the second kind allows the price to vary based on volunteer demand [24]. Several rewarding schemes have been proposed based on the latter kind, mainly based upon an auction mechanism where users bid to win a task to complete [25].

In this work, we focus exclusively on user-initiated task assignment, with a fixed price. We propose a classification of these incentive strategies into 3 broad categories, which can be further distinguished by their anonymity properties, as shown in Table 1. Incentives based on **interest** rely on intrinsic motivations of volunteers, whereby they participate in the crowd-sensing task because of pre-existing interest or the enjoyment they find in the task itself. Volunteers may be allured by the introduction of game-like elements [26]. **Community** incentives are based on moral or ethical motivations. Communities promoting the crowd-sensing task may award volunteers with immaterial rewards such as reputation or trust. Games may leverage competition between participants. In case of anonymous contributions, volunteers may act out of sheer altruism. **Monetization** is based on financial rewards in exchange for contributions, which may be offered in the form of money—real or virtual. Pecuniary transfers usually require some form of user identification. Monetary incentives in the form of anonymous vouchers (which give access to goods outside of the crowd-sensing system) or credits (which give access to services within the platform) do not require knowledge about the user's identity. Incentives in this category do not depend on the nature of the task and can be applied to any kind of crowdsourced

Table 1. Rewarding schemes classification in terms of motivation provided and anonymization of user information.

Motivation	Non-anonymous	Anonymous
Interest	Social inclusion, belonging, social good.	Enjoyment, entertainment.
Community	Reputation, trust, competition.	Altruism.
Monetization	Virtual or *fiat* currency exchange, bidding, monetary transfers.	Vouchers, credits.

activity. Also, they are easy to adjust (i.e., doubling the incentives on a specific task can be done by doubling the prize, but it not so straightforward when dealing with interest- or community-based incentives) [27]. However, incentives in the monetary category risk attracting cheating users, willing to deceive the system in order to get access to higher financial gains [5].

C. Anonymity

A critical aspect of crowd-sensing systems is that they collect potentially sensitive data from sensors, which can be used to disclose personal information about individual contributors. In the design of participatory sensing platforms, the privacy of users must be protected both in terms of information inferred directly from the sensor readings as well as information implicitly conveyed by the interaction of users with the crowd-sensing system [2].

It has been shown that geolocation readings from a GNSS receiver can be effectively used to reconstruct information about the individual, such as commute patterns, routines, or private locations [28]. Start and end points of periodic vehicle trips can be used to infer the home or work address of drivers. Different approaches have been proposed in literature to prevent user tracking in a dataset of GNSS tracks [29]. Other kinds of data, such as microphone or camera sensor data, can also be effectively cross-linked with other information provided by individuals, in order to infer their participation to crowd-sensing systems [30].

Privacy requirements are usually very user-specific (i.e., each user has a different perception of the information that they are willing to share privately or publicly within a crowd-sensing service), but the adoption of a crowd-sensing service heavily depends on its privacy guarantees and its perceived trustworthiness. It is crucial that no additional information can be inferred by third-parties (i.e., cannot be "leaked" from context or via cross-linking) that the promised privacy criteria are ensured by the system, and that sensitive information is either securely stored or never collected in the first place [1]. In addition to third-parties, it is often desirable for user contributions to be also protected from the crowd-sensing service provider itself, which might act in an "honest but curious" fashion and attempt to access sensible private information [31].

However, privacy and anonymity usually clash with other requirements such as accountability, non-repudiation, and quality control of collected data. Also, user anonymity often precludes the establishment of reputation systems, even if recent research efforts have addressed this problem with reputation schemes that do not leak sensitive information about user activities [32], [33]. Crowd-sensing systems face high security, data integrity, and quality requirements, which usually require state-of-the-art authentication and identification mechanisms. In the most general case, these systems must establish verified associations between contributions and user identities, which negate most privacy-preserving precautions.

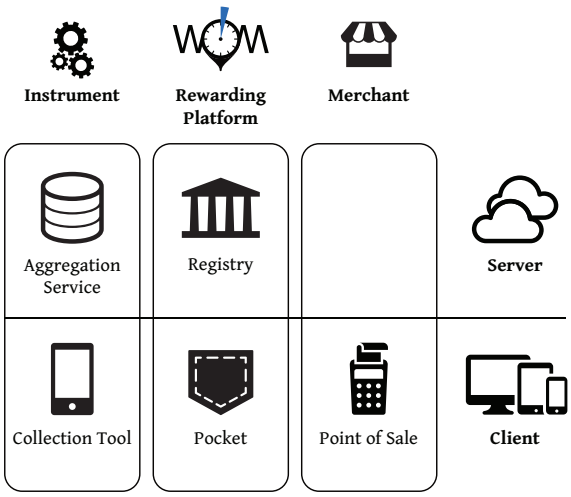

Fig. 1. Overview of the platform's components.

In order to ensure an adequate privacy level despite the presence of user-identifying information, different techniques have been proposed in literature. For instance, *k-anonymity* [34], by which a data set including personal information can be transformed to ensure that no information can be linked to sets of less than k individuals, or pseudonym schemes [35], which make use of derived identifiers that are usable for authentication but do not contain personal information. Other techniques proposed include differential privacy, which adds noise to the contents of a data set in order to hide information of individuals while retaining the results of aggregate analyses [36].

While these techniques provide a formal model for ensuring that published data cannot be effectively cross-linked, it has been argued that anonymized sensitive data still leads to privacy risks and that further data obfuscation may be desirable to ensure user protection [37], [38].

In this work, partial data disclosure and obfuscation techniques are used to trade between the granularity of the information-based incentive schemes and the robustness of the privacy-preserving data sharing mechanisms.

III. DESIGN OF THE WOM PLATFORM

The WOM platform has been designed bearing in mind the peculiar features of contributions in typical mobile crowd-sensing systems but is not limited to crowd-sensing alone. Rather, the platform is intended to support rewarding in any scenario where volunteers contribute to the common good and provide intrinsic social value.

Each voucher generated by the platform represents compensa-

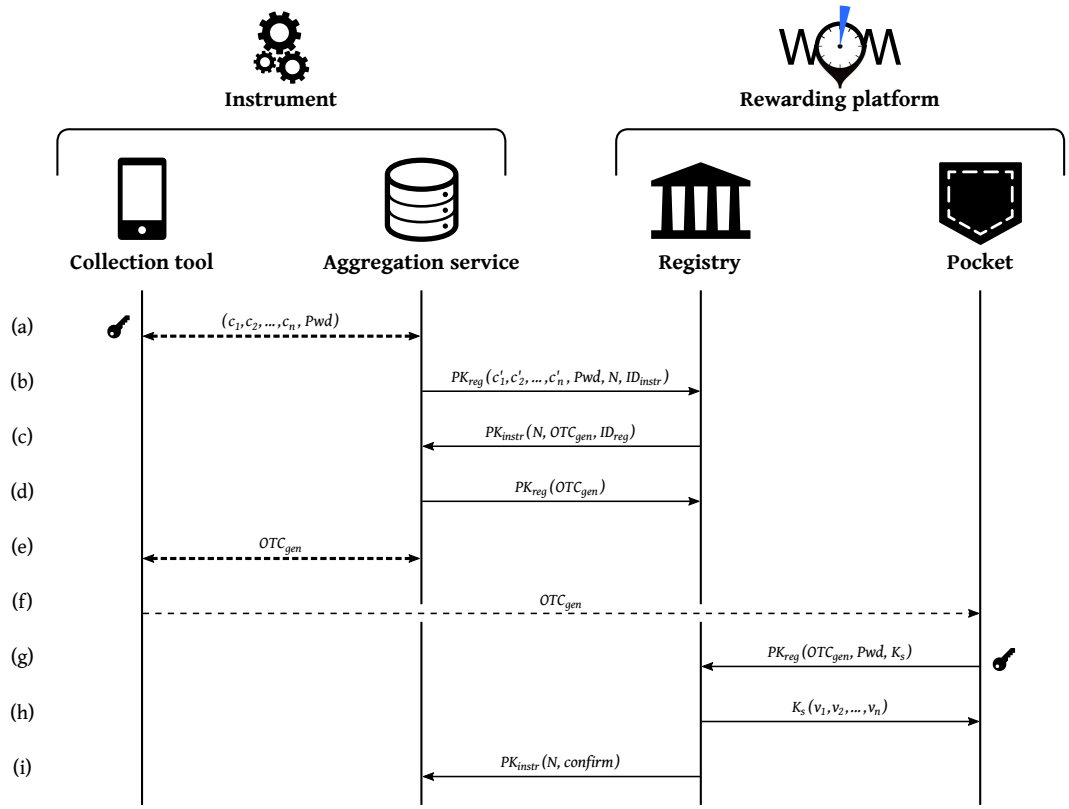

Fig. 2. Diagram of the communication protocol for generating vouchers.

tion for one minute of work performed towards a cause. As such, a voucher is "worth one minute" of the volunteer's time (or an equivalent effort). Vouchers take the name of "WOMs" within the "WOM platform", by virtue of this. As a homogeneous way of rewarding the efforts by individual volunteers, it turns commitment to a collective cause into an effort-based currency. The voucher system eschews the complications of real currencies while also preventing common virtual currency misbehaviors (e.g., forgery, double spending, cheating, or speculation) [39].

Vouchers are produced as compensation for specific user contributions and thus are intrinsically tied to a geographical position (i.e., *where was the contribution generated?*), a timestamp (i.e., *when was the contribution generated?*), and a purpose (i.e., *which application was used by the user and for what common cause?*). Moreover, vouchers are designed not to include any information about the user, nor are they tied to any particular identity.

A. Use Cases

WOMs are designed for mobile crowd-sensing, but are intended to reward any kind of effort towards the common good: preliminary tests focused on offline educational scenarios have been performed, as reported in a previous study [11]. The design of the online platform has been shaped by the following use case scenarios:

- *UC1:* A mobile crowdsensing application that collects geolocalized data through smartphone sensors (such as *SmartRoadSense*, which collects road roughness data through smartphone accelerometers made available by volunteer drivers [40]).
- *UC2:* A crowdsensing application that collects sensor data from fixed sensors (such as *hackAIR*, which collect air quality measurements from stationary sensing stations [41]).
- *UC3:* A short-term volunteer-based initiative, focused on 'citizen science' [42], environmental issues, or other common good subjects (for instance the "Christmas Bird Count" or a beach litter cleanup action).
- *UC4:* Personal development or education, such as university courses, schools, cultural initiatives, or online courses.

While only *UC1* and *UC2* fit within crowdsensing in a strict sense, in the context of the WOM platform, all of these use-cases represent valuable contributions from individuals to their community and to the common good as a whole. These use-cases represent a non-exhaustive set of initiatives that can be rewarded by the platform by converting efforts by individuals into WOM vouchers.

B. Platform Architecture and Actors

The proposed voucher system takes care of the following basic **operations**: (a) Generating vouchers, (b) transferring them to the intended recipient, (c) verifying their validity, and (d) exchanging them in verifiable transactions.

The following **actors** take part in the proposed voucher system and are shown in Fig. 1:

- *Aim*: A goal or cause towards the common good that volun-

teers may contribute their efforts to and that is recognized by the rewarding platform;
- *Volunteers*: Individuals that invest time and effort in order to pursue a common aim using an *Instrument*;
- *Registry*: Central authority that issues vouchers and processes payments;
- *Instrument*: Any kind of system participating in the rewarding platform and used by volunteers in order to perform work towards a common *Aim*;
- *Merchant*: Third-party interested in one or more *Aims*, which may reward volunteers by exchanging vouchers for goods or services;
- *Pocket*: Tool made available by the rewarding platform that allows volunteers to collect and store vouchers, implemented as a mobile application;
- *Point of Sale* (POS): Technical end-point that allows merchants to accept vouchers.

In Fig. 1, actors are separated into server-side and client-side components, based on how they will be technically implemented. As is the case for most mobile crowd-sensing systems, the *Instrument* is split up into a client-side "collection tool" (usually a mobile application or other local software that performs the sensing task) and a remote "aggregation service" that receives the data and processes it. Both components are not controlled in any way by the rewarding platform. The *Instrument*'s server-side component is able to communicate with the *Registry*.

All instances of *Instruments* and *Merchants* participating in the platform are known and registered by the *Registry*. Single users that contribute in crowd-sensing initiatives adopting *Instruments* are not known to the platform's *Registry*. Likewise, single *Pocket* installations on user devices are not registered and not linked to any user identity.

Registry and *Instrument* entities control the generation of vouchers: they both must be considered as trusted entities in the context of the platform. Single *Instruments* have an established trust relationship with their users, whose private data they collect (measurements, locations, and/or other sensible information). Privacy and security issues between users and *Instruments* are out of the scope of this work: communication between these entities is considered to be secure.

C. Platform Management and Voucher Value

The WOM platform is designed to attract volunteer-based initiatives on one side and third-party subsidizers on the other one, both pursuing shared causes for the common good. Given that voucher creation is linear with the amount of effort invested by volunteers and there is no upper bound to the number of existing vouchers, control must be exercised over the behavior of voucher creators (i.e., *Instruments*). The platform needs to limit the risk of inflation and guarantee fair treatment of volunteer efforts, in spite of the diversity of aims they pursue and instruments they adopt.

The addition of a new *Instrument* to the platform must be carefully evaluated, because of the trust relationship that is established with the *Registry*. The platform provides a formal approval process through a **transparent ethical committee**, whose purpose is that of evaluating the pertinence of *Instruments* joining the platform and their contributions to shared aims. An objective metric used to measure user contributions and efforts, collected and validated by an *Instrument*, is established and approved by the committee. The committee also establishes to which common *Aims* vouchers by an *Instrument* are attributed to. Technical correctness of the *Instrument*'s client-side tools must be certified, to ensure that volunteers cannot exploit the system to gain uncontrolled access to vouchers and that generated vouchers are proportional to the actual effort provided by users. Once an *Instrument* is registered it obtains the ability to request new vouchers on behalf of its users and its compliance with the platform's ethical and technical requirements is publicly certified. This ability can be revoked in case of misbehavior.

As the *Instrument* creates vouchers on behalf of the user for units of work that are "worth one minute", it acts as a validator for the contributed work: in *UC1* for instance, the mobile crowd-sensing system must adequately verify that user contributions are significant and that users are not allowed to cheat (i.e., obtaining vouchers for faked work). Similarly, in *UC4*, initiative organizers verify and guarantee the work done by participants (e.g., lessons have been attended, courses have been passed, etc.).

Conversely, *Merchants* exchanging vouchers for rewards shall not be subject to the same approval process, since voucher spending raises fewer concerns for the platform's fairness than voucher generation. Integration with the platform through a *Point of Sale* is encouraged and requires no formal evaluation and certification. Once a *Merchant* and its *Point of Sale* are registered, they obtain the ability to receive vouchers in payment. This ability can also be revoked by the *Registry* in case of misbehavior.

Instruments participating in the platform independently determine how to fairly attribute vouchers, while the platform does not discriminate between more or less "useful" work. *Merchants* however will be able to discriminate the vouchers to accept in payment, based on voucher source, aim, position, and/or time. This approach is intended to allow merchants to determine which contributes to incentivize, while still ensuring that all user contributions to the common good are perceived as equally worthy.

IV. IMPLEMENTATION

A. Voucher Generation Protocol

This protocol is used to generate a number of vouchers and grant them to a user, in compensation for previous contributions. The procedure, which is shown in Fig. 2, is initiated by the *Instrument*. The *Instrument* requires new vouchers from the *Registry*. Once the voucher creation has been initiated, the process is completed by an additional interaction between the volunteer's *Pocket* and the *Registry*.

In detail, the generation protocol is articulated as follows:

(a) Within the *Instrument*, the collection tool transfers contributions $(c_1, \cdots, c_n)$ to the aggregation service. Each c_i contains geolocation, a timestamp, and a reference to an *Aim* for which a voucher needs to be generated. The user may choose to omit or partially obfuscate this information at the desired granularity level. Hence, the *Instrument* provides a set of contributions $(c'_1, \cdots, c'_n)$ to the *Registry* that may be altered based on the user settings (see Section IV.E for the details). In this phase, the collection tool establishes a fresh secret

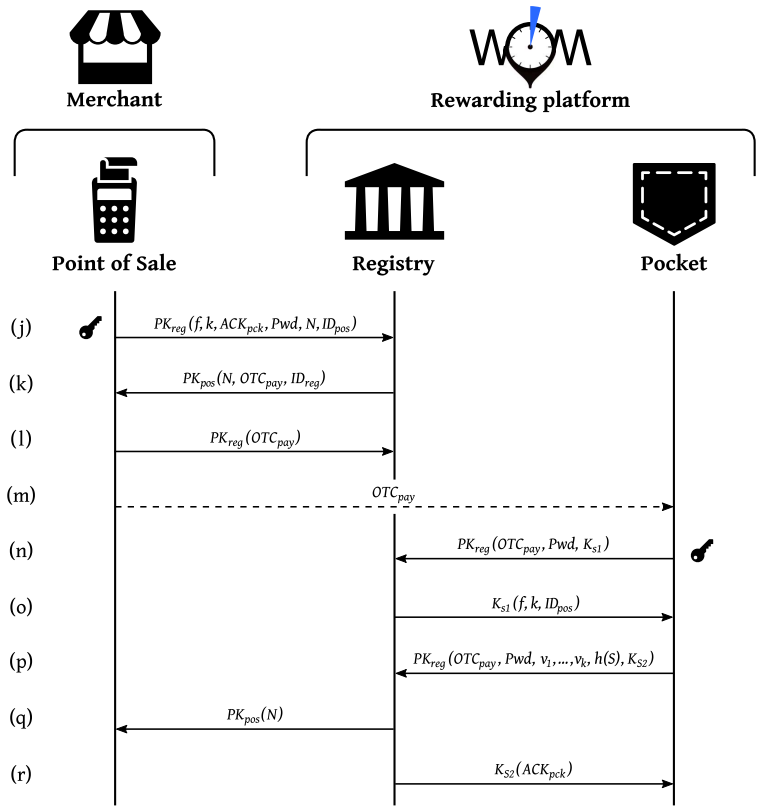

Fig. 3. Diagram of the communication protocol for performing payments.

Pwd, known to the user and shared by the two parties. The secret can be generated randomly by the *Instrument* or picked by the user, and it is never transmitted after this step. *Pwd* must be communicated out of band (e.g., shown on screen) to the user, who will use it to confirm the process in step (g).

(b) The *Instrument*'s back-end registers the volunteer's contributions and requests the generation of n vouchers from the *Registry*. The message contains contribution proofs c_i, possibly including details such as geographical position, timestamp, and aim of the original contributions. The message also contains a random nonce N and ID_{instr}, an identifier of the *Instrument*. The request is encrypted with the *Registry*'s public key PK_{reg}.

(c) The *Registry* issues new vouchers and generates a one-time code, OTC_{gen}. The code, together with the nonce N and a unique identifier of the *Registry*, is returned to the *Instrument*, encrypted using its public key PK_{instr}.

(d) The *Instrument* sends back a confirmation message containing OTC_{gen}, encrypted with the *Registry*'s public key.

(e) The collection tool receives the one-time code. As for step (a), this transfer is out of the scope of this paper and will depend on the *Instrument*'s implementation.

(f) OTC_{gen} is transferred to the volunteer's *Pocket*. This transmission is in the clear. Invocation of the *Pocket* relies on the one-time code being represented as a URL, as described in Section IV.F.

(g) The *Pocket* sends a redeem request to the *Registry*. It asks the user to provide *Pwd*, the secret known to *Instrument* and *Registry* after step (b). Then, OTC_{gen}, *Pwd*, and a fresh session key K_s are included in a message encrypted using the public key PK_{reg} and sent to the *Registry*.

(h) The *Registry* verifies the one-time code's validity and if *Pwd* matches the known secret between it and the *Instrument*. If the request can be satisfied, vouchers v_i are encrypted using the session key K_s and returned to the *Pocket*, which stores them. If *Pwd* does not match the known secret, the generation request is invalidated and cannot be used again.

(i) The *Registry* acknowledges the successful transfer with a message to the *Instrument*, containing the nonce N (as a unique identifier for the transaction).

Instrument and *Registry* are known entities within the platform and have public keys PK_{instr} and PK_{reg} used to encrypt messages in (b)–(d), (g), and (i). The *Pocket* is represented by instances of a mobile app installed on a user device: Single installation instances are not known to the platform. All communication between *Pocket* and *Registry* rely on public key PK_{reg} and a temporary session key K_s.

At step (a) and (g) the user must provide *Pwd*, a secret value that ensures that OTC_{gen} is transferred to the intended recipient and that vouchers are not reclaimed by malicious users. The secret may be established beforehand by the *Instrument* or it may be generated by the *Instrument*'s collection tool before requesting vouchers. The *Pocket* will explicitly ask the user to input *Pwd* before issuing the request message at (g).

Details of the internal communication protocol adopted by the *Instrument* depend on the crowd-sensing service and are out of scope for this paper. The message protocols at step (a) and (e) are considered reliable and secure.

B. Payment

This action consists in the exchange of a number of a volunteer's vouchers with a third-party *Merchant*. The exchange is made possible by the interaction between the merchant's *Point of Sale* and the volunteer's *Pocket*, as shown by the protocol diagram in Fig. 3.

The protocol is specular to the communication protocol between *Instrument* and *Registry*. In detail:

(j) The *Merchant* creates a new "payment instance" through the *Registry*. This can be done in advance (for future goods and services offered) or in response to user action (the user accesses the *Point of Sale* and requests goods or services). The *Merchant* establishes a secret *Pwd* and sends it to the *Registry*, together with a voucher filter f (see Section IV.D), the number of requested vouchers k (i.e., the "cost"), a confirmation URL ACK_{pck}, a unique nonce N, and the *Point of Sale* identifier ID_{pos}. The message is encrypted with PK_{reg}.

(k) The *Registry* generates a new one-time code OTC_{pay} for the payment and sends it back with the nonce N and the unique identifier of the *Registry*, encrypted using the *Merchant*'s public key PK_{pos}.

(l) The *Merchant* sends back a confirmation containing OTC_{pay}, encrypted with the *Registry*'s public key.

(m) OTC_{pay} is transferred from the *Merchant* to the volunteer's *Pocket*. This transmission is in the clear, akin to step (f) in Fig. 2.

(n) The *Pocket* asks the user to provide *Pwd*, the secret known to *Merchant* and *Registry* after step (j). Then, *Pwd*, OTC_{pay} and a fresh session key K_{s1} are included in a message sent to the *Registry* and encrypted using PK_{reg}.

(o) The *Registry* provides information about the payment instance, including the voucher filter f, the requested amount k, and the *Merchant*'s identity ID_{pos}, included in a message sent to the *Pocket* and encrypted using the fresh session key K_{s1}. The *Pocket* determines whether payment conditions can be satisfied (i.e., enough vouchers satisfying the filter f are owned by the volunteer). If they are, payment information is explicitly shown to the user for confirmation, including the *Merchant*'s identity, the amount k, and the filter f. If not, the payment cannot proceed and the process is terminated. As discussed in Section IV.E, when confirming a payment the *Pocket* is disclosing that the user owns at least k vouchers satisfying f, which might leak personal information if very specific filters are used. Users must be fully aware of the *Merchant*'s filter and identity before accepting a payment.

(p) An amount k of vouchers is transferred to the *Registry*. After this step, vouchers are considered to be lost to the *Pocket* and the user. The *Pocket* generates a "secret" in the form of a random sequence S. The secret is stored by the *Pocket* and its digest $h(S)$ is transmitted to the *Registry*. The payment request to the *Registry* contains OTC_{pay}, *Pwd*, a sequence of k vouchers v_i that satisfy f, $h(S)$, and a fresh session key K_{s2}. The message is encrypted using PK_{reg}.

(q) The *Registry* independently verifies that all vouchers v_i satisfy the payment conditions. If so, the payment is confirmed and the *Registry* notifies the *Merchant*, using the nonce N as a unique identifier. Vouchers and their information are never transmitted to the *Merchant*.

(r) The *Registry* sends a payment confirmation to the *Pocket*, containing the URL ACK_{pos}, encrypted using K_{s2}. The *Pocket* invokes ACK_{pos} to confirm the payment to the user.

Like in the voucher generation protocol in Section IV.A, *Merchant* and *Registry* are known entities within the platform and have public keys PK_{pos} and PK_{reg}, used to encrypt messages in (j)–(l), (n), (p)–(q). Communication between *Registry* and *Pocket* is secured by temporary session keys K_{s1} and K_{s2}.

Before step (p), a random secret S is generated by the *Pocket* and stored. A hash $h(S)$ is transmitted to the *Registry*, which stores it when confirming the payment. If at any point the proof of payment is needed to resolve a payment controversy, the *Pocket* can provide S as indisputable proof of having performed the payment. This mechanism allows the platform to forego *Pocket* registration and user identification.

C. Security Discussion

The analysis of the protocols refers to a threat model respecting the classical Dolev-Yao security assumptions [43]. Hence, we consider an external intruder with full control of the network and without any cryptanalysis capability.

The security properties of interest for the protocol of Fig. 2 are mutual authentication of the servers involved (*Instrument* and *Registry*) and the confidentiality of the vouchers, which shall be known only to the Registry and the legitimate user.

The initial phase of the protocol of Fig. 2 relies on the data exchange between the client and the server components of the *Instrument* and is specific of the kind of application that is connected to the rewarding platform (see e.g. [40] for an example crowd-sensing system). Hence, all the communications between these two parties, represented by thick dashed lines, are secured by hypothesis. In particular, for the security conditions related to the rest of the protocol execution, it is sufficient to assume that these parties agree on the confidential secret *Pwd*.

The rest of the protocol is decoupled to make the voucher management independent of the specific *Instrument* and involves two steps: the voucher generation by the *Registry* in response to a legitimate *Instrument* request and the claim of the vouchers by the *Pocket* app of the legitimate user.

As far as the first step is concerned, the critical part of the protocol of Fig. 2 is represented by the handshake of messages (b)–(d), which is an instance of the Needham-Schroeder-Lowe authentication protocol [44], [45]. The protocol, which enables the mutually authenticated transmission of data over an insecure network using a set of private and public keys, is represented in its original version by the following message exchange between two agents A and B:

$$\begin{aligned} A &\rightarrow B : PK_B(N_A, ID_A) \\ B &\rightarrow A : PK_A(N_A, N_B, ID_B) \\ A &\rightarrow B : PK_B(N_B) \end{aligned}$$

where N_A, N_B are fresh nonces, generated by A and B, respectively. In particular, the role of the nonce N_A is played by the

nonce N of the message (b) and generated by the *Instrument* server, while the role of the nonce N_B is played by the fresh secret OTC_{gen} generated by the Registry. Therefore, by virtue of the security properties formally satisfied by the Needham-Schroeder-Lowe protocol, after the handshake the two parties, the *Instrument* server and *Registry*, are mutually authenticated and confidentially share the fresh secret (N, Pwd), generated at the *Instrument* side (we recall that Pwd is the secret shared between client and server) and the fresh secret OTC_{gen}. These shared secrets form the base for the validation of the rest of the protocol of Fig. 2.

The second step of the protocol is modeled by messages (e)–(i). After the handshake described above, the *Registry* is ready to issue the vouchers associated uniquely to the shared secrets. To this aim, the latter secret, OTC_{gen}, is securely communicated from the *Instrument* server to the *Instrument* client, see message (e), which then reveals it to the *Pocket* app, see message (f). As discussed more exhaustively in the following Section IV.F, this usually happens locally on the same device.

Afterwards, the *Pocket* app claims the vouchers from the *Registry*, see message (g), which are then transmitted to the *Pocket* app, see message (h). For this purpose, by using a two-message handshake as done, e.g., in SSL, message (g) is encrypted with the public key of the *Registry* and includes a fresh session key K_s, which will be used by the *Registry* to encrypt the following message (h). Exactly as proven in the case of SSL (see, e.g., [46], [47]), the handshake of messages (g) and (h) guarantees the confidentiality of the vouchers claim/transfer, as only the *Registry* can decrypt message (g) and only the user generating such a message can decrypt message (h). Moreover, notice that the validity of message (g) is guaranteed by the pair (OTC_{gen}, Pwd), where Pwd is asked to the user. If the pair transmitted in message (g) does not match the pair stored by the *Registry*, then the claim is not valid and the related vouchers are not issued, otherwise the claim is successful and the vouchers are delivered through message (h). Such a behavior prevents attacks against the shared secrets via brute force or statistical procedures. Hence, thanks to the validity condition surveyed above, only the legitimate user can generate a successful claim message and only the legitimate parties share the vouchers at the end of the handshake. Notice also that the freshness of the shared secrets protects the handshake against replay attacks.

The vulnerabilities deriving from denial of service attacks (as in the case of an adversary blocking some message) do not compromise the security conditions of interest, as the vouchers are transmitted only at the last stage. Moreover, by employing the feedback provided by the final acknowledgment—see message (i), which is sent by the *Registry* to the *Instrument* server to notify the result of the vouchers claim—a possible extension could be proposed to design the *Instrument* in such a way to repeat the protocol in case of failure.

The security analysis of the protocol of Fig. 3 is based on the same argumentations. The security properties of interest are mutual authentication of *Merchant* and *Registry*, and the correctness of the payment, which shall be completed only by using legitimate vouchers.

As in the previous case, the handshake of messages (j)–(l) turns out to represent an instance of the Needham-Schroeder-Lowe authentication protocol, after which the two parties are mutually authenticated and share the fresh secrets exchanged during the interaction. Then, both the handshake of messages (n)–(o) and (p)–(r) represent two separate instances of the SSL-like handshake used also in the previous protocol. They allow a confidential interaction between *Registry* and *Pocket* to be instantiated thanks to which: (1) The payment request is issued, see message (n), and confirmed, see message (o); and (2) the payment is completed, see message (p), and acknowledged, see messages (q) and (r).

The secrecy and authentication properties of interest for the two protocols have been verified successfully by using *ProVerif*, an automatic cryptographic protocol verifier based on the Applied Pi Calculus and the formal adversary model of Dolev-Yao [48].

D. Vouchers and Filtering

Vouchers generated by the *Registry* are transmitted to the *Pocket*, which stores them until they are spent in a payment. Vouchers include the following information fields:

$$v = (ID, PIN, lat, lng, ts, ID_{\text{aim}}, ID_{\text{instr}}) \tag{1}$$

ID is a globally unique identifier for the voucher. The *Registry* assigns a randomly-generated unique identifier to each voucher. PIN is a secret string that is generated randomly by the *Registry* upon voucher generation. This secret value is intended to protect vouchers from abuse: at step (p) in Fig. 3 both ID and PIN must be provided for each voucher in order for the *Pocket* to use them in a payment. This prevents malicious *Pockets* from brute force attempts that use vouchers they have not earned.

Additional, optional fields represent information about the user contribution that the voucher rewards: couple *lat* and *lng* (respectively latitude and longitude) represent where the user contribution was generated and thus where the voucher was earned. The voucher's timestamp is described by ts, while ID_{aim} and ID_{instr} respectively represent the *Aim* and the *Instrument* of the contribution. Both values are unique identifiers known to the *Registry*.

In order to keep the payment system as simple as possible, WOM vouchers can either be spent completely or not at all. They have a unitary non-fractional value and cannot be further split. Change cannot be returned for a transaction.

When assigning goods and services in exchange for user contributions, *Merchants* may decide to incentivize work done through a particular *Instrument*, within a particular geographical region, or during a specific timespan. These preferences can be expressed as a **voucher filter**, indicated as f at step (j) of Fig. 3. The voucher filter restricts which vouchers can be used to satisfy a given payment, effectively limiting payment access to users with contributions that are significant to the *Merchant*.

The filter can combine one or more of the following acceptance criteria:

- Geographical boundaries in the form of a rectangle or a simple polygon,
- Time reference as a relative timespan from now (i.e., the *age* of the contribution),
- Identifier of the *Instrument* that generated the voucher,
- *Aim* of the volunteer's original contribution.

A voucher must satisfy all criteria, if specified, to be used within a payment. More complex payment filters can be expressed joining multiple filters with *OR* logical conjunctions.

When payment information (including f) is received at step (o) of Fig. 3, the *Pocket* filters the vouchers available to the user and determines whether the payment can be completed or not (i.e., if k or more vouchers satisfy filter f). At step (p), the *Registry* independently checks whether all vouchers satisfy the filtering conditions and accepts the payment. If more vouchers satisfy the same payment conditions, they can be picked randomly by the *Pocket* or they may be selected manually by the user.

E. Privacy Discussion

The proposed platform is designed to require no user registration and to avoid any form of user identification.

The platform is not aware of the transfer protocol used within the *Instrument* to provide user contributions and cannot directly associate voucher issue requests to specific *Instrument* users.

Despite that, the platform's *Registry* stores data about user contributions that includes geolocations, timestamps, which *Instrument* provided the information, and the *Aim* the volunteer contributed to (as per the voucher structure detailed in Equation 1). While users are not directly identifiable, the collection of this data could still expose them to potentially being identified by a "honest but curious" *Registry* [31], [37]. For this purpose, the user can specify that, in step (b) of Fig. 2, the *Instrument* has to hide or partially obfuscate information about contributions on the user's behalf: for instance, providing an approximation of the geolocation, or reducing the timestamp to week- or month-level resolution, or abstracting the details of the *Aim*. This constrains the *Registry*'s capacity to identify users, while keeping intact the platform's ability of rewarding contributions based on their properties. With reference to use-cases in Section III.A, mobile data collection scenarios like in *UC1* could call for a coarsening of location and time data. Domestic stationary data collection, like in *UC2*, can clearly expose where a user's home is located, thus suggesting an obfuscation of the location (at city- or regional-level), while timestamps can be kept intact. Time information related to specific initiatives or educational courses, like in *UC3* or *UC4*, can also provide links to private user information: in these cases time information can be reduced to year-level or stripped completely.

The *Instrument* has knowledge about the vouchers it issued, but it has no knowledge of which user actually redeemed them, nor whether they have been spent or not, or which *Merchant* accepted them as payment.

Conversely, *Merchants* can express a voucher filter f to select vouchers for payment, but they have no access to actual voucher data when they are spent. Thus, the *Merchant* gains no knowledge of specific details on user contributions that are stored within the voucher (location, time, *Instrument*, and *Aim*), which remain exclusive to the *Registry*. A malicious *Merchant* could however devise filters in order to verify whether a particular user owns vouchers satisfying certain constraints and thus identify the user's past behavior: this potential privacy compromise is countered by displaying filtering conditions to the user at step (o) in Fig. 3 and explicitly warn about the information the user is about to disclose before performing the payment. If the potential privacy leak is considered inappropriate, the user may refuse payment, thus invalidating the transaction. In such a case the *Merchant* will not be aware of the reasons of the failure, either based on user decision or the lack of vouchers satisfying the filtering requirements.

F. One-Time Codes

The protocols make use of *one-time codes* (OTCs) both for identifying a voucher creation request and a payment instance waiting to be completed. In both cases, the one-time code uniquely identifies a pending voucher operation on the *Registry*'s side.

In practice, unique one-time codes take the form of an URL using a common *scheme* and including the operation's unique identifier in their *path* section. For instance:

```
wom://payment/7d9bd006
```

One-time codes have been designed to be expressed as simple URLs to ease interoperation with mobile applications handling voucher collection and expenditure. On most mobile application platforms, including Android and iOS, mobile applications can register as handlers for specific URL *schemes* or *hosts*. Matching URLs act as so-called "deep links" to the applications, seamlessly transitioning from the URL to the application and supplying custom launch parameters (that can be encoded within the *path* like the unique identifier in the sample URL above) [49]. This design choice allows for seamless voucher acquisition and payment on most mobile platforms.

In most scenarios, one-time codes are generated by the *Instrument*'s client on the user's device and are invoked as "deep links" on the device itself. The *Pocket*, if installed on the user's device, will locally handle the request. That is, the dashed communication at (f) in Fig. 2 and (m) in Fig. 3 never leaves the user's device.

Optionally, the use of URLs with the standard HTTP *scheme* provide a fallback mechanism for when target mobile applications (e.g., the *Pocket*) is not installed on the user's device: in this case the built-in browser will display a landing Web page, which can then prompt the user to install the mobile application and join the platform.

However, URL invocations can be handled by any mobile application installed, which makes OTCs susceptible to be intercepted by malicious applications even if the user's device is not compromised. On most modern mobile platforms, URL-based application activations can be ensured to target only authorized applications using "App Links" [49]. On platforms that do not support this feature or on compromised devices, OTCs can be intercepted. In this scenario, voucher generation or payment instances are protected by the secret *Pwd*, which is known to the user, the *Instrument*, and the *Registry*, after the initial handshake at (b) and (j) respectively. Malicious applications, in this case, can deny the service to the user or they must explicitly and visibly ask for the user's secret through a *phishing* attack, which can be countered with appropriate methods in the *Pocket* implementation [50].

Finally, one-time codes in URL form also allow to encode OTC_{gen} or OTC_{pay} instances as QR Codes, that can be shown on

screen or printed out, enabling a set of offline scenarios described in the next Section.

G. Offline Scenario

The WOM platform is designed not only to accommodate common mobile crowd-sensing scenarios but also to be used as a rewards system for any kind of initiative towards the common good, including ones that are offline or may not rely on connected devices (see *UC3* or *UC4*). While *Registry* and *Pocket* must be connected at the time that vouchers are effectively transmitted, *Instruments* and *Merchants* can provide the same services of assigning vouchers and accepting payments by pre-generating one-time codes OTC_{gen} or OTC_{pay} in advance, splitting both protocols into two phases.

In the case of an offline *Instrument* (for instance, a teaching course that wants to reward the efforts of a student), a one-time code for a preset amount of vouchers can be generated in advance of the activity. The *Instrument* (which in this scenario will not be composed of independent client and server tools) will specify the contribution details in step (b) of Fig. 2, receiving an OTC_{gen}. Likewise, an offline *Merchant* can generate a payment OTC_{pay} for each item on offer, setting appropriate voucher filtering options and voucher amounts. In this scenario, one-time codes can be exposed as QR Codes and thus work just like a price tag for goods or services on offer.

However, in an offline scenario, users cannot provide the custom secret *Pwd*, which is needed at (b) in Fig. 2 and (j) in Fig. 3. The secret must thus be randomly pre-generated by the *Instrument* (or the *Merchant*, respectively) and communicated to the user. Since both the one-time code and the secret are needed to redeem vouchers or to perform the payment, they should be ideally transmitted separately, following common username and password security guidelines.

While both protocols feature acknowledgments of the procedure (step (i) in Fig. 2 and step (q) in Fig. 3) that notifies *Instrument* and *Merchant* of its outcome, this cannot be replicated in an offline scenario. In the case of an offline payment, the *Pocket* acknowledgment in step (r) in Fig. 3 is designed to provide the means of giving proof of the payment to the *Merchant*. During payment setup, the *Merchant* supplies an ACK_{pck} URL that may include unique information about the payment. The value is transmitted back to the *Pocket*, which will display the URL either as a QR Code or by invoking it. The QR Code can easily be scanned even by an offline *Merchant*, verifying if it matches the issued payment request. Otherwise, the URL can be used by the *Pocket* to invoke a Web page or a local mobile application, also providing proof of payment and finalizing the transaction. As mentioned previously, in case of dispute the *Pocket* may provide the random secret generated when performing the payment, which provides indisputable proof of payment to an online *Merchant*.

V. DISCUSSION

The growth of mobile crowd-sensing systems based on mobile and edge devices, in a scenario of almost ubiquitous sensors made available by 'Internet of Things' devices, enables users to easily and significantly contribute to data collection initiatives that they find appealing or useful. Many of these initiatives address real-world problems or pursue goals of public utility.

In this paper we presented a novel user rewarding platform, called "Worth One Minute", specifically designed for mobile crowd-sensing contributions but open to any initiative that aims at rewarding efforts towards the common good and the intrinsic social value of volunteer work. The basic tenets of the platform are: (a) it provides rewards for each unit of work performed by volunteers towards a common cause, turning vouchers into an effort-based currency; (b) it provides a flexible form of anonymity for its users (it requires no registration and completely eschews any form of user identification, while users are allowed to tune the granularity of the information populating the vouchers); (c) it decouples the data collection system from the rewarding system, effectively providing a platform for multiple systems based on volunteer contributions and third-party stakeholders subsidizing volunteer work; (d) it allows reward providers to independently choose how to incentivize efforts based on their location, time, and aims, thus encouraging specific kinds of volunteer work and implementing incentivization strategies and policies; (e) it allows "offline" scenarios for *Instruments* and *Merchants* that cannot or wish not to integrate with the platform at a technical level, but are still able to generate or consume vouchers.

The proposed platform's operations are based on two communication protocols, allowing *Instruments* to generate vouchers and *Merchants* to accept them as payments. Details of both protocols have been presented in this paper, with a thorough discussion of their security and privacy implications.

A. Platform Release

The implementation of the WOM platform has been developed in the open and the source code is released publicly on GitHub under an MIT License (`https://github.com/WOM-Platform`). The two components managed by the platform itself, *Registry* and *Pocket*, have reached full development and, at the time of writing, are released for an internal beta. *Merchant* and *Instrument* interface points allow third-parties to integrate with the platform and to make use of the rewarding scheme.

B. Future Work

In order to encourage adoption by *Merchants*, additional easy-to-use software interfaces will be developed for the integration with a variety of systems. This will include a simple Web dashboard to generate payments instances in the form of QR Codes, which can be scanned by users with the *Pocket* application.

The long-term behavior and stability of the system, the effect of merchant-side targeted incentives, and the effective inflation risk will be evaluated in a follow-up study after significant adoption of the platform has been achieved.

Acknowledgments

We wish to thank Niko Bizzarri and Gian Marco Di Francesco for their work in the implementation of the WOM *Registry* and *Pocket*.

We also wish to thank reviewers of a previous version of this work for their insightful comments.

REFERENCES

[1] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, R. A. Peterson, H. Lu, X. Zheng, M. Musolesi, K. Fodor, and G.-S. Ahn, "The rise of people-centric sensing," *IEEE Internet Comput.*, vol. 12, no. 4, pp. 12–21, July 2008.

[2] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *J. Systems Software*, vol. 84, no. 11, pp. 1928–1946, Nov. 2011.

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

[4] D. C. Brabham, "Crowdsourcing as a model for problem solving: An introduction and cases," *Convergence*, vol. 14, no. 1, pp. 75–90, 2008.

[5] B. Guo, Z. Wang, Z. Yu, Y. Wang, N. Y. Yen, R. Huang, and X. Zhou, "Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm," *ACM Comput. Surveys*, vol. 48, no. 1, pp. 1–31, 2015.

[6] T. Luo, S. S. Kanhere, J. Huang, S. K. Das, and F. Wu, "Sustainable incentives for mobile crowdsensing: Auctions, lotteries, and trust and reputation systems," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 68–74, 2017.

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

[8] L. C. Klopfenstein *et al.*, "Mobile crowdsensing for road sustainability: exploitability of publicly-sourced data," *International Review Applied Economics*, pp. 1–22, July 2019. [Online]. Available: https://doi.org/10.1080/02692171.2019.1646223

[9] C. Shapiro and H. R. Varian, "Information rules: A strategic guide to the network economy," *J. Economic Education*, vol. 30, no. 2, pp. 189–190, 1999.

[10] G. G. Parker, M. Van Alstyne, and S. P. Choudary, *Platform revolution: How networked markets are transforming the economy and how to make them work for you*. W. W. Norton New York, 2016.

[11] L. C. Klopfenstein, S. Delpriori, A. Aldini, and A. Bogliolo, "Introducing a flexible rewarding platform for mobile crowd-sensing applications," in *Proc. IEEE PerCom Workshops*, Mar. 2018, pp. 728–733.

[12] L. Pournajaf, D. A. Garcia-Ulloa, L. Xiong, and V. Sunderam, "Participant privacy in mobile crowd sensing task management: A survey of methods and challenges," *ACM SIGMOD Record*, vol. 44, no. 4, pp. 23–34, 2016.

[13] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," *IEEE Commun. Mag.*, vol. 48, no. 9, 2010.

[14] N. Györbíró, Á. Fábián, and G. Hományi, "An activity recognition system for mobile phones," *Mobile Netw. Applications*, vol. 14, no. 1, pp. 82–91, 2009.

[15] M.-Z. Poh, D. J. McDuff, and R. W. Picard, "Non-contact, automated cardiac pulse measurements using video imaging and blind source separation." *Optics express*, vol. 18, no. 10, pp. 10 762–10 774, 2010.

[16] O. Omokaro and J. Payton, "Flysensing: A case for crowdsensing in the air," in *Proc. PerCom Workshops)*, Mar. 2014, pp. 545–550.

[17] P. Schneider, N. Castell, M. Vogt, F. R. Dauge, W. A. Lahoz, and A. Bartonova, "Mapping urban air quality in near real-time using observations from low-cost sensors and model information," *Environment International*, vol. 106, pp. 234–247, 2017.

[18] P. Dutta, P. M. Aoki, N. Kumar, A. Mainwaring, C. Myers, W. Willett, and A. Woodruff, "Common sense: participatory urban sensing using a network of handheld air quality monitors," in *Proc. ACM Sensys*. Nov. 2009, pp. 349–350.

[19] S. Coulson, M. Woods, M. Scott, D. Hemment, and M. Balestrini, "Stop the noise! enhancing meaningfulness in participatory sensing with community level indicators," in *Proc. ACM DIS*, June 2018, pp. 1183–1192. [Online]. Available: http://doi.acm.org/10.1145/3196709.3196762

[20] A. Donnelly, O. Crowe, E. Regan, S. Begley, and A. Caffarra, "The role of citizen science in monitoring biodiversity in ireland," *International J. Biometeorology*, vol. 58, no. 6, pp. 1237–1249, Aug 2014. [Online]. Available: https://doi.org/10.1007/s00484-013-0717-0

[21] B. Simon, M. Loewy, S. Stürmer, U. Weber, P. Freytag, C. Habig, C. Kampmeier, and P. Spahlinger, "Collective identification and social movement participation." *J. personality social psychology*, vol. 74, no. 3, p. 646, 1998.

[22] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *IEEE Commun. Surveys Tutorials*, vol. 18, no. 1, pp. 54–67, 2016.

[23] L. Gao, F. Hou, and J. Huang, "Providing long-term participation incentive in participatory sensing," in *IEEE INFOCOM*. Apr. 2015, pp. 2803–2811.

[24] R. I. Ogie, "Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: from literature review to a conceptual framework," *Human-centric Comput. Information Sciences*, vol. 6, no. 1, p. 24, Dec. 2016.

[25] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, "Enabling Privacy-Preserving Incentives for Mobile Crowd Sensing Systems," in *Proc. IEEE ICDCS*, June 2016, pp. 344–353.

[26] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: defining "gamification"," in *Proc. ACM MindTrek*, Sept. 2011, pp. 9–15.

[27] J. J. Horton and L. B. Chilton, "The labor economics of paid crowdsourcing," in *Proc. ACM EC*, June 2010, pp. 209–218.

[28] J. Krumm, "A survey of computational location privacy," *Personal Ubiquitous Comput.*, vol. 13, no. 6, pp. 391–399, 2009.

[29] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking," *IEEE Trans. Mobile Comput.*, no. 8, pp. 1089–1107, 2010.

[30] L. Juhász and H. H. Hochmair, "Cross-linkage between Mapillary street level photos and OSM edits," in *Geospatial Data in a Changing World*. Springer, 2016, pp. 141–156.

[31] K. Yang, K. Zhang, J. Ren, and X. Shen, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 75–81, 2015.

[32] X. O. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Artsense: Anonymous reputation and trust in participatory sensing," in *Proc. IEEE INFOCOM*, April 2013, pp. 2517–2525.

[33] E. Zhai, D. I. Wolinsky, R. Chen, E. Syta, C. Teng, and B. Ford, "AnonRep: Towards tracking-resistant anonymous reputation." in *Proc. USENIX NSDI*, Mar. 2016, pp. 583–596.

[34] L. Sweeney, "k-anonymity: A model for protecting privacy," *International J. Uncertainty, Fuzziness Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[35] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[36] C. Dwork, "Differential privacy: A survey of results," in *Proc. TAMC*, Apr. 2008, pp. 1–19.

[37] H. Zang and J. Bolot, "Anonymization of location data does not work: A large-scale measurement study," in *Proc. ACM MobiCom*, Sept. 2011, pp. 145–156.

[38] M. Backes, P. Berrang, O. Goga, K. P. Gummadi, and P. Manoharan, "On profile linkability despite anonymity in social media systems," in *Proc. ACM WPES*, Oct. 2016, pp. 25–35.

[39] A. Bogliolo, P. Polidori, A. Aldini, W. Moreira, P. Mendes, M. Yildiz, C. Ballester, and J.-M. Seigneur, "Virtual currency and reputation-based cooperation incentives in user-centric networks," in *Proc. IEEE IWCMC*, Aug. 2012, pp. 895–900.

[40] G. Alessandroni, L. C. Klopfenstein, S. Delpriori, M. Dromedari, G. Luchetti, B. D. Paolini, A. Seraghiti, E. Lattanzi, V. Freschi, A. Carini, and A. Bogliolo, "SmartRoadSense: Collaborative road surface condition monitoring," in *Proc. UBICOMM*. Aug. 2014.

[41] E. Kosmidis *et al.*, "hackAIR: Towards Raising Awareness about Air Quality in Europe by Developing a Collective Online Platform," *ISPRS International J. Geo-Information*, vol. 7, no. 5, 2018.

[42] J. Silvertown, "A new dawn for citizen science," *Trends Ecology Evolution*, vol. 24, no. 9, pp. 467–471, Sept. 2009.

[43] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[44] G. Lowe, "An attack on the Needham-Schroeder public-key authentication protocol," *Information Processing Letters*, vol. 56, no. 3, pp. 131–133, 1995.

[45] G. Lowe, "Breaking and fixing the Needham-Schroeder public-key protocol using FDR," in *Tools and Algorithms for the Construction and Analysis of Systems*, ser. LNCS, T. Margaria and B. Steffen, Eds., vol. 1055. Springer, 1996, pp. 147–166.

[46] J. C. Mitchell, V. Shmatikov, and U. Stern, "Finite-state analysis of ssl 3.0," in *Proc.USENIX SSYM*, Jan. 1998, pp. 16–16.

[47] M. Avalle, A. Pironti, and R. Sisto, "Formal verification of security protocol implementations: a survey," *Formal Aspects Computing*, vol. 26, no. 1, pp. 99–123, 2014.

[48] B. Blanchet, "Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif," *Foundations and Trends® in Privacy and Security*, vol. 1, no. 1-2, pp. 1–135, Oct. 2016. [Online]. Available: https://www.nowpublishers.com/article/Details/SEC-004

[49] F. Liu, C. Wang, A. Pico, D. Yao, and G. Wang, "Measuring the insecurity of mobile deep links of Android," in *The 26th USENIX Security Symposium (USENIX Security '17)*, Vancouver, Canada, 2017. [Online]. Available: http://hdl.handle.net/10919/81987

[50] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Computers Security*, vol. 68, pp. 160–196, 2017.

Lorenz Cuno Klopfenstein is a Research Fellow and Lecturer at the University of Urbino 'Carlo Bo'. His interests include software architecture, mobile and Web-based software development, mobile crowdsensing, and conversational interfaces. Co-founder of Digit srl, benefit corporation for digital social innovation.

Saverio Delpriori is a Research Fellow and Lecturer in Applied Computer Science at the University of Urbino 'Carlo Bo'. His current research interests include mobile crowdsensing, wireless sensor networks, and digital social innovation.

Alessandro Aldini is Associate Professor in Computer Science at the University of Urbino 'Carlo Bo'. His current research interests are focused on the study and application of automated methodologies for the design and verification of computer and network systems, with an emphasis on foundations of security, trust, and performance analysis and design.

Alessandro Bogliolo is full Professor of Computer Systems at the University of Urbino, Italy. He received the Laurea degree in Electrical Engineering and the Ph.D. degree in Electrical Engineering and Computer Science from the University of Bologna, Italy, in 1992 and 1998. From 1992 to 1999 he was with the Department of Electronics and Computer Science (DEIS), University of Bologna. In 1995 and 1996 he was with the Computer Systems Laboratory (CSL), Stanford University, CA. From 1999 to 2002 he was with the Department of Engineering (DI), University of Ferrara, Italy. He joined the University of Urbino in 2002. His research interests include mobile crowdsensing, sensor networks, and digital platforms for sustainability and participatory social innovation. In 2019 he co-founded Digit srl, benefit corporation for digital social innovation.