Internet of Entities (IoE): A Blockchain-based Distributed Paradigm for Data Exchange between Wireless-based Devices

Roberto Saia, Salvatore Carta, Diego Reforgiato Recupero and Gianni Fenu
Department of Mathematics and Computer Science, University of Cagliari, Via Ospedale 72 - 09124 Cagliari, Italy

Keywords: Internet of Things, Internet of Entities, Mobile Network, Blockchain, Distributed Ledger.

Abstract: The exponential growth of wireless-based solutions, such as those related to the mobile smart devices (e.g., smartphones and tablets) and Internet of Things (IoT) devices, has lead to countless advantages in every area of our society. Such a scenario has transformed the world a few decades back, dominated by latency, into a new world based on an efficient real-time interaction paradigm. Recently, cryptocurrency has contributed to this technological revolution, whose fulcrum is a decentralization model and a certification function offered by the so-called blockchain infrastructure, which makes it possible to certify the financial transactions, anonymously. This paper aims to indicate a possible approach able to exploit this challenging scenario synergistically by introducing a novel blockchain-based distributed paradigm for data exchange between wireless-based devices defined Internet of Entities (IoE). It is based on two core elements with interchangeable roles, entities and trackers, which can be implemented by using existing infrastructures and devices, such as those related to smartphone, tablets, and IoT systems. The employment of the blockchain-based distributed paradigm allows our approach ensuring the anonymization and immutability of the involved data, which is key in many scenarios and domains (e.g. financial applications, health and legal applications dealing with personal and sensitive data), requirements more and more searched in recent innovations. The possibility to exchange data among a huge number of devices gives rise to a novel and widely exploitable data environment, whose applications are possible in different domains, such as, in Security, eHealth, and Smart Cities.

1 INTRODUCTION

Currently, the everyday life is dominated by an enormous number of wireless-based smart devices that allow us to perform in real-time an increasing number of activities that until a few years ago were time consuming, such as requests for documents, job applications, purchases, authentication (Abate et al., 2017; Barra et al., 2018) and so on. Such opportunities have been further revolutionized by the decentralized paradigms introduced with the advent of the Bitcoin (Bonneau et al., 2015) cryptocurrency, which has traced a new way to exchange currency. A synergistic combination of security and anonymity stands at the base of its success, since this paradigm allows the users to exchange currency without the need to involve trusted authorities as intermediaries. The strategy behind this revolutionary way to operate is mainly based on a digital signature scheme, which is combined with the effort needed to solve a quite hard mathematical problem. The fulcrum of this mechanism is an immutable public ledger where all the transactions are recorded. It is implemented on the so-called blockchain-based infrastructure by exploiting a distributed consensus protocol that operates in a peer-to-peer network (Nakamoto, 2008).

The idea on which the proposed IoE paradigm revolves is the exploitation of the wireless-based ecosystem, where some existing devices (hereinafter referred to as trackers) are used in order to track the activity of other devices associated to people or things (hereinafter referred to as entities), registering a series of immutable information about the latter by using the features offered by a blockchain-based distributed ledger. This idea relies on what affirmed by several authoritative studies, which indicate that by the end of this decade the number of smartphones and tablets will be about 7.3 billions of units (Pop-Vadean et al., 2017), as well as the number of IoT devices, which will be between 20 and 30 billions by 2020 (Reyna et al., 2018). Although in a rather coarse manner, Figure 1 shows the placement of the proposed IoE paradigm, with respect to already existing wireless-based scenarios.
The implementation of such a paradigm can be made by adding simply functionalities to the existing devices used as trackers (IoT, smart-phones, etc), since we only need to append few entity data (i.e., unique identifier and sensors data) with few tracker data (e.g., time-stamp, geographic location, sensors data, etc.) and sent them to a blockchain-based distribute ledger. It should be observed that in case of mobile devices (e.g., smart-phones and tablets) such an operation can be easily performed by installing an application, whereas for other devices (e.g., IoT) it can be done through a software update.

About the entity-side of this scenario, an interesting aspect related to the IoE paradigm is its capability to use both custom devices (e.g., light wearable devices) and existing widespread devices (e.g., smart-phones) as entities. In addition, the IoE paradigm operates anonymously, since only the entity owner can associate its unique identifier to the registration performed on the remote ledger through the trackers. The inclusion, when it is applicable, of one or more neighbor entities (i.e., those detected by the tracker near the entity within a given time-frame) offers an additional tracing opportunity, since it allows us to reconstruct an entity activity in a wide manner, without jeopardizing the anonymity of the involved neighbor entities.

It should be observed that there are many areas where the IoE paradigm can be profitably exploited (e.g., Security, eHealth, Smart Cities, etc.).

In the security domains, such a paradigm can represent an effective mechanism for the localization of people and things, which exploits both the huge number of existing wireless-based devices and the blockchain-based distributed ledger technology, overcoming the limits of traditional localization approaches, but without jeopardizing the user privacy.

About the eHealth scenario, all the sensors data available in the tracker environment (temperature, humidity, smog, light level, location, altitude, etc.) can be combined to those provided by a series of wearable sensors placed on the entity (e.g., heart rate, pressure, etc.). This configuration allows us to trace, in an exhaustive manner, the health status of an entity, highlighting hidden person-environment interactions, otherwise not obvious. In other words, the data-flow existing between trackers and entities enriches the information provided by the individual sensors placed on an entity body, since the IoE environment allows us to extend them with the information related to all the sensors placed on the near involved trackers. This data-shared modality provides targeted (and more accurate) measurements and/or alerts, since it allows the system to have an overview of the real health-status of an entity, with regards to a specific location and with regard to some near entities.

Similar interactions between entities and trackers can be also exploited in the Smart Cities context, raising a number of interesting applications. Considering that the trackers can be devices that operate, specifically, in such a context, their sensors data can be integrated to those related to a group of entities in order to create functionalities aimed to specific groups of users.

The blockchain-based distributed paradigm allows us to ensure the anonymization and immutability of the involved data, which is crucial in many scenarios and domains, such as those related to the financial, health, and legal applications, which deal with personal and sensitive data. In all the scenarios where there is no need to obtain information with these characteristics, it is possible to use a canonical distributed-database solution rather than a blockchain-based one.

Summarizing, this is an approach that leads towards two interesting advantages: it is able to uncover implicit characteristics of the involved entities by following non canonical criteria; each group of entities can be anonymously characterized on the basis of the sensors data of the entities that belong to it.

The main scientific contributions of this paper are therefore the following:

i. introduction of the novel concept of entities and trackers, able to exchange roles, which operates within a specific wireless-based environment;

ii. definition of interaction models between entities and trackers, and trackers and blockchain-based distributed ledgers, in terms of unique identification of the involved devices and communication techniques/protocols;

iii. formalization of the entity-to-tracker and tracker-to-blockchain-based distributed ledger communication protocol data structures.

The paper is organized into the following sections: Section 2 provides an overview about the background and related work; Section 3 reports the adopted formal notation; Section 4 describes the implementation of the proposed IoE paradigm; Section 5 discusses about some future directions related to IoE; Section 6
closes the paper with some concluding remarks.

2 BACKGROUND AND RELATED WORK

This section introduces the most important concepts related to the context taken into account in this paper.

Mobile Network: A mobile (or cellular) network is a wireless-based network geographically distributed in a number of areas defined cells (Rappaport et al., 1996), as shown in Figure 2. This mechanism based on cells divides the mobile network area into many overlapping geographic areas. It can be imagined as a mesh of hexagonal cells, where each cell has a base-station at its center. A slight overlapping between neighbor cells offers to the mobile devices a continue radio coverage, since in this way they are covered by at least one base-station. Such a base-station that serves a cell works as a hub, since the radio signal transmitted by a mobile device is retransmitted from the base-station to another mobile device, transmitting and receiving by adopting different frequencies in order to avoid interferences. In addition, the base-stations are connected through a central switching service that allows them to track the mobile device calls, transferring these from a base-station to another one, when a mobile device moves between cells.

The most important characteristics of the current mobile network that can be profitable exploited in the proposed IoE paradigm are the wide coverage (that offer us a stimulating initial environment) and the high bandwidth (that allows us to quickly transfer the data between entities and trackers and between trackers and distributed ledgers).

Internet of Things: In recent years we have seen how Internet has given life to a new revolution that involves billions of devices. These are characterized by both a low-cost and a capability to communicate in wireless through Internet. They are the main actors of this revolution named Internet of Things (IoT). Within the IoT environment there are heterogeneous devices, such as computers, smart-phones, wearable devices, IP cameras, RFID devices, as well as a large number of actuators and sensors based on low-cost hardware, which represent the backbone of the IoT environment. This gives life to a kind of ecosystem founded on the communication paradigm, considering that each device is uniquely identified and all the devices can communicate with each other without any geographic limitation by exploiting the Internet. Another important IoT characteristic is that each connected device is uniquely identified.

Let us start by saying that an IoT device is potentially able to communicate directly with another one, a common IoT communication paradigm is that exemplified in Figure 5: each device communicates to the others through two basic activities, publishing and subscription; they use a protocol in order to publish data on a server conventionally defined Broker (in the example of Figure 5, they use one of the most common IoT protocols, MQTT); other devices can subscribe the published data by selecting the topic where it has been stored; the topic represents the channel that allows a selective intercommunication between IoT devices.

Blockchain-based Applications: A blockchain, in the context of the cryptocurrency applications such as Bitcoin (Nakamoto, 2008) and Ethereum (Wood, 2014), represents a shared and transparent distributed ledger. It allows the users to perform secure financial transaction by exploiting a cryptographic mechanism and it can be imagined as an ever-growing chain of blocks, where each block stores a sequence of transactions that are freely inspectable by anyone and are tamper-proof at the same time. Each of these blocks contains the cryptographic signature of the previous one and this mechanism does not allow anyone to alter or remove a block without the removal of all related following blocks.

The blockchain functionality can be exploited also in non-financial contexts, in all the cases where an application needs to ensure trust services. In other words, such a technology can be used as a platform to define the underlying trust level of an application. The blockchain ability to verify an identity through a reliable authentication process (Pilkington, 2016) is indeed exploited in the context of heterogeneous environments, such us, for instance, those related to the eHealth (Castaldo and Cinque, 2018), smart cities (Sun et al., 2016), and IoT (Xu et al., 2018) applications.

The core of each application based on the

---

1Message Queue Telemetry Transport
blockchain infrastructure is the Distributed Ledger Technology (DLT), since it is clear how the identification process relies on the functionality offered by such a ledger, which protects the anonymity of the entities, assuring at the same time a certain identification.

The process of insertion and validation of an operation (e.g., a financial transaction), carried out by using a distributed public ledger based on the blockchain, has been exemplified in Figure 3. Also worth to mention is the work of authors in (Consoli et al., 2014c; Consoli et al., 2014a; Consoli et al., 2014b; Consoli et al., 2017) that presented a prototype based on the case of Catania, one of the main cities of Sicily, with the aim of standardizing the Internet of Things. In particular their aim was to achieve syntactic and semantic interoperability as a result of transforming heterogeneous sources into Linked Data. The presented data model for smart cities integrates several different data sources, including geo-referenced data, public transportation, urban fault reporting, etc. The prototype has been embedded into an open, interoperable, cloud-computing-based citizen engagement platform for the management of administrative processes of public administrations (Recupero et al., 2016).

3 FORMAL NOTATION

Let us start by saying that we use the term entity to indicate a device designed to operate in a IoT environment, associated to a person or thing, and that we use the term tracker to indicate a generic (new or already existing) device that operates in a wireless-based environment, which is aimed to interact with the entities, we introduce the following formal notation:

i. we denote as \( E = \{e_1, e_2, \ldots, e_M\} \) a set of entities, and we use \( E(e) \) to indicate such information related to an entity \( e \);
ii. we denote as \( E_t = \{e_1, e_2, \ldots, e_N\} \) the entities in \( E \) detected by a tracker within \( \tau \) seconds after the detection of an entity (then \( E_t \subseteq E \)), and we use \( E_t(e) \) to indicate such information related to an entity \( e \);
iii. we denote as \( L = \{l_1, l_2, \ldots, l_Q\} \) a set of geographic locations, with \( l = \{\text{latitude}, \text{longitude}\} \), and we use \( l(e) \) to indicate such information related to an entity \( e \) when it is detected by a tracker;
iv. we denote as \( T = \{t_1, t_2, \ldots, t_P\} \) a set of timestamps, with \( t = \{\text{yyyy-mm-dd-hh-mm-ss}\} \), and we use \( t(e) \) to indicate the time-stamp related to the detection of an entity \( e \) by a tracker;
v. we denote as \( I = \{i_1, i_2, \ldots, i_Q\} \) a set of GUIDs\(^2\), using the notation \( i(e) \) to indicate the GUID associated to an entity \( e \), as well as the notation \( i(\text{tracker}) \) to indicate the GUID associated to a tracker;
vi. we denote as \( P = \{p_1, p_2, \ldots, p_W\} \) a payload, with \( p = \{\text{key}, \text{value}\} \), and we use \( P(e) \) to indicate a payload related to an entity \( e \);
vii. we denote as \( R = \{r_1, r_2, \ldots, r_Y\} \) a set of registration made on a blockchain-based distribute ledger, with \( r = \{i(e), E_t(e), l(e), t(e), P(e)\} \), and we use \( r(e) \) and \( R(e) \) to indicate, respectively, a registration related to an entity \( e \) and all the registrations related to that entity.

4 APPROACH FORMULATION

This section describes the implementation of the proposed IoT paradigm, which has been divided into the following steps:

i. Elements Definition: it introduces the concept of entity and tracker in the IoT environment, as well as the method to use in order to assign a GUID to them, outlining some possible operative scenarios;
ii. Elements Detection: the detection process of an entity is here described, from the detection-time by a tracker to the recording-time of the collected data on a blockchain-based distributed ledger;
iii. Elements Communication: it formalizes the data structures and the software procedures able to merge the information related to the involved entities and trackers, generating the data-structure

\(^2\)Globally Unique IDentifiers, whose structure is formally defined in the RFC-4122.
that represents the information to store on the blockchain-based distributed ledger.

4.1 Elements Definition

The concept of entity is usually related to a person, but it could also be extended to a large number of objects such as, for instance, vehicles or goods, and each entity e is always associated to a GUID.

The concept of tracker is instead related to a generic device able to detect the entities, capturing their GUIDs and sensors data, and performing a registration into a blockchain-based distributed ledger. Such a registration (i.e., the set r) is defined by joining entity and tracker data.

The unique identifier of the trackers could be already available (e.g., IP-address), while that of the new entities placed in the IoE environment needs to be defined and assigned. Its generation can be made in several ways (Jones et al., 2012; Watson, 1981). In our IoE paradigm we perform this operation by using one of the most effective methods, the GUID previously introduced in Section 3.

Globally Unique Identifier: The Globally Unique Identifier (GUID), also known as Universally Unique Identifier (UUID), is a 128-bit integer number which is commonly used in order to identify resources uniquely (Leach et al., 2005). If it is necessary, such an information can be combined with additional information (e.g., related to one or more resource characteristics) in order to identify the same device in different contexts. Several algorithms able to generate this information are described in literature (Leach et al., 2005).

Through the application of the birthday paradox (Hankerson et al., 2004; Mironov et al., 2005) we can obtain a mathematically demonstration of the GUID robustness in terms of hash collision probability. Considering that a GUID is a 128-bit long number, we can identify a million billion entities before we have a one in a billion possibility (i.e., $10^{15}$) to get a collision, as shown in Equation 1, which is based on the aforementioned birthday paradox.

$$n \approx \sqrt{2^{128} \ln(1-10^{-9})} \approx 1,000,000,000,000,000$$ (1)

Some considerations can be made about the policies to adopt in order to assign the GUID to each entity that operates into the IoE environment, assuring that this information remains stable along the time.

Some solutions involve either a centralized GUID distribution, such as in (Manku et al., 2003), offered as service to the users by following a free or paid modality, or an autonomous generation of this information made directly by the users (Leach et al., 2005).

It should be added that in order to distinguish the IoE devices from the other classes of devices that operate in the wireless-based environment, it is appropriate to reserve part of the GUID information for this purpose.

Operative Scenarios: About the hardware to use in the IoE environment in order to allow the entities to interact with the trackers, we can outline several scenarios:

i. the entity is characterized by limited or absent hardware resources (e.g., CPU, memory, etc), then it performs the identification process by exploiting passive technologies such as, for instance, RFID (i.e., Radio-Frequency Identification). In this first scenario, the tracker must be able to manage this identification process;

ii. the entity has hardware resources that allow it to adopt active technologies for the identification process (e.g., 6LoWPAN and ZigBee, both defined by the technical standard IEEE 802.15.4). This is the most common scenario, where the entity uses canonical wireless technologies and the tracker does not need any additional capability in order to interact with it;

iii. the entity is able to perform processes that require considerable hardware/software resources. Such a scenario allows us to move on the entity-side some processes usually performed in the tracker-side and it also allows the entity to handle complex...
4.2 Elements Detection

As shown in the high-level working model of Figure 4, when an entity e enters within the coverage area of a tracker, such a tracker detects its identifier i (i.e., its GUID), and it creates and submits a registration r on a blockchain-based distributed ledger. The detection time of an entity e is indicated in Figure 4 as data capture and it coincides with the time-stamp t, which represents the point in the space where the entity is detected by a tracker and the r information are submitted to the blockchain-based distributed ledger.

4.3 Elements Communication

The communication between an entity e and a tracker can be performed by adopting very simple data structures, whose possible formalization are proposed in Figure 6 and Figure 7. They refer, respectively, to the data structure used to transmit data from an entity to a tracker (i.e., entity-side) and to the data structure used to transmit the registration data from a tracker to the blockchain-based distributed ledger (i.e., tracker-side).

About the Entity-side data structure, the GUID information, which is J28-bit long, is stored by using 5 groups of hexadecimal digits, with the following size: 8 hexadecimal digits, 4 hexadecimal digits, 4 hexadecimal digits, 4 hexadecimal digits, and 12 hexadecimal digits. The registration data r are defined by merging a series of identification data (Tracker Primary Data) with the sensors data related both to the entities and trackers activity (Tracker Payload Data). In some contexts, the Payload Data could be partially (only the entity or tracker sensors data) or completely absent (no sensors data) and, in this cases, the entity information will be the GUID, the location, and the time-stamp.

The hardware/software process performed in the entity-side is aimed to broadcast its data (GUID and local payload) regularly through the wireless functionality. About the tracker-side hardware/software process, when there are not active other priority tasks, the tracker operates a listening activity aimed to detect entities in its wireless coverage area, sending the collected entity and tracker data to the blockchain-based distributed ledger.

It should be observed that in the data structures we classified the payload on the basis of the data which it refers, using the term local to indicate that generated by the entity and global to indicate that generated by the tracker, which also includes the local payload. The data anonymity and data immutability offered by a blockchain-based distributed ledger, joined with the low-cost of the devices needed for the data transmission and with the wireless coverage offered by the ever increasing number of wireless-based devices, given life to a powerful environment on which is based the proposed IoE paradigm.

The data that we need to store on the blockchain-based distributed ledger is that described in Section 3: the first field i contains the GUID of the IoE entity; the field $E_\text{r}$ contains, when it is applicable, a list of GUIDs related to the other entities captured together with the entity e in a defined temporal frame $\tau$; the l field contains the geographic location (i.e., $l \in L$) of the tracker that detected the entity e; the field t reports the event occurred, in the format yyyy-mm-dd-hh-mm-ss; the last field P contains a series of values in the format key:value which refer to the sensors data of the entity (local payload) and to the sensors data of the tracker (global payload).

It should be added that the information related to the geographic location of an entity may be classified according to its different resolution, which depends on the operative range of the tracker.

Software Procedures: The software to use in order to perform the entity-tracker and tracker-ledger communications has to fulfill the IoE paradigm needs, from the entity-detection to the data-registration, by performing the following operations:

1. entity-side: it broadcasts the entity GUID and payload (i.e., local sensors data), by using the built-in
wireless device functionality:

ii. tracker-side: it performs a listening activity aimed to detect and recognize entities within its wireless coverage area (distinguishing them from the other devices by using, for instance, a GUID preamble);

iii. tracker-side: it appends the tracker data (i.e., primary and payload data) with the data transmitted by the entity (i.e., GUID and payload), preparing the data for the registration on the blockchain-based distributed ledger;

iv. tracker-side: it submits the defined data packet on the blockchain-based distributed ledger, in order to perform an immutable registration of the entity activity;

v. tracker-side: it waits in order to receive from the blockchain-based distributed ledger the registration acknowledgment of the submitted packet, otherwise it repeats the data submission.

A series of custom data-dashboards (i.e., a management tool able to display, track, and analyze a series of information) can be also designed in order to manage all the processes involved in the IoE paradigm. The needed data, for instance those related to an entity e, can be obtained by querying the Blockchain-based distributed ledger, as shown in Algorithm 1.

5 FUTURE DIRECTIONS

As happened with other similar technologies, even in the case of the proposed IoE one, the greatest obstacle to overcome is the spread across users of such a technology. Although it is possible to create a new network of devices that operate according to the proposed IoE paradigm, we can substantially reduce this problem by integrating the IoE network into the existing wireless-based ones (e.g., IoT and mobile). This process, which allows us to maximize the IoE potential, can be facilitated by adopting several strategies, such as, the following ones:

i. designing simple and transparent procedure of integration of the needed IoE functionalities in the existing trackers, for instance, by integrating these as a service in the new devices, by recurring to a simple firmware/software upgrade process, or by making available an application, in those cases where the trackers or the entities are implemented in devices that allow us this solution (e.g., smartphones, tablets, etc.);

ii. making effective campaigns of information aimed to underline the advantages for each user that joins the IoE network, emphasizing the gained opportunity to exchange information among a large community of users, an huge amount of valuable data that they can exploit in many contexts;

iii. offering benefits to the users that join their devices to the IoE network as trackers, allowing the system to perform the entity detection and the distributed-ledger registration tasks. Such a benefits could include the free-use of some services related to the IoE network.

6 CONCLUSION

This paper introduces a new data-exchange paradigm that we baptized Internet of Entities (IoE). It has been designed to join the capabilities offered by the wireless-based devices environment with the certification capability offered by the blockchain-based distributed ledgers. Such an interaction is based on two core components, entities and trackers, billion of devices able to operate across the IoE environment, interchangeably.

Although the proposed paradigm is based on existing and wide spread technologies, it offers a novel way to trace in a certified and anonymous way the activity of an entity, exploiting a combination of wireless-based and blockchain-based technologies, which produce valuable, exploitable, and (if needed) investigative-valid data.

The concept of robust network in its unstructured simplicity, expressed by Satoshi Nakamoto during his Bitcoin formulation (Nakamoto, 2008), well describes also the Internet of Entities network, whose potential capabilities are destined to grow, day after day, thanks to the continuous introduction of new wireless-based devices, which provide an ever expanding IoE coverage area.

Concluding, although the proposed IoE paradigm can be easily implemented by exploiting existing and wide spread technologies and infrastructures, it offers a series of advantages for the community thanks to its capability to operate in many real-world scenarios.
ACKNOWLEDGEMENTS

This research is partially funded by: Regione Sardegna under project Next generation Open Mobile Apps Development (NOMAD), Pacchetti Integrati di Agevolazione (PIA) - Industria Artigianale e Servizi - Annualità 2013; Italian Ministry of Education, University and Research - Program Smart Cities and Communities and Social Innovation project ILEARNNTV (D.D. n.1937 del 05.06.2014, CUP F74G14000200008 F19G14000910008).

REFERENCES


