Internet of Entities (IoE): a Blockchain-based Distributed Paradigm to Security

Roberto Saia

Department of Mathematics and Computer Science
University of Cagliari, Via Ospedale 72 - 09124 Cagliari, Italy
roberto.saia@unica.it

Abstract. The exponential growth of wireless-based solutions, such as those related to the mobile smart devices (e.g., smart-phones 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 have contributed to this technological revolution, the fulcrum of which are a decentralization model and a certification function offered by the so-called blockchain infrastructure, which make it possible to certify the financial transactions, anonymously. However, it should be observed how this challenging scenario has generated new security problems directly related to the involved new technologies (e.g., e-commerce frauds, mobile bot-net attacks, blockchain DoS attacks, cryptocurrency scams, etc.). In this context, we can acknowledge that the scientific community efforts are usually oriented toward specific solutions, instead to exploit all the available technologies, synergistically, in order to define more efficient security paradigms. This paper aims to indicate a possible approach able to improve the security of people and things by introducing a novel blockchain-based distributed paradigm to security defined Internet of Entities (IoE). It represents 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. Its operation is based on two core elements with interchangeable roles, entities and trackers, which can be very common elements such as smart-phones, tablets, and IoT devices, and its implementation requires minimal efforts thanks to the existing infrastructures and devices. The possibility of including further information to those of localization, such as those generated by device sensors, gives rise to a novel and widely exploitable data environment, whose applications can be extended to contexts different from that of the localization of people and things, e.g., eHealth, Smart Cities, and so on.

Keywords: Internet · Internet of Things · Internet of Entities · Mobile Network · Blockchain · Distributed Ledger · Localization · Security

1 Introduction

The meaning of the personal security is day after day closer to that of the data security. This is given by the growing number of activities related with everyday life, which are somehow performed in a virtual way (e.g., requests for documents, job applications, purchases, and so on).

Such a scenario has been further revolutionized by the decentralized paradigm introduced with the advent of the *Bitcoin* [14] 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 intermediates.

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, but the real 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 operate in a peer-to-peer network [49].

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 ones 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 *smart-phones* and *tablets* will be about *7.3* billion of units [53], as well as the number of *IoT* devices, which will be between *20* and *50* billion by *2020* [56].

Although in a rather coarse manner, Figure 1 shows the placement of the proposed *IoE* paradigm, with respect to the other already existing *wireless-based* paradigms: it is straddled on their operative areas.

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 devices such as *smart-phones* and *tablets*, such a operation can be performed in a quite transparent way, by installing a simple application, while for the *IoT* devices, it can be done by performing a software update.

About the *entity*-side of this scenario, an interesting aspect related to the *IoE* paradigm is its capability to exploit as *entities* both custom devices (e.g., light wearable devices) or existing widespread devices (e.g., *smart-phones*). 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 recon-

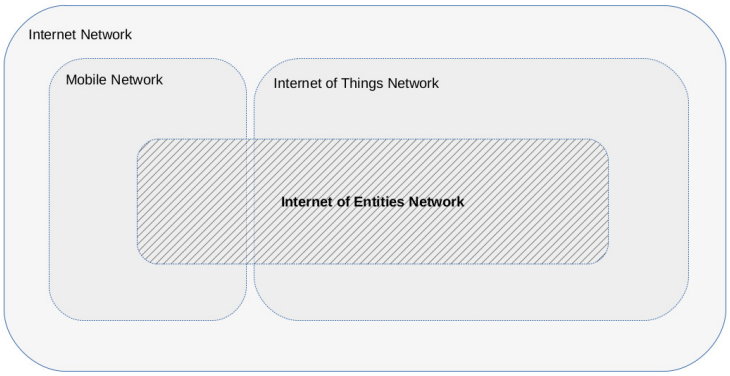

Fig. 1. *IoE Placement*

struct an *entity* activity in a wide manner, without jeopardize the anonymity of the involved *neighbor entities*.

In should be observed how in addition to the domain strictly related to security, such as that proposed in this paper, there are other areas where the *IoE* paradigm can be profitably exploited (e.g., *eHealth*, *Smart Cities*, etc.).

About the *eHealth* scenario, all the sensors data available in the *tracker* environment (*temperature*, *humidity*, *smog*, *light level*, *position*, *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* enrich the information provided by the individual sensors placed on an *entity* body, since the *IoE* environment allows us to add them the information related to all the sensors placed on the near involved *tracker* devices. 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, giving rise to 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.

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 [17, 60]; each group of *entities* can be anonymously characterized on the basis of the sensors data of the *entities* that belong to it.

In light of the previous observations, we can consider the *security* as one of the possible application scenarios of the *IoE* paradigm proposed in this paper, which main scientific contributions have been summarized in 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;
(iv) definition of criteria able to trace an *entity* by exploiting the previous *blockchain-based distributed ledgers* registrations, on the basis of a series of, directly or indirectly, strategies.

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 aims to introduce the most important concepts related to the context taken into account in this paper, starting by offering an overview on the *Mobile Network* and *Internet of Thing* concepts, continuing by introducing the *blockchain-based* applications together with other concepts that revolves around them, and concluding with some consideration about the security aspects related to the aforementioned scenarios.

2.1 Mobile Network

A *mobile* (or *cellular*) network is a *wireless-based* network geographically distributed in a number of areas defined *cells*[54, 32]. This mechanism based on *cells* divides the mobile network area into many of overlapping geographic areas.

It can be imagined as a mesh of hexagonal *cells*, where each *cell* has a base-station (*bs*) at its center, as shown in Figure 2. 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 an other 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*).

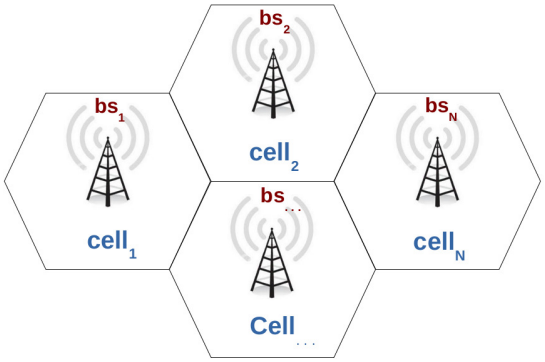

Fig. 2. *Mobile Network Structure*

2.2 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 way through *Internet* and they are the main actors of this revolution named *Internet of Things* (*IoT*). Into the *IoT* environment operates heterogeneous devices, such as *computers*, *smartphones*, *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 can communicate with other devices and all the devices can communicate with each other without any geographic limitation, thanks to *Internet*. Another important *IoT* characteristic is that each connected device is uniquely identified.

Premising that an *IoT* device is potentially able to communicate directly with another one, a common *IoT* communication paradigm is that exemplified in Figure 3: each device communicate to the other ones through two basic activities, *publishing* and *subscription*; it uses a protocol in order to *publish* data on a server defined *Broker* conventionally (in the example of Figure 3, it uses one of the most common *IoT* protocols, *MQTT*[1]); 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.

Internet of Everything The growth of the *Internet of Things* model and, more generally, the growth of the *wireless-based* technologies, has contributed to the definition of a model called *Internet of Everything* [75, 27]. Such a model is characterized by the integration of *data*, *processes*, *things*, and *people*, combining several elements that in the past were separated from each other. Some cases in

[1] Message Queue Telemetry Transport

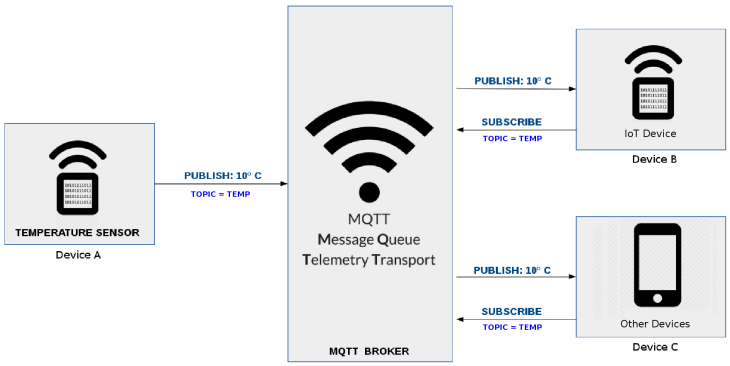

Fig. 3. *IoT Communication Paradigm*

point are the smart things such as *smart-watches*, *eHealth-devices*, and *smart-vehicles*.

In other words, the *Internet of Everything* model is used to refer to the intelligent interconnection of *data*, *processes*, *things*, and *people*, a scenario that involves billions of objects connected over public or private networks by using different protocols (*standard* or *proprietary*), which are able to detect the environment around them (*sensors*) and/or able to interact with it (*actuators*).

Summarizing, the *Internet of Everything* model is different from the *Internet of Things* one, since its paradigm is based on four elements (*data*, *processes*, *things*, and *people*), instead of one (*things*).

Identity of Things The *Identity of Things* represents a concept mainly related to the *Internet of Things* environment. Basically, it refers to the need to assign an unique identifier to all objects that operates in such a environment, in order to allow their real-time interaction with people and other objects (*things*). A centered and quite recent example of the aforementioned scenario is that of the *autonomous vehicles* [24], where the concept of unique identification becomes day after day even more crucial [65].

The identifier can be created by using information that characterize, uniquely, the *IoT* device such as, for instance, the manufacturer, the serial number, and so on. Alternatively, the identifier can be assigned to the *IoT* device by using a centralized or decentralized assignation remote service, manually or automatically. Some possible approaches able to perform this operation are presented in Section 4.1.

2.3 Blockchain-based Applications

A *blockchain*, in the context of the cryptocurrency applications such as *Bitcoin* [49, 21] and *Ethereum* [73], 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 a ever-growing chain of blocks, where each block stores a sequence of transactions that are freely *inspectable* by anyone but that are *tampering-proof*. Each of these blocks contains the cryptographic signature of the previous one and this mechanism does not allow anyone to *alter* or *remove* a previous block without the removal of all the blocks after it.

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 [52] is indeed exploited in the context of heterogeneous environments, such us, for instance, those related to the *eHealth* [35, 15], *smart cities* [13], and *IoT* [74] applications.

Generalizing the concept, the *blockchain* can be be profitably used in all the applications where there is the need to *identify* an object (people, vehicles, documents, etc.) in a certain way. For instance, it is used in [1] to get a verifiable identity through a reliable authentication process, in [76] in order to introduce *blockchain-based* intelligent transportation systems, in [47], where the *blockchain* has been exploited to define a public identities ledger in the context of an identity management system, and in [2] in order to face the *Value Added Tax* (*VAT*) fraud problem.

Double-spending Issue The *double-spending* issue arises due to the absence of a central intermediary. Explaining it in a few words, we suppose that *Alice* has *100-coins* and send all of them to *Bob*: the *double-spending* problem is related to the fact that *Bob* can not know that *Alice* had sent the same *100-coins* to another person (e.g., *Charlie*), because there is not a central intermediary (e.g., a bank) that verify such a transaction.

This problem, graphically summarized in Figure 4, has been faced by adopting a distributed *time-stamp* mechanism able to determine which transactions should be accepted and which should be rejected. In the context of the *Bitcoin* has been adopted a *hash-chain* mechanism to perform this operation [35].

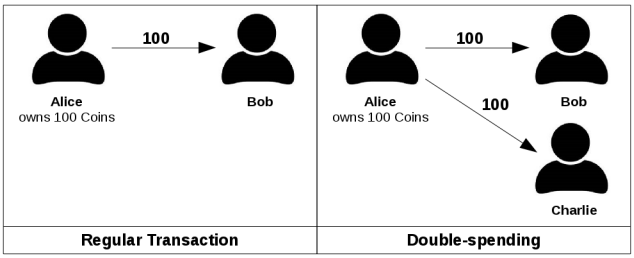

Fig. 4. *Double-spending Issue*

Relating to the previous example, hypothesizing that the transaction from *Alice* to *Charlie* is stored in *block*-1 and the transaction from from *Alice* to *Bob* is instead stored in *block*-2: through the *hash-chain* mechanism each participant can verify that *block*-1 is older than *block*-2 by verifying the hashed *blockchain*, avoid a *double-spending* event by rejecting the transaction from *Alice* to *Bob*.

Consensus Mechanism The *consensus mechanism* stands at the base of the *blockchain* paradigm, since it allows the system to append new blocks to the *blockchain*. In order to perform this operation, this mechanism exploits the so-called *proof-of-work* (PoW) [29], a criterion based on the solution of a mathematical cryptological problem that involves as input the transactions stored into the block to add to the *blockchain*.

Literature defines as *miners* the users that operate in order to solve this kind of problem. When a *miner* finds its solution, it is communicated to all the other users, who confirm its correctness and validate the new block, allowing the system to append it to the *blockchain*.

The PoW has been introduced during the *Bitcoin* [49] formalization and it assumes that each *peer*[2] votes by using its *computational power* by solving the mathematical cryptological problem and adding the current block to the *blockchain*. This mechanism, based on the users consensus, is aimed to protect the system against alterations and other fraudulent activities, since the PoW activity (i.e., the solution of the mathematical cryptological problem) needs a very high computation load, which involves resources that are not normally available for a single user or for a small group of users.

It should be noted that the literature offers other consensus mechanisms to use instead of the PoW one, such as, for instance, the so-called *Proof of Stake* (PoS) [39].

Distributed Ledger Technology As it emerges from the cited literature examples, the core of each application based on the *blockchain* infrastructure is the *Distributed Ledger Technology* (DLT). It is indeed 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 operations (e.g., a financial transaction), carried out by using a *distributed public ledger* based on the *blockchain*, has been exemplified in Figure 5.

Through a *blockchain* is possible to implement two different type of ledger: *unpermissioned ledger* and *permissioned ledger* (also known as *private blockchain*). Well-known example of *unpermissioned ledger* are the *Bitcoin* and *Ethereum* environments, which have been designed to be *open* and *uncontrolled*. In more detail, they do not have single owners and this means that they allow anyone to add data to the ledger and any user that uses the ledger has identical

[2] Equipotent node: in our case, it represents each *blockchain* participant.

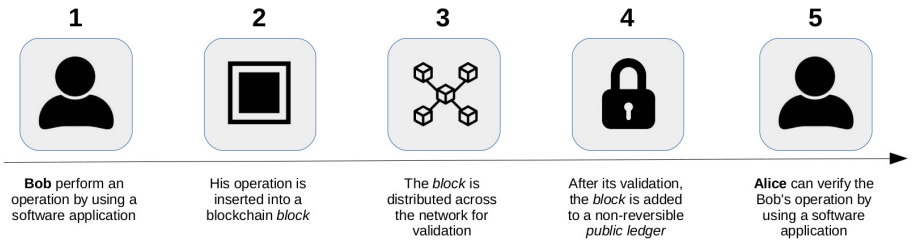

Fig. 5. *Blockchain Distributed Public Ledger*

copies of it. Users maintain the ledger integrity by reaching a consensus about its state.

The *unpermissioned ledger* are different from the *permissioned* ones, which are ledgers where the users need a permission to get the access to them. This means that, when a new record is added to the ledger, its integrity is checked by following a restricted consensus process. The *blockchain-based permissioned ledgers* add a security level, since the consensus process generates a digital signature.

In the aforementioned context the term *unpermissioned* is then a synonym of the term *uncontrollable*, and for this reason most of the implementation adopt the *unpermissioned* paradigm, since it is the only one able to provide the *decentralization* that stand at the base of the *blockchain* philosophy.

The working model adopted by any *blockchain-based* ledger is based on the complete storage of all the information since its creation. Such a model produces a constant and continue increasing of its size and this generates a crucial *scalability issue* that must be effectively faced in the future [20]. By way of example, at the beginning of *2018* the size of *Bitcoin* ledger has been evaluated about *145-gigabyte* and that of *Ethereum* ledger about *40-gigabyte* [11].

Decentralized Storage Network The *blockchain-based* technology also given rise to a new *decentralized model* on which the *Decentralized Storage Networks* (*DSN*) are based. By adopting this model, instead of using many servers (i.e., a *server farm*), as it happens by adopting a canonical *centralized storage model*, every network user (*node*) stores part of network data. Each user has an incentive to be part of the system and to keep the data available, for reasons similar to those that regulate the *BitTorrent* file distribution system, a protocol that adopts a decentralized model that exploits the capability of the participants to network *peer-to-peer* among themselves.

Some examples of *blockchain-based* decentralized storage approaches are *Filecoin*[3], *SAFE Network*[4], *Swarm*[5], *Storj*[6], and *Sia*[7].

Considering that the traditional distributed models adopted for the cloud storage services, such as, for instance, those offered by *Amazon's cloud storage*[8], represent a market that generates profits in the billions of dollars: the growth of the decentralized storage model is cutting out part of this total market. In addition to offer to the users a cheaper way for data storage, such a decentralized model also contributes to increase the availability of storage space.

Blockchain and IoT Integration Scenarios characterized by the integration of *blockchain-based* infrastructures with *IoT* devices have been discussed in literature, such as in [56], where the authors have been identified the following operative modalities:

- *IoT-IoT*: it is characterized by a low-latency and an high-level of security, since the involved *IoT* devices operates between them for most of the time, by exploiting the canonic protocols and by limiting the *blockchain* use for storing only few information;

- *IoT-Blockchain*: by following this strategy, all the *IoT* information are stored on the *blockchain*, assuring their immutability and traceability, but increasing the bandwidth consumption and the latency-time;

- *Hybrid Paradigms*: this last strategy combines the aforementioned ones, performing part of the activities directly between the *IoT* devices, limiting to the data storage activity the interaction with the *blockchain*.

For the needs of the proposed *IoE* paradigm, the second and third strategies (i.e., *IoT-Blockchain* and *Hybrid*) are the most suitable, although by adopting optimized criteria, the best strategy results the *Hybrid* one, since it is the only one that allows us to balance the advantages offered by the *IoT-IoT* and *IoT-Blockchain* strategies.

2.4 Security Aspects

Some considerations should also be made about the security scenario related to the *wireless-based* technologies, since such a technological evolution did not keep up with the security one. It means that the big opportunities offered by the new technologies have been jeopardized by a series of problems that affect the security in a broad sense.

[3] https://filecoin.io/
[4] https://safenetwork.org/
[5] https://github.com/ethereum/go-ethereum/tree/master/swarm
[6] https://storj.io/
[7] http://sia.tech/
[8] https://aws.amazon.com/

Some cases in point are the frauds related to the E-commerce infrastructure, which we have been dealt with in [61, 62, 58, 63, 64, 59], where retroactive, proactive, transformed-domain-based, and multidimensional approaches have been experimented in order to face such problems, as well as the ever-increasing number of identity theft [12, 18] or, even more simply, the countless frauds made by exploiting the people's trust [28, 4], often by recurring to *social engineering* techniques [46].

Also in the *mobile network* context we can observe similar problems, because the smart devices that operate in this environment inherit the security risks that characterize the *Internet-based* devices (e.g., *desktop computer*, *laptop*, and so on), such as the aforementioned ones. In addition, there are a series of more specific risks related to this context [40] such as, for instance, those related to the *bot-net-based* attacks [68], or those that jeopardize the user privacy [23].

Even with regard to the *blockchain-based* technologies (e.g., those related to the *cryptocurrency*), their potential advantages have been flanked by a series of security issues related to the criminal efforts, which are aimed to exploit those new technologies, fraudulently. In this specific case, the security issues have been boosted by the fact that such criminal activities can not be easily detected by surveillance authorities [44].

An example of security issue is related to the *blockchain* consensus mechanism needed to add a new block, which involves many people called *miners* that spend computation time (GPU/CPU type) to solve a kind of mathematical problem (*hash-checking*). A group of people can operate jointly as a *mining-pools* in order to mining many blocks and this can leads towards the *blockchain* control, if the achieved computing *power* is at least the 51% of the total [19, 22]. This type of attacks are known in literature as *Majority Attack* and they have been also theorized in the famous *Satoshi Nakamoto Bitcoin* white-paper [49].

It should be observed how the PoW mechanism that stands at the base of the *blockchain* paradigm should not be too hard to solve, in order to avoid a very long block generation time that would bring toward the total block of all the transactions. However, such a problem can not be overly simple to solve, because in this case the system would be vulnerable to many types of attacks such as, for instance, the *Denial of Service* (DoS) one [50, 71].

Other cases in point about the security issues in this context are the vulnerabilities that affect the *Ethereum smart contracts* [7] and the fraudulent games implemented through the *blockchain* platform, such as those based on the well-known *Ponzi schemes* [5, 6]. They have been introduced on the web many years ago [45, 38] and recently re-proposed on *Bitcoin* [70] and *Ethereum* [9].

3 Formal Notation

Considering that we use the term *entity* to indicate a device designed to operate in a IoE 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 $E_\tau = \{e_1, e_2, \ldots, e_N\}$ the *entities* in E detected by a *tracker* device within τ seconds after the detection of an *entity* (then $E_\tau \subseteq E$), and we use $E_\tau(e)$ to indicate such information related to an *entity* e;
(iii) we denote as $L = \{l_1, l_2, \ldots, l_O\}$ a set of geographic locations, with $l = \{latitude, longitude\}$, and we use $l(e)$ to indicate such information related to an *entity* e, when it is detected by a *tracker* device;
(iv) we denote as $T = \{t_1, t_2, \ldots, t_P\}$ a set of *time-stamps*, with $t = \{yyyy\text{-}mm\text{-}dd\text{-}hh\text{-}mm\text{-}ss\}$, and we use $t(e)$ to indicate the *time-stamp* related to the detection of an *entity* e by a *tracker* device;
(v) we denote as $I = \{i_1, i_2, \ldots, i_Q\}$ a set of $(GUIDs)$[9], using the notation $i(e)$ to indicate the $GUID$ associated to an *entity* e, as well as the notation $i(tracker)$ to indicate the $GUID$ associated to a *tracker* device;
(vi) we denote as $P = \{p_1, p_2, \ldots, p_W\}$ a *payload*, with $p = \{key, value\}$, 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 $r = \{i(e), E_\tau(e), l(e), t(e), P(e)\}$, 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 *IoE* paradigm, which has been divided in the following steps:

(i) **Elements Definition**: it introduces the concept of *entity* and *tracker* in the *IoE* environment, as well as the method to use in order to assign them a *Globally Unique Identifier*, outlining some possible operative scenarios;
(ii) **Elements Detection**: the detection process of an *entity* device is here described, from the *detection-time* by a *tracker* device to the *recording-time* of the collected data on a *blockchain-based distributed ledger*, focusing on the characteristics of the state-of-the-art wireless technologies able to perform these activities;
(iii) **Elements Communication**: it formalizes the data structures and the software procedures able to merge the information related to the involved *entity* and *tracker* devices, generating the *data-structure* that represent the information to store on the *blockchain-based distributed ledger*;
(iv) **Elements Localization**: extensively, it describes the activities made in order to trace an *entity*, introducing some baseline strategies and a series of localization rules aimed to exploit the available information on the *blockchain*, directly or indirectly.

[9] *Globally Unique IDentifiers*, whose structure is formally defined in the *RFC-4122*, which is explained in Section 4.1.

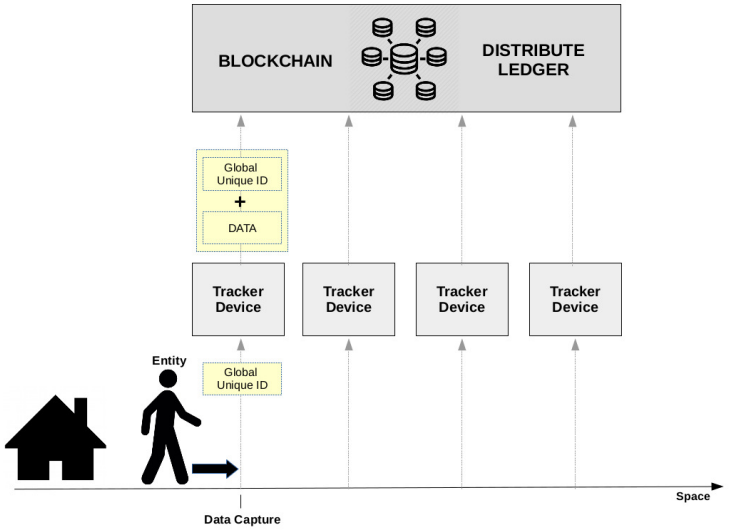

Fig. 6. *IoE Working Model*

4.1 Elements Definition

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

The concept of *tracker* is instead related to a generic device able to detect the *entity* devices, 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, according to the formal notation defined in Section 3.

Listing 1.1. *Globally Unique Identifier Data Structure*

```
GUID =  time-low "-" time-mid "-"
        time-high-and-version "-"
        clock-seq-and-reserved
        clock-seq-low "-" node
time-low = 4hexOctet
time-mid = 2hexOctet
time-high-and-version = 2hexOctet
clock-seq-and-reserved = hexOctet
clock-seq-low = hexOctet
node = 6hexOctet
hexOctet = hexDigit hexDigit
hexDigit = "0" / "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9" /
           "a" / "b" / "c" / "d" / "e" / "f" /
           "A" / "B" / "C" / "D" / "E" / "F"
```

The unique identifier of the *tracker* devices could be already available (e.g., *MAC-address*, *IP-address*, etc.), while that of the new *entity* devices placed in the *IoE* environment needs to be defined and assigned. Its generation can be

made in several ways [31, 72], but the two most common methods are: (*i*) on the basis of a *serial numbers* created by following an incremental or sequential criterion; (*ii*) on the basis of a *random numbers* generated by using a range of numbers enough larger to classify the expected number of objects. In the proposed approach, we perform this operation by using one of the most effective methods: the *Globally Unique Identifier*.

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 [37]. When it needs, such a information can be combined with additional information (e.g., related to one or more resource characteristics) in order to identify the same resource in different contexts. Listing 1.1 reports the formal definition of a *GUID* string, and *f81d4fae-7dec-11d0-a765-00a0c91e6bf6* represents an example of this one. Several algorithms able to generate this information are described in [37].

Through the application of the *birthday paradox* [26, 43] we can obtain a mathematically demonstration of the *GUID* robustness in terms of hash collision probability. By following this mathematical approach, 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*.

$$n \approx \sqrt{-2^{129} \cdot ln(1 - 10^{-9})} \approx 1,000,000,000,000,000 \tag{1}$$

Some considerations can be made about the policies to adopt in order to assign the *GUID* to each *entity* device that operates into the *IoE* environment, assuring that this information remains stable along the time. This because the *IoE* tracing mechanism is based on such information and a change of it (i.e., the device *GUID*) during the life of an *entity* device leads towards inconsistent data.

Some solutions involve or a centralized *GUID* distribution, such as in [41], 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 [37]. 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 *entity* devices to interact with the *tracker* ones, we can outline several scenarios:

(i) the *entity* device 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*[10]. In this first

[10] Radio-Frequency IDentification.

scenario, the *tracker* device must be able to manage the identification process adopted by the *entity*;

(ii) the *entity* device 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* device uses canonical wireless technologies and the *tracker* device does not need any additional capability in order to interact with it;

(iii) the *entity* device is able to perform processes that require considerable hardware/software resources. Such a scenario allows us to move on the *IoE*-side some processes usually performed in the *tracker*-side and it also allows the *IoE* device to handle complex processes related to its sensors.

The scenario taken into consideration in this paper is the second one, where the *IoE* device is characterized by enough hardware/software resources that allow it to use active technologies for its identification, because it allows us to implement the *IoE* immediately and in a transparent way, postponing the other scenarios to possible future implementations.

4.2 Elements Detection

As shown in the high-level working model of Figure 6, when an *entity* e enters within the coverage area of a *tracker* device, such a device detects its identifier i (i.e., the *GUID*, as formalized in Section 3), 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 6 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* device and the r information are submitted to the *blockchain-based distributed ledger*.

All the above operation are managed by using specific data structures, whose possible implementation has been proposed in Section 4.3.

Wireless Technologies: About the technology to use in order to broadcast the *entity GUID*, the literature offers several solutions in terms of technologies and protocols able to perform this operation [3]. Some examples of them are: *Internet Protocol Version 6 over Low-Power Wireless Personal Area Networks* (*6LoWPAN*), *Bluetooth Low Energy* (*BLE*), *Z-Wave*, *ZigBee*, *Near Field Communication* (*NFC*), *Radio Frequency IDentification* (*RFID*), *SigFox*, and *2G/3G*. *SigFox* and *2G/3G* are classified as *Low-Power Wide Area Network* (*LPWAN*) protocols, while the other ones as *Short-range Wireless* protocols.

Their characteristics have been summarized in Table 1, where the reported ranges (i.e., *frequency range* and *operative range*) indicates only the lowest and the highest supported value (e.g., if the protocol supports $125KHz$, $13.56MHz$, and $860MHz$, we report $125KHz \div 860MHz$).

The choice of protocol should be made by taking into account the *entity* type, since in case of a *person* such a choice should be oriented toward protocols able to

ensure a low-power consumption and a mid/short operative range, while in case of *objects* (e.g., a vehicle) the choice could be instead oriented toward protocols characterized by a long operative range and a mid/high power consumption.

However, the above considerations are strongly related to the context of a custom *IoE* device, since when it is a standard device such as, for instance, a *smart-phone* or a *tablet*, the choice of the wireless protocols is driven by those supported by the operating system (e.g., *802.11 b/g/n* [69] and *Bluetooth Low Energy* (*BLE*) [25] protocols).

Table 1. Wireless Technologies

Wireless technology	Frequency range	Data rate	Operative range	Power consumption	Security protocols	Literature reference
6LoWPAN	868MHz÷2.4GHz	250KBps	10÷100m	low	AES	[48]
BLE	2.4GHz	1MBps	15÷30m	low	E0, Stream, AES-128	[25]
Z-Wave	868MHz÷908MHz	40KBps	30÷100m	low	AES-128	[36]
ZigBee	2.4GHz	250KBps	10÷100m	low	AES	[33]
NFC	868MHz÷902MHz	106÷424KBps	0÷1m	Ultra-low	RC4	[16]
RFID	125KHz÷928MHz	4MBps	0÷200m	Ultra-low	RSA,AES	[30]
SigFox	125KHz÷860MHz	100÷600Bps	10÷50Km	low	no-specific	[55]
2G/3G	380MHz÷1.9GHz	10MBps	Several Kms	High	RC4	[51]

4.3 Elements Communication

The communication between an *entity e* and a *tracker* device can be performed by adopting very simple data structures, whose possible formalization are proposed in Figure 7 and Figure 8.

They refer, respectively, to the data structure used to transmit data from an *entity* device to a *tracker* device (i.e., *entity-side*) and to the data structure used to transmit the registration data from a *tracker* device to the *blockchain-based distributed ledger* (i.e., *tracker-side*).

About the *Entity-side* data structure, the *GUID* information, which is *128*-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.

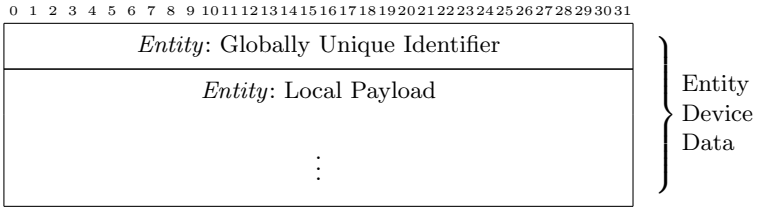

Fig. 7. *Entity-side Data Structure*

The registration data r are defined by merging a series of identification data (*Tracker Primary Data*) with the sensors data related both to the *entity* and *tracker* devices 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*.

About the hardware/software process performed in the *entity-side*, it is limited to broadcast its data (*GUID* and *local payload*) at regular time intervals, by using the wireless functionality. About the *tracker-side* hardware/software process, when there are not active other priority tasks, the *tracker* device 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* device and *global* to indicate that generated by the *tracker* device, which also include the *local payload*.

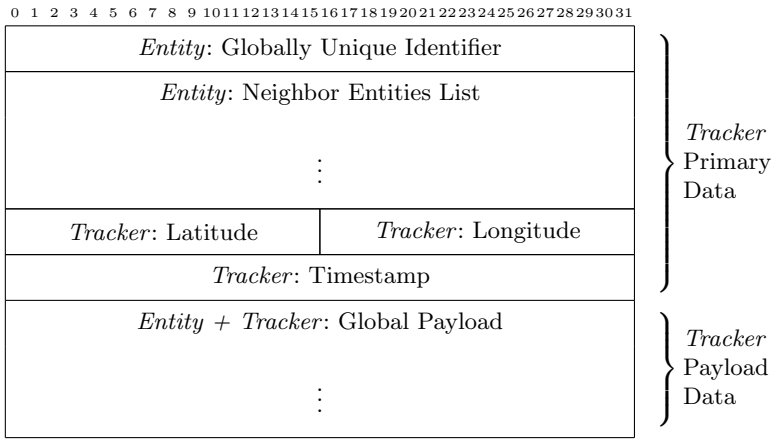

Fig. 8. *Tracker-side Data tructure*

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 *Globally Unique Identifier* of the *IoE entity*; the field E_τ contains, when it is applicable, a list of *Globally Unique Identifiers* related to the other *entities* captured together with the *entity* e in a defined temporal frame τ; the l field contains the geographic position (i.e., *latitude* and *longitude*) of the *tracker* device that detected the *entity* e; the field

t reports when the *data capture* 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* device (*local payload*) and to the sensors data of the *tracker* device (*global payload*).

Software Procedures: The software to use in order to perform the *entity-tracker* and *tracker-ledger* communications can be an update, in case of *IoE* and *custom devices*, or an application (*app*), in most of the other cases (i.e., *smartphones*, *tablets*, and similar devices). It has to fulfill the *IoE* paradigm needs, from the *entity-detection* to the *data-registration*, by performing the following operations:

1. *entity-side*: it provides to broadcast the device *GUID* along with the *payload* (i.e., local sensors data), by using the built-in wireless device functionality;
2. *tracker-side*: it performs a listening activity aimed to detect and recognize (distinguishing them from the other devices through the mechanism adopted in the implementation phase, for instance, a specific *GUID* preamble) *entities* within its wireless coverage area;
3. *tracker-side*: it appends the *tracker* device data (i.e., *primary* and *payload* data) with the data transmitted by the *entity* device (i.e., *GUID* and *payload*), building a data packet suitable for a registration on the *blockchain-based distributed ledger*;
4. *tracker-side*: it submits the defined data packet on the *blockchain-based distributed ledger*, in order to perform an immutable registration of the *entity* device activity;
5. *tracker-side*: it waits to receive from the *blockchain-based distributed ledger* the registration acknowledge of the submitted packet, otherwise it repeats the submission.

A series of custom *data-dashboards*[11] can be also designed in order to manage all the processes involved in the *IoE* paradigm, first of all, that related to the constant tracking of the *entities*.

Algorithm 1 Blockchain-based distributed ledger data gathering

Require: e=Entity, R=Blockchain-based distributed ledger registrations
Ensure: $\hat{R}$=Registrations related to entity e
1: **procedure** GETENTITYREGISTRATIONS(e, R)
2: **for each** r **in** R **do**
3: $i \leftarrow getEntityGUID(r)$
4: **if** $i(e) == \hat{e}$ **then**
5: $\hat{R} \leftarrow r(e)$
6: **end if**
7: **end for**
8: **return** $\hat{R}$
9: **end procedure**

[11] A management tool able to display, track and analyze a series of information.

4.4 Elements Localization

When we need to investigate about an *entity* e, first we get all needed data related to it by performing a *data gathering* process, such as that reported in Algorithm 1, then we can manage such data through different strategies, such as the baseline ones described below:

1. **Direct Tracing**: by following this strategy, the movements of an *entity* e, from its first introduction in the *IoE* environment, are traced by using the information $l(e)$ and $t(e)$ in $r(e), \forall r(e) \in R(e)$, according to the formalization given in Section 3.
   This process is shown in Figure 9, which refers to six detection points l of an *entity* e, chronologically numbered by using the *time-stamp* information t. In more detail, we first query the *blockchain-based distribute ledger* in order to extract all the registrations $R(e)$, then we number each location $l(e) \in r(e), \forall r(e) \in R(e)$ (i.e., *latitude* an *longitude*) along the chronological sequence given by the *time-stamp* information $t(e) \in r(e)$.
   More formally, given a series of *entity* locations $l(e) \in L$, we introduce a *Trace Location Set* $\omega = \{l_1, l_2, \ldots, l_Z\}$ aimed to store, in the chronologically order determined by the *time-stamp* information $t(e) \in T$, all the locations $l(e) \in L$, as formalized in Equation 2.

$$\begin{aligned} &\omega \leftarrow\ l(e)\ \mid\ \forall\ l(e)\ \textbf{in}\ L \\ &\textbf{with}\ \ l_1 < l_2 < \ldots < l_Z\ \ \wedge\ \ l \in \omega \end{aligned} \tag{2}$$

   It should be noted that the localization resolution is directly related to the *tracker* device that has detected the *entity*. We can obtain a *high-resolution* localization when the *tracker* device runs a localization service (e.g., *GPS*) and then its location is near that of the detected *entity*. We instead obtain a *low-resolution* localization when the localization data are related to another device, as happens when the *tracker* device operates in the mobile network but without any active localization service, since in this case the location could refer to the mobile network *cell*.
   This is represented in Figure 9 and Figure 10: the *high-resolution* localization coincides with the *entity map-point*, while the *low-resolution* localization can be considered any *map-points* within the *grid-square* where the *entity* is placed, which represents the mobile network *cell*.

2. **Interpolate Tracing**: in this strategy we take into account the information $l(e)$, $t(e)$, and $E_\tau(e)$ in $r(e), \forall r(e) \in R(e)$. The $E_\tau(e)$ information contains, when it is applicable, the other *entities* detected by the *tracker* device within τ seconds from the e (the *entity* under analysis) detection, as described in Section 3.
   We exploit the new information in order to reconstruct the *entity* movements by interpolating the $l(e) \in r(e), \forall r(e) \in R(e)$ data with the same data of the *entities* in $E_\tau(e)$ (neighbor *entities*). This process is graphically shown

Fig. 9. *IoE Direct Tracing*

in Figure 10, where $+$ denotes the *entity* under analysis and N a neighbor *entity* in $E_\tau(e)$.
In the example of *interpolate tracing* shown in figure, we can observe how the first localization of the *entity* $+$ includes a neighbor N that we found another time in the third location of the location chronology of $+$. This represents a naive example of *interpolate tracing*, based on the reasonable probability that such a configuration indicates that the neighbor *entity* is somehow related to the main *entity* under analysis, especially when this pattern repeats over time. In other words, it is very likely that in the second localization of N, the entity $+$ was also present, and that it has not been detected for some reasons such as, for instance, a temporary *tracker* device overload, or because the *entity* device was out of the *tracker* wireless range. This pattern, repeated over time, could underline interesting connections between *entities*, as well as the last location of a missing *entity*.
More formally, given the *Trace Location Set* $\omega = \{l_1, l_2, \ldots, l_Z\}$ previously defined and given a series of *entity* locations $L(e) = \{l_1, l_2, \ldots, l_O\}$, at each location $l \in L(e)$ (with $O \geq 3$) we extract from the set $E_\tau(e)$ a subset of valuable[12] neighbor *entities* by following the criterion in Equation 3.

$$\begin{aligned} &\omega \leftarrow l(e) \mid \textbf{if } e \textbf{ in } E_t(l_{o-1}) \ \wedge \ e \textbf{ in } E_t(l_{o+1}), \ \forall \ e \textbf{ in } E_\tau \\ &\textbf{with } l_1 < l_2 < \ldots < l_Z \ \wedge \ l \in \omega \end{aligned} \tag{3}$$

We can generalize the aforementioned criterion by varying the distance between the step $E_\tau(e)$ (i.e., where we extract the valuable neighbor *entities* from $E(e)$) and the previous and next step that we take into account. Denoting as α such a distance (i.e., the number of considered locations), we can re-formalize the former criterion as shown in Equation 4.

$$\begin{aligned} &\omega \leftarrow l(e) \mid \textbf{if } e \textbf{ in } E_t(l_{o-\alpha}) \ \wedge \ e \textbf{ in } E_t(l_{o+\alpha}) \\ &\textbf{with } l_1 < l_2 < \ldots < l_Z \ \wedge \ l \in \omega \end{aligned} \tag{4}$$

[12] Entities able to be exploited in the context of the *Interpolate Tracing* strategy.

It should be underlined how during this activity we do not infringe the privacy of the involved *neighbor entities*, since the *entity* data are collected anonymously into the *blockchain-based distributed ledger*.

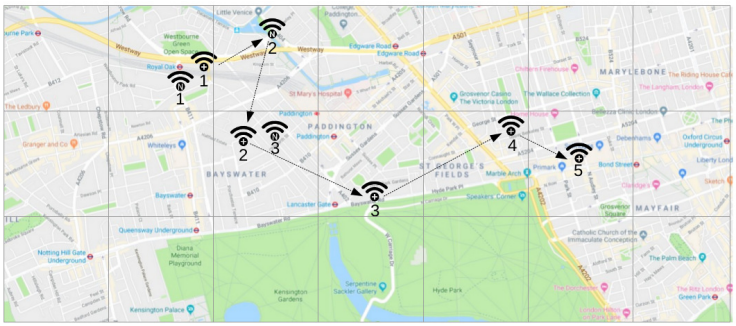

Fig. 10. *IoE Interpolate Tracing*

3. **Spread Tracing**: this last baseline criterion exploits all the neighbor *entities* in E_τ, with $e \neq \hat{e}$ and $|E_\tau| \geq 2$, where $\hat{e}$ denotes the *entity* under analysis. We add as valuable neighbor *entities* of $\hat{e}$ all the *entities* that in their locations in L have $\hat{e}$ as neighbor *entity*, as shown in Equation 5.

$$\begin{aligned} &\omega \leftarrow \ l(e) \ \mid \textbf{if} \ \hat{e} \ \textbf{in} \ E_\tau(e), \ \forall \ l(e) \ \textbf{in} \ L \\ &\textbf{with} \ \ l_1 < l_2 < \ldots < l_Z \ \ \wedge \ \ l \in \omega \end{aligned} \tag{5}$$

The result can be expressed as the *tracing matrix* Ξ shown in Equation 6, where each row refers to a different valuable *entity* e. In other words, each matrix-row refers to a different valuable *entity* e and it reports the locations l where the *entity* e has the *entity* $\hat{e}$ as neighbor in $E_\tau(e)$.

$$\Xi(e) = \begin{bmatrix} l_1, l_2, \cdots, l_O \\ l_1, l_2, \cdots, l_O \\ \vdots \ \ \vdots \ \ \ddots \ \ \vdots \\ l_1, l_2, \cdots, l_O \end{bmatrix} \tag{6}$$

After ordering the matrix-row elements by location and after counting how many *entities* $\hat{e}$ are involved in each matrix-column, we can evaluate the probability that the entity e was in a specific position, although it has not been detected by a *tracker* device. This criterion is graphically shown in Figure 11, where the *grid-size* (i.e., *square-side*) represents a tolerance value, which we denoted as Δ. This meand that all the *entity-detections* that occur into the same *grid-square* refer to the same *matrix-row-index* (i.e., Equation 6).

Fig. 11. *IoE Spread Tracing*

It should be noted how the grid of Figure 11 represents a different information, with respect to that of Figure 9 and Figure 10, since in this case it does not represent the mobile network *cells* but the tolerance value Δ.

All the aforementioned criteria can be combined in order to define a more complex criterion based on different localization rules. In addition, all criteria have been formalized by exploiting only few of the available information, which can be fully exploited in order to improve the localization strategies (e.g., by inferring further details from the sensors data).

5 Future Directions

Considering that a complete and fully-functional implementation of the proposed *IoE* paradigm is beyond the scope of this paper, which is mainly aimed to expose the theoretical concepts that revolve around our core idea, delineating several application scenarios, this section introduces some future directions, making also some general considerations about its potential spread.

5.1 Secure Payload Storing

A future extension of the *IoE* paradigm could be designed in order to manage as *payload* large and/or sensitive sensors data, by recurring both to external storage services and encryption protocols. Such a problem arises with regard to the payload data generated by the *tracker* device that detect an *entity*, since such data could be refer to sensitive information generated by some classes of sensors such as, for instance, *microphones* and *video cameras*, instead than non-sensitive information generated by other classes of sensors (e.g., *temperature sensors*, *humidity sensors*, etc.).

A possible and effective solution able to face this problem is based on the *asymmetric encryption* model [66], which analogously to the canonical encryption mechanism adopted nowadays in a number of applications (e.g., *SSH*,

OpenPGP, *S/MIME*, etc.)[13], is exploited in order to encrypt the data locally (when the *tracker* functionalities allow us this operation) or remotely (e.g., in a *distributed database*).

Data Encryption: The data encryption is performed by using the *tracker* device *public key*. In this way only it has the possibility to decrypt the data by using its *private key*, although the involved *entity* has the access to that data in encrypted form. The entire process has been summarized in Figure 12.

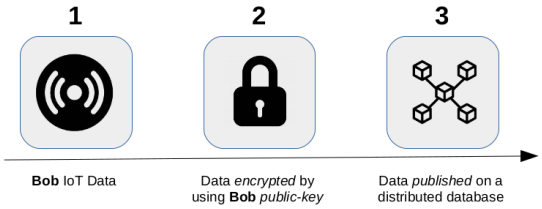

Fig. 12. *Data Encryption Process*

How already happens in the context of the *blockchain* technology, where the private key cryptography mechanism provides a powerful ownership method that fulfills the authentication requirements (i.e., the ownership is *private-key-based*), without the need to share more personal information, also in this context such a mechanism grants both *privacy* and *ownership*.

When there is the need to investigate about an *entity* by using such encrypted data, for instance in case of a criminal event, such as a kidnapping or a theft, the data access can be obtained through the involved authorities in charge. In case of minor events, it is possible to exclude this information, using the other ones (e.g., *location*, *time-stamp*, etc.).

Data Hashing: The connection between the encrypted data, stored locally or remotely, and the entity is possible by using as data-name a string generated by a *hash function* [8]. Such a function is a special class of *hash* functions largely used in cryptography. Some common examples are: *MD4* [57], *SHA* [10], *TIGER* [42], and *WHIRLPOOL* [67].

In more detail, by adopting a mathematical algorithm is possible to map data (characterized by arbitrary size) to a bit string (characterized by a fixed size). The result is defined *hash* and it represents a one-way function that is infeasible to invert. The literature usually refers to the input data as *message* and to the output data (i.e., the *hash*) as *message digest* or *digest*.

Through an *hash* process, whose process is shown in Figure 13, is possible to validate the data integrity of a file, detecting all modification since each of

[13] *Secure Socket Shell*, *Open Pretty Good Privacy*, *Secure Multi-Purpose Internet Mail Extensions*

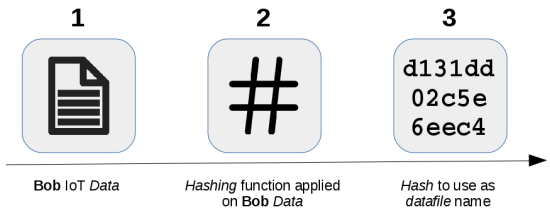

Fig. 13. *Data Hashing Process*

them changes the *hash* output. While an encryption process represents a *two-way function* based on the *encryption* and *decryption* operations, hashing represents a *one-way function* that transforms in an irreversible manner the source *data* used as input into a plain text output (i.e., the *hash* of *data*).

5.2 IoE Technology Spread

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 facilitate 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 *tracker* devices, for instance, by integrating these as a *service* in the new devices, by recurring to a simple and well documented 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., *smart-phones*, *tablets*, etc.);
(ii) making effective campaigns of information aimed to underline the advantages for each user that joins the *IoE* network, empathizing the gained opportunity to exchange information between a large community of users, an huge amount of valuable data that they can exploit in many contexts, such as that of *security* taken into account in this paper;
(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, such as, for instance, the services used for the remote data storage.

As previously underlined, the exploitation of the mobile network contributes to impress a substantial acceleration to the spread of the *IoE* network, since such

a network already involves an enormous number of devices that are potentially configurable, by recurring to simple applications, to operate according to the *IoE* paradigm. In this case, the information related to the geographic *location* of the *trackers* can be obtained by a local service (i.e., *GPS*) or by querying the mobile *cell* to which the *tracker* is connected. The sensors data related to the *tracker*-side will be those available for that device, otherwise this kind of data will be absent.

A consideration should be made about the fact that the use case taken into account in this paper is based on the interaction between *entities* and *trackers*, implementing by using custom (e.g., wearable solutions) or standard (*IoT*, *smart-phone*, and *tablet*) devices, but the *IoE* potentiality could be improved by adding to the *IoE* network other classes of devices such as, for instance, *routers*, *access-points*, *hot-spots*, and many others. Although this type of expansion is potentially practicable, it requires an implementation effort that is greater than that required by using the devices we considered in this paper.

Business Models: Some conclusive general observations are about the exploitation of the proposed *IoE* paradigm in the context of a hypothetical commercial scenario. From the point of view of a *Business-to-Business* (*B2B*) model, we can start by observing that many financial analysts underline that only the area related to the *IoT* has given rise to an interesting and profitable financial market, whose value in the next *5-10* years has been estimated around trillions of dollars [34].

Consequently, as specialized sub-area of the *wireless-based* technologies market, the proposed *IoE* paradigm could offer new stimulating and profitable opportunities, considering that its applications involve a huge number of customers, both private and commercial ones. Summarizing, the activity core could be oriented towards the development of *IoE* solutions for business customers, who in turn can offer this service to their customers, according to a *Business-to-Consumer* (*B2C*) model.

Such solutions involve both hardware and software aspects, from the hardware/software development of the *IoE* devices (e.g., *wearable devices*, *smartphone applications*, *vehicle equipments*, etc.) to the management of the needed services (e.g., *unique identifier distribution*, *remote storage*, etc).

In some cases, these opportunities could be further expanded by defining and offering services in partnership with public and/or private investigative agencies (e.g., *security guards*, *local police*, etc), giving rise to a very interesting transversal market.

A *B2C* scenario could also include other services such as, for instance, the management of *entities* initially directly managed by customers or the development and commercialization of custom hardware and software solutions.

6 Conclusion

In this *Internet*-based age, the enormous benefits related to the new technologies are dramatically jeopardized by a series of security issues given by an ever increasing number of people that try to get advantages from them, in a fraudulent way. This scenario of insecurity is further complicated by the traditional security issues that affect our modern societies, such as, for instance, kidnappings, frauds, thefts, and so on.

The state-of-the-art security paradigms do not exploit in a better way the opportunities offered by some powerful technologies such as those related to the *wireless-based* smart devices or the *Internet of Things*, which involves millions of active devices, or those related to the *blockchain-based distributed ledgers*, which allow to certify a series of events.

This paper introduces a new security paradigm, which we baptized *Internet of Entities* (*IoE*), designed to join the capabilities offered by the *wireless-based* devices environment with the certification capability offered by the *blockchain-based distributed ledgers*. It is mainly based on two core components, *entities* and *trackers*, which are billion of new or already-existing devices able to operate interchangeably across the *IoE* environment.

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*, *person* or *object*, exploiting a combination of *wireless-based* and *blockchain-based* technologies, which produce valuable, exploitable, and investigative-valid data.

The same mechanisms adopted in the *blockchain-based* applications have been exploited in the proposed paradigm in order to ensure the *immutability* of data remotely stored on a *blockchain-based* distribute ledger, as well as their *anonymity*.

The concept of *robust network in its unstructured simplicity*, expressed by *Satoshi Nakamoto* during his *Bitcoin* formulation [49], well describes also the *Internet of Entities* network, whose 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, if on the one hand, the proposed *IoE* paradigm can be easily implemented by exploiting existing and wide spread technologies and infrastructures, on the other hand, it produces a series of advantages for the community, revealing a great potential for growth in many real-world scenarios, such as that of the security taken into consideration in this paper.

References

1. Abbasi, A.G., Khan, Z.: Veidblock: Verifiable identity using blockchain and ledger in a software defined network. In: Companion Proceedings of the10th International Conference on Utility and Cloud Computing. pp. 173–179. ACM (2017)
2. Ainsworth, R.T., Shact, A.: Blockchain (distributed ledger technology) solves vat fraud (2016)

3. Al-Sarawi, S., Anbar, M., Alieyan, K., Alzubaidi, M.: Internet of things (iot) communication protocols. In: Information Technology (ICIT), 2017 8th International Conference on. pp. 685–690. IEEE (2017)
4. Arachchilage, N.A.G., Love, S., Beznosov, K.: Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior 60, 185–197 (2016)
5. Artzrouni, M.: The mathematics of Ponzi schemes. Mathematical Social Sciences 58(2), 190–201 (2009), http://dx.doi.org/10.1016/j.mathsocsci.2009.05.003
6. Artzrouni, M.: The mathematics of ponzi schemes. Mathematical Social Sciences 58(2), 190–201 (2009)
7. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (sok). In: Principles of Security and Trust, pp. 164–186. Springer (2017)
8. Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J., et al.: Cryptographic hash functions: A survey. Tech. rep., Citeseer (1995)
9. Bartoletti, M., Carta, S., Cimoli, T., Saia, R.: Dissecting ponzi schemes on ethereum: identification, analysis, and impact. arXiv preprint arXiv:1703.03779 (2017)
10. Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 92–111. Springer (1994)
11. Benčić, F.M., Žarko, I.P.: Distributed ledger technology: Blockchain compared to directed acyclic graph. arXiv preprint arXiv:1804.10013 (2018)
12. Bilge, L., Strufe, T., Balzarotti, D., Kirda, E.: All your contacts are belong to us: automated identity theft attacks on social networks. In: Proceedings of the 18th international conference on World wide web. pp. 551–560. ACM (2009)
13. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on. pp. 1392–1393. IEEE (2016)
14. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. In: IEEE S & P. pp. 104–121 (2015)
15. Castaldo, L., Cinque, V.: Blockchain-based logging for the cross-border exchange of ehealth data in europe. In: International ISCIS Security Workshop. pp. 46–56. Springer (2018)
16. Cerruela García, G., Luque Ruiz, I., Gómez-Nieto, M.Á.: State of the art, trends and future of bluetooth low energy, near field communication and visible light communication in the development of smart cities. Sensors 16(11), 1968 (2016)
17. Chong, W.H., Lim, E.P.: Exploiting user and venue characteristics for fine-grained tweet geolocation. ACM Transactions on Information Systems (TOIS) 36(3), 26 (2018)
18. Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, J.C., et al.: Client-side defense against web-based identity theft. In: NDSS (2004)
19. Courtois, N.T., Bahack, L.: On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718 (2014)
20. Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., et al.: On scaling decentralized blockchains. In: International Conference on Financial Cryptography and Data Security. pp. 106–125. Springer (2016)
21. Danezis, G., Meiklejohn, S.: Centrally banked cryptocurrencies. arXiv preprint arXiv:1505.06895 (2015)

22. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM 61(7), 95–102 (2018)
23. Firoozjaei, M.D., Yu, J., Choi, H., Kim, H.: Privacy-preserving nearest neighbor queries using geographical features of cellular networks. Computer Communications 98, 11–19 (2017)
24. Gerla, M., Lee, E.K., Pau, G., Lee, U.: Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In: Internet of Things (WF-IoT), 2014 IEEE World Forum on. pp. 241–246. IEEE (2014)
25. Gomez, C., Oller, J., Paradells, J.: Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors 12(9), 11734–11753 (2012)
26. Hankerson, D., Vanstone, S., Menezes, A.: Cryptographic protocols. Guide to Elliptic Curve Cryptography pp. 153–204 (2004)
27. Hussain, F.: Internet of everything. In: Internet of Things, pp. 1–11. Springer (2017)
28. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Communications of the ACM 50(10), 94–100 (2007)
29. Jakobsson, M., Juels, A.: Proofs of work and bread pudding protocols. In: Secure Information Networks, pp. 258–272. Springer (1999)
30. Jia, X., Feng, Q., Fan, T., Lei, Q.: Rfid technology and its applications in internet of things (iot). In: Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. pp. 1282–1285. IEEE (2012)
31. Jones, A.R., Quah, E.E.L., Nielsen, D.J., Eminovic, L.: Creating a globally unique identifier of a subscriber device (Jul 3 2012), uS Patent 8,213,935
32. Kaufman, B., Aazhang, B.: Cellular networks with an overlaid device to device network. In: Signals, Systems and Computers, 2008 42nd Asilomar Conference on. pp. 1537–1541. IEEE (2008)
33. Kinney, P., et al.: Zigbee technology: Wireless control that simply works. In: Communications design conference. vol. 2, pp. 1–7 (2003)
34. Kranz, M.: Industrial applications are the juicy part of the internet of things. LSE Business Review (2017)
35. Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association 24(6), 1211–1220 (2017)
36. Kuzlu, M., Pipattanasomporn, M., Rahman, S.: Review of communication technologies for smart homes/building applications. In: Innovative Smart Grid Technologies-Asia (ISGT ASIA), 2015 IEEE. pp. 1–6. IEEE (2015)
37. Leach, P., Mealling, M., Salz, R.: A universally unique identifier (uuid) urn namespace. Tech. rep. (2005)
38. Lewis, M.K.: New dogs, old tricks. why do ponzi schemes succeed? In: Accounting forum. vol. 36, pp. 294–309. Elsevier (2012)
39. Lin, I.C., Liao, T.C.: A survey of blockchain security issues and challenges. IJ Network Security 19(5), 653–659 (2017)
40. Liu, P., LaPorta, T.F., Kotapati, K.: Cellular network security. In: Computer and Information Security Handbook, pp. 183–203. Elsevier (2009)
41. Manku, G.S., Bawa, M., Raghavan, P., et al.: Symphony: Distributed hashing in a small world. In: USENIX Symposium on Internet Technologies and Systems. p. 10 (2003)
42. Mendel, F., Rijmen, V.: Cryptanalysis of the tiger hash function. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 536–550. Springer (2007)

43. Mironov, I., et al.: Hash functions: Theory, attacks, and applications. Microsoft Research, Silicon Valley Campus. Noviembre de (2005)
44. Moore, T.: The promise and perils of digital currencies. IJCIP 6(3-4), 147–149 (2013)
45. Moore, T., Han, J., Clayton, R.: The postmodern Ponzi scheme: Empirical analysis of high-yield investment programs. In: Financial Cryptography and Data Security. pp. 41–56 (2012)
46. Mouton, F., Leenen, L., Venter, H.S.: Social engineering attack examples, templates and scenarios. Computers & Security 59, 186–209 (2016)
47. Muftic, S.: Blockchain identity management system based on public identities ledger (Apr 25 2017), uS Patent 9,635,000
48. Mulligan, G.: The 6lowpan architecture. In: Proceedings of the 4th workshop on Embedded networked sensors. pp. 78–82. ACM (2007)
49. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
50. Needham, R.M.: Denial of service. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. pp. 151–153. ACM (1993)
51. Novo, O., Beijar, N., Ocak, M., Kjällman, J., Komu, M., Kauppinen, T.: Capillary networks-bridging the cellular and iot worlds. In: Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on. pp. 571–578. IEEE (2015)
52. Pilkington, M.: 11 blockchain technology: principles and applications. Research handbook on digital transformations p. 225 (2016)
53. Pop-Vadean, A., Pop, P., Latinovic, T., Barz, C., Lung, C.: Harvesting energy an sustainable power source, replace batteries for powering wsn and devices on the iot. In: IOP Conference Series: Materials Science and Engineering. vol. 200, p. 012043. IOP Publishing (2017)
54. Rappaport, T.S., et al.: Wireless communications: principles and practice, vol. 2. prentice hall PTR New Jersey (1996)
55. Raza, U., Kulkarni, P., Sooriyabandara, M.: Low power wide area networks: An overview. IEEE Communications Surveys & Tutorials 19(2), 855–873 (2017)
56. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with iot. challenges and opportunities. Future Generation Computer Systems (2018)
57. Rivest, R.: The md4 message-digest algorithm. Tech. rep. (1992)
58. Saia, R.: A discrete wavelet transform approach to fraud detection. In: NSS. Lecture Notes in Computer Science, vol. 10394, pp. 464–474. Springer (2017)
59. Saia, R.: Unbalanced data classification in fraud detection by introducing a multi-dimensional space analysis. In: IoTBDS. pp. 29–40. SciTePress (2018)
60. Saia, R., Boratto, L., Carta, S.: A latent semantic pattern recognition strategy for an untrivial targeted advertising. In: Big Data (BigData Congress), 2015 IEEE International Congress on. pp. 491–498. IEEE (2015)
61. Saia, R., Boratto, L., Carta, S.: Multiple behavioral models: A divide and conquer strategy to fraud detection in financial data streams. In: Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K), 2015 7th International Joint Conference on. vol. 1, pp. 496–503. IEEE (2015)
62. Saia, R., Boratto, L., Carta, S.: A proactive time-frame convolution vector (tfcv) technique to detect frauds attempts in e-commerce transactions. International Journal of e-Education, e-Business, e-Management and e-Learning 5(4), 229 (2015)
63. Saia, R., Carta, S.: Evaluating credit card transactions in the frequency domain for a proactive fraud detection approach. In: SECRYPT. pp. 335–342. SciTePress (2017)

64. Saia, R., Carta, S.: A frequency-domain-based pattern mining for credit card fraud detection. In: IoTBDS. pp. 386–391. SciTePress (2017)
65. Shao, J., Xie, G., Wang, L.: Leader-following formation control of multiple mobile vehicles. IET Control Theory & Applications 1(2), 545–552 (2007)
66. Simmons, G.J.: Symmetric and asymmetric encryption. ACM Computing Surveys (CSUR) 11(4), 305–330 (1979)
67. Stallings, W.: The whirlpool secure hash function. Cryptologia 30(1), 55–67 (2006)
68. Traynor, P., Enck, W., McDaniel, P., Porta, T.L.: Mitigating attacks on open functionality in sms-capable cellular networks. IEEE/ACM Transactions on Networking (TON) 17(1), 40–53 (2009)
69. Uzcátegui, R.A., De Sucre, A.J., Acosta-Marum, G.: Wave: A tutorial. IEEE Communications magazine 47(5) (2009)
70. Vasek, M., Moore, T.: There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In: Financial Cryptography and Data Security. pp. 44–61 (2015)
71. Vasek, M., Thornton, M., Moore, T.: Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. In: International Conference on Financial Cryptography and Data Security. pp. 57–71. Springer (2014)
72. Watson, R.W.: Identifiers (naming) in distributed systems. In: Distributed SystemsArchitecture and Implementation, pp. 191–210. Springer (1981)
73. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper 151, 1–32 (2014)
74. Xu, Q., Aung, K.M.M., Zhu, Y., Yong, K.L.: A blockchain-based storage system for data analytics in the internet of things. In: New Advances in the Internet of Things, pp. 119–138. Springer (2018)
75. Yang, L.T., Di Martino, B., Zhang, Q.: Internet of everything. Mobile Information Systems 2017 (2017)
76. Yuan, Y., Wang, F.Y.: Towards blockchain-based intelligent transportation systems. In: Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on. pp. 2663–2668. IEEE (2016)