Blockchain based distributed trust management in IoT and IIoT: a survey

Asma Lahbib, Khalifa Toumi, Anis Laouiti, Steven Martin

▶ **To cite this version:**

Asma Lahbib, Khalifa Toumi, Anis Laouiti, Steven Martin. Blockchain based distributed trust management in IoT and IIoT: a survey. Journal of Supercomputing, 2024, 80 (15), pp.21867-21919. 10.1007/s11227-024-06286-4 . hal-04906562

HAL Id: hal-04906562
https://hal.science/hal-04906562v1

Submitted on 23 Jan 2025

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Blockchain based Distributed Trust Management in IoT and IIoT: a survey

Asma Lahbib , Khalifa Toumi , Anis Laouiti , Steven Martin

***Abstract*—Internet of Things (IoT) is the interconnection of objects sensing, communicating and interacting with each other on a cooperative basis to meet a standard goal. The integration of such paradigm within the manufacturing environment and processes in combination with other technologies has introduced Industry 4.0 that represents the fourth industrial revolution. In this scenario, security requirements represent a crucial issue whose satisfaction is a key to achieve users acceptance of such technologies. Such requirements include data confidentiality, integrity and authentication, identity management, privacy and trust among the different devices. Trust management plays a crucial role in IoT and particularly in IIoT for qualified services development, reliable data collection, device authentication and secure decision making situations. Recent research works have focused on the integration of the blockchain technology within trust management systems for IoT and IIoT environments. The inherent features of such technology could provide promising solutions to trust management systems specifically the decentralization of the trust process, the transparency and the traceability of shared trust data, the effective sharing of historical trust information, and finally the confidentiality, the integrity and the availability of the trust evidences. In this work, our focus is to provide a comprehensive and an investigated survey of current works carried out towards blockchain based trust approaches in IoT and IIoT systems. Following this, we discuss and identify raised issues and open challenges of blockchain based trustworthy IoT and IIoT in attempt to give an overview on strategies and directions for future research in this field.**

***Index Terms*—Trust management, Blockchain, Security, Internet of Things, Industrial Internet of Things.**

Copyright Registration

I. Introduction

Internet of Things (IoT) is the interconnection of objects sensing, communicating and interacting with each other on a cooperative basis to meet a standard goal [1], [2]. The integration of such paradigm within the manufacturing environment and processes in combination with other technologies such Cloud Computing (CC), Cyber Physical Systems (CPS), Information and Communication Technologies (ICT) as well as Enterprise Architecture (EA), has introduced the fourth wave of the industrial revolution called also Industry 4.0 [3], [4], [5], [6]. In this scenario, security requirements represent a crucial issue whose satisfaction is a key to achieve users acceptance of such technologies. Such requirements include data confidentiality, integrity and authentication, identity management, privacy and Trust among the different devices. Trust management plays a crucial role in IoT and particularly in IoT based smart factories for qualified services development, reliable data collection, exchange, analysis and mining, preserved privacy and secure decision making situations.

This concept is essential when participating devices, without being previously interacted with each other, want to cooperate and to use provided services with a certain degree of trust among themselves. It is needed also to achieve trustworthy data during collection, exchange, analysis, fusion and mining phases which is inevitably crucial in IoT and especially in smart factories where devices continuously collect data with great amounts and important information within that is needed for critical decision making. It is needed as well for many other decision making situations such as access control, intrusion detection, authenticating devices and isolating misbehaving ones before interaction and other purposes.

In the current literature, trust management mechanisms have been extensively studied in different research areas, specifically in IoT environments. Yet, a number of issues within trust management systems such as the confidentiality and the integrity of trust evidences during their collection, propagation and communication; the identity management and the ability to link an identity to a single entity; the sharing and the storage of trust information; the preserving of interacting entities privacy and sensitive information, etc. have not been extensively examined. On the other hand, currently in the scientific research, numerous efforts have been emerged leading to significant advances in the fields of attacks resiliency, cryptography, identity management and decentralized computer networks resulting in the emergence of the blockchain technology, which has the potential to fundamentally overcome raised challenges and to solve almost of the above mentioned issues.

The inherent features of such technology make it a natural fit to developing distributed and secure frameworks for IoT and IIoT environments.

That's why many research works have proposed and are proposing until the date the integration of this technology within trust management systems so as to solve encountered issues and especially to take advantages of security

features it provides.
Applying the blockchain technology to trust management systems could provide promising possibilities and solutions to issues they encounter mainly: (i) the decentralization of the trust process that will no longer depends on centralized third parties, (ii) the transparency and the traceability of shared trust related information, (iii) the effective sharing of histrorical trust information, and finally (iv) the confidentiality, the integrity and the availability of the trust evidences.
As mentioned above, in the literature, trust management models have been extensively investigated in IoT networks. However very little work focused on the security and trust of both IoT and Industrial based IoT in a decentralized manner with the integration of the blockchain technology. A limited number of surveys of blockchain based trust management were conducted in the context of IoT [7], [8]. These latter have surveyed the integration of the blockchain technology within trust and reputation management systems in IoT environments. In this direction, this paper presents a comprehensive survey of blockchain based trust management mechanisms designed and developed for IoT and IIoT environments. Our major contributions through this paper could be summarized as follows:

- Raised issues and challenges of trust management systems for IoT environments have been identified.
- A detailed literature review of distributed and blockchain based trust management schemes has been presented for both IoT and IIoT systems. An outline of the main contributions and limitations of presented schemes is as well presented.
- An analysis of investigated mechanisms regarding their application scenario, the adopted methodology, the blockchain type, the considered performance metrics, as well as their strengths and weaknesses is provided.
- A comparative analysis of investigated schemes' versatility regarding a set of comparative criteria is also given.
- Raised issues and challenges are identified and future research directions for blockchain based trust management in IoT and IIoT are suggested.

More specifically this paper is organized as follows. In Section 2, we recall the basic concepts of IoT and IIoT as well as the main challenges and issues related to their appearance. The concept of Trust management in IoT and IIoT is therefore explained, distributed trust management systems are surveyed and raised issues and limitations are as well discussed. The second part of this section is devoted to present background information related to the blockchain technology. The classification, the review and the comparison of blockchain based trust management mechanisms in IoT and IIoT systems are presented in Section 3. Thereafter in Section 4, a comparative analysis of investigated schemes' versatility regarding a set of comparative criteria is given and we discuss raised issues and challenges in attempt to give an overview on strategies and techniques taken for the design of blockchain based trust management mechanisms for IoT and that could be applied to IIoT. Finally Section 6 concludes this paper.

II. Background Information and Basic Concepts

In this section we will point out first the basic principles of Internet of things (IoT) and Industrial IoT. We will overview then the main challenges and issues related to their appearance and we will focus on some important recurring topics that could be integrated within these concepts in order to obtain benefits in specific application scenarios.

A. Internet of Things

1) Definition: As an arising technology, IoT is expected to offer promising solutions that will revolutionize not just the conduct but also the services to be provided across several industries such as health-care, transportation, energy and manufacturing. Building upon a complex network connecting billions of devices, objects, services and humans into a multitechnology, multi-protocol and multi-platform infrastructure, this paradigm main vision is to create an intelligent world while bridging the physical world, sensing/actuating, processing, analytics, to the digital, cyber, and virtual worlds on a global scale [10].
In other words, IoT could be defined as the intelligent connection of objects that equipped with sensors, collect data and take decisions locally or collectively. These objects communicate with each other without human interaction, however they just need to have Internet connectivity in order to retrieve and send their data to be kept in a database or even in a Cloud infrastructure for further processing that requires many other networks to be realized.
For example, production processes will be organized and monitored remotely, machines will talk to machines to coordinate their actions function of the information collected by different sensors and exchanged with other entities among the production line in order to control the corresponding value chain.
It is clear here that the fact of exploiting IoT basic technologies including sensor networks, embedded technologies, communication standards and Internet protocols will impact the nature of involved objects, making them capable of communicating and interacting with other external entities while sharing information and coordinating decisions.

2) Reference Architecture: Although several architectures have been proposed to model the Internet of Things, the basic one is still the well-known three-layer architecture [11], [12] consisting of the application, the network, and the perception layers.
As illustrated in Fig. 1, the perception layer is made up of smart devices, actuators and wireless sensing devices. Its main tasks are perceiving, identifying, collecting information and automatic control. To ensure such functions,

Submitted manuscript

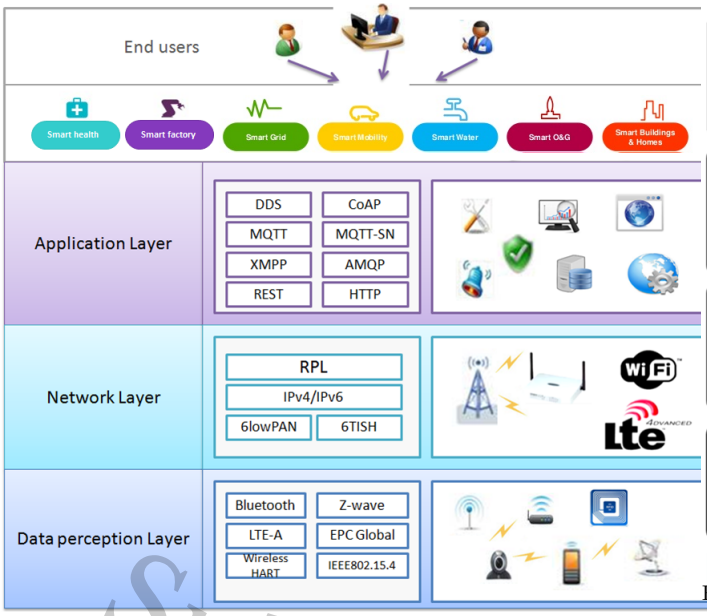


Fig. 1. Internet of Things reference architecture

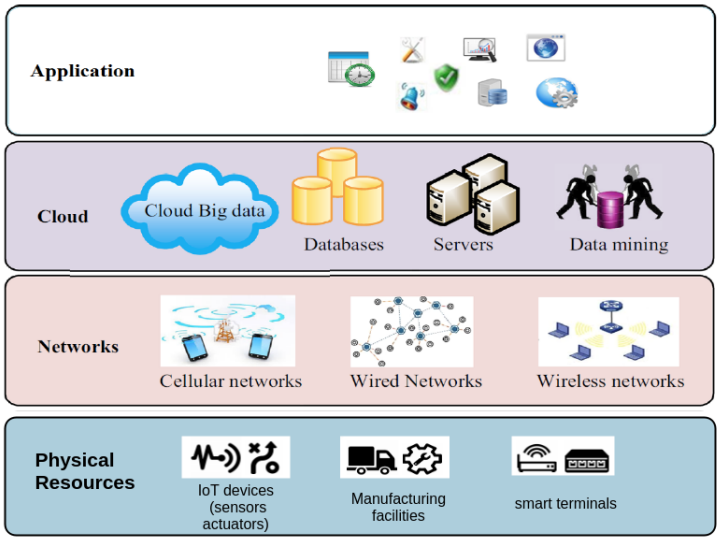


Fig. 2. Industrial IoT reference architecture

Submitted manuscript

several standards and communication protocols were proposed such as IEEE 802.15.4, Bluetooth, LTE-A, WirelessHART, ISA100.11a, etc.

As a second layer, the network layer ensures the processing, the addressing, and the information transmission and routing from the perception layer to the application layer safely and reliably through the use of infrastructure protocols such as 6LowPAN, 6TiSCH, IPv4/IPv6, RPL, etc.

Finally, the application layer takes in charge the control and the management of transmitted information, the activation of relative events and the generation of requested services by both customers and end users. To do so, several application and service discovery protocols were proposed such as DDS, COAP, AMQP, MQTT, XMPP, REST, HTTP, mDNS, DNS-SD.

B. Industrial Internet of Things

1) Definition: The vision of Industry 4.0, also referred to as the fourth industrial revolution, represents the integration of emerging information technologies within industrial and manufacturing processes what could make production operates in an efficient, flexible and economic manner with constantly high quality and low cost. This concept has introduced the Industrial IoT (IIoT) devoted to using the Internet of Things paradigm for ensuring the interconnection of connected intelligent devices, ubiquitous networking and computing, storing and analytics abilities within industrial and manufacturing environments. As a consequence thereof, every- thing in and around the manufacturing supply chain will be interconnected such as machines, data, processes, suppliers, customers, distributors, even the product itself. By this way, data about business operations will be shared between involved entities and locations, production lines will be remotely monitored and automatically handled, machines will communicate with each other to organize the production, to adapt their functioning to both operating conditions and received orders , and also to coordinate their actions function of the information collected by the different sensors regarding their location, their status, as well as the encountered faults, exceptions and problems.

2) Reference Architecture: Fig. 2 illustrates the general layout of IIoT within Industry 4.0. This framework is composed of four main layers [24], [25], including the physical resource layer, network layer, Cloud layer, and application layer. The physical resources layer comprises smart IoT devices such as sensors, actuators, manufacturing objects and facilities, and other industrial manufacturing and automation related objects. These resources acquire and compute data while communicating with each other through the industrial network for the completion of mechanical tasks and the achievement of the system-wide goal. These resources communicate not only with each other but also with the data servers and the industrial Clouds through the industrial networks. These last are made up of cellular, wireless, wired and other industrial networks transmitting data in realtime among the involved entities. The Cloud layer is responsible for storage, analytics, mining, computation, high performance processing and so on. Once activated and operated, the physical resources begin to collect and produce huge amounts of information data transferred to the Cloud via the network layer in order to be processed after by application systems. Hence the Cloud is an important infrastructure that provides the bridge between the networked resources and the application layer. This last links users, workmen, and management to the smart factory systems. Through the terminals they use such as computers, LCD screens, smart phones and tablets, they can access the statistics provided by the Cloud, apply a different configuration and provide key parameters according to their needs by

choosing some different options or perform maintenance and diagnosis of the production process, even remotely through the Internet.

C. IoT and IIoT

After presenting the basic principles of IoT and IIoT, it is useful to determine a common understanding of the way they differ. In this section, we will explore the existing difference between IoT and IIoT before outlining in the next the main challenges and issues related to their appearance. In Table I, we outline the major differences between IoT and IIoT systems according to specific aspects. In general Industrial IoT is thought to be a subset of IoT that requires higher levels of security, safety, reliability, fault tolerance and real time monitoring of industrial operations. Such specificity is mainly due to the type of environments in which it is applied. The presence of harsh environmental conditions often cause repeated failures and interruption of industrial processes hard to readjusted. As an example of harsh conditions, we can notice temperature variations and radio interference that could easily increase latency, packet loss and energy consumption affecting as a consequence thereof key attributes of industrial systems such as availability, reliability and timeliness [29]. Another property differentiating Industrial IoT from regular IoT is the type of interconnected devices utilized in industrial settings such as sensors, actuators, production lines, industrial equipments, controllers, facility utilities, etc. Such application is proven to have a great potential to make the industrial production operates in an intelligent, efficient, flexible, and safe manner with constantly high quality and low cost.
However and even so IIoT have higher and stricter security and safety requirements, proposed solutions for IoT could quite easily be applicable to a specific IIoT scenario. This is especially true for requirements derived out of common challenges such as resource constraints, dynamic changes and identity management.

D. Research challenges

The integration of IoT technologies within the industrial environments makes production processes and operations operate in an efficient, intelligent and flexible manner with constantly high quality and low cost. However, such integration will create also various challenges that have gained increasing attention from the public and the research area [11] [13] [14]. In the following, we will cover five main challenges coming from both IoT and IIoT unconventional characteristics namely scalability, heterogeneity, reliability, dynamic changes, and security as presented in Fig. 3.

1) Artificial intelligence: With the increase in the global number of IIoT connections from 17.7 billion in 2020 to 36.8 billion in 2025 according to Juniper Research's new Industrial IoT research, specific attention must be paid to communication, storage, access, and processing of the huge amount of data to be produced by dynamic and complex

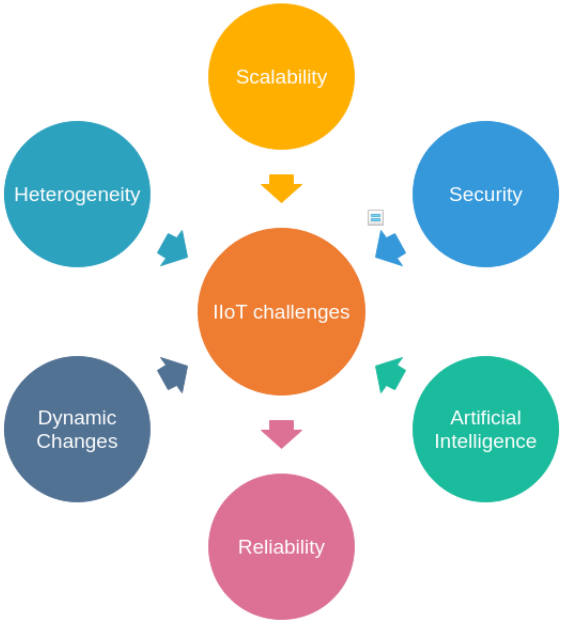


Fig. 3. Industrial IoT raised challenges

manufacturing environments with additional uncertainties and interdependencies. Moreover as this data is multi-sourced, heterogeneous, redundant, dynamic, sparse and considered having highly useful, valuable and most of the time deeply hidden information within [**?**], [**?**], it has been a challenge to handle this data, to aggregate it, to extract and to analyze the useful information it contains.

Recent advances in Artificial intelligence have demonstrated the potential of this technology to assist manufacturers in tackling the challenges associated with this digital transformation of CPSs, through its data-driven predictive analytics and capacity to assist decision-making in highly complex, non-linear and often multistage environments.
In the context of Trust management, data fusion and mining techniques have become crucial of importance for the guaranteed success of IoT Trust management systems, In fact they play a fundamental role in reputation generation approach by applying filtering, fusion and grouping techniques in order to generate a concrete reputation value from the opinions and feedbacks targeting a specific node within the network. The use of such approach could reduce the amount of data to be forwarded and transmitted in the network which will conserve the energy consumption of the network nodes, reduce the traffic load and avoid exhaustion of network resources what would consequently lead to a longer network lifetime.

2) Scalability: With the explosive growth of Internet connected devices, both IoT and IIoT based applications and services must be able to support the increasing number of connected objects, end users as well as the application features, processing and analytics capabilities without causing any significant decrease nor degradation in the quality of the service offered to their customers.

Copyright manuscript

Selected Aspects	Internet of Things	Industrial Internet of Things
Connected devices	Devices located in end users or commercial settings	Devices located in industrial settings: factory floors, production lines, automation control, power grids, etc.
Focus	Guarantee personal data and assets protection	Ensure intelligent industrial operations Prevent process interruptions Enhance industrial safety Save Time and cost
Service model	Human centric	Machine centric
Prioritized Security requirements	Confidentiality, Integrity, Availability	Availability, Integrity, Confidentiality
Resilience	Not required	Fault Tolerance highly required
Maintenance	Customer preferred	Scheduled and planned
Devices failure implications	No critical consequences	Interruption of process, impact on production, potential physical threats
Type of environment	Regular environments	Harsh environments

TABLE I
COMPARISON OF IOT AND IIOT

Submitted manuscript

Scalability is therefore essential to meet the inherent features of such systems. In such vast networks of interconnected objects, designing related frameworks such as authentication, authorization and access control mechanisms should take into full consideration the scalability feature of such environments so that all participating and involved entities from organizations and humans to devices, assets and services should be identified and authenticated to grant access and authorization tokens to entities requesting to use their resources at anytime and from anywhere. These mechanisms therefore should be extensible in size, structure, and number of users and resources. Besides, the unbounded number of connected entities exposes them to potential threats and attacks that imposes to move towards distributed approaches and infrastructures without centralized control of any security authority or management system.

3) Heterogeneity: The IoT interacts with a large number of devices presenting very different technologies, services and capabilities from the computational and communication standpoints thus making them incompatible. Differences between those devices can be the operating system, the connectivity, the I/O channels and the performance which will lead certainly to different computational power, storage capacity and energy consumption. Since IoT devices would be connected through an interface in common in order to communicate all together, the management of their heterogeneity should be guaranteed at both architectural and protocol levels [23]. Thus the task of standardization needs to be considered to ensure interoperability among devices and also to standardize the communication among the network.

4) Reliability: The reliability within the Smart factory is an important evaluation factor that reflects the performance of the whole system insofar as it evaluates both data and results consistency as well as the stability of the offered services.

In an industrial environment, the reliability is concerned with how much data is received successfully at the receiver end with minimum delay. However, the reliability of the transmitted data is affected by the environment dynamic topology where packets transmission is susceptible to link availability, interference, channel state change and protocol overheads. Therefore, high communication reliability is essential to provide accurate and precise supervision of industrial processes.

In this context, authors in [**?**] have presented some of the approaches used to increase the reliability of wireless sensor networks used in industries such as redundancy, frequency-hopping and interference minimization. In addition, many other works [26], [27], [28] have assumed that the use of the fifth generation (5G) mobile technology will address effectively the industrial requirements associated with Industry 4.0 based Smart factory by reducing the communication latency, increasing the longevity of devices battery life and more importantly improving the reliability of communication in indoors as well as in outdoors.

5) Dynamic changes in industrial environments: In the context of IoT, states often describe devices' behaviors. Transitions between states are quite common and frequent, e.g., started and standby, sleeping and waking up, leaving and joining networks. Besides, the number of connected devices can also evolve. Environments in which IoT devices operate are subject to contextual changes. The characteristic of dynamic changes is the intrinsic properties of the IoT. However, many threats emerge due to dynamic changes in IoT systems. For instance, in intelligent transportation systems with characteristics of the high mobility of connected vehicles, rapidly changing network topology and unbounded network size, hackers could even hijack a moving car and take the control. Particularly, IoT devices, such as vehicles or wearable devices equipped with strong mobility, often make great demands on across domain authentication and authorization to prevent malicious attacks from adversaries. Therefore, the secure IoT infrastructure should be able to resilient to this dynamic changes environment and provide a peer-to-peer authentication and authorization services.

6) Security: Many Other challenges have been discussed in the context of IoT but one of the most im-

portant ones is the security challenge [14], [15], in fact traditional security mechanisms could not be used directly within IoT applications due to its different technologies, standards and communication stacks [16]. In addition, the existence of such a large network with a high number of interconnected entities will definitely imply various scenarios of attacks and eavesdropping which could threaten those entities and put them in danger thus harming the corresponding users.

To cope with this challenge, cyber security systems must offer adapted mechanisms to protect the collected data from physical devices and this since it may include and manage sensitive user information. This means that data confidentiality, integrity, and availability should be provided by the IoT system [17] which could be done by considering encryption primitives [18], [19], redundancy techniques as well as authentication [20], access control and authorization [21], [22] mechanisms in order to prevent unauthorized users to access the system.

Recently, many other security challenges have been arised especially with the full increasing implications of ubiquitous connectivity and on the other hand as regards to the frequent integration of IoT services and applications to carry out daily activities.For example, data providers can behave deceitfully by providing false information. Users personal and sensitive data could be collected, accessed and interpreted by third parties what could make data providers hesitant about sharing their information. Hence both privacy and trust represent real and major issues that may limit the potential and the development of IoT applications. The increasing amount of production data uploaded and shared between smart devices deployed in heterogeneous and distributed architectures and communicating with each other independently within and beyond the factory site put the corresponding industrial system at a greater cyber risk that need to be seriously considered in the near future. For example, attackers can manipulate and infiltrate industrial systems, malware injection can disturb their functioning and put them out of action, which could cause significant damage to the whole production area.

E. Trust management in IoT and IIoT

In the current literature, various trust definitions have been proposed. these last range from specific scenarios to wide and general systems. Meanwhile, the trust meaning across existing proposals differs from one work to another insofar that each one of them has considered trust from different perspectives. According to [120], trust is defined as the subjective expectation of others future behavior as expected by their evaluators on the basis of the history of their encounters. An- other definition was given in [69] where trust was defined as the firm belief that other entities are competent enough to act in a secure, dependent, and reliable way within a specified context. A trust management system is often needed to produce reaction based on the real time evaluation of entities behaviors during established interactions in addition to feedbacks and recommendations gathered from other entities. These last aggre- gated together form an overall trust score that once shared and propagated over the network, participating entities could decide whether to continue or not the collaboration. This concept plays a key role in IoT in general and has a great importance for in- dustrial IoT based environments. It is essential when participating devices, with- out being previously interacted with each other, want to cooperate and to use provided services with a certain degree of trust among themselves. It is needed also to achieve trustworthy data during collection, exchange, analysis, fusion and mining phases which is inevitably crucial in IoT and especially in smart factories where devices continuously collect data with great amounts and important infor- mation within that is needed for critical decision making. It is needed as well for many other decision making situations such as access control, intrusion detection, key management, isolating misbehaving nodes for effective routing, authenticat- ing devices before interaction and other purposes. Regarding this set of security requirements, in this survey, we will focus mainly on trust mechanisms specifically those based on the blockchain technology. Details about the notion of trust and the operations considered for trust computation are given in Appendix A.

1) Challenges of Trust Management Systems in IoT and IIoT: To provide trustworthy IoT, research on Trust management should respect the following criteria as marked in Fig. 4.

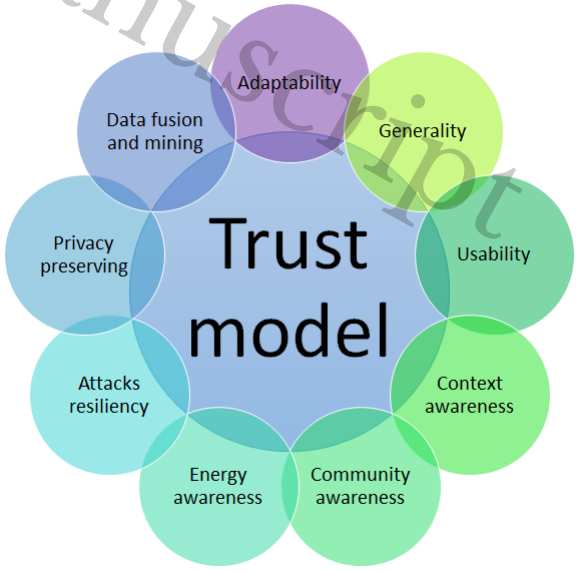


Fig. 4. Trust management challenges in IoT

- Generality (G): A Trust evaluation mechanism should be suitable for various IoT systems and services that can be commonly considered and widely applied in different application scenarios.

Submitted manuscript

- Usability (U): A Trust management system should be usable for users with regard to user-device interaction in order to provide more intelligent services interacting with humans.
- Energy awareness (EA): Energy awareness is an important factor that should be considered when designing a Trust management system for IoT networks. Thus a Trust evaluation mechanism should take into consideration the remaining energy levels when selecting trusted entities.
- Context awareness (CxA): A Trust evaluation mechanism should evaluate the Trust level of an entity by taking into account additional parameters and details concerning the current context in which the evaluation has been conducted.
- Community awareness (CmA): A Trust management system should be able to adapt to different communities and also to be aware of the impact and community specific properties on the trustworthiness evaluation.
- Adaptability (Ad): The Trust evaluation can be based on such customized criteria or on a general metric to compute the corresponding trustworthiness. Here the Trust management system must be adaptable in order to be able to update Trust values in response to changing criteria and according to the evaluating entity's characteristics.
- Attacks resiliency (AR): The trust management system must provide strong defenses against attacks that could be launched by malicious parties including those related to Trust composition (bad mouthing attack, self promoting attack, on-off attack, etc.), those related to Trust propagation (at the communication level : man-in-the middle, sniffing, etc) and those related to the accesslevel (Sybil, spoofing, etc.).
- Privacy preserving (PP): While sharing and communicating Trust related information, the entities' identities and personal information must be flexibly preserved. The trust management system here should not leak private details as well as behavioral information related to each part within the network.
- Data fusion and mining (DFM): the huge amount of data collected in IoT should be processed and analyzed in a trustworthy way with regard to reliability, holographic data process, privacy preservation and accuracy. This objective also relates to trusted social computing in order to mine user demands based on their social behaviors and social relationship exploration and analysis.
- Decentralization: A trust management system is often needed to produce reaction based on the real time evaluation of entities behaviors during established interactions in addition to feedbacks and recommendations gathered from other entities. Towards this aim, current TM frameworks are built on a centralized model where a central server determines the trust values of participating entities. This approach necessitates high-end servers and proves to be unsuitable for scenarios where objects are required to autonomously exchange trust data and where end-to-end communications do not have to go through a centralized server for performing trust management services especially when these last could be analyzed to reveal sensitive information about trust providers and targets.

2) Distributed Trust Management Systems in IoT and IIoT: This section presents distributed trust management schemes. In this, each of the devices is liable for trust management owing to the fact that devices in IoT are capable enough to evaluate, process, propagate trust information to other nodes upon request, and even aggregate trust information (including self evaluations) for trust assessment toward other participating devices. Further, the process of trust computation is accomplished by relying on the information observed directly by the devices or received as the recommendations from the other devices in the system.

In [35], [36] as well as in [37], every entity acts autonomously to collect evidence (through self-observations or recommendations) and also serves as a recommender upon request. Hence it is based on distributed on demand trust management. An entity first collects evidence of the service quality trust and social similarity trust of adjacent entities. Then it collects recommendations from qualified adjacent entities about other ones in the system. Respectively, three Trust properties were considered to evaluate nodes' trustworthiness namely honesty, cooperativeness, and community-interest.

In [37], the scalabilty of IoT devices was considered by designing a storage scheme. Instead of storing trust information for all the devices, trust information about a group of devices meeting the interest is kept. The validity of the proposed model has been evaluated by the simulation for trust convergence and hit ratio.

A trust model for service composition in IoT, based on the service-oriented architecture (SOA), is proposed by [40]. The proposed model uses Beta Distribution over positive and negative feed- backs along with the social attributes to compute direct and indirect trust. A filter-based approach (distributed collaboration filtering) is adopted to select feedbacks using social contacts, similarity rating of friendship, and CoT relationships.

The advanced vision of the proposed approach is presented in [38] where authors considered a smart storage scheme and resilience towards more sophisticated trust-related attacks.

Authors in [39] proposed and analyzed an adaptive trust management scheme for social IoT where relationships between IoT devices and their owner change dynamically. The authors presented a trade-off between trust convergence speed and trust fluctuation, aiming to identify the best and appropriate parameter setting for trust propagation and aggregation.

In [41], a decentralized trust evaluation model was presented for vehicular IoT where a where a fuzzy logic-based approach was considered to compute direct

Submitted manuscript

Work	Applicability	Adopted Methodology	Considered Model	Performance metrics	Advantages	Limitations
[35]	Service Composition	EX-REC	Statistical model	Honesty, Cooperativeness, Community-interest	- Takes into account social relationships. - Accumulates the past behaviors and weighs them based on time.	- Does not address issues pertaining to scalability and dynamicity. - Does not take into account the context while evaluating trust.
[36]	Service Composition	EX-REC	Statistical model	Honesty, Cooperativeness, Community-interest	- Considers a social IoT environment with dynamically changing conditions. - Defines a weighting factor to evaluate the confidence put into recommendations.	- Does not address issues pertaining to scalability. - Estimates the Trust when providing reports basing on its trustworthiness score when assisting in a service.
[37]	Service Composition	EX-REC-K	Statistical model	Honesty, Cooperativeness, Community-interest	- Meets the scalability, compatibility, extendibility, dynamic adaptability and resiliency requirements. - Computes trust in communities of interest.	- Assumes that a CoI will have same social interest, which may not be true always. - Very computation intensive
[38]	Service Composition	EX-REC	Beta distribution and statistical model	Friendship, social contact, and community of interest.	- Uses distributed collaborating filtering to select feedbacks of nodes sharing similar social interests. - Trust parameters are adjusted dynamically by an adaptive filtering technique.	- Assumes the availability of a high-end device for every user, which cannot be guaranteed.
[39]	Service Composition	EX-REC	Statistical model	Satisfaction level, capability, and sociability.	- Proposes a clustering architecture based on the similarity of interest. - Computes Trust at both node level and admin level.	- Additional complexity in implementing the Kalman filter for Trust prediction.
[40]	Service Composition	EX-REC	Beta distribution and statistical model	Friendship, sociability, and community of interest.	- A filter-based approach (distributed collaboration filtering) is adopted to select feedbacks. -An adaptive technique is used to compute the weight for direct and indirect trust.	- ..
[41]	Service Composition	EX-REC	Fuzzy logic, Q-learning	Honesty, cooperativeness, responsibility	- Learning based approach to assess recommendations for indirect trust computation with discounted rate	- Susceptible towards trust related attacks
[42]	Service Composition	EX-REC	Bayes distribution	Positive and negative interactions, Time duration	- Effective and fast methodology to detect on off attack with lower latency in information centric IoT.	- Ineffective to address dishonest recommendation based attacks.

TABLE II
DISTRIBUTED TRUST MANAGEMENT SYSTEMS FOR IOT AND IIOT

Submitted manuscript

trust using cooperativeness, honesty, and responsibility metrics. For indirect trust, reinforcement learning has been adopted.

Another distributed trust management scheme was presented in [42] for defending against on-off attacks in information-centric networking based IoT. In the proposed scheme, trust is computed using Bayes Probability distribution over positive and negative feedbacks. To observe on-off behavior, the time duration between higher and lower trust value is considered.

Authors in [43] have followed also the distributed scheme where each node maintains its own trust assessment towards other nodes and propagates its recommendation trust toward other nodes. The computation of trust was inspired by clustering techniques that are adopted in WSNs..

In the context of Industrial IoT, authors have proposed in [44] an adaptive context-based trust evaluation system, which calculates distributed trust at the node level to achieve edge intelligence. Each edge node takes

recommendations from its context-similar nodes to calculate the trust of serving nodes. This collaborative trust calculation mechanism helps in filtering out malicious nodes in the network.
Another trust management approach suitable for industrial environments was presented in [45] where authors have proposed to change the traditional centralized architecture of IIoT networks in automotive plants into a hybrid architecture based on a set of new industrial relationship rules.
Table II summarizes discussed schemes based on different measures such as their applicability, adopted methodology, considered model, and performance metrics while highlighting their strength and weakness.

3) Limitations and open issues of distributed TMS in IoT and IIoT: The emergence of distributed networks of embedded IoT and IIoT devices has generated new challenges for trust management. Traditional schemes, even decentralized, as the ones introduced above, suffer from several shortcomings:

- According to the carried review, existing trust management schemes generally consider a common small set of parameters to evaluate trustworthiness which are either related to QoS, social or reputation aspects without focusing on the security aspect that consists of verifying the confidentiality and integrity of trust evidences during their collection, propagation and communication between participating devices. Instead, they assume that collecting information from a large number of entities and executing aggregation operations on the exchanged trust related information will result in a relatively accurate assessment.
- Another issue that has not been extensively studied within proposed trust models is the sharing of trust information. In fact existing trust models do not explain how trust scores are represented and how they are interpreted by involved and participating entities during the evaluation.
- A third issue that trust management systems face is the ability to link an identity to a single entity and to prevent that a specific entity obtain more than one identity. Whereas identity management can play an important role in measuring the credibility of exchanged trust related information and resisting against Sybil attacks where a malicious entity can forge different identities to trick the system with multiple fake entities. As a partial solution to this issue, authors in [33] have introduced a framework to detect possible sybil attacks against trust management schemes within peer-to-peer (P2P) networks. This has been shown to almost entirely prevent a Sybil attack, although the cost to the network in terms of the resources required to verify each peer is high which makes the solution unsuitable for IoT networks.
- Finally, a last but not least important issue is the storage of trust information, In fact and regarding IoT networks with tight resource constraints, some of the existing trust systems store trust information for devices with the highest trust values [39], others for those that have been recently encountered and interacted with which is not that good deal especially as trust computation depends on the past evaluations of all behaviors and interactions.

Promising solution: Decentralizing Trust Management Systems in a Secure Way Through the Blockchain

A decentralized, resilient, fault tolerant, secure and censorship resistant approach to trust management systems in both IoT and IIoT networking would solve many of the encountered issues. Currently, the blockchain technology is considered as one of the most appropriate candidate technologies capable of supporting a distributed and secure trust management system for both the IoT and the Industrial IoT. The inherent characteristics of this technology make it a convenient tool for developing secure and distributed frameworks for these environments. In this context, a trusted communication environment is created using smart contracts, policies, or set of rules. Relevant trust information, in the form of transactions, is computed, stored and shared using a distributed ledger and can be accessed either publicly or with permission. The idea of a blockchain based trust frameworks for IoT and IIoT has attracted considerable interest from researchers for the following potential benefits:

- The decentralization feature of the blockchain technology enables device autonomy and self organisation where entities interact with each other without any central control, and where end to end communications do not have to go through a centralized server for performing trust related services such as trustworthiness evaluation, recommendation sharing and trust computation. Participants in the blockchain can verify the integrity of trust related data they sent, as well as the identity of the sending participant.
- Since no single entity controls the contents of blockchain, trust related data and event logs stored on the distributed ledger are immutable and practically impossible to be tampered. Similarly, all historic trust records are also immutable and, in order to modify any previous data, an attacker would need to compromise the majority of entities involved in the blockchain network. Otherwise, any changes in the distributed contents are easily detected.
- By Providing effective and consistent sharing of historical trust information, the blockchain technology guarantees transactions transparency and traceability. In the area of IoT applications such as smart manufacturing, tracing historical trust data is crucial. For instance, by reviewing trust data, we can predict the future behavior of malicious and attacker entities launching especially on-off attacks.
- Since all participating peers hold a copy of the

Submitted manuscript

distributed ledger, they can access all timestamped transaction records. This transparency allows peers to look up and verify transactions involving specific blockchain addresses. Blockchain addresses are not associated with identities in real life, so the blockchain provides a manner of pseudo-anonymity. While records of a blockchain address cannot be traced back to the owner specific blockchain addresses can indeed be held accountable, and inferences can be made on the transactions a specific blockchain address engages in.

F. Blockchain Technology for IoT and IIoT

We provide in this section a detailed description of what a blockchain is, how a blockchain network operates, what are its main characteristics and concepts, how smart contracts allow us to radically redefine how interactions between transacting parties on a network can be set up and automated, and finally what are the different security application scenarios a blockchain is used for in IoT and IIoT.

1) Definition: Originally designed for keeping a financial ledger and meeting the purpose of cryptocurrency applications, the blockchain paradigm can be extended to provide a generalized framework for managing any movements of data related to goods, devices, information records, etc. This last could be defined as a distributed ledger of transactions across a decentralized network whereby records of all established interactions are registered providing thereof a proof of existence, of ownership and modification of this data during interaction [81], [82], [83]. These transactions are hold within blocks chained together through cryptographic hashes contained within their headers in order to ensure immutability insofar that blocks once chained, data contained within will be available and could never be changed or altered. Each block references the hash of the block that came before it. This establishes a link between the different blocks, thus creating a chain of blocks, or blockchain.

2) Blockchain Types: Based on several criteria and how they are used in different application scenarios, blockchain systems can be classified into three main types namely public, private, and consortium blockchains [84], [81]. These three are compared in Table III and described as follows:

- Public Blockchains: This category provides an open platform that allows users from different organizations and backgrounds to join, transact, mine and perform read and write operations on the blockchain. There are no restrictions on any of these factors and anyone can send transactions, maintain a copy of the distributed ledger and engage in validating and adding new blocks to the chain where the nomination of permissionless blockchains. Moreover the blockchain is open and transparent, there are no specific validator pre-selected set of nodes and all users can publish new blocks to the blockchain by solving either computationally expensive puzzles, or staking one's own cryptocurrency.
- Private Blockchains: This kind of blockchain is mainly set up to facilitate the private sharing and exchange of data among a group of known members within a single organization. Private blockchains are also called permissioned blockchains insofar that external users cannot have access nor participate unless they are authorized to do. Users' participation is decided either by a set of rules or by the network that controls access. This inclines the network more toward centralization, while derogating the elementary blockchain features of complete decentralization and openness as defined. In a private blockchain system, once nodes become part of the network, they contribute in running a decentralized network, with each node maintaining a copy of the ledger and collaborating to reach a consensus for updating. But, unlike public blockchain, the writes are restricted.
- Consortium Blockchains: This kind of blockchain could be considered as a partly private and permissioned blockchain, in which no single organization handle consensus process and block validation but rather a set of pre-selected set of nodes. These nodes decide who can participate in the network and who can partake in the consensus mechanism. Thus, it is a partially centralized system, owing to the control by some selected validator nodes.

3) Blockchain Technology Features and Working Principles: In order to understand the potential applications of blockchains in IoT and IIoT, it is important to have a clear understanding of the main concepts and working principles of blockchains.

1) Consensus mechanisms: To ensure that all entities agree on the transactions and the order in which these are listed on the newly validated block so that they have the same copy of the ledger, an agreement is required to maintain the blockchain architecture and to ensure its functioning and consistence. Otherwise, the individual copies of the blockchain will diverge and we will end up with forks. A distributed consensus mechanism is therefore needed in every blockchain network in order to make sure that an agreement is reached between the set of predefined entities to support a decision making. The type of the considered consensus mechanism depends mainly on the blockchain network as well as the characteristics and the capabilities of the participating entities.
To reach consensus among validating entities, several ways could be considered [85], [86]. Below, a brief introduction to a few of them is given.
   - PoW (Proof of Work): this consensus strategy is used in the Bitcoin network in addition to many other cryptocurrencies to confirm transactions and produce new blocks to the chain. In such a strategy, publishing new blocks to the blockchain is called "mining", and miners engage in a race to

Submitted manuscript

	Public blockchain	Consortium blockchain	Private blockchain
Registration authorities	Anyone	Multiple entities (organizations)	Single entity Defined before initializing the network
Access	Public read/write	Can be restricted	Can be restricted
Identity	Pseudo-anonymous	Approved participants	Approved participants
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Participation in consensus	All nodes	Selected nodes in multiple organizations	Single organization
Transaction Speed	Slow	Lighter and faster	Lighter and faster

TABLE III
TYPES OF BLOCKCHAINS

find a nonce that, when hashed with the hash of a block, produces a resultant smaller than a predefined threshold. In the decentralised network, all participants have to calculate the hash value continuously by using different nonces until the target is reached and get rewarded.

- PoS (Proof of Stake): this consensus strategy is an alternative approach for PoW that requires less CPU computations for minting. Meanwhile, the more currency forgers held, the greater chance they have to generate the next block.
- PBFT (Practical byzantine fault tolerance): this consensus strategy is based on a replication algorithm to tolerate byzantine failures. All entities, in this method, should participate in the voting process in order to validate and to add the next block. Here, the consensus is reached when more than two-thirds of all nodes agree upon that block. Meanwhile, PBFT can tolerate malicious behavior from up to one-third of all nodes to perform normally.
- RR (Round Robin): This mechanism is mostly used in private blockchain networks, where mining is restricted only to select identifiable entities. Within this consensus strategy permitted entities create blocks in rotation in order to generate a valid blockchain. More specifically, every entity in a given time window can only create a finite number of blocks calculated using a network parameter called mining diversity that determines the number of blocks that should be wait for before attempting to mine again.

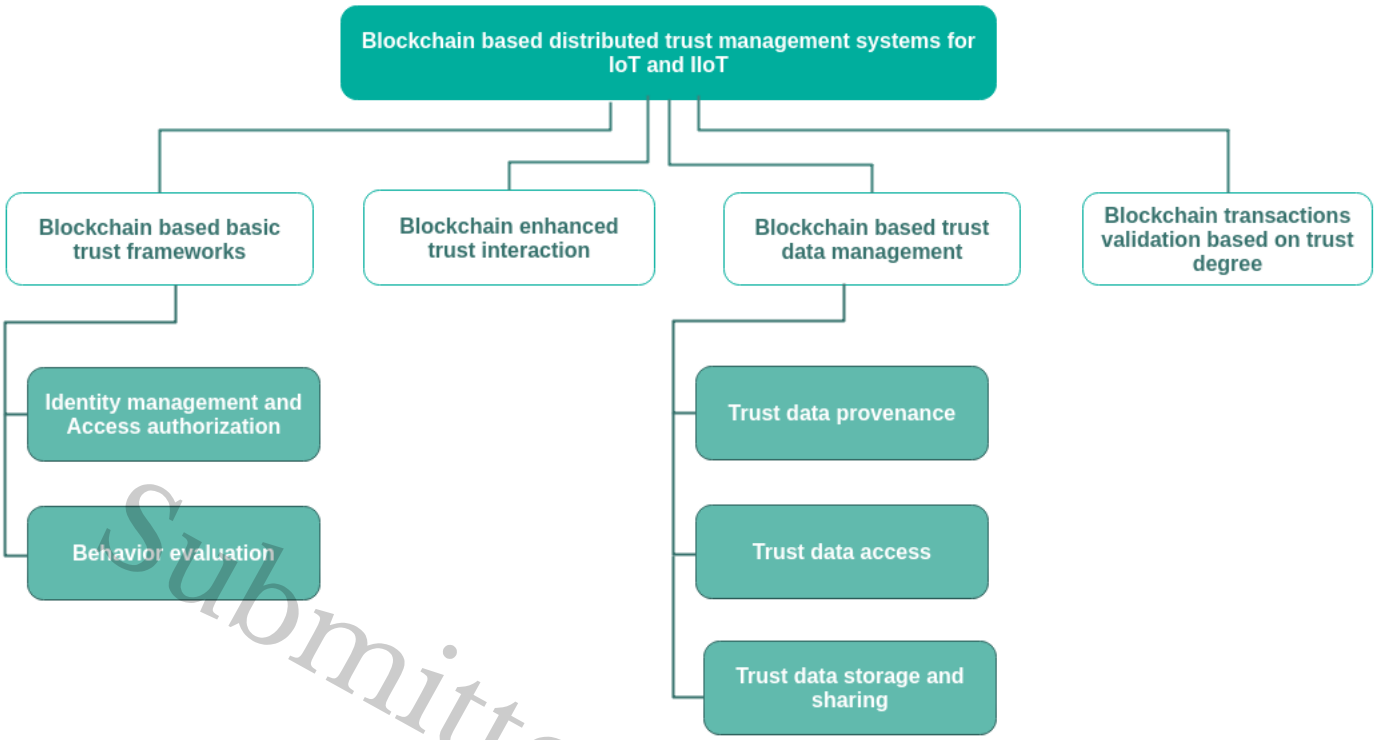
2) Smart contracts: A smart contract is an executable code deployed and residing at a specific unique address on the blockchain network. This last is triggered by addressing a transaction to it. The main aim of a smart contract is to automatically execute the terms of an agreement once specified conditions are met. It include a set of data which are the state variables and code corresponding to the executable functions. These last are executed when transactions are made, broadcast to the network and addressed to its address. Called smart contract then runs independently and automatically in a prescribed manner on every node in the network, according to the data that was included as input in the related transaction, as a result an eventual return value is shown to the outside.
Smart contracts can be developed and deployed in different blockchain platforms where each one of them offers distinctive features for development supported by different high-level programming languages. In Ethereum blockchain platform, advanced and customized smart contracts are supported with the help of Turing complete programming language. The code of an Ethereum contract is in a low-level, stack-based bytecode language referred to as Ethereum virtual machine (EVM) code. Users define contracts using high-level programming languages compiled into EVM code.

3) Peer to peer networks: The continuous and widespread growth of Internet based applications in terms of number of users and computational resources, has challenged the centralised nature of the client-server paradigm which has led to the emergence of peer to peer networks. These last provide a good substrate for creating large-scale data sharing, content distribution and application-level multicast applications [87], where neither hierarchical organization nor central governing authority is needed within the network. Instead a set of autonomous entities called peers form self-organizing overlay networks that are overlayed on the IP networks, offering a set of various properties as follows:

a) Self-organisation: where nodes are able to interact with each other without any central control. This is the main property of peer to peer systems that makes the difference against the client-server paradigm.
b) Decentralised resource usage: available resources of nodes (CPU, storage, and bandwidth) are distributed and shared with the best effort regarding its load distribution.
c) Fault tolerance: where the failure of a single node within the peer to peer network must not compromise the correct operation of the whole system.

When it comes to blockchains, one of the main goals of this technology is to minimize the number of intermediaries being involved in the process. As a

Non-printed manuscript



Submitted manuscript

Fig. 5. Classification of blockchain based distributed trust management systems for IoT and IIoT

result, the use of the peer to peer architecture was a necessity to offer security, decentralization, and censorship resistance.

4) Cryptographic techniques: In blockchain, cryptography technology is mainly used to protect user privacy, transaction information, ensure data consistency and immutability, and guarantee the blockchain as a distributed ledger with tamper proof and public verifiability [88]. In what follows, we will present an overview of the commonly and widely used cryptographic primitives and algorithms in blockchain platforms.
   - Hash functions: Hash functions are generally used to guarantee data integrity and immutability and to ensure that it has not been illegally tampered with. In the context of blockchains, hash functions can be used to perform block and transaction integrity verification where the hash value of the information of the previous block is stored in the header of each block, and any user can compare the calculated hash value with the stored hash value. In turn, the integrity of the information of the previous block is detected. The most popular hash function used in blockchains is SHA256, which is one of the algorithms from a family of cryptographic hash functions named SHA (Secure Hash Algorithms).
   - Digital Signatures: Besides hash functions, digital signatures are another inevitable cryptographic primitive in blockchains. Generally speaking, these primitives are used for ensuring source authentication, source non-repudiation and integrity. A digital signature scheme usually consists of two algorithms: a signature generation algorithm and a verification one. In the context of blockchains, ECDSA and EdDSA are the two digital signature schemes frequently used in blockchains [88]. In principle, both of them are based on the hardness of the elliptic curve version of discrete logarithm problem. ‘
   - Other primitives: To enhance more transactions and identites privacy, some other primitives are applied in some blockchain based applications such as ring signatures, multi-signatures, non interactive zero knowledge proof, commitment proof and so on [89], [90].

III. Blockchain based Trust Management for IoT and IIoT

In this section we will review first how existing works deal with the concept of blockchain based trust management in IoT systems and exceptionally for Industrial IoT. Therefore, we will investigate the different dimensions on which they are based and the criteria that could be considered to compare existing models and frameworks. According to the usage and the role of blockchain technology within the trust management process in both IoT

and IIoT systems, we classified blockchain based trust mechanisms into four categories as it is illustrated in Fig. 5: Blockchain based basic trust frameworks, Blockchain based enhanced trust interaction, Blockchain based trust data management and Blockchain transactions validation based on trust degree. Below we will introduce the research progress in each of the above areas. Therefore we will outline the aspects that can be considered as done and we will point out where we still have some gaps that need further research.

A. Blockchain based basic trust frameworks

Generally speaking, trust comprises both identity trust and behavior trust. Behavior trust is a key factor in assessing and predicting the credibility of entities' behaviors while identity trust is concerned with verifying the authenticity of participating devices and determining the authorizations they are entitled to access.

1) Identity management and Access authorization: In [58], a blockchain based trusted IoT environment for robust identification and authentication of IoT devices is presented. In the proposed work, a secure virtual zone, called a bubble of trust (BoT) is created for enabling devices trusting each other. Each zone has a master device that signs tickets for its follower devices using group ID, object ID, public key, and signature. The uniqueness of both the master's object ID and the group ID is verified using smart contracts.

Authors in [59] have introduced a trust and reputation system incorporating blockchain to control the access between IoT devices. Their approach considers attribute based access control policies for dynamic management of access rights. The automatic execution of imposed policies is carried out by composing three types of smart contracts automating the process of attribute validation, trust computation, and access policy validation.

For lightweight IoT devices, a blockchain based authentication and access control mechanism was proposed in [64]. This model is decentralized in nature which performs its operations based on fog computing and public blockchain. A smart hospital is used as a use case for the implementation study of this model. This model protects IoT systems from many attacks such that non-repudiation attacks, message reply attack substitution attacks, etc. This model provides security of nodes from the same IoT system as well as other IoT systems. However, this model uses a huge amount of energy and power which can be avoided by using a lightweight smart contract mechanism.

Another blockchain based authentication system is presented in [51] where a fully distributed large scale trust management model based on a new technology called Holochain is considered. This model is designed to address the limitations of the blockchain technology such as scalability and slow transaction rate. A distributed fog layer is used along with an IoT layer to store and manage all related trust information of IoT devices. Security issues like the bad behavior of nodes, the integrity of data, and the availability of services are addressed. To provide security, a copy of this protocol is included in every fog to join the system. However, no mechanism is presented against different attacks of IoT trust. This model may have some attack-specific mechanisms which make it more secure.

In [65], authors have designed IoT Passport, a blockchain based trust mechanism for collaborative IoT systems. The proposed framework comprises blockchain driven authentication, authorization and trust management within the perception layer. Therefore it is built upon a trust based collaboration and an hierarchical trust synchronization within the network layer for data sharing across trust domains. Finally, the Application layer at the top includes a collection of essential services called collaborative IoT services. The proposed components are associated with smart contracts to manage access control policies, collaborative rules for cross platform trust and incentive policies for participants reward.

2) Behavior evaluation: In [52], a scalable blockchain based trust management protocol with mobility support in distributed IoT systems, named BC-Trust was proposed. The presented scheme based on both the blockchain and the fog computing technoology, allows highly mobile IoT devices to accurately assess and share trust recommendations about other devices in a scalable way without referring to any pretrusted entity which makes it resilient against bad-mouthing, ballot-stuffing and cooperative attacks.

In [56], a blockchain-based IoT monitoring framework, named IoTCop was designed to detect and isolate compromised devices. These last are identified by checking their behavior against the organization's security policies. Moreover three inherent challenges of IoT systems were adressed in this work namely latency, applicability, and resource constraints using Hyperledger Fabric blockchain framework and add-on hardware modules.

Another scheme was presented in [46] where authors have introduced ITM, an IoT trust management solution based on the blockchain technology as a decentralized system that interacts with decentralized applications and IPFS. The presented solution manages IoT devices trust to share a trusted content through the blockchain network.

In [66], a blockchain based trust management mechanism called BBTM is proposed where the trustworthiness of sensor nodes is evaluated by the mobile edge nodes based on exchanged trust feedbacks for specific contexts. The evaluation of trust computation outcomes is therefore completed via three smart contracts running on the blockchain network. The performance of the proposed BBTM mechanism is analyzed in terms of trust accuracy, convergence, and resiliency against bad mouthing and ballot stuffing attacks attacks.

Another blockchain based and energy efficient trust mechanism was presented in [67] for analyzing IoT

Submitted manuscript

devices' behaviors as well as detecting and isolating suspicious nodes to enable reliable and trusted network communication, to minimize network latency, traffic congestion, and message overhead for enhanced network lifetime. For trust assessment, gathered information involve details about the forwarding behavior and the energy consumption of neighboring nodes. Therefore the Subjective Logic Framework is considered for deriving a trust score that will be stored on the blockchain ledger and updated according to smart contract rules.
Another approach was presented in [68] where a game theory based decentralized trust management mechanism was proposed for IoT applications. The proposed work proposed to exploit on game theory to identify malicious nodes executing ballot stuffing and bad mouthing attacks by sending false trust scores. For trust composition, the fuzzy theory is considered for trust scores classification. Therefore for trust update, the Dempster-Shafer combination rule is used to combine the collected scores for trust derivation.

Submitted manuscript

B. Blockchain enhanced trust interaction frameworks

Once the trust is computed on target by any of the network entities, the resources, the time and the complexity spent on re-evaluation and re-computation of trust by other entities could be avoided in case where trust gets propagated in the network, which is particularly important in IoT environments which are characterized by resource scarcity, dynamicity, autonomy, mobility and lack of infrastructure. Recommendations are the simplest case of trust propagation, these latter could be propagated either on request from relying entities or autonomously to other immediate neighboring entities. On the other hand it can be of multi hop thus the transitivity property of trust. Moreover, the core factor to be considered for trust propagation is the existing cooperation between network entities in communicating, exchanging and transmitting the trust related information. In the traditional trust systems, two schemes are considered for trust propagation including centralized and distributed approaches, where in centralized schemes, a third party (e.g. a centralized server, a cloud platform, a virtual service, etc.), came into play to propagate the trust information over the network in order to make it publicly available. Whereas in the distributed scheme, each entity will record locally the trust information and provide it either on request from relying nodes or communicate it autonomously to other entities it interacts and collaborates with. In this context, the blockchain technology acts as the reliable platform for ensuring the secure propagation and sharing of trust related information among collaborating entities.

In [60] a decentralized solution based on the blockchain technology for IoT data trusted exchange is proposed to improve data utilization and benefit from the trade. Three data exchange requirements were introduced namely trusted trading, privacy preservation, and data access, similarly three smart contracts were created namely access contract for providing trusted data permission management, auto exchange contract for setting access rights, and communication contract for recording the whole communicated process of data exchange.
Another work was presented in [61] where authors proposed PrivySharing, a blockchain-based framework for privacy preservation and secure data sharing in smart cities. The proposed solution divides the blockchain into multiple channels where each channel processes data from a specific domain, for example, smart city, smart home. Interactions with the blockchain network is secured with dual security in the form of an API Key and OAuth 2.0.
[62] presents a blockchain enabled data collection and sharing for industrial IoT with deep reinforcement learning. Their solution uses deep reinforcement learning to help each mobile terminal to sense nearby points of interest to achieve maximum data collection amount, geographic fairness, and minimum energy consumption and blockchain for secure data sharing among mobile terminals.
One other work was presented in [63] where a collaborative trust based and blockchain aware unbiased control transfer mechanism was proposed for industrial automation. To do so, a scalable trust propagation protocol is devised to enable the monitor and control center (MCC) and infrastructures can receive the publicly verifiable trust values from the terminals. Moreover a collaborative trust based delegated proof of stake (CT-DPoS) mechanism is proposed, which make sure the blockchain can select control nodes randomly and unbiasedly.

C. Blockchain based trust data management

In many cases we are also interested in how trustworthy a data is rather than the nodes who forward it or produce it, whereas an attacker can easily conduct eavesdropping, tampering and forgery attacks what could falsify the transmitted data and hence cause a grievous damage to the system in question. That's why evaluating the data trustworthiness and integrity is inevitably crucial in IoT and especially in IIoT where devices collect a large amount of data that convey important information for critical decision making. Thus, being able to guarantee the security and trust of data during collection, exchange, processing, invocation and storage become crucial and no more important than ever.
Blockchain based enhanced trust data management schemes include three sub research areas whereas: a) trust data provenance, b) trust data access, and c) trust data storage and sharing. In the following, we will present the research progress in each of the mentioned areas.

1) Blockchain based trust data provenance: Data provenance has the potential to guarantee the trustworthiness of trust related data by assessing the history of trust data sets and recording information about its origins, the operations executed on and all

its processing history from the initial source to its current state so as to achieve traceability, auditability, accountability, and privacy protection of both IoT and Industrial data. Although, the state of the art research on data provenance is often too complex and lacks effectiveness.

In [70], authors proposed ProvChain, a decentralized blockchain based data provenance architecture to guarantee data integrity and verifiability. The proposed framework stores the provenance data in blockchain to record and check the data usage history so as to make data operation transparent and traceable, thereafter establishing a trustworthy relationship among participating entities.

To achieve automatic blockchain based data provenance, several works have considered smart contracts into the provenance system. Smart contracts include a function for tracking data changes and define access rules for data. With the specific functions defined in smart contacts, the privacy of shared data can be guaranteed.

In [71], an end-to-end blockchain based framework was proposed for data trust. The proposed framework introduces a trust model to assess the quality of data using three trust parameters namely data owner's reputation, data asset endorsement and confidence level in the data provided. All these parameters are stored on the blockchain and updated with each new transaction. Moreover three primary smart contracts are considered mainly for access control, consent management and data provenance. The data asset provenance contract is responsible for monitoring access regulations and modifications on each data asset by exploiting both the provenance and the audibility features of the blockchain.

Another provenance system was proposed in [72] where trust concerns coming from various IoT edge devices in cloud infrastructure are addressed by a provenance mechanism to record sensor data and origins of the related entities. The provenance system structure is based on a combination of IoT edge devices organized with a blockchain network. Blockchain transactions are used to record all actions within the ledger with data provenance.

A last but not least work was proposed in [74] where a secure IoT framework called BlockPro was proposed. Based on the Blockchain technology and using physical unclonable functions (PUFs) in addition, this work ensures not only data provenance but enforces data integrity by providing an immutable storage system. Within the proposed framework, PUFs are used to give each IoT object a unique hardware fingerprint that is mainly utilized to identify data origins. Moreover the blockchain based decentralized storage and retrieval enforces data integrity with its immutable chain of records.

In the context of Industrial IoT, in [73] authors presented AgriBlockIoT, a fully decentralized blockchain-based model to maintain the data traceability for Agri-Food supply chains. The mechanism provides immutable, fault-tolerance, and auditable records of the whole supply chain system from production to consumption. The history of the purchased product is recorded in the blockchain system thus enabling effective data retrieval for consumers.

Another distributed provenance aware framework for traceability was proposed in [75] for IoT based supply chain systems. The proposed scheme monitor the different items within the supply chain according to their provenance such as the origin, the production, the different modifications and the process of custody. The monitored data are therefore stored in the IOTA Tangle distributed ledger whereas two smart contracts are deployed to ensure the storage and the distribution of the related provenance data.

2) Blockchain based trust data access: In [76], authors used the blockchain technology to provide a decentralized data management system for IoT networks. Within the proposed framework data access permissions among IoT users and IoT service providers are enforced using smart contracts while the audit trail of data access is kept stored in the distributed ledger. Moreover, a trusted execution environment is used to provide raw encrypted data protection from unauthorized access by adversaries.

In [77] a distributed resource management framework for Industry 4.0 environments (DRMF) was proposed. The presented work utilizes the blockchain technology to keep a living document trace about the flow of resources being shared among collaborating parties while using an access control model to implement fine grained and secure resource data access authorization through smart contracts. The proposed framework adds the notion of trust management to the access control model. Here a trust framework is integrated to evaluate the trustworthiness degree of shared resources as well as requesting entities guaranteeing thereof dynamicity of security policies insofar that they would be defined and validated function of the access requester entity's behavior.

3) Blockchain based trust data storage and sharing: Secure sharing and storage of trust information is inevitably crucial for its confidentiality, integrity and immutability especially in IoT enabled industries environments where devices collect a large amount of data conveying important information for critical decision making. That's why ensuring that the authentic data collected by physical devices can be transmitted, exchanged and stored within the IoT network without being unauthoritatively tampered, altered or stolen before being injected into the information system become crucial and no more important than ever. In this direction and given the noted features of blockchain technology, this last applied to trust management systems provide promising solutions. Taking that into account, many distributed and blockchain based schemes have been proposed in the current literature.

The work proposed in [48] intends to secure the storage and sharing of trust related information in IoT environments. The proposed mechanism is designed to

Submitted manuscript

Work	Application scenario	Adopted Methodology	Blockchain type	Performance metrics	Advantages	Limitations
[58]	IoT devices' identification and authentication	Smart contract based	Ethereum blockchain	Follower device's id Follower's ticket Follower's public key	- Creates secure virtual zones for enabling trusted communications. - Protects against sybil attacks, spoofing attacks, message based attacks and DOS/DDOS attacks	- Not adapted to real time IoT applications - requires an initialization phase that needs the intervention of the service vendor.
[59]	IoT devices' access authorization	Smart contract based	Ethereum blockchain	Delay analysis Computation efforts Trust and reputation evolution	- Dynamic management of access right for resource utilization based on devices attributes.	- Data structure is not adaptive with change in contracts. - Demands sufficient computational power for asymmetric cryptography
[64]	IoT devices authentication and authorization	smart contract based	Ethereum blockchain		- Considers a smart hospital as a use case for the implementation study Relies on fog computing to address the latency issues - Protects IoT systems from non repudiation, message reply and substitution attacks	- Uses a huge amount of energy and computation power
[52]	IoT devices behavior evaluation	Rule based	Tendermint blockchain	Satisfaction level of provided services Average of recommendations given	- Allows highly mobile IoT devices to assess and share trust recommendations. Addresses bad-mouthing, ballot-stuffing and cooperative attacks	- Devices connectivity is always needed for the entire process.
[66]	Sensor nodes behavior evaluation	Smart contract based	Private Bitcoin blockchain	Sensor nodes' feedback scores	- Solves the resource shortage problem of constrained devices during the trust process. Calculates the accuracy of trust evaluation outcomes. Defends against ballot stuffing and bad mouthing attacks.	- Needs to validate the proposal with real world IoT application scenario.
[68]	IoT nodes' behavior evaluation	Smart contract based	Hyperledger Fabric	Reputation scores	- Combines Game and Dempster-Shafer theories to realize robust trust estimation Uses Fuzzy logic for trust scores classification Defends against ballot stuffing and bad mouthing attacks.	- The performance is required to be evaluated against potential attacks in IoT.
[71]	Trust data provenance and access control	Smart contract based	Hyperledger Fabric	Data owner reputation, Data asset endorsement Confidence level	- Calculates trust for data sets and only trusted assets are recorded on the ledger. - Implements a secure and automatic access management system. - Utilizes smart contracts for querying data asset provenance.	- Needs to validate the proposal with real world IoT application scenario. -
[48]	Trust data storage and sharing	Policy based	Multichain blockchain	Cooperativeness, Competence, Community of interest	- Provides tamper proof data - Enables a more reliable trust information integrity verification during sharing - Defends against ballot stuffing, bad mouthing and on-off attacks.	- Lacks to demonstrate computation cost involved
[67]	Sensor nodes behavior evaluation	Smart contract based	Ethereum blockchain	Packet forwarding Energy consumption	- Detects blackhole and greyhole attacks in sensor nodes powered IoT - Improves the message overhead, malicious node detection time, optimizes the network lifetime	- Needs to validate the proposal with real world IoT application scenario.

TABLE IV
BLOCKCHAIN BASED DISTRIBUTED TRUST MANAGEMENT SYSTEMS FOR IOT AND IIOT

Submitted manuscript

collect trust evidences, to define a trust score for each device and to securely store and share them with other entities within the network by embedding them into blockchain transactions.

In [49], authors proposed SLTA, a blockchain based secure and lightweight triple trusting architecture for IoT systems. The proposed architecture includes an oracle-based data collection mechanism, used to ensure the immutability of IoT collected data, the credibility of participating IoT devices identities without relying on trusted third parties and finally to guarantee trusted, decentralized, reliable and privacy preserving data sharing.

In [50], a lightweight trust model based on the blockchain technology was proposed for supply chain management systems to enhance industrial data (including the key product data, sensor data, and data from some additional sources) storage and sharing among supply chain parties while reducing computational, storage and latency requirements.

A detailed comparison of blockchain based distributed trust management systems regarding the application scenario, the adopted methodology, the blockchain type, the performance metrics, the advantages and limitations is provided in Table IV.

Discussion

As seen in Tab. IV, almost all blockchain based trust management schemes have adopted the structure of public blockchain (Bitcoin or Ethereum blockchain) for building trust relationships and setting up fully distributed trust frameworks. On the other hand, little works have considered private and consortium blockchains for defining their trust management systems. These last are mainly considered to facilitate the private sharing and exchange of data within a closed or semi closed network with a known hierarchical structure. Moreover, proposed trust management systems are often designed to handle security services such as identity management, malicious nodes detection and behavior evaluation, access control management, and data assessment. From surveyed papers, we notice that more focus is given for designing distributed basic trust frameworks specifically for access authorization and behavior evaluation. Trust based access control systems make use of security policies and rules within the decision making process in order to map Trust values to the access permissions and to decide whether the access request is allowed or denied. The definition, the management and the update of these policies are distributed and supported by smart contracts running on the blockchain network.

When it comes to smart factories, controlling access to and within the manufacturing zone and protecting information and automation systems from violation is a business essential. Physical or digital security lapses, especially malicious behaviors can cause significant damage, particularly when it harms the factory equipments, or impacts the quality process. That's why access control mechanisms are essential in order to prevent unauthorized access to the system.

For the trust assessment, we have seen that this last takes into account in most investigated papers the reputation score of the trust target computed through the feedbacks and the recommendations provided by its neighbors. This last mainly refers to the social aspect of IoT and IIoT networks where devices are capable of autonomously establishing social relationships not only between each others but also between their owners and the community to which they belong.

Moreover, we can interpret from Tab. IV that some works have considered the energy consumption level in several existing works so that to address the energy efficiency challenge present in almost IoT based environments.

To validate the performance of proposed blockchain based trust management systems as well as their relevance and adequacy to IoT and IIoT environments, different perspectives were considered such as the effectiveness, the latency, the system throughput, the computational cost and the resiliency against malicious trust based attacks. However, and for some works, the performance evaluation of the proposed scheme was just done on the basis of a theoretical argumentation without presenting a real world application scenario or case study.

Moreover non of the investigated schemes explained how to implement the presented frameworks and how to deal with blockchain related concepts especially incentives schemes and consensus mechanisms where most works consider basic mechanisms as the PoW and the PoS. Miners selection and incentives payment for actively creating blocks with trustworthiness assessment are not discussed as well.

In this context, a considerable number of trust and reputation based consensus protocols have been proposed in the current literature. These last are investigated in the next Section.

D. Blockchain transactions validation based on trust degree

To ensure that all entities agree on the transactions and the order in which these are listed on the newly validated block so that they have the same copy of the ledger, an agreement is required to maintain the blockchain architecture and to ensure its functioning and consistence. To reach consensus, several protocols have been developed. Well established consensus mechanisms include PoW, PoS, PBFT, and their variants. Recently several alternatives have been proposed as an ongoing effort to improve these protocols such as those based on the trust or the reputation. Consensus mechanisms based on trust allow nodes with good conduct and legitimate behavior to agree on the global state of the chain. More specifically, nodes having a trust score higher than a given threshold are selected to publish new blocks in the chain.

In [91], a reputation based consensus protocol is proposed for peer to peer networks. Reputation values, in the proposed protocol, are used as incentives for block

Submitted manuscript

validation and participating entities are rewarded with trustworthiness instead of network coins for block creation as well as for legitimate behavior and good conduct.

Another reputation based consensus protocol is proposed in [92] for blockchain enabled IoT systems. The proposed mechanism, called Proof of X Repute PoXR, combines the distributed reputation system with PoX (Proof of X) consensus protocols. Entities having acceptable behavior history are chosen to participate in the mining process based on their accumulated reputation scores. Once accomplished, publishing entities receive repute rewards with reduced difficulty in the consensus process of the considered PoX. However, malicious ones are punished and have their reputation scores reduced.

A third trust based consensus fusion scheme was proposed in [93] for consortium chain enabled and self organized collaborated learning systems along with X-BFT consensus protocols. The proposed scheme, called TX-BFT, combines the trust evaluation system with the X-BFT consensus protocol to build a trust layer, evaluates consensus candidates' trust level and maintains consensus fusion stable. In each consensus process, participating entities assess eachothers' behavior and verifies corresponding trust degrees. These last are assessed while referencing to their historical behaviors stored in the blockchain ledger. Finally, trust rewards and punishments method are considered to realize trust incentive consensus.

Another trust based consensus protocol was proposed in [94] for XBFT consensus mechanisms. The proposed algorithm called T-PBFT use the EigenTrust trust model to evaluate participating nodes trust degrees and build a trustworthy consensus group called primary group responsible for building, recording and confirming new generated blocks. The trust assessment is based on the direct observation of nodes behavior in addition to received recommendations from indirect neighbors. After the group construction, the consensus process is launched where a consensus is made first within the primary group and therefore between the remaining nodes and the primary group.

One more trust based consensus protocol was proposed in [95] with proof-of-trust negotiations to identify the compromised fixed miners. With negotiation rules, a trusted random selection algorithm is introduced to select proposers and validators in a round of block creation while avoiding more communication overload of consensus protocols. As the proposers know nothing about each other, collusion to fake blocks among the proposers can be avoided.

A last but not least scheme was presented in [96] where authors have proposed a consensus protocol that can be used in IoT systems that uses the reputation (behavior) of the nodes within the blockchain network.

In Table V, a comparison of presented trust based consensus mechanisms against Proof of Work is presented regarding four metrics especially the energy consumption, the scalability, the throughput and the resilience against attacks.

Discussion

As seen in the previous paragraph, for trust/reputation based consensus alternatives, entities with a good conduct resulting in a high trust value have a greater chance of being chosen to agree on the global state of the ledger. However entities that depict malicious behavior are detected, punished and their trust/reputation values are reduced consequently. For this reason, entities have an incentive to positively participate in the consensus mechanism for a long time in order to increase their trust value as the incentive in this class of alternatives is non transferable.

Moreover, according to the carried study, we found that a large number of proposed alternatives have been designed especially for private and permissioned protocols such as BFT based blockchains and PoR. These alternatives are more energy efficient, resist more against a larger number of attacks, support higher scalability and manage a greater number of transactions than the underlaying protocols.

Regarding public and permissionless protocols and according to the study made, PoXR [92], proposed for blockchain enabled IoT systems, combines the distributed reputation system with PoX (Proof of X) consensus protocols such as PoW and PoS. Entities having acceptable behavior history are chosen to participate in the mining process based on their accumulated reputation scores. The reputation module applied to the Proof of Stake consensus enables entities having a good reputation score in addition to their moderate stake to have a better chance for being selected for the block publication process. Besides, this alternative enhances the PoX corresponding protocol related efficiency and improves their security aspect and attacks resilience.

IV. Conclusion

In this survey, we pointed out the importance of trust management in IoT and IIoT and we identified raised issues and challenges of trust management systems. In order to conduct holistic IoT distributed trust management based on the blockchain technology, we introduced a review of blockchain based trust management approaches in IoT and IIoT systems. The investigated mechanisms are classified into four categories namely blockchain based trust frameworks, blockchain enhanced trust interaction, blockchain based trust data management and blockchain transactions validation based on trust degree. In a next step, we surveyed the existing blockchain based trust management schemes developed for both IoT and IIoT systems. An outline of the main contributions and limitations of presented schemes is as well presented. Afterwards an analysis of investigated mechanisms regarding their application scenario, the adopted methodology, the blockchain type, the considered performance metrics, as well as their strengths and weaknesses is provided. Finally, we identified gaps in IoT Trust computation research and suggested future research areas.

Submitted manuscript

Work	Description	Energy consumption	Scalability	Throughput	Attacks resilience	Advantages	Limitations
PoR [91]	Distributed ledger of reputation for permissioned blockchains	Low	High	51 tps as average for different network sizes	Bad mouthing attack Replay attack On Off attack Sybil attack	Reputation incentives for block creation Malicious nodes could not compromise the consensus as they must gather reputation incentives which is not possible	Designed only for permissioned blockchain systems
PoXR [92]	A repute model built on the existing PoX consensus protocols such as PoW or PoS for IoT systems	depending on PoX	depending on PoX	depending on PoX	51% attack of PoW Sybil attack	Improves the security of the underlying protocols through the integration of reputation incentive Users with lower computing power can easily participate in the mining process	Inherits the limitations of the underlying protocols
TX-BFT [93]	A trust evaluation system built on the X-BFT consensus protocols in IoT domains.	Low	depending on X-BFT		takeover parliament attacks.	Improves the trust level of blockchain enabled collaborated learning IoT systems Defends malicious users and data within the parliamentary and leader election	Inherits the limitations of the underlying protocols
T-PBFT [94]	A multi-stage consensus algorithm based on the EigenTrust model with the PBFT consensus protocol.	Low	Moderate	Increased	Not considered	Construct a more trustworthy consensus group based on EigenTrust model to improve the efficiency and scalability of PBFT	Inherits the limitations of the underlying protocols

TABLE V
COMPARISON OF TRUST BASED CONSENSUS MECHANISMS BENCHMARKED AGAINST PROOF OF WORK

Submitted manuscript

APPENDIX A
TRUST MANAGEMENT SYSTEMS IN IOT AND IIOT

In the current literature, various trust definitions have been proposed. these last range from specific scenarios to wide and general systems. Meanwhile, the trust meaning across existing proposals differs from one work to another insofar that each one of them has considered trust from different perspectives. In this section we will give a generic definition for trust in the context of IoT. Then, we will describe trust properties, the operations considered within the trust management process, and therefore we will review how proposed works have dealt with the concept of trust management within each operational block in IoT systems.

In the context of IoT, trust could be defined as a relationship established between two entities: a trustor and a trustee, where the trustor is the evaluating entity while the trustee is the evaluated one. The trustor when needing to collaborate with the trustee, to use the services or the information it provides, when it receives outcomes through the established communication while coming in touch to it, will evaluate its competence to act just as predicted for a specific period and within a specified context. Thus this relationship is always related to a time value which corresponds to the trust evaluation time, a context where the relationship resides in, and a parameter on which the evaluation depends.

In this appendice, we present more details about the notion of trust, and we will review how proposed works have dealt with this last during the trust composition process in IoT systems and exceptionally in smart industries.

A. Trust properties

Due to the different requirements of IoT applications and regarding the nature of the harsh industrial environment, the concept of trust can be viewed in a different way and accordingly its evaluation can depend on several properties and characteristics. In this section, we will define the main trust properties as illustrated in Fig. 6.

a) Trust is unidirectional: When evaluating the trustworthiness of a specific entity, the trustor generally rely on the evidence it has about the trustee. This evidence may be acquired either through its direct observations, either through the policies it specifies, either from the recommendations it receives from the neighboring nodes,

Fig. 6. Trust properties

or other means.
Obviously, the trustee may not necessarily know the trustor or has established previous interaction with him and therefore it may not trust him. Even in the case where previous interactions have been existed between the two entities, the disposition of the trustee, its willingness to trust, its perception on the trustor's performance and benevolence may differ.
Hence trust may not be mutual or reciprocal . This property could be formalized as follow:

$$\exists(e_i, e_j) : trust(e_i \longmapsto e_j)_t^c \neq trust(e_j \longmapsto e_i)_t^c$$

b) Trust may not be transitive: [**?**], [**?**] If the trustor e_i needs to evaluate the trustworthiness of e_j to collaborate with for the first time, e_k which e_i trusts, comes and recommends e_j, in this case should e_i consider the received recommendation and trust e_j?
The answer may be yes and no. This fact is so large to be as simple as this. In fact many other factors come into play to determine whether trust could be transitive or not such as the context in which the trustor e_i trusts the recommender e_k, the community to which each entity belongs and the relationships that exists between them.
This property could be formalized as follow:

$$trust(e_i \longmapsto e_k)_t^c \wedge trust(e_k \longmapsto e_j)_t^c \not\Longrightarrow trust(e_i \longmapsto e_j)_t^c$$

c) Trust is dynamic: Present entities in IoT environments are generally resource constrained and mobile in nature and due to these two characteristics, the network topology changes at every instant and consequently data in transmit will be typically incomplete and can change rapidly. To accommodate the different changes related to the environment in question, various approaches were considered in the literature.
Some have considered event driven scheme [**?**], [**?**], [**?**], where trust is updated after a communication or an event is made between two entities or after ratings and feedbacks are sent to the evaluating entity.
Others have considered time-driven scheme [**?**], [**?**], [**?**], as trust evidence is collected periodically, trust needs to be updated at each period, past evidence can be considered also while updating trust either by applying aggregation techniques or by using exponential time decay function.

d) Trust is social based: The exploitation and the integration of social concepts within IoT environments has introduced SIoT, the Social Internet of Things paradigm [**?**], [**?**]. This last is mainly related to the fact that objects within IoT environments are able to establish social relationships in an autonomous way with regard to their owners. The evaluation and the computation of trust therefore will depend not only on the trustee's competence and capability to perform the requested task, but also on its commitment and on the type of the relationship towards the trustor.

e) Trust is subjective: The evaluation of trustworthiness depends not only on the behavior of the trustee, its performance, reputation or technical properties but also on how this evidence is perceived and interpreted by the evaluating entity. Hence trust can be influenced by the subjective properties of both the evaluating and the evaluated entities [**?**] such as the evaluated entity's honesty, benevolence, goodness and on the other side, the evaluating's confidence, expectation, belief and willingness to trust, etc.

B. Trust operational blocks

The design, the implementation and the development of a trust management model generally goes through a succession of operations that are considered essential for trust computation in dynamic networks [**?**].
In Fig.7 we present the possible trust operational blocks that need to be implemented within a trust framework for IoT. These phases include: (i) the computation of a trust value based on a specific parameters, considering some metrics and using certain factors, (ii) the computed values are propagated over the network in order to establish trust between entities having neither prior knowledge nor previous interaction, (iii) As trust values are sent by several evaluating entities and since they are propagated through multiple paths, they need to get aggregated into one single value which will be used in a later trust compositions, (iv) Whenever a change occurs due to the network dynamicity, trust could be predicted potentially using the present and past trust values, (v) The trust values will be applied into the network in order to achieve the desired purposes.

Submitted manuscript

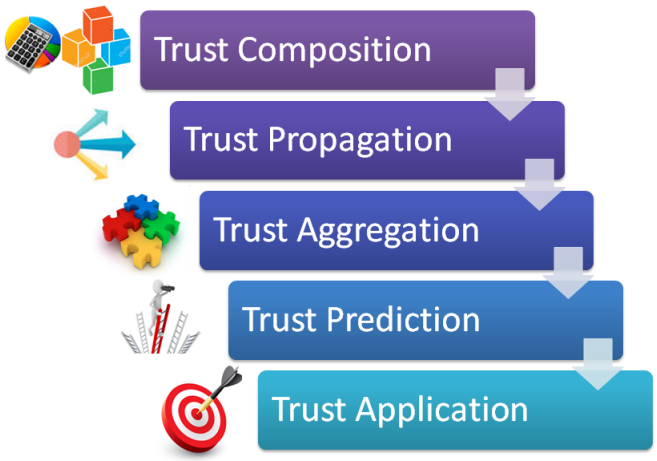


Fig. 7. Trust operational blocks

These five phases the trust composition process is made up of are detailed in the following paragraphs.

a) Trust Composition: Before producing a trust score and judging an entity either trustworthy or not, the trust management system should collect enough information about a specific entity in order to define its trust score regarding its behavior as it will be considered by other network entities.
The questions to be asked here:

- What approaches to use to determine trust?
- Which kind of aspects to consider?
- How to compute the gathered information and to provide a final trust value?

The process to be realized within this block is illustrated in Fig 8

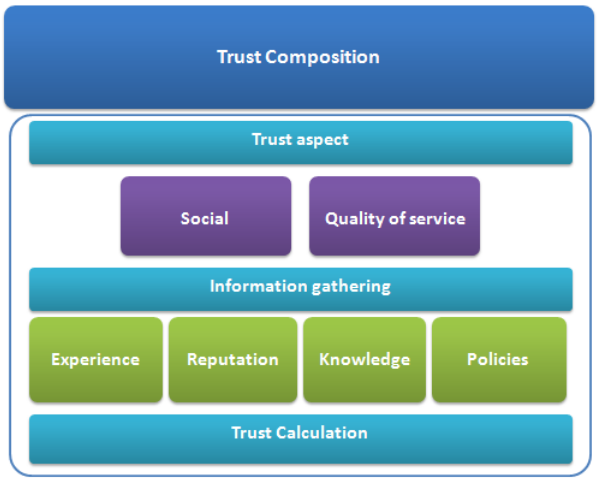


Fig. 8. Trust composition process

As seen, the first step within trust composition is to determine and to specify which kind of aspect the information gathering will focus on. Here we can distinguish between social trust and technical trust (or QoS trust) [?]. Social trust derives from established social relationships among IoT entities while quality of service trust is determined by the belief on entities ability to guarantee a certain quality of service in response to a service request. When reviewing the current literature, we can interpret that almost all trust management systems have considered both technical (QoS) and social trust as an aspect on which the information gathering focuses for the trust evaluation phase. This fact is mainly related to the introduction of the social Internet of Things [?], [?] according to which participating entities are capable of setting up social relationships that are generally affected by those existing between their corresponding owners. Among social properties, friendship [38], [?], [?] and community of interest [35], [36], [37], [38], are the most used ones for the evaluation of social trust. This refers to the fact that having a good friendship, sharing a common interest or belonging to the same community implies a good confidence on the provided service and the established communication. For the technical trust, we have seen that this last considers several parameters such as the energy consumption level [?], [?] and the device related capability [?], [?], [?], [?] in order to address respectively the energy efficiency and the resource constraints challenges present in almost IoT based environments.
As a next step and once the aspect is determined, the information gathering process can be launched. This last may be based on several approaches such as experience, reputation, knowledge and policies which represents the trust parameters [?], [?], [?]. The experience parameter corresponds to each node's interpretation of the previous interactions and events established with its immediate neighbors at a specific period of time. These evaluations will be kept within each node and updated at regular periods and regarding regular events. Moreover, they will be propagated as trust recommendation part to other network nodes. Subsequently, the past gathered trust information will be regularly kept and considered after as the knowledge part of trust. Another approach to evaluate trust is to use well-defined languages and semantics as policies to make trust decisions. For the information gathering process, we have seen that some works in the current literature have considered the context while assessing the trustworthiness degree of each entity within the network [?], [?], [?]. The context awareness is an important feature that should be considered while designing a trust management system insofar that some nodes could act honestly in such a context and maliciously in other one.
Finally a last step within the trust composition process is the trust calculation where a trust value will be computed and modeled according to a specific method such as probability, mean, difference, etc.

b) Trust Propagation: In Fig. 9, we illustrate the functional sub-blocks corresponding to the trust propagation process. In fact, once trust is composed regarding a specific entity, the trust value will be propagated to the network entities what would effectively optimize the resource utilization as entities will spend no more resources to recompute trust.
The main questions here are:

Submitted manuscript

- How to propagate trust values?
- Shall an entity propagate trust autonomously and periodically to other entities within its neighborhood?
- Shall it wait until it receives a request from another entity to propagate trust?
- Or shall it send it to a centralized entity for further processing and storage?

Generally, there are three schemes of trust propagation namely centralized, distributed, and decentralized. where in the distributed scheme, each entity will record locally the trust information and provide it either on request from relying nodes or communicate it autonomously to other entities it interacts and collaborates with. On the other hand, in the centralized scheme, a third party (i.e. a centralized server, a cloud platform, a virtual service, etc.), came into play to propagate the trust information over the network in order to make it publicly available. As it is seen here, the process of trust propagation could be launched either on demand from the relying entities or autonomously, freely and independently by the evaluating ones.

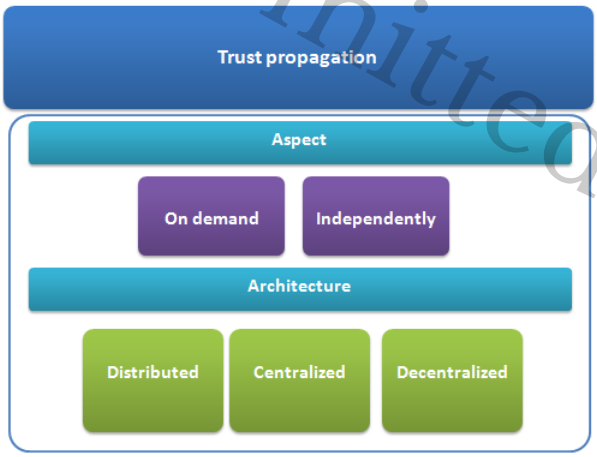


Fig. 9. Trust propagation process

After reviewing the existing works, we have seen that existing proposals mostly consider the distributed scheme for trust scores propagation [35], [36], [37], [38]. These last are sent either upon demand to nodes requesting their use or autonomously and independently to serve within the trustworthiness evaluation process of target nodes. The consideration of such a scheme seems to be the most convenient to the inherent requirements of IoT systems where devices scattered over a wide area could have always access to a centralized system to send and get trust information regarding nodes to be assessed. Moreover no work far discusses how to ensure the integrity, the validity and the authenticity of the transmitted data during the propagation phase. Instead, existing works assume that collecting information from a large number of entities and executing aggregation operations on the exchanged trust related information will result in a relatively accurate assessment.

c) Trust Aggregation: Generally speaking, when trust values regarding a specific entity are requested, different evaluating entities will send their assessed values which will be obviously propagated through multiple paths within the network, thus different trust values will be received and multiple versions of each value will be created as well. For this reason an aggregation technique is needed to combine the received value into a final one.
The main question to be asked here is:

- Which technique to use for trust aggregation?

In the current literature, many aggregation techniques have been presented. According to [**?**], these last include belief theory, weighted sum, fuzzy logic, regression analysis and Bayesian inference.

d) Trust Prediction: Whenever a change occurs due to the network high dynamicity, trust could be predicted potentially using the entities' present and past trust values. Moreover, when two entities lose contact and there is no edge between them, it will be so important to be able to estimate the trust relationship nature to be established before it took place in the reality.
The main questions to be raised here are:

- Which approach to consider for the trust prediction?
- How to guarantee the accuracy of trust prediction?
- How to trust the prediction in itself and take actions based on it?

Various approaches have been considered in the literature, some of them used the kalman-filter approach to predict the trust system future state [**?**], [**?**], others have focused on the unsupervised methods to predict trust [**?**], while several ones have used the principles of machine learning [**?**] and data mining [**?**] as a basis for creating a prediction enabled trust model.

e) Trust Application: Applications of trust management are enormous in mobile networks and particularly in IoT environments where trust management systems are often designed to handle effectively many security services as illustrated in Fig 10. These services include : intrusion detection, key Management, secure routing, malicious nodes detection, quality of information assessment, access control management etc.

Fig. 10. Trust design purposes and applications

Appendix B

Appendix two text goes here.

Submitted manuscript

Acknowledgment

References

[1] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516.

[2] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[3] Lu, Yang. Industry 4.0: a survey on technologies, applications and open research issues. Journal of Industrial Information Integration 6 (2017): 1-10.

[4] D. Georgakopoulos , P.P. Jayaraman , M. Fazia , M. Villari , R. Ranjan ,Internet of things and edge cloud computing roadmap for manufacturing, IEEE Cloud Comput. 3 (4) (2016) 66–73

[5] Zhou, Keliang, Taigang Liu, and Lifeng Zhou. Industry 4.0: Towards future industrial opportunities and challenges. Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on. IEEE, 2015.

[6] Wang, Shiyong, et al. Implementing smart factory of industrie 4.0: an outlook. International Journal of Distributed Sensor Networks 12.1 (2016): 3159805.

[7] Kumar, Rajesh, and Rewa Sharma. "Leveraging blockchain for ensuring trust in IoT: A survey." Journal of King Saud University-Computer and Information Sciences (2021).

[8] Bellini, Emanuele, Youssef Iraqi, and Ernesto Damiani. "Blockchain-based distributed trust and reputation management systems: A survey." IEEE Access 8 (2020): 21127-21151.

[9] Sharma, Avani, et al. "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes." Computer Communications 160 (2020): 475-493.

[10] Peter Friess. Digitising the industry-internet of things connecting the physical, digital and virtual worlds. River Publishers, 2016.

[11] Rafiullah Khan et al. "Future internet: the internet of things architecture, possible applications and key challenges". In: 2012 10th international conference on frontiers of information technology. IEEE. 2012, pp. 257–260.

[12] Miao Wu et al. "Research on the architecture of Internet of Things". In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Vol. 5. IEEE. 2010, pp. V5–484.

[13] John A Stankovic. "Research directions for the internet of things". In: IEEE Inter- net of Things Journal 1.1 (2014), pp. 3–9.

[14] Daniele Miorandi et al. "Internet of things: Vision, applications and research challenges". In: Ad hoc networks 10.7 (2012), pp. 1497–1516.

[15] Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in internet of things: Challenges, solutions and future directions. In System Sciences (HICSS), 2016 49th Hawaii International Conference on (pp. 5772-5781). IEEE.

[16] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[17] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.

[18] E. Mykletun, J. Girao, D. Westhoff, Public key based cryptoschemes for data concealment in wireless sensor networks, in: Proceedings of IEEE ICC, Istanbul, Turkey, 2006, pp. 2288–2295.

[19] Yao, X., Chen, Z., & Tian, Y. (2015). A lightweight attribute-based encryption scheme for the Internet of Things. Future Generation Computer Systems, 49, 104-112.

[20] J.-Y. Lee, W.-C. Lin, Y.-H.Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next-Generation Electronics, ISNE 2014, Kwei-Shan, 2014, pp. 1–2.

[21] Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (iacac) for the internet of things. Journal of Cyber Security and Mobility, 1(4), 309-348.

[22] Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the internet of things. Mathematical and Computer Modelling, 58(5), 1189-1205.

[23] Luigi Atzori, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey". In: Computer networks 54.15 (2010), pp. 2787–2805.

[24] Li, Xiaomin, et al. "A review of industrial wireless networks in the context of industry 4.0." Wireless networks 23.1 (2017): 23-41.

[25] Xu, Hansong, et al. "A survey on industrial Internet of Things: A cyber-physical systems perspective." IEEE Access 6 (2018): 78238-78259.

[26] Anitha Varghese and Deepaknath Tandur. "Wireless requirements and challenges in Industry 4.0". In: 2014 International Conference on Contemporary Computing and Informatics (IC3I). IEEE. 2014, pp. 634–638.

[27] Shehzad A Ashraf et al. "Ultra-reliable and low-latency communication for wire- less factory automation: From LTE to 5G". In: 2016 IEEE 21st International Con- ference on Emerging Technologies and Factory Automation (ETFA). IEEE. 2016, pp. 1– 8.

[28] Yang Lu. "Industry 4.0: A survey on technologies, applications and open re- search issues". In: Journal of industrial information integration 6 (2017), pp. 1–10.

[29] Foukalas, Fotis, et al. "Dependable wireless industrial iot networks: Recent advances and open challenges." 2019 IEEE European Test Symposium (ETS). IEEE, 2019.

[30] Sharma, Avani, et al. "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes." Computer Communications (2020).

[31] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A survey on trust management for Internet of Things." Journal of network and computer applications 42 (2014): 120-134.

[32] Xu, Hansong, et al. "A survey on industrial Internet of Things: A cyber-physical systems perspective." IEEE Access 6 (2018): 78238-78259.

[33] Khan, Wazir Zada, et al. "Industrial internet of things: Recent advances, enabling technologies and open challenges." Computers Electrical Engineering 81 (2020): 106522.

[34]

[35] F. Bao, & I. R. Chen, Trust Management for the Internet of Things and Its Application to Service Composition. in IEEE WoWMoM 2012 Workshop on the Internet of Things: Smart Objects and Services, San Francisco, CA, USA, June 2012.

[36] Bao, F., & Chen, I. R. (2012, September). Dynamic trust management for Internet of things applications. In Proceedings of the 2012 international workshop on Self-aware Internet of things (pp. 1-6). ACM.

[37] Bao, F., Chen, R., & Guo, J. (2013, March). Scalable, adaptive and survivable trust management for community of interest based internet of things systems. In Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on (pp. 1-7). IEEE.

[38] Chen, R., Guo, J., & Bao, F. (2016). Trust management for soa-based iot and its application to service composition. IEEE Transactions on Services Computing, 9(3), 482-495.

[39] Chen, Ray, Fenye Bao, and Jia Guo. "Trust-based service management for social internet of things systems." IEEE transactions on dependable and secure computing 13.6 (2015): 684-696.

[40] Chen, Ray, Jia Guo, and Fenye Bao. "Trust management for service composition in SOA-based IoT systems." 2014 IEEE wireless communications and networking conference (WCNC). IEEE, 2014.

[41] Guleng, Siri, et al. "Decentralized trust evaluation in vehicular Internet of Things." IEEE Access 7 (2019): 15980-15988.

[42] Fang, Weidong, et al. "FETMS: Fast and efficient trust management scheme for information-centric networking in Internet of Things." IEEE Access 7 (2019): 13476-13485.

[43] Alshehri, Mohammad Dahman, et al. "A Distributed Trust Management Model for the Internet of Things (DTM-IoT)." Recent Trends and Advances in Wireless and IoT-enabled Networks. Springer, Cham, 2019. 1-9.

[44] Altaf, Ayesha, et al. "Context-oriented trust computation model for industrial Internet of Things." Computers Electrical Engineering 92 (2021): 107123.

Original Manuscript

[45] Boudagdigue, Chaimaa, et al. "Trust management in industrial internet of things." IEEE Transactions on Information Forensics and Security 15 (2020): 3667-3682.
[46] El Sayed, Ammar Ibrahim, Mahmoud Abdel Aziz, and Mohamed Hassan Abdel Azeem. "Blockchain Decentralized IoT Trust Management." 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT). IEEE, 2020.
[47] Di Pietro, Roberto, et al. "A blockchain-based trust system for the internet of things." Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies. 2018.
[48] Lahbib, Asma, et al. "Blockchain based trust management mechanism for IoT." 2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019.
[49] Shi, Peichang, et al. "Blockchain-based trusted data sharing among trusted stakeholders in IoT." Software: practice and experience 51.10 (2021): 2051-2064.
[50] Al-Rakhami, Mabrook S., and Majed Al-Mashari. "A blockchain-based trust model for the internet of things supply chain management." Sensors 21.5 (2021): 1759.
[51] Frahat, Rzan Tarig, Muhammed Mostafa Monowar, and Seyed M. Buhari. "Secure and scalable trust management model for IoT P2P network." 2019 2nd International Conference on Computer Applications Information Security (ICCAIS). IEEE, 2019.
[52] Kouicem, D. E., Imine, Y., Bouabdallah, A., Lakhlef, H. (2020). A Decentralized Blockchain-Based Trust Management Protocol for the Internet of Things. IEEE Transactions on Dependable and Secure Computing.
[53] Putra, Guntur Dharma, et al. "Trust management in decentralized iot access control system." 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.
[54] Abou-Nassar, Eman M., et al. "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems." IEEE Access 8 (2020): 111223-111238.
[55] Fortino, Giancarlo, et al. "Using blockchain in a reputation-based model for grouping agents in the Internet of Things." IEEE Transactions on Engineering Management 67.4 (2019): 1231-1243.
[56] Seshadri, Sreenivas Sudarshan, et al. "Iotcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems." IEEE Internet of Things Journal (2020).
[57] Putra, Guntur Dharma, et al. "Trust-based Blockchain Authorization for IoT." IEEE Transactions on Network and Service Management (2021).
[58] Hammi, Mohamed Tahar, et al. "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT." Computers Security 78 (2018): 126-142.
[59] Putra, Guntur Dharma, et al. "Trust management in decentralized iot access control system." 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.
[60] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, L. Xie, A decentralized solution for iot data trusted exchange based on blockchain, in: 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, IEEE, 2017, pp. 1180–1184.
[61] Makhdoom, Imran, et al. "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities." Computers Security 88 (2020): 101653.
[62] Liu, Chi Harold, Qiuxia Lin, and Shilin Wen. "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning." IEEE Transactions on Industrial Informatics 15.6 (2018): 3516-3526.
[63] Chen, Jianing, et al. "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation." IEEE Transactions on Industry Applications 56.4 (2019): 4478-4488.
[64] Khalid, Umair, et al. "A decentralized lightweight blockchain-based authentication mechanism for IoT systems." Cluster Computing 23.3 (2020): 2067-2087.
[65] Tang, Bo, et al. "Iot passport: A blockchain-based trust framework for collaborative internet-of-things." Proceedings of the 24th ACM symposium on access control models and technologies. 2019.
[66] Wu, Xu, and Junbin Liang. "A blockchain-based trust management method for Internet of Things." Pervasive and Mobile Computing 72 (2021): 101330.
[67] Tariq, Noshina, et al. "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in internet of things." Sensors 21.1 (2021): 23.
[68] Esposito, Christian, et al. "Robust decentralised trust management for the internet of things by using game theory." Information Processing Management 57.6 (2020): 102308.
[69] Zhaofeng, Ma, et al. "Blockchain-enabled decentralized trust management and secure usage control of IoT big data." IEEE Internet of Things Journal 7.5 (2019): 4000-4015.
[70] Liang, Xueping, et al. "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability." 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). IEEE, 2017.
[71] Rouhani, Sara, and Ralph Deters. "Data Trust Framework Using Blockchain Technology and Adaptive Transaction Validation." IEEE Access 9 (2021): 90379-90391.
[72] Pahl, Claus, et al. "An architecture pattern for trusted orchestration in IoT edge clouds." 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 2018.
[73] Caro, Miguel Pincheira, et al. "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation." 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany). IEEE, 2018.
[74] Javaid, Uzair, Muhammad Naveed Aman, and Biplab Sikdar. "Blockpro: Blockchain based data provenance and integrity for secure iot environments." Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. 2018.
[75] Al-Rakhami, Mabrook S., and Majed Al-Mashari. "ProChain: Provenance-Aware Traceability Framework for IoT-Based Supply Chain Systems." IEEE Access 10 (2021): 3631-3642.
[76] Ayoade, Gbadebo, et al. "Decentralized IoT data management using blockchain and trusted execution environment." 2018 IEEE International Conference on Information Reuse and Integration (IRI). IEEE, 2018.
[77] Lahbib, Asma, et al. "DRMF: a Distributed Resource Management Framework for industry 4.0 environments." 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA). IEEE, 2019.
[78] Malik, Sidra, et al. "Trustchain: Trust management in blockchain and iot supported supply chains." 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019.
[79] Liu, Dongxiao, et al. "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain." IEEE Transactions on Industrial Informatics 15.6 (2019): 3527-3537.
[80] Boudagdigue, Chaimaa, et al. "Trust management in industrial internet of things." IEEE Transactions on Information Forensics and Security 15 (2020): 3667-3682.
[81] Konstantinos Christidis and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things". In: Ieee Access 4 (2016), pp. 2292–2303.
[82] Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin. "Blockchain for the Internet of Things: A systematic literature review." 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). IEEE, 2016.
[83] Crosby, Michael, et al. "Blockchain technology: Beyond bitcoin." Applied Innovation 2.6-10 (2016): 71.
[84] Ali, Muhammad Salek, et al. "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys Tutorials 21.2 (2018): 1676-1717.
[85] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14.4 (2018): 352-375.
[86] Baliga, Arati. "Understanding blockchain consensus models." Persistent 4 (2017): 1-14.
[87] Lua, Eng Keong, et al. "A survey and comparison of peer-to-peer overlay network schemes." IEEE Communications Surveys Tutorials 7.2 (2005): 72-93.
[88] Licheng Wang et al. "Cryptographic primitives in blockchains". In: Journal of Network and Computer Applications 127 (2019), pp. 43–58
[89] Feng, Qi, et al. "A survey on privacy protection in blockchain system." Journal of Network and Computer Applications 126 (2019): 45-58.
[90] Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Privacy preservation in blockchain based IoT systems:

Submitted manuscript

Integration issues, prospects, challenges, and future research directions." Future Generation Computer Systems 97 (2019): 512-529.
[91] Gai, Fangyu, et al. "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network." International Conference on Database Systems for Advanced Applications. Springer, Cham, 2018.
[92] Wang, Eric Ke, et al. "Proof of X-repute blockchain consensus protocol for IoT systems." Computers Security 95 (2020): 101871.
[93] Wang, Ke, et al. "A trusted consensus fusion scheme for decentralized collaborated learning in massive IoT domain." Information Fusion 72 (2021): 100-109.
[94] Gao, Sheng, et al. "T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm." China Communications 16.12 (2019): 111-123.
[95] Feng, Jingyu, et al. "PoTN: a novel blockchain consensus protocol with proof-of-trust negotiation in distributed IoT networks." Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things. 2019.
[96] Yuan, Xu, et al. "Efficient Byzantine Consensus Mechanism Based on Reputation in IoT Blockchain." Wireless Communications and Mobile Computing 2021 (2021).

Submitted manuscript