2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress

Blockchain-based Trust Management in Social Internet of Things

Mohammad Amiri-Zarandi
School of Computer Science
University of Guelph
Guelph, ON, Canada
mamiriza@uoguelph.ca

Rozita A. Dara
School of Computer Science
University of Guelph
Guelph, ON, Canada
drozita@uoguelph.ca

***Abstract*—Social Internet of Things (social IoT) is a paradigm that integrates the social network concepts with IoT in which objects in the network are able to establish social relationships with each other. In these networks, to preserve privacy and security, the access to IoT resources can be handled based on social trust evaluation of the devices. This paper examines a blockchain-based trust management system for edge-enhanced IoT that uses social information of the system to strengthen the trust evaluation. Moreover, this system leverages information entropy to enhance security. We also developed a proof of concept system to show that the proposed solution can effectively assess trust factors in social IoT.**

Keywords—Social IoT; Trust, Security; Privacy; Blockchain; Smart Contract; Entropy

I. INTRODUCTION

In the Internet of Things (IoT), numerous devices are connected to perform tasks and services in different applications such as smart homes, wearables, smart cities, and healthcare. We are experiencing the exponential growth of IoT devices in almost every industry. These devices include but are not limited to sensors, cameras, smart devices, and Radio-frequency identification (RFID) tags, which aim to exchange data without human intervention. Although providing a seamless and remote connection among devices is an excellent feature for IoT, it also raises some concerns regarding security and privacy.

Being ubiquitous, these systems are attractive targets for attackers to access IoT resources maliciously. These devices are also numerous and have complex interactions. These factors add challenges in utilizing traditional data and system access management practices. Trust management systems have been proposed as a mechanism to automatically assess the access requests in the system and handle the permissions based on the trust between IoT nodes [1]. Trust management helps IoT devices to overcome perceptions of uncertainty and risk and prevent adversaries from accessing the services and applications in the network.

Using social features of connected devices is a potentially effective approach to manage trust in IoT systems. A social IoT [2] can be regarded as a combination of an IoT network and a social network in which IoT devices can be assumed socially connected based on the relations among their owners. With this concept in mind, IoT devices can be defined as a group of things that establish social relationships with each other. Using this concept, in addition to the previous experience in the system, the social relations among the IoT devices can be another valuable source of information to evaluate the trustworthiness of devices.

One of the state-of-the-art technologies that can be used for trust management in IoT is blockchain [3][4]. Blockchain is a distributed database that leverages a decentralized approach to record all changes by transactions [5]. It was originally used for financial applications. But, using smart contracts as a medium to generate and run computer programs on the blockchain infrastructure, these solutions gained more attractions in IoT applications due to their strong security, reliability, and transparency [6]. Since blockchain is decentralized by nature, it is aligned with the distributed structure of IoT and can be used as an alternative solution to cloud services.

Blockchain can overcome many of the drawbacks of using cloud-based solutions for trust management systems [7]. The centralized cloud-based approaches suffer from single point vulnerability in the system. Cloud servers are the host for trust management, identification, and authentication as well as computation, and storage. These servers are tempting targets for adversaries, and in the case of penetration, the entire network can be disrupted. Furthermore, centralized cloud-based systems are vulnerable to manipulation. The companies that own these servers can censor, change, remove, or misuse data. They also can manipulate the output of applications.

In blockchain solutions, there is no central point of failure in the system. Besides, the identity management system in blockchain leverages strong cryptography that guarantees a high level of security and privacy for transactions. Furthermore, smart contracts can automatically run distributed workflows. Using blockchain, the trust management system is able to store the trust data transparently. These data will be immutable, and the adversaries cannot manipulate this data. Moreover, the traceability of the transactions in the blockchain allows us to trace back the adversaries in the system and set limitations for these nodes.

Blockchain technology can enable the IoT nodes to work together and maintain a consistent dataset regarding the misbehaviours in the network and evaluate the trust level for the different elements in the network [4]. Increasing the use of edge/fog computing in IoT has provided new opportunities to utilize blockchain in IoT [8][9]. The edge/fog nodes have more storage and computation resources than sensors and can effectively participate in mining blocks in the blockchain. They also can perform a part of computation at the edge of a network to decrease the data and processing load in the blockchain.

In this paper, we propose a blockchain-based trust management system for social IoT, which not only allows different IoT devices to participate in the trust evaluation of

978-1-7281-6609-4/20/$31.00 ©2020 IEEE
DOI 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00024

other nodes, but also stores and evaluates trust values in a consistent, reliable, and secure format. This system evaluates the trust level for IoT nodes based on the reputation and social relations of the objects. It also leverages information entropy to strengthen the system against several security attacks. The results show that this approach is an effective approach to reach this goal. To the best of our knowledge, this study is the first attempt to use the social relations of IoT devices along with blockchain technology for trust management in IoT. The remainder of this paper is organized as follows: In Section 2, we will review the related works. The problem definition will be introduced in Section 3. In Section 4, the proposed method will be illustrated. In Section 5 we will analyze the privacy and security of the system. We will demonstrate the results and discussion in Section 6, and Section 7 concludes the paper.

II. Related Work

Trust management in social IoT has been studied and implemented in several technology solutions. Nitti et al. [10], for instance, presented social trustworthiness management from two different perspectives: subjective and objective. The subjective approach uses each nodes' experience and the information from its friends to evaluate the trust factor of other objects. In contrast, in the objective approach, the information from nodes will be distributed in the network, and using that, a value will be evaluated for each node as the trust factor. Chen et al. [11] proposed a trust evaluation mechanism for service management of social IoT. The presented model is adaptive and works based on dynamic relationships among the owners of IoT devices. Another trust evaluation mechanism is designed in [12] that uses the reputation, knowledge, and experience of IoT objects to calculate the trust measure for devices. This trust evaluation method is produced to provide trust evaluation as a service.

Although blockchain technology has not been used in social IoT yet, it has been utilized to address some challenges in other domains of IoT. In [13], the authors justified the necessity to shift toward a decentralized architecture for IoT to be more sustainable. Current centralized models jeopardize the privacy and security of IoT. The authors made the case that the security concerns will be decreased considerably by using blockchain as a scalable and transparent architecture. Kshetri [7] described different ways that blockchain can strengthen security and access control in IoT. In another study, lightweight instantiation of blockchain was proposed to boost the computational capabilities of IoT devices [8]. The proposed method utilizes centrally managed private information to increase the performance of the network. Dwivedi et al. [14] proposed another blockchain platform optimized for IoT-based healthcare. Fortino et al. [15] used blockchain to design a reputation-based model in multi-agent systems, and Hammi et al. [16] introduced a blockchain-based authentication for IoT. Despite all the attempts to use blockchain in IoT, none of these studies have leveraged the social features of IoT. The objective of our work is to use blockchain technology for trust management in social IoT.

III. Problem Definition

A. System Model

In our system, the fog-enhanced IoT system mainly includes these elements:

IoT Devices: A set of devices that are deployed in a system in which each device can collect data and communicate with other devices. In our model, we consider that these devices will interact with other devices to transfer data or serve defined services. The IoT devices are connected to the fog nodes send access requests through them.

Fog Nodes: these nodes are deployed at the edge of the IoT network to handle communication tasks. They are able to perform local processes to decrease the needed bandwidth. Besides, in our model, these nodes are responsible for running the feedback module which is responsible for access assessment for IoT devices. After each access, the feedback module assigns an evaluation value to the access, which will be used for the trust evaluation of the device in the future. The details of the feedback module operation are out of the scope of this study.

Trustor: An IoT device that has been requested to get access.

Trustee: An IoT device that requests access to another device.

We assume that due to misbehavior or malfunctions, the devices in the system are not necessarily trustable. The proposed trust management system will assess the trustworthiness between each pair of trustor/trustee based on their previous behavior as well as their social connections. Trust value is a tuple of different values, and each device can have independent thresholds for each of these metrics to approve a request.

B. Adversary Model:

In Fog-enhanced IoT systems, both IoT devices and fog nodes are vulnerable to attacks. In this study, we do not consider the attacks on the fog nodes and will be focused on the attacks that target IoT devices and assume that adversaries are motivated to make these types of attacks:

Bad-Mouthing Attack: Malicious nodes may send unfair evaluations regarding some nodes in the system to ruin their trust level in the network [17].

Ballot Stuffing Attack: Attackers may also aim to improve the reputation of other malicious nodes by sending fake positive feedback [11].

Denial of Service (DoS) Attack: In this type of attack, the adversaries can send plenty of fake requests to the system in order to disturb the normal operation of the system [18].

Storage Attack: In this type of attack, an adversary node tries to access the stored feedback data to change, delete, or add fake ones [14].

The proposed design will protect the system against these attacks. We will explain how the system will be protected in Section 5.

C. Design Goals:

This paper focuses on trust management of IoT, based on the previous behavior feedback as well as social connections among the devices. The objective here is to store and evaluate this information without a central decision unit. Therefore, the proposed trust management system must achieve these goals:

Decentralization: In cloud-based trust management systems, the central trust assessment is a high-risk point of failure in the system. Furthermore, having control over data

and procedure, the service providers are prone to misuse or manipulation of data or other resources in the system. The new trend in the IoT domain is to avoid these kinds of centrality and use distributed solutions [19].

Security and Privacy: It is essential to store and transfer information regarding the nodes in the system securely. Besides, real identity should remain protected, and data encryption is necessary to prevent sensitive data leakage.

Transparency: The trust information should be transparent to all nodes in the system in a way that authorized nodes in the system are able to access the data that they need.

Availability: Trust values should be available for IoT devices and fog nodes when they want to know the trustworthiness of any other device in the system.

IV. Proposed Solution

Fog-enhanced IoT is an architecture that leverages fog nodes at the edge of the IoT network. These nodes can perform some tasks to decrease the computation load on the IoT devices and also reduce the amount of transmitted data across the network. Social IoT is indeed well-aligned with fog-enhanced IoT. In the proposed architecture, the devices that are connected to the same edge node can be categorized in the same community and make relationships based on their social interactions. In this scenario, we aim to design a blockchain-based trust management system to evaluate the trust factors among the devices. This system is decentralized and hosted on a blockchain. Figure 1 demonstrates the architecture.

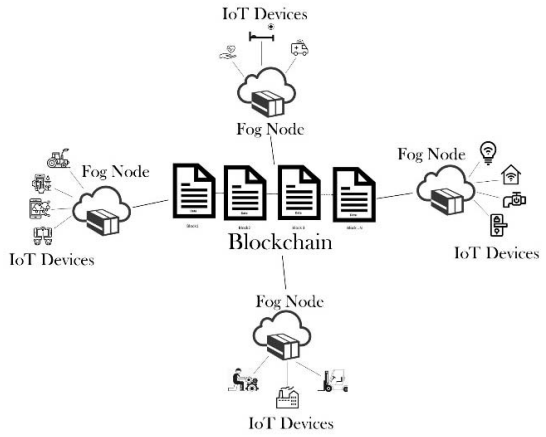

Figure 1: The proposed architecture for blockchain-based social IoT

The framework utilize the Ethereum platform [20] which can store data and run smart contracts. A smart contract is responsible for running the trust management system on the blockchain. The code is in Ethrerum-specific binary format and store the feedbacks and also provides functions for trust evaluation. These functions are called by transactions that are signed and sent by the IoT devices, and an assigned cost should be paid by the requester. The IoT devices interact with the blockchain edge nodes, and these edge devices participate in the mining process.

To create a community, any client in the system can register as an owner. To this aim, the client should send a transaction to the blockchain including the identifier (ID) the community it wants to create. The blockchain checks the uniqueness of the suggested ID and if it is approved, the owner will be added to the owner list of the smart contract. Each owner has a list of devices and a list of friend owners.

The devices can be added to the system through a community owner. When the owner tries to register a device in the system, the blockchain checks its address to find out if this device was registered before, if not the device will be added to the device list of the community. The owners can create or update the friend list for the devices in their community. □

Trustworthiness for each node will be updated dynamically based on the feedback on its behaviour. In this study, we selected reputation, cooperativeness, and community interest as the metrics to describe the trust status of a node [17] that is denoted by:

$$T_{ij}(t) = (reputation, cooperativeness, community\ interest) \quad (1)$$

in which i and j are trustor and trustee nodes, respectively, and t is the time. Each of the trust factors can evaluate one aspect of trust measurement in social IoT.

Reputation illustrates how much an object is trustable from other objects' perspective. Each node uses its own direct experience and indirect feedback from other nodes to evaluate the reputation of an object in the network. This metric means that other nodes can share their experience regarding their previous interaction with the trustee. Cooperativeness shows how much two nodes are socially connected. This factor is assessed based on mutual friends between the objects. Finally, community interest describes the level of cooperativeness between the communities that devices belong to.

Each resource in the social IoT system has a threshold on each of these metrics. A node will be able to access a resource or a service in the network if it can pass all three thresholds. The computation for trust factors is performed on the edge nodes, and then it is sent to the blockchain.

A. Reputation Calculation

To evaluate reputation, the proposed model uses a feedback system that reports the evaluation of given access to a device. This feedback is a number in the range of [0,1]. The value is 1 when a node behaves well, and any detected misbehavior in the access procedure decreases this feedback value.

Reputation is a measurement that uses two trust factors: direct experience, and indirect experience. It is defined as below:

$$R_{ij}(t) = \alpha D_{ij}(t) + (1-\alpha) I_{ij}(t) \quad (2)$$

in which $D_{ij}(t)$ is the direct experience of object I regarding object j in time t, and $I_{ij}(t)$ is the indirect experience between these two nodes. Moreover, α is a parameter to weight these trust factors.

1) Direct Experience Calculation:

This factor is evaluated based on past interactions between two nodes. An evaluation is generated by the feedback system after each interaction and is sent to the blockchain. We define $f_{ij}(\Delta t)$ as the collection of feedback of interaction to the node I from node j on the latest time slide that and is defined as follow:

$$f_{ij}(\Delta t) = \{ {f_{ij}}^1, {f_{ij}}^2, \dots, {f_{ij}}^{(\Delta t)} \} \quad (3)$$

Δt can also be defined as a specific number of latest transactions.

The $D_{ij}(t)$ is defined as the following:

$$D_{ij}(t) = \frac{number\ of\ positive\ feedback\ in\ f_{ij}(\Delta t)}{total\ number\ of\ feedback\ in\ f_{ij}(\Delta t)} \quad (4)$$

Positive feedback is the one that is bigger than a defined expectation in the system, and this value can be adjusted based on the application.

2) Indirect Experience Calculation:

To calculate the indirect experience assessment of node i about node j, we use the experience of other nodes of node j. After each transaction, its feedback will be stored in the blockchain and other nodes can utilize it. The weights for the feedback from different nodes can be weighted manually or subjectively, but using manual weights, the model will be dependent on the assigned weights. To eliminate this limitation, we used information entropy [21], which is a measurement of the disorder degree of a system. Using this measure, we can reinforce the contribution of more useful data in the reputation evaluation. Besides, this method is fast, lightweight, and therefore more appropriate for the IoT systems. Moreover, avoiding static weighting of the experience of different nodes makes the model robust against bad-mouthing and Ballot-stuffing attacks.

Based on the information entropy formula entropy of a node can be defined as [21]:

$$H_k = -\sum_i D_{ik} log D_{ik} \quad (5)$$

Using the entropy of nodes, we define the weight of each node in indirect experience calculation as:

$$w_k = \frac{1-H_k}{N-\sum_k H_k} \quad (6)$$

In which N is the number of nodes, and based on this formula, w is a normalized vector for weights.

Now using these weights, the indirect experience will be calculated as follows:

$$I_{ij}(t) = \sum_{k=1}^{n} w_k D_{kj}(t) \quad when\ k \neq j \quad (7)$$

That k is the index of other devices that have had interaction with node j.

B. Cooperativeness Calculation

Cooperativeness shows how much two nodes are socially willing to interact [22]. In the proposed system, each node has a list of friends. This list can be assigned based on the application that they work on or business preferences that are defined by their owners. The list friend of nodes is stored in the blockchain, and it can be dynamically updated anytime. Being in the friend list of other nodes shows that they are socially connected, and it is more likely to be willing to interact. Having mutual friends is another fact that demonstrates a level of connection between two nodes; therefore, we used Jaccard similarity [23] to calculate the cooperativeness between nodes i and j in time t as:

$$C_{ij}(t) = \frac{friends(i) \cap friends(j)}{friends(i) \cup friends(j)} \quad (8)$$

C. Community-Interest Calculation

Community-interest describes that the trustor/trustee pair belongs to communities that are socially connected. In edge-enhanced IoT, we can assume devices that are connected to an edge node, build a community. These communities can have a friend list just like the friend lists of devices. It means that the edge nodes that are more socially willing to interact can introduce another useful aspect of trust. The information about these lists are stored in the blockchain as well and can be adaptively changed by edge nodes. Using Jaccard similarity, $S_{ij}(t)$ shows the community-interest between nodes i and j in time t, and is defined as:

$$S_{ij}(t) = \frac{friends(k) \cap friends(l)}{friends(k) \cup friends(l)} \quad (9)$$

in which k and l are the edge nodes that devices i and j are connected to, respectively.

V. Privacy & Security Analysis

In this section, we will analyze how the presented blockchain-based trust management system can meet the security requirements in social IoT and is secure against attacks in the network.

Bad-Mouthing Attack: In our model, feedback is stored on the blockchain; therefore, is transparent for all nodes to access. In the proposed trust evaluation procedure, each node uses its own experience in addition to the experience from other nodes. Using entropy in indirect reputation evaluation decrease the impact of this type of attack by limiting the effect of fake feedback, and makes the trust evaluation more reliable. The other factor that prevents this attack is social connection assessment. Trustors leverage cooperativeness and community-interest evaluation metrics in addition to the reputation metric, and because the social connections are issues by trusted owners, it will limit the access of devices with weak social connection to the trustor.

Ballot Stuffing Attack: Just similar to the bad-mouthing attack, using a combination of direct and indirect experience among nodes in the system, leveraging entropy in reputation assessment, and using social connection evaluation in the network, the proposed algorithm is resistant against this type of attack.

Denial of Service (DoS) Attack: In our system, random nodes cannot join the system without permission from known owners. Moreover, if any authorized node wants to send fake transactions to the network, the reputation of the node will be ruined rapidly in the trust management system, and the system can block the transactions from the nodes. Furthermore, because the requester should pay the transactions' cost, it will significantly decrease the motivation of a malicious node to make this type of attack.

Storage Attack: The presented method is resistant against these malicious attempts because it uses blockchain, and the stored data on the blockchain is immutable.

VI. Performance Evaluation

To conduct performance analysis, a proof of concept has been developed to evaluate the feasibility of our proposed trust management system and the relevant protocols. The system is deployed on a private Ethereum-based blockchain system [20]. We developed a smart contract on this blockchain using

Solidity language. The end nodes applications are developed using JavaScript.

Our interest in this study is focused on the performance of the proposed trust management system in evaluating the trust level for the nodes and detecting malicious nodes. As is described in the previous sections, the trust level of a node consists of three metrics. Reputation is based on the prior behaviour of a node in the network, while cooperatives and community-interest are based on the social relationships among the owners. At the start of each transaction, a trustee sends an access request through the network, then the system evaluates the requests. If the trustee can pass the trust requirements, it will be permitted to receive the requested service. After each transaction, the evaluated feedback of the access is reported to the blockchain. The trust factors are evaluated in a period, so the misbehaved nodes have the chance to rebuild their reputation through time.

In the simulation set up, we considered 50 IoT devices that are connected to six different fog nodes. The percentage of malicious nodes was set 0.15, 0.20, 0.25, 0.30 in different scenarios. To calculate reputation, the direct trustworthiness has been weighted by 20%, and the indirect experience weight is 80%.

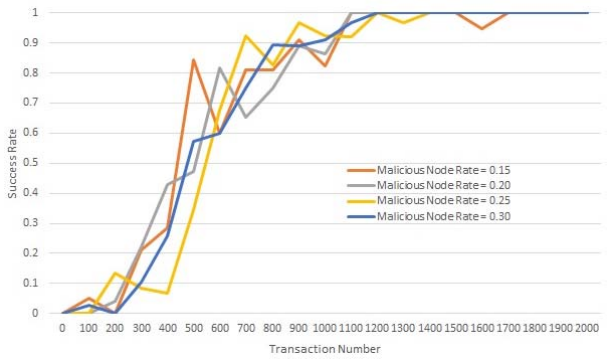

Figure 2: Malicious node success rate in the proposed method when accepted reputation threshold is 0.8 and omega is 0.2.

Figure *2* plots the success rate for malicious node detection through the iterations when the reputation threshold in the system is set as 0.8. This means that, in this scenario, the nodes with the trust value less than 0.8 will be assessed as untrustable nodes. As is demonstrated in this Figure, after around 1000 transactions, the trust management system detects almost all malicious nodes. After this phase, in some cases, the success rate drops by a small value and then will be increased again to 1. The reason for this is that the trust value is evaluated in a time slide, and after that, some old feedback will not be evaluated anymore. Therefore, after receiving new negative feedback, the trust management system can again detect these nodes as untrustworthy.

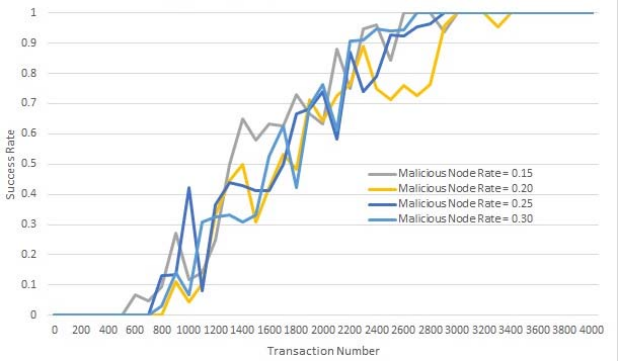

Figure 3: Malicious node success rate in the proposed method when accepted reputation threshold is 0.5 and omega is 0.2.

In Figure *3*, the rate of successful malicious node detection is depicted in the case that the reputation threshold in the system is 0.5. This plot shows that the behaviour in the system is similar to the previous scenario, and it just needs more transactions to converge to the success rate 1. After around 3000 transactions, again, almost all untrustable nodes are detected by the system.

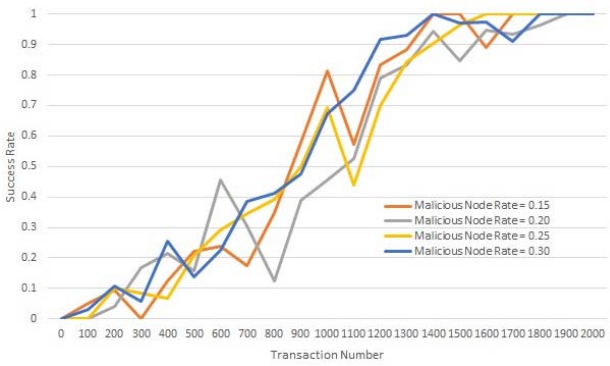

Figure 4: Malicious node success rate in the proposed method when accepted reputation threshold is 0.8 and omega is 0.5.

In Figure *4*, The effect of increasing the value of direct trust weight is demonstrated. In this case, this value is 50%, and it means that direct trust and indirect trust are equally contributing to global reputation evaluation. The results show that the convergence is slower than the case that indirect trust weight was 80%. The reason is that direct experience between each pair is considerably less than the collective experience between all other pair devices, and it is a wise decision to rely on the indirect experience from pairs more.

The results from all experiments show that the proposed trust management system can reach a high level of accuracy in detecting the adversaries in a limited number of transactions. Considering the empirical performance depicted in this Section in addition to the security, transparency, and availability that are resulted from blockchain [24][25], the proposed trust management system can address the trust challenges imposed by centrality in social IoT. Besides, leveraging blockchain, the proposed system uses peer-to-peer networking, which is known as one of the best approached to guarantee scalability in large networks [26].

VII. Conclusion

In this paper, we proposed a blockchain-based trust management system for social IoT. Using blockchain technology, this system provides a secure and transparent mechanism for trust evaluation. To reach better performance, we utilized information entropy in the reputation assessment procedure. The implemented system results show its ability to manage trust in a social IoT securely. We demonstrated that this system is resistant to attacks in social IoT. As a next step, we aim to consider how the trust management system can be used to encourage social relations among IoT devices based on reputation and mutual interactions.

REFERENCES

[1] Z. Yan, P. Zhang, and A. V Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, 2014, doi: 10.1016/j.jnca.2014.01.014.

[2] G. M. Luigi Atzori, Antonio Iera, "From ' Smart Objects ' to ' Social Objects ': The Next Evolutionary Step of the Internet of Things," *IEEE Commun. Mag.*, vol. 52, no. 1, pp. 97–105, 2014.

[3] Z. Yang *et al.*, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, 2019, doi: 10.1109/JIOT.2018.2836144.

[4] A. Moinet, B. Darties, and J. Baril, "Blockchain based trust & authentication for decentralized sensor networks," *arXiv Prepr. arXiv1706.01730*, 2017.

[5] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond : A Technical Survey on Decentralized Digital Currencies," vol. 18, no. 3, pp. 2084–2123, 2016.

[6] K. Christidis and G. S. Member, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[7] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Prof.*, vol. 19, no. 4, pp. 68--72, 2017.

[8] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, 2016, doi: 10.1109/JIOT.2016.2584538.

[9] N. K. Giang, M. Blackstock, and R. Lea, "Developing IoT Applications in the Fog : a Distributed Dataflow Approach," in *2015 5th International Conference on the Internet of Things (IOT)}*, 2015, pp. 155--162.

[10] M. Nitti, R. Girau, L. Atzori, and S. Member, "Trustworthiness Management in the Social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, 2014, doi: 10.1109/TKDE.2013.105.

[11] I. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 6, pp. 684–696, 2016, doi: 10.1109/TDSC.2015.2420552.

[12] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a Trust Evaluation Mechanism in the Social Internet of Things," *Sensors*, vol. 17, no. 6, p. 1346, 2017, doi: 10.3390/s17061346.

[13] B. Value, "Device democracy: Saving the future of the internet of things," *IBM Inst. Bus. Value*, 2014.

[14] A. D. Dwivedi, G. Srivastava, and S. Dhar, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019, doi: 10.3390/s19020326.

[15] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using Blockchain in a Reputation-Based Model for Grouping Agents in the Internet of Things," *IEEE Trans. Eng. Manag.*, vol. PP, pp. 1–13, 2019, doi: 10.1109/TEM.2019.2918162.

[16] M. Tahar, B. Hammi, and P. Bellot, "Bubbles of Trust : A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, no. 2018, pp. 126–142, 2020, doi: 10.1016/j.cose.2018.06.004.

[17] J. Yuan and X. Li, "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion," *IEEE Access*, vol. 6, pp. 23626–23638, 2018, doi: 10.1109/ACCESS.2018.2831898.

[18] J. Li, N. Li, and X. Wang, "Denial of Service Attacks and Defenses in Decentralized Trust Management."

[19] S. Huh, S. Cho, and S. Kim, "Managing IoT Devices using Blockchain Platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 464–467, doi: 10.23919/ICACT.2017.7890132.

[20] G. W. Founder and E. Gavin, "Ethereum: a secure decentralised generalised transaction ledger," *Ethereum Proj. yellow Pap.*, vol. 151, pp. 1–32, 2014.

[21] R. Dai and I. F. Akyildiz, "A spatial correlation model for visual information in wireless multimedia sensor networks," *IEEE Trans. Multimed.*, vol. 11, no. 6, pp. 1148–1159, 2009, doi: 10.1109/TMM.2009.2026100.

[22] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *2010 Proc. IEEE INFOCOM*, pp. 1–9, 2010, doi: 10.1109/INFCOM.2010.5462138.

[23] R. B. Zadeh, "Dimension Independent Similarity Computation," vol. 14, pp. 1605–1626, 2012.

[24] S. Underwood, "Blockchain Beyond Bitcoin," *Commun. ACM*, vol. 59, pp. 15–17, 2016, doi: 10.1145/2994581.

[25] H. Watanabe and S. Fujimura, "Blockchain Contract : A Complete Consensus using Blockchain," in *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)*, 2015, pp. 577–578, doi: 10.1109/GCCE.2015.7398721.

[26] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A Survey and Comparison of Peer-to-Peer Overlay Network Schemes," *IEEE Commun. Surv. tutorials*, vol. 7, pp. 72--93, 2005.