A Survey on Blockchain-Based Trust Management for Internet of Things

Yijia Liu, Jie Wang, Zheng Yan, *Senior Member, IEEE*, Zhiguo Wan, *Member, IEEE*, and Riku Jäntti, *Senior Member, IEEE*

***Abstract*—Internet of Things (IoT) aims to create a vast network with billions of things that can seamlessly create and exchange data, establishing intelligent interactions between people and objects around them. It is characterized with openness, heterogeneity, and dynamicity, which inevitably introduce severe security, privacy, and trust issues that hinder the widespread application of IoT. Trust management (TM) holds great promise in identifying malicious nodes, maintaining trust relationships, and enhancing system security. Traditional TM systems (TMSs) can be classified into centralized, semi-centralized, and distributed ones, all three of which suffer from critical challenges and thus are not sufficient for facilitating IoT development. Blockchain, as a disruptive technology, can help addressing the challenges of TM in IoT, thanks to its advanced features, such as decentralization, consistency, and tamper-proofing. As a result, blockchain-based TM (BC-TM) has been extensively studied in recent years to achieve decentralized TM in IoT. However, it still lacks a comprehensive survey on the current state of the arts. To fill this gap, in this article, we conduct a serious survey on BC-TM in IoT. We first propose a set of evaluation criteria that should be met by a TMS in IoT. Then, we propose a taxonomy of TMSs and continue with a thorough review on BC-TM in IoT by employing the proposed criteria. In the end, based on the review, a series of open issues are identified, and future research directions are suggested.**

***Index Terms*—Blockchain, Internet of Things (IoT), privacy, security, trust management (TM).**

I. Introduction

AS THE core technology of the 4th industrial revolution, Internet of Things (IoT) has become an important development direction in the world [1]. Its related applications, such as smart homes, smart grids, smart healthcare, smart agriculture, and wearable devices, are also flourishing and have a great impact on people's production and lifestyle. IoT allows various objects ubiquitous around us to interact with each other through a unique addressing scheme in order to achieve a dynamic network environment of interconnected computing devices with different components [2], [3]. The way of transmitting information over the network without human–computer interaction significantly brings convenience to users. However, the unique characteristics of IoT, such as openness, resource constraints, and heterogeneity, introduce a number of challenges and issues: 1) IoT suffers from internal attacks. Traditional security solutions are only available in countering external attacks but fail to cope with internal ones; 2) IoT devices are resource-constrained so that high-cost cryptography-based solutions are not applicable; and 3) IoT is a network composed of heterogeneous devices, networks, applications, and so on. Hence, there is a demand of a unified way to deal with such heterogeneous issues.

Trust management (TM), as a useful means to control and maintain trust, is promising to address the above critical challenges and issues in IoT systems. TM involves such processes as useful information collection, trust relationship assessment, decision making, and trust maintenance, as well as automating the above processes [4]. Basically, there are three types of traditional TM systems (TMSs), i.e., centralized, semi-centralized, and distributed. In the centralized TM, a central authority, such as a cloud server, is responsible for providing a global view of nodes and managing trust. However, it lacks scalability and suffers from a single point of failure [5]. In the semi-centralized or distributed TM, low reliability and the single point of failure are tackled to some extent [6], but still insufficient. In the distributed TM, issues regarding data auditing and consistency remain unsolved [7]. It is challenging for distributed TM to provide a global view of trust values. As a result, prior TMSs face with several challenges, which limit their application and development in IoT.

Blockchain is a time-stamped series of immutable data records, which holds the characteristics of decentralization, consistency, tamper-proofing, and transparency. Owing to these characteristics, blockchain is considered as a feasible tool to advance TMSs, thereby effectively improving trust and security among IoT devices. Specifically, decentralization enables direct peer-to-peer interactions and eliminates single point of failures. Consistency means that information maintained by each party is consistent. In other words, blockchain is an effective means to support global trust consensus. Tamper-proofing ensures that data recorded in blockchain cannot be tampered so that malicious behaviors can be traced. The

Manuscript received 27 September 2022; revised 28 December 2022; accepted 13 January 2023. Date of publication 18 January 2023; date of current version 24 March 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Key Research Project of Shaanxi Natural Science Foundation under Grant 2023-JC-ZD-35; in part by the Open Research Project of ZheJiang Lab under Grant 2021PD0AB01; in part by the Academy of Finland under Grant 345072 and Grant 350464; and in part by the 111 Project under Grant B16037. *(Corresponding author: Zheng Yan.)*

Yijia Liu, Jie Wang, and Zheng Yan are with the State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: liuyijia42@foxmail.com; jiewang.xidian@foxmail.com; zyan@xidian.edu.cn).

Zhiguo Wan is with Zhejiang Laboratory, Hangzhou 311121, Zhejiang, China (e-mail: wanzhiguo@zhejianglab.com).

Riku Jäntti is with the Department of Communications and Networking, Aalto University, 02150 Espoo, Finland (e-mail: riku.jantti@aalto.fi).

Digital Object Identifier 10.1109/JIOT.2023.3237893

TABLE I
COMPARISON OF OUR SURVEY WITH EXISTING RELATED SURVEYS

Covered topics	[8]	[9]	[10]	[11]	Our survey
Propose evaluation criteria for BC-TMSs	○	○	◐	○	●
Summarize attacks on TM and blockchain	●	●	◐	○	●
Propose a taxonomy of TMSs	●	●	○	●	●
Review BC-TMSs for all IoT application areas	●	○	○	○	●
Discuss the benefits of applying blockchain to TM	●	●	●	●	●
Discuss the benefits of applying TM to blockchain	○	○	○	○	●
Discuss the roles of both blockchain and TM in IoT layered architecture	○	○	○	○	●

●: Discussed; ◐: Partially discussed; ○: Not discussed.

characteristic of transparency is in a sense an extension of tamper-proofing, facilitating the auditing raised by participants. In addition, smart contracts can enable TM automation. Therefore, blockchain becomes a promising technology to overcome the problems of existing TMSs and achieve decentralized TM.

Considering the fast development of IoT networks, the public's increasing concerns of trust, as well as the great success of blockchain, researchers have made a number of attempts to employ blockchain for TM in different fields of IoT, such as healthcare [12], supply chain management [13], and smart city [14]. Through investigation, we found that there is still a lack of a related survey until 2021. While there are four highly relevant surveys that have emerged from 2021 to date, they are not comprehensive. Specifically, Kumar and Sharma [8] discussed blockchain-based TMSs (BC-TMSs) for an entire IoT network, but overlooked how to evaluate them in a qualitative manner. Wei et al. [9] focused on BC-TMSs in service-oriented IoT, but neglected those in other areas of IoT (e.g., transport industry). Ul Ain Arshad et al. [10] presented evaluation criteria, but they are not comprehensive, especially the criteria related to blockchain were ignored. The survey presented in [10] also lacks a summary of attacks on blockchain and a taxonomy of TMSs. Moreover, only four application areas of IoT were discussed, i.e., Internet of Medical Things (IoMT), Internet of Vehicles (IoV), Social IoT (SIoT), and Industrial IoT (IIoT). Rahmani et al. [11] proposed a taxonomy of TMSs, but they only studied a small area of IoT, failed to qualitatively evaluate BC-TMSs, neither summarized the attacks on BC-TMSs. In addition, the mutual benefits of blockchain and TM as well as their roles in IoT are seldom covered in the above surveys.

In this article, we aim to help researchers and developers capture the recent advances, open issues, and future research directions toward realizing reliable and sound BC-TMSs for IoT. To be specific, we first introduce the background of IoT, TM, and blockchain, illustrate the mutual benefits between TM and blockchain, and explore the roles of TM and blockchain in all layers of IoT. Second, we propose 14 evaluation criteria that a sound TMS should meet, and divide them into three categories: 1) fundamental properties; 2) effectiveness; and 3) security and privacy. Third, we classify TMSs into three categories: 1) trust value-based; 2) trust value-free; and 3) hybrid ones. The classification is further refined based on used models. Subsequently, we conduct a thorough review on BC-TMSs in IoT by employing the proposed criteria as a measure to study existing schemes' pros and cons. In the end, based on the review, a series of open issues are identified, in parallel with suggestions on future research directions.

Table I provides a detailed comparison of our survey with highly related surveys. We can see that our survey is the most comprehensive, which covers all of the above-mentioned aspects. Note that none of the four related existing surveys discuss the last two topics in the table, which are unique in our survey. Specifically, the main contributions of this article can be summarized as follows.

1) We discuss the mutual benefits between TM and blockchain with regard to BC-TMSs, as well as their respective roles in IoT layered architecture.
2) We summarize a set of evaluation criteria regarding fundamental properties, effectiveness, and security and privacy, which should be satisfied by a TMS in order to ensure a trusted IoT environment.
3) We propose a taxonomy of TMSs and conduct a comprehensive review on BC-TMSs in IoT by employing the proposed criteria as a measure to analyze their pros and cons.
4) We point out a series of open issues and further suggest future research directions to advance the research on BC-TM in IoT.

The remainder of this article is organized as follows. In Section II, we introduce the preliminaries of IoT, TM, and blockchain. In Section III, we provide a set of criteria for evaluating the performance of existing BC-TMSs, followed by a thorough review on BC-TMSs in IoT in Section IV. In Section V, we discuss open issues and suggest future directions. Finally, a conclusion is drawn in the last section.

II. PRELIMINARIES

In this section, we introduce the background knowledge of IoT, TM, and blockchain. Specifically, we first present their concepts and characteristics. Then, we summarize the applications of IoT in different fields. Third, we discuss the challenges and issues faced by IoT TM. Finally, we summarize the benefits that TM and blockchain can bring to each other as well as their emerging roles in each of the three layers in the IoT system. An overview of the relationship between IoT, TM, and blockchain is shown in Fig. 1.

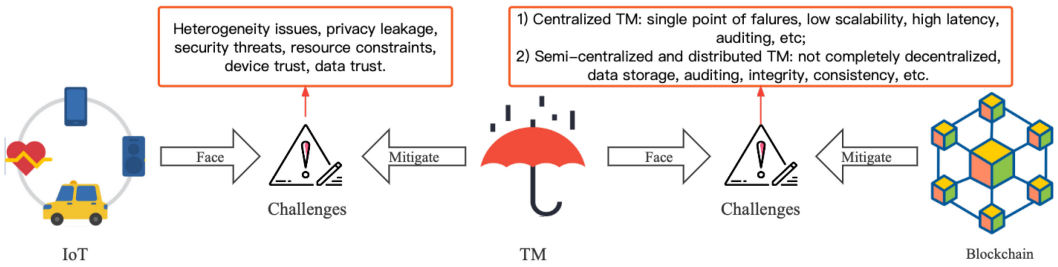

Fig. 1. Overview of the relationship between IoT, TM, and blockchain.

A. IoT

1) Concepts and Characteristics: The IoT refers to the Internet-based technology that enables various objects prevalent around us to interact with each other through unique addressing schemes, in order to realize a real-time dynamic network environment consisting of interconnected computing devices with different components [2], [15], [16]. One of the most fundamental architectures for IoT is the three-layer architecture [17] that contains a perception layer, a network layer, and an application layer. We focus on this architecture as it is easy to understand and widely accepted by the research community. The IoT system holds such basic characteristics as heterogeneity, dynamic change, enormous scale, and resource constrain [18], [19].

2) Applications: IoT applications cover the "smart" environment/space and can be found in almost every aspect of our daily life. In this article, we concern the following main applications: smart city [20], smart home [21], smart healthcare [22], smart transport [23], smart industry [24], smart agriculture [25], and personal and social life [21]. For example, smart transport systems can provide effective traffic control and management by using advanced sensors, information, and network technologies [26], [27]. For more details, please refer to the references after each application.

3) Challenges and Issues: The unique characteristics of IoT introduce a number of challenges and issues related to privacy, security, and trust caused by heterogeneity and resource constraints.

a) Heterogeneity: IoT networks consist of different types of devices with different computation capability, storage capacity, and power supply [28]. These devices can form many heterogeneous subnetworks. Therefore, a unified approach to deal with such heterogeneity is needed to accommodate different application domains, different communication environments, and a large number of devices with various types.

b) Privacy: Privacy is a major concern in IoT due to its nature of sensing human-being's activities. The sensed data of an IoT device may contain private information about its owner or user, which may be leaked through communication, transmission as well as memory cleanup. Moreover, devices with limited resources may focus on functionality at the expense of ignoring privacy.

c) Security: In IoT, each device is connected to each other, the change of IoT scale and device interactions may lead to significant security threats [29]. Traditional security measures in IoT are cryptography and access control. They maintain the robustness of a system in the presence of external attacks, data inconsistency, and privacy leakage [28]. However, in complex and heterogeneous IoT, cryptography alone cannot provide sufficient security because internally compromised devices can generate false information and still pass authentication with valid keys (i.e., internal attacks) [28]. As for access control, a device is allowed to enter the network only if its identity is legitimate and exists in an access control list. Nevertheless, access control mechanisms are neither immune to changeable behaviors, nor suitable for distributed environments [30]. Moreover, traditional security countermeasures and privacy enforcement cannot be directly applied into IoT due to the limited computation capability of IoT devices [31].

d) Trust: The heterogeneous nature of an IoT network requires a wide variety of data to be collected in different networks, and trustworthiness assurance of data and devices is a big challenge, e.g., trust in data aggregation and data processing. If the aggregated data from different devices are malicious and not sufficiently trusted, it becomes difficult for users to accept related IoT services even though trust is adequately provided at the application and network layers [32]. Therefore, measures are needed to manage and coordinate the trustworthiness of data for users, as well as the process of trust evaluation.

B. Trust Management

1) Concepts and Characteristics: The concept of trust is complex and subjective, involving confidence, beliefs, and expectations about the reliability, integrity, security, dependability, competence, and other characteristics of an entity. Its dynamic nature allows the level of trust to be changed over time, objects, and context. Reputation is a public opinion on trust, which is aggregated trust based on a group of entities' opinions on a trustee, although it is often used interchangeably with trust [5]. Trust and reputation play a critical role in IoT security [33]. Yan and Prehofer [4] indicated that TM concerns gathering useful information, assessing trust relationships, making decisions as well as maintaining trust, and automating the above processes. Serving as an effective means, TM can control and maintain trust in IoT systems, which is expected to solve the above-mentioned key challenges and issues of IoT. Generally speaking, there are three types of TMSs, i.e., centralized, semi-centralized, and distributed [6], [28].

2) Benefits of Applying TM for IoT: TM plays an important role in IoT as an effective means to control and maintain trust in IoT systems, which is expected to solve the above-mentioned key challenges and issues of IoT.

a) Resisting internal attacks: TM can identify and counter internal attacks by monitoring and analyzing variable behaviors and interaction instances of system entities [28], which is not available in the traditional security methods.

b) Offering flexibility: The TM methods based on trust evaluation are more flexible, efficient, expressive, and scalable than the traditional security methods that usually make binary decisions [34]. Each participant can define one or more policies to evaluate trustworthiness according to their requirements in different contexts [30].

c) Resolving collaboration uncertainty: TM can address cooperation uncertainties, such as information asymmetry (i.e., one party does not have all the information about the others) and opportunism (i.e., trading partners have different goals) [30].

d) Providing unified decision-making: There are a large number of heterogeneous devices and subnetworks in the IoT. How to manage them in a unified way requires an abstraction (i.e., trust) that simplifies the environment and relationships, maps complexity and uncertainty into a unified standard and then makes decisions based on that standard [30].

e) Mutual benefits: TM can mutually utilize and benefit from other security protocols and mechanisms [30].

3) Challenges and Issues: Traditional TMSs in IoT still face some challenges and problems.

a) Nondecentralization of TMSs: Centralized TMSs store trust-related information at a centralized single authority, which raises single point of failures and low scalability. Although distributed TMSs can solve the above issues, most of them are not fully decentralized, i.e., normally there is still a hidden central authority [35].

b) Lack of trust evaluation auditability: A centralized TMS relies on a central entity and if it behaves maliciously (e.g., tamper with data), other entities have no way to know, thus it cannot support auditability well. A semi-centralized TMS or a distributed TMS also has the risk of data tampering since more than one entity calculates, maintains, and propagates trust. Thus, transparency and traceability regarding trust evaluation cannot be guaranteed in existing TMSs.

c) Inconsistency of trust evaluation results across the network: Centralized TMSs do not have this problem because an central authority manages trust independently. However, semi-centralized and distributed TMSs suffer from trust inconsistency. For example, a set of leader nodes independently perform trust evaluation and management of the nodes within their scope. When a node in region A moves to region B, its trust value in region A may not be known to the leader node in region B in a timely and accurate manner due to transmission delay of trust propagation and the possibility that the leader in region A is malicious and arbitrarily propagates the trust value.

C. Blockchain

1) Concepts and Characteristics: Blockchain integrates cryptography, consensus protocols, P2P networks, and smart contract technologies [15] to form a decentralized distributed ledger, i.e., a consensus record with a cryptographic audit trail maintained and verified by multiple participating nodes [36]. The consensus protocol can be performed in various ways, e.g., Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated PoS (DPoS), practical Byzantine fault tolerance (PBFT), and round robin (RR). Blockchain owns several advanced properties, including decentralization, transparency, consistency, and tamper-proofing [37]. Based on visibility and accessibility, blockchain can be classified into three main types: 1) public; 2) private; and 3) consortium [38].

2) Benefits of Applying Blockchain for TM: Owing to its advanced features, blockchain can be used to address the key challenges and issues faced by traditional TM, thereby enhancing trust and security among IoT devices.

a) Decentralization: This nature of blockchain makes the right and obligation of every node in IoT equal, and blocks containing trust-related information are jointly maintained by nodes with maintenance functions in the whole system. This provides fairness and eliminates the possibility of single point of failures.

b) Tamper-proofing: This nature ensures that the data recorded in the blockchain cannot be tampered with, thus facilitating the audibility of TM.

c) Automation: Smart contracts can help to automate the entire process of TM in a reliable way. This is because they are programs that run on the blockchain, where the code cannot be modified, nor forced to stop in mid-run. Thus, atomicity of trust evaluation and security of code execution are possible to be guaranteed.

d) Consistency: Since the information stored on the blockchain is consistent all over the network. This can ensure the consistency, continuity, and integrity of trust evaluation within the IoT network.

D. Benefits Between TM and Blockchain

In this section, we discuss the mutual benefits between TM and blockchain, as well as explore their roles in the three key layers of an IoT system.

We have discussed the benefits that blockchain can bring to TM, such as the items indicated in the blue dashed box on the right in Fig. 2. In addition, we also look ahead to what benefits TM can bring to blockchain, such as the items indicated in the red dashed box on the left in Fig. 2.

1) TM can serve as an auxiliary tool for developing new consensus mechanisms. Specifically, the trustworthiness of blockchain participants is evaluated in a decentralized manner. A trust value can be expressed as the weight held by a node in the system, and the higher the weight, the higher the probability of being selected as a miner. This consensus process is similar to PoS, i.e., using trust values instead of coins in the network to decide the weights of consensus [39]. The update of trust is dynamic and faster than the update of held coins, so it also improves the efficiency of blockchain.
2) TM is promising to guarantee the trustworthiness of data before being recorded to the blockchain. Blockchain can only guarantee that the data stored in it cannot

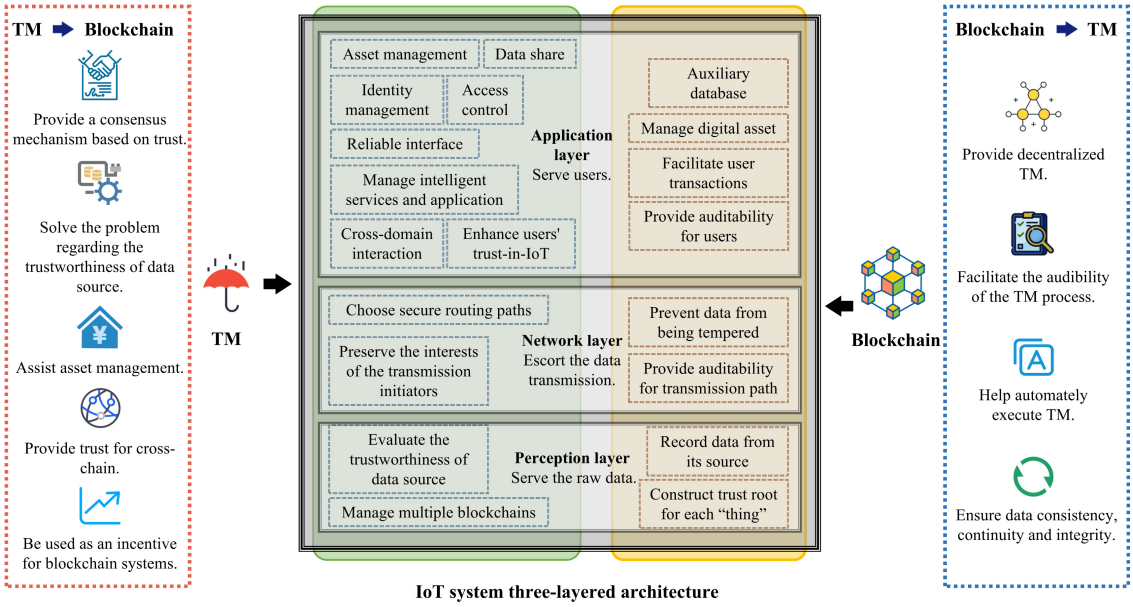

Fig. 2. TM and blockchain in IoT and their mutual benefits.

be tampered with, but it cannot guarantee that the data would not be contaminated before written to the block. Fortunately, TM can evaluate the credibility of data providers and reduce the probability of recording malicious data.

3) TM can assist in blockchain asset management. Blockchain can store digital assets, including but not limited to digital currencies. Asset verification and transfer require a desired level of "trust" in the counterparty. TM provides a solution for measuring this trust.
4) TM can provide trust to cross blockchains. There are multiple subnetworks in an IoT network and they may use different blockchains. Communications across chains require mutual trust as a bridge.
5) Reputation credits can be used as an incentive in blockchain systems. Blockchain systems, especially private and consortium blockchains, need proper incentives to stimulate node participation to actively maintain the blockchain. Note that the benefits that TM can bring to the blockchain are not only limited in the IoT domain but also in other domains to establish a trustworthy environment.

In what follows, we discuss roles of TM and blockchain in the three layers of an IoT system, shown in the middle part of Fig. 2.

1) Perception Layer: IoT devices (e.g., sensors, cameras, RFID, and barcodes) collect real-world data for processing. In this layer, the credibility of the data source is particularly important. That is, in order to have a good evaluation of the trustworthiness of IoT devices, TM is needed to prevent them from playing tricks with data collection. Recording the data generated by highly trusted devices on a blockchain can form a complete chain of trust from data generation to processing. To summarize, both TM and blockchain serve the collection of raw data at this layer.

2) Network Layer: The transport medium (wired or wireless) is responsible for connecting physical devices to the network or other physical devices. In this layer, data transfer is not constrained and may go through multiple intermediaries (i.e., gateways or IoT devices). Each intermediary has the opportunity to process the data passing by or change a forwarding endpoint. Hence, TM is needed to constrain the behavior of the intermediary and preserve the interests of transmission initiators. Blockchain provides auditability by acting as a strong recorder of the transmission path and as a verifier to verify whether the data has not been altered. Overall, both TM and blockchain escort the data transmission in this layer.

3) Application Layer: This layer serves as an interface between users and IoT services, providing intelligent services and application management. In this layer, TM can help increasing the confidence of users to choose devices or services. It can also assist trustworthy service provision to users through secure data sharing, access control, identity management, asset management, privacy preservation (PP), auditing, and tracking during cross-domain interaction. Blockchain can be used not only as a database to assist in application management but also as a digital asset (e.g., digital currency) to facilitate user transactions. To summarize, both TM and blockchain serve users in this layer.

III. Evaluation Criteria

In this section, we summarize 14 important evaluation criteria that a BC-TMS needs to meet in order to ensure a trustworthy IoT environment. As shown in Fig. 3, we evaluate BC-TMSs from the following perspectives, i.e., fundamental properties, effectiveness, and security and privacy.

A. Fundamental Properties

A BC-TMS should first support the intrinsic nature of trust, including subjectivity, dynamicity, and context-awareness.

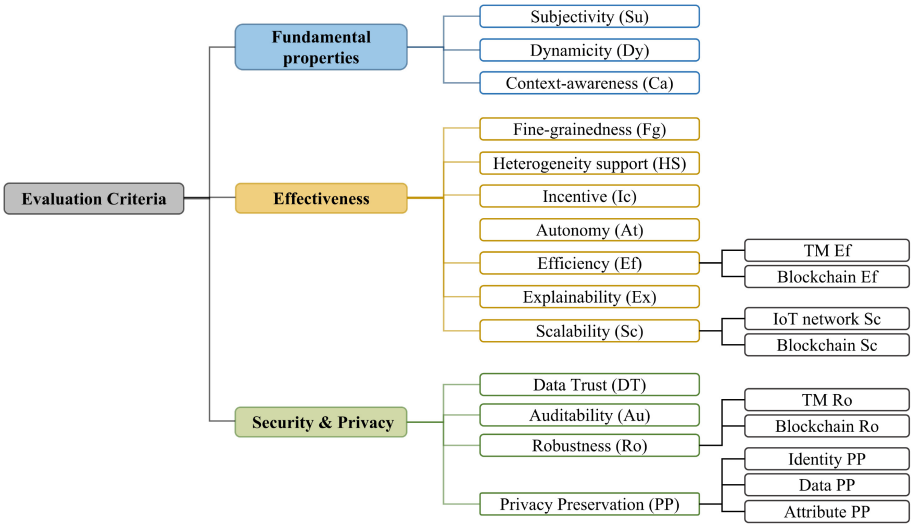

Fig. 3. Taxonomy of evaluation criteria.

1) Subjectivity (Su): The criteria of trust that different trustors on a trustee could be totally different, with various subjective opinions. In general, the subjective factors that affect trust can be divided into subjective attributes of a trustee (including honesty, benevolence, and kindness) and subjective attributes of a trustor (including confidence, disposition, and belief) [5], [40]. A TMS needs to consider such subjective factors when evaluating trust, making decisions, and managing trust relationships as subjectivity is an inherent nature of trust.

2) Dynamicity (Dy): This criterion is also called sustainability. In order to maintain trust relationships between IoT devices over time, a TMS should be able to understand the trust relationships of all related entities driven by time or events [41]. Time-driven means that the evaluation and update of trust relationships are executed based on time, while event-driven means that the evaluation and update are triggered by specific events. Overall, it is desirable for a TMS to update trust relationships as often as appropriate.

3) Context-Awareness (Ca): Context-awareness refers to the ability to differentiate various contexts. A logical model of trust must take into account the context and goal of entities [42]. Contexts should be paid attention during trust evaluation [43] as trust exists in one context but may disappear in another. For example, a physical education teacher is trusted to teach a sport program, but cannot be trusted to solve a difficult math problem. In the process of trust evaluation, only the evidence of trust that falls into the underlying context can be used [44]. Therefore, context-awareness is a significant requirement of a TMS. Common context information includes the time and location of the event, the location of a device and its remaining energy, the purpose of an action that needs TM, etc.

B. Effectiveness

A BC-TMS should offer sound effectiveness to facilitate its continuous operation and widespread usage. The attributes related to effectiveness includes but not limited to fine-grainedness, heterogeneity support (HS), incentive, autonomy, efficiency, explainability, and scalability.

1) Fine-Grainedness (Fg): Fine-grainedness of trust values reflects the sensitivity of trust in IoT nodes. The numerical expressions of trust values is divided into two categories: discrete and continuous. In a blockchain-enabled TMS, all participants are equal nodes, acting as both clients and servers at the same time. Therefore, a basic problem is how to select a reliable node from a large number of candidates [45]. Taking a Quality-of-Service (QoS) demand as an example, it is hard to say one node is totally good or bad [46]. Hence, it is not precise to use a binary expression, like whether a trust value exceeds a threshold, to judge node credibility. Meanwhile, some safety-critical contexts require a highly trustworthy node, which cannot be supported by the binary expression. To summarize, a TMS is possible to handle complex situations and has flexibility to satisfy personalized demands if adopting continuous trust values.

2) Heterogeneity Support: The network architectures and devices of IoT systems, e.g., wireless sensor networks, vehicular networks, and mobile communication networks, are inherently heterogeneous [47]. Meanwhile, as IoT services become abundant, data sharing within and across IoT networks becomes common. If a TMS of IoT ignores to support cross-domain trust, a situation of "local trust" could occur, i.e., trust is only valid within a same domain, and node trust cannot be dynamically migrated [5]. This could lead to serious security and trust issues, such as white-washing attacks. In short, a TMS that supports cross-domain can well adapt to complex and changeable real-world IoT scenarios.

3) Incentive (Ic): Effective incentives can stimulate nodes in an IoT network to jointly participate in trust evaluation and management [48]. No matter centralized or semi-centralized, or even distributed TMSs, they rely on one or many entities to calculate, manage, and maintain trust. However, there may be free-riders that do not participate in TM cooperation, but use the services provided by other benign nodes [27]. Therefore, in order to prevent these behaviors and guarantee the profits of each node in a TMS, incentives are needed.

4) Autonomy (At): Autonomy means that a TMS can be executed automatically without external interaction once its evaluation process and algorithms are set. Traditional TMSs may face some emergent situations (e.g., malicious modification of trust evaluation rules) in the process of TM, which makes the original trust evaluation algorithm terminated or even related data lost. Smart contracts can help automate the entire process of TM. All trust evaluation rules are encoded through a smart contract. The contract contains execution logic and execution conditions and when the conditions are satisfied, trust evaluation is automatically executed [49]. To fully manage trust without human intervention, BC-TMSs can benefit from the advantage of smart contracts.

5) Efficiency (Ef): IoT devices are resource-constrained, which reflects in limited storage capacity, computation capability, and energy. If a device costs too much resources to calculate trust, it may fail to complete other tasks [28]. In comparison with the cost of trust evaluation, the cost of achieving trust consensus on blockchain is much higher. Therefore, in this article, we pay attention to both TM and blockchain efficiency. We assess the efficiency through time complexity and space complexity.

6) Explainability (Ex): Explainability enables human-beings to understand how a trust model works, i.e., which trust-related factors impact trust in which way with which weight or strength. The trust model is an algorithm or method for building and managing trust relationships. An explainable trust model refers to that its input, output, and operating mechanism can be easily understood by human beings [61]. Such models with explainability can be easily accepted by their users due to improved transparency, increased credibility, and optimized rationality [62]. Some specific techniques can help in achieving explainability. For instance, model simplification, feature relevance estimation, and the visualization methods are the ways of improving explainability of the machine learning (ML) models (MLMs), which may also feasible to trust models [48]. To sum up, this criterion relates to the acceptance of a TMS, thus should be considered.

7) Scalability (Sc): Scalability refers to the adaptability to the change of the scale of an IoT network. With the rapid development of IoT regarding open resources, open standards, and open interfaces, the functionality and scale of the IoT network is quickly extended [63]. Meanwhile, due to restricted power and storage capacity, it is inevitable for IoT devices to frequently join and leave the network. Therefore, a sound TMS needs to flexibly adapt to the changeable number of nodes. In addition, scalability of blockchain is a key obstacle of the practical deployment of BC-TMSs, despite its many promising features. Throughput, storage, and network are three aspects of blockchain scalability [64]. In this article, we consider the scalability of TMSs in a comprehensive way regarding both the IoT network and blockchain.

C. Security and Privacy

A BC-TMS confronts both internal and external security threats and privacy issues, including data trust (DT), auditability, robustness, and PP. It needs to be resilient to those possible threats to enhance the security of the system.

1) Data Trust: DT refers to the authenticity of the data provided by data providers. If this criterion is ignored in the trust evaluation process, malicious devices could generate false information to mask their misbehaviors or deliberately provide false information to reduce the trustworthiness of their peers. Therefore, DT should be taken into account, usually in relation to the trustworthiness of data providers. For instance, for the process of aggregating recommendations from multiple independent entities, the trust of a recommender and the recommendation trust should be taken into account to mitigate the bad effect of malicious recommendations.

2) Auditability (Au): Auditability refers to whether data processing can be controlled and execution records can be checked [65]. In a TMS that combines local trust generated from direct interaction and global trust obtained via recommendations, some malicious and selfish entities may not provide recommendations or provide wrong ones to their neighbors. Therefore, the TMS should have such an ability of auditing the process of TM in order to check the correctness and validity of its each step with sufficient data or information.

3) Robustness (Ro): Robustness refers to the discernibility and tolerance of the false inputs provided by malicious attacks, as well as the adequate ability to deal with them [66], [67]. Due to the heterogeneous and dynamic natures of IoT [68], IoT device privacy, security, and trust are vulnerable to not only information attacks but also device attacks as well [69]. Fortunately, blockchain technology can help mitigating such impacts. Nevertheless, due to the overall low credibility of participating nodes, the existing form of blockchain technology is not able to resist attacks on trust perfectly [70]. What is more, the definition of trust is not clear for most IoT networks. Attackers could abuse this vague assumption of trust to disrupt a blockchain network and manipulate the reputation of IoT devices [71]. They may directly affect IoT network stability by sending erroneous inputs, fabricate an insincerity identity to puzzle peers and so on. As shown in [72], an attacker can paralyze a vehicle interior system by using simple means of offensive. Hence, a TMS must have the ability to resist various attacks. In order to study robustness, we focus on attacks against TM and blockchain. The detailed description of these two types of attacks is shown in Table II.

4) Privacy Preservation: We divide privacy into identity privacy, data privacy, and attribute privacy. First, private information about a user's identity (e.g., ID, name, email address, and public-key certificate [73]) is inevitably collected as input parameters when evaluating trust. When IoT devices communicate with each other or access services provided by the blockchain that requires pre-evaluation of trust, they are vulnerable to identity privacy leakage. Second, opinions or evidence provided by nodes/entities are needed and important for trust evaluation. Such data may reveal sensitive information of related nodes/entities if not protected during transmission and analysis. Third, due to the transparency of blockchain, trust-related information (e.g., behavior data used for trust evaluation and trust levels) stored on the blockchain could be at risk of being leaked if not protected. In other words, the real identity of a user or an entity relates to identity privacy. The information exchanged between devices that are intercepted causes data privacy leakage. The specific information stored

TABLE II
ATTACKS ON BC-TMSS

Attacks	Targets	Features	Consequences
Bad-mouthing attack	TM	Provide bad recommendations [50].	Damage the reputation of a target node.
Ballot-stuffing attack	TM	Collude with each other and provide fabricated and false positive recommendations [18].	Increase the reputation of malicious nodes to achieve a certain goal [50].
On-off attack	TM	Behave well or badly in an alternate way [5].	Regain trust before the next attack [5].
Self-promoting attack	TM	Report false positive recommendations or feedback [28].	Improve an attacker's own credibility to achieve certain goals [5].
White-washing attack	TM	Exit and rejoin the IoT network to obtain a higher trust value than previous one [18].	Erase the bad reputation of an attacker.
Sybil attack	TM & Blockchain	Set up nodes with multiple identities to control a network. [51].	Create confusion and consume connection resources between nodes [51].
Man-in-the-middle attack	TM & Blockchain	Intercept normal network communication data between benevolent parties [52].	Degrade/increase the reputation of honest/malicious nodes [52].
Eclipse attack	Blockchain	Control a victim's input and output connections [53].	Isolate a target node from other nodes in a blockchain network, and further control its effective computational power [54].
51% attack	Blockchain	A miner node happens to have more computing resources than other nodes, i.e., it has more than half of total processing power [55].	Dominate the validation and approval of transactions on a blockchain [56].
Replay attack	Blockchain	An attacker uses hard forked blockchain to obtain the same address and transaction information [57].	Attackers can go to another chain and replay transaction details [57].
Selfish mining attack	Blockchain	Attackers keep mined blocks in order to cause a fork of blockchain [54].	Make honest miners futile, thus force them to join a dishonest camp [57].
Block withholding attack	Blockchain	Attackers always send a partial proof of work to the pool manager and discards the complete proof of work [58].	Cause serious injury to block mining [57].
Distributed Denial of Service (DDoS)	Blockchain	Multiple systems overwhelm the resources and bandwidth of a target system [59]. A blockchain network can be used as a DDoS attack engine.	Make a target node denied for transactions [60].

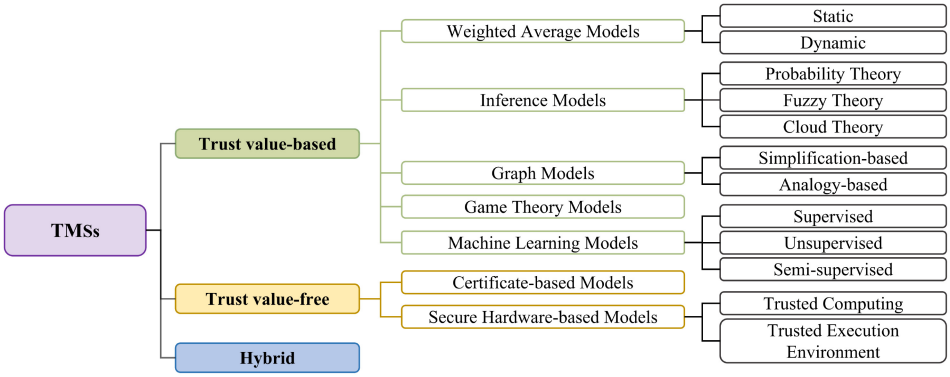

Fig. 4. Taxonomy of TMSs.

on the blockchain that can express the features or characteristics of some entity (e.g., gender, age, height, occupation, interests, and access control policies) is related to attribute privacy of the entity. In summary, a well-developed TMS is required to protect all three types of privacy and if this criterion is neglected, the TMS could suffer from some severe security flaws.

IV. REVIEW ON BC-TMSS IN IOT

In this section, we seriously review recent research breakthroughs on BC-TMSs in IoT. We find a total of 70 related research papers published during 2018 to 2022, searched from Web of Science, IEEE Xplore, ACM library, Elsevier, and Google Scholar. We further filtered these papers based on their qualities and finally selected 31 papers to perform a timely review on BC-TM techniques.

According to the techniques applied for TM, we divide the related works into three main categories in Section IV-A. Then, Sections IV-B–IV-D, respectively, review the works in each category by using the criteria presented in Section III as a measure to judge their pros and cons. Finally, we discuss our findings and compare the reviewed works in Section IV-E.

A. Taxonomy of Trust Management Systems

Pourghebleh et al. [25] classified existing TMSs into four categories, including recommendation-based, prediction-based, reputation-based, and policy-based. Based on this classification, we reclassify BC-TMSs according to whether there is a need to compute trust values, as shown in Fig. 4. The first category, named trust value-based TMSs, uses specific trust values to express trust. The second category, named trust value-free TMSs, does not distinguish trust relationships in detail, in other words, it does not depend on a fixed trust

evaluation method [41]. The combination of trust value-based and trust value-free systems falls into a hybrid category. We introduce the three categories in detail as below.

1) Trust Value-Based TM: This category uses trust values when determining the trustworthiness of entities. A decision can be made by calculating the trust value of the entity through a trust model [e.g., weighted average models (WAMs)] based on the evidence collected from multiple sources, and then comparing it with a threshold [74]. It can also be the case that trust values are taken to assist the trust model [e.g., game theory models (GTMs)] in making decisions [75]. According to trust evaluation models, we further classify this category into the following five subcategories.

a) Weighted average models: The basis for trustworthiness judgments of IoT entities usually originates from multiple sources, such as direct observations and indirect recommendations. WAM multiplies the data collected from multiple sources with their weights separately, and the result is used as the entity's trust value. This category of model can be divided into *dynamic* WAM and *static* WAM according to whether the weights change throughout the process of trust evaluation.

b) Inference models: IMs use a great deal of trust evidence to achieve a quantitative description of trust through inference. According to underlying theories, it can be divided into TM based on probability theory, TM based on fuzzy theory and TM based on cloud theory.

1) *TM Based on Probability Theory:* With discrete trust evidence, probability-based inference models (IMs) introduce probability distributions or density functions together with likelihood regarding occurrence of events to compute trust values and facilitate trust reasoning [76]. This type of models, including the Bayesian Inference, the Markov Model, the D–S Evidence Theory as well as Subjective Logic, takes the probability value as a measure of trustworthiness. However, these models suffer from such defects as difficulty in acquiring prior knowledge, difficulty in setting up rules, and reliance on some prior assumptions [5].
2) *TM Based on Fuzzy Theory:* The ambiguity of trust is first manifested in the fact that trust is not a binary judgment, but a fuzzy state between trust and distrust, which is difficult to quantify precisely. A model based on fuzzy theory, i.e., fuzzy logic, can cope with imprecision and uncertainty, and achieve a quantitative analysis of trust fuzziness [77]. Nevertheless, it is not flexible enough in integrating prior knowledge [78].
3) *TM Based on Cloud Theory:* It combines fuzzy theory with probability theory, which fully integrates ambiguity and randomness to describe the uncertainty of trust [79]. The cloud model realizes the uncertainty conversion between the concept of trust together with quantitative values through its three characteristic parameters: a) expectation; b) entropy; and c) super-entropy.

c) Graph models: Trust evaluation models based on graph theory can be divided into two types: 1) a graph *simplification-based* approach that simplifies the trust graph to multiple paths with disjoint nodes/edges or directed series-parallel graphs (DSPGs) and 2) a graph *analogy-based* approach that uses reliability theory or mathematical algorithms to directly process the trust graph for trust reasoning [80]. TMSs based on graph models (GMs) are intuitive for expressing trust relationships or trust levels [81].

d) Game theory models: Game theory can model strategic behaviors between different entities [82]. It is also useful for analyzing cooperative behaviors in IoT [83]. If the game has a unique equilibrium, it is easy to predict the behavior of attackers and ensure the security of the interaction process of things [84].

e) ML models: To facilitate learning from massive trust-related data, ML models are used to train and generate general trust predictive models by using the learning algorithms [85]. They can be divided into three categories: 1) *supervised* learning (e.g., decision trees, support vector machines, and artificial neural networks); 2) *unsupervised* learning (e.g., clustering and principal component analysis); and 3) *semi-supervised* learning (e.g., [86] and [87]). Although MLMs can achieve high-evaluation accuracy owing to their strong learning abilities, they suffer from high-computational overhead, large-data dependencies, and low explainability [5].

2) Trust Value-Free TM: In this category, there is no value of trust applied, a security-enhanced TMS is more likely employed. It applies sound security models and cryptographic theories to ensure the trustworthiness of IoT. It involves root trust modules, security policies, certificates, PP schemes to ensure trust relationships in an IoT system [88]. However, this category mainly addresses security issues in IoT, but does not fully consider other attributes of trust (e.g., usability, maintainability, etc.). Moreover, it is still possible for legitimate entities to provide untrustworthy information due to selfish or malicious intentions [35]. We further classify this category into two categories: 1) certificate-based models (CBs) and 2) secure hardware-based models (SHBs).

a) Certificate-based models: Current distributed TMSs are not fully distributed because the overhead of distributed TM is too high for the IoT. Some TMSs still set up pretrusted third-party authority centers, that perform the first step of TM to prevent external attacks, i.e., verifying the identity of entities joining the network and then issuing certificates to authorize their legitimate identities [89]. The issuance of a certificate indicates that the entity is considered as trusted by the trusted third party under some specific conditions. However, certificates alone cannot resist internal attacks [35].

b) Secure hardware-based models: The IoT is concerned with efficiency and productivity in addition to reliability and security. So it is not enough to depend on software-based security solutions to build up trust, a more reliable way to maintain security is to rely on hardware. Popular hardware security techniques used in IoT are trusted computing (TC), trusted execution environment (TEE), etc. [90].

1) *TC:* The main idea of TC is to embed a trusted platform module (TPM) based on cryptography as the root of trust in the existing computing platform, which is gradually extended by certificate or hash code verification to finally establish a trustworthy application environment [91], [92].

2) *TEE:* It is an industry standard written by GlobalPlatform to offer a trustworthy code execution environment for secure data processing [93]. In TEE, only trusted resources can access other trusted resources, so it ensures the integrity and confidentiality of resources within the environment [94].

3) Hybrid TM: This category is a combination of the above two categories. The TMS in this category manages two types of trust conditions: 1) initial trust authentication based on identity authentication and 2) on-going TM based on trust-value evaluation. As a result, the hybrid TMSs are more resilient to potential attacks and have potential to preserve privacy.

B. Trust Value-Based BC-TMSs

In this section, we review trust value-based BC-TMSs, as summarized and compared in Table III.

1) WAMs: To ensure the secure storage and sharing of trust information in IoT environments, Lahbib et al. [95] proposed a BC-TMS. The core part of the system architecture is a management layer embedded with trust managers, authenticators, and miners. The trust manager is responsible for deriving the overall trust score by taking a weighted average of direct and indirect subjective trust, and then sending transactions (e.g., trust scores and established interactions) to the miners. Transactions are packaged into blocks by miners and published on the blockchain through RR consensus. However, the presence of the trust manager indicates this TMS is not fully decentralized. Dy is satisfied by time-driven. Fg is met by continuous trust values. Results of each action completed by the management layer are stored in the blockchain to support Au. Since the blockchain is assumed fully trusted, only attacks against TM (e.g., bad-mouthing attacks) are discussed, thus Ro is partially supported. Ef is not mentioned. Ca, DT, HS, Ic, At, Ex, Sc, and PP are not supported.

In order to provide end-to-end trust between IoT devices and trust in data sources, Dedeoglu et al. [96] proposed a layered architecture (i.e., data layer, blockchain layer, and application layer). For TM, the authors introduced a DT module and a gateway reputation module. The former obtains trust values using a WAM of three types of data: 1) long-term reputation of observers; 2) subjective confidence of source data; and 3) evidence from neighboring observers. The latter provides the participants' reputation information to the blockchain and application layers. However, this architecture requires multiple sensors for the same observation in order to solve the problem of data accuracy, which causes data redundancy [110]. Dy is supported by event-driven. Inspired by [111], i.e., a lightweight and scalable blockchain, the blockchain used for TM can improve the scalability of the proposed trust model and adapt to different contexts, so it satisfies Ca. Fg is met by expressing trust level with continuous trust values. This hierarchy considers both the scale of the IoT network and the scale variation of the blockchain, thus Sc is satisfied. Moreover, the trust value is calculated by considering the trustworthiness of data providers, so that DT is fulfilled. In addition, the architecture considers attacks on both TM and blockchain, so it has sound Ro. Nevertheless, only the computational complexity of trust evaluation is analyzed, which is $O(n^2)$. The blockchain efficiency is not mentioned. HS, Ic, At, Ex, Au, and PP are not supported.

To enable IoT devices to evaluate the trustworthiness of any service provider without depending on any pretrusted entities, Kouicem et al. [50] proposed a decentralized BC-TM protocol (BC-Trust). It has three layers: 1) the IoT layer; 2) the blockchain layer; and 3) the fog node layer. The fog node calculates the recommendation value of a service provider based on the recent transaction recorded in the blockchain and sends it to a device. After completing a service, the device calculates the final trust value using a WAM combining historical trust values, subjective direct observations and indirect recommendations and sends it to its nearest fog node. Finally, the fog node collects the trust value and the service into a block, which is added to the blockchain by applying a joint PBFT and PoS consensus. Trust update is supported in both time-driven and event-driven ways. Fg is met by expressing trust with a continuous value. Ex is satisfied since the authors gave guidelines for selecting trust parameters. In addition, BC-Trust scales very well regarding the blockchain, as well as the IoT network with the support of fog nodes. DT is satisfied as recommenders' trustworthiness is taken into account when aggregating recommendations. Nonetheless, BC-Trust is only available in countering trust-related attacks (e.g., bad-mouthing and ballot-stuffing attacks), indicating Ro is partially satisfied. The communication complexity of TM is $O(1)$, and that of blockchain is $O((sp*N+1)*\log(sp*N))$, where sp is the percentage of service providers. Ca, HS, Ic, At, Au, and PP are not supported.

Putra et al. [97] developed a trust and reputation system (TRS), as a complement to an access control scheme, by using auto-executive smart contracts in blockchain. In TRS, each service consumer's trust score is incorporated into the necessary attributes for accessing resources. Smart contracts store the logic of trust calculation. In the TRS, the trustworthiness and reputation of nodes are calculated based on a WAM that incorporates prior subjective interactions and aggregated trust relationships. The system uses two blockchains: a main public blockchain is responsible for storing access policy, and logic for trust calculation; a private sidechain stores sensitive information, such as user properties. However, the system inherits the latency problems of Ethereum [112]. Trust update is supported in an event-driven way. Ca is supported because an access policy incorporates context parameters. Fg is met by describing trust with continuous scores. Ic is supported since the TRS sets rewards to motivate service consumers to provide honest feedback. Moreover, only network scalability is considered, thus Sc is partially satisfied. The authors considered attacks on trust (e.g., replay attacks) while ignoring attacks on blockchain, thus Ro is partially supported. Additionally, the identity and attribute privacy are preserved by the private sidechain. The authors pointed out that the complexity of trust computation and storage are both $O(1)$. Nevertheless, HS, Ex, DT, and Au are not supported.

To mitigate insider attacks and improve the throughput of vehicular networks, Kudva et al. [98] provided a blockchain-based two-level trust score system. At the first level, vehicles

TABLE III
SUMMARY AND COMPARISON OF TRUST VALUE-BASED BC-TMSS

Cat.	Tech.	Ref.	Su	Dy	Ca	Fg	HS	Ic	At	Ex	Sc	DT	Au	Ro	PP	Ef	App.	Limitations
WAM	Static	[95]	●	TD	○	●	○	○	○	○	○	○	●	AT	○	○	Ind.	Not fully decentralized.
		[96]	●	ED	●	●	○	○	○	○	●	●	○	●	○	T: $O(n^2)$	-	Bring redundancy to TM.
		[50]	●	●	○	●	○	○	○	●	●	●	○	AT	○	T:$O(1)$ B:$O(X)$	-	Preloading data to an edge layer reduces the flexibility of the TMS.
		[97]	●	ED	●	●	○	●	●	○	NS	○	○	AT	Id,Da	T:$O(1)$	-	The system inherits the latency problem of Ethereum.
		[98]	○	●	○	●	○	●	○	○	●	○	○	●	○	○	Tra.	The AODV protocol has several security vulnerabilities.
	Dynamic	[99]	●	ED	○	●	○	○	○	○	NS	●	○	AB	○	○	Tra.	High computational overhead and vulnerable to single point of failures.
		[6]	●	ED	●	●	○	○	○	○	NS	○	○	●	Id	○	Tra.	The protocol for group signatures is not efficient.
		[100]	○	ED	○	●	○	○	○	○	○	●	○	AT	●	○	P.S.	Decentralized database may lead to data integrity problems.
		[101]	○	TD	○	○	○	○	○	○	○	●	○	AT	○	○	Ind.	Long-term data cannot be stored in the blockchain.
		[102]	●	ED	○	●	●	○	○	●	NS	●	●	○	Da	T: $O(n^2)$	-	Not a fully decentralized architecture.
IM	Bayesian Inference	[103]	○	ED	●	●	○	○	○	○	NS	○	○	AT	○	○	Tra.	The authenticity of vehicles' identities cannot be guaranteed.
		[78]	○	ED		●	○	●	○	○	NS	○	○	AT	○	○	Hea.	Blockchain only serves as a database.
		[104]	○	ED	●	●	○	●	●	○	●	●	●	●	○	○	Tra.	Traffic information is removed from blocks.
	Subjective Logic	[105]	●	ED	○	●	○	○	○	○	NS	●	●	●	○	T: $O(n^2)$	Tra.	Limited accuracy in miner reputation calculations.
GM	Analogy-based	[106]	○	TD	○	●	○	●	●	○	●	●	○	AT	○	○	-	Not fully decentralized.
GTM	-	[107]	●	TD	○	○	○	●	●	○	NS	○	○	AT	○	○	-	Lack comprehensive performance evaluation.
MLM	Super-vised	[108]	○	●	●	●	○	○	○	○	NS	●	●	AT	○	○	Tra.	Cannot resist cooperative attacks.
	Unsup-ervised	[109]	○	ED	●	○	●	○	○	○	NS	○	○	●	Da,Ar	○	Cit.	Difficulty in selecting highly correlated input features.

●: Meet the criterion; 'Alphabets': Partially meet; ○: Not meet; '-': Not Available. WAM: Weighted Average Model; IM: Inference Model; GM: Graph Model; GTM: Game Theory Model; MLM: Machine Learning Model; Cat.: Category; Tech.: Technique; Su: Subjectivity; Dy: Dynamicity (TD: Time-Driven, ED: Event-Driven); Ca: Context-awareness; Fg: Fine-grainedness; HS: Heterogeneity Support; Ic: Incentive; At: Autonomy; Ex: Explainability; Sc: Scalability (NS: IoT Network Scalability, BS: Blockchain Scalability); DT: Data Trust; Au: Auditability; Ro: Robustness (AT: Attacks on TM, AB: Attacks on Blockchain); PP: Privacy Preservation (Id: Identity, Da: Data, Ar: Attribute); Ef: Efficiency (T: efficiency of TM, B: efficiency of Blockchain); App.: Application (Cit.: City, Hea.: Healthcare, Tra.: Transport, Ind.: Industry, P.S.: Personal and Social life). X: $(sp * N + 1) * log(sp * N)$.

independently calculate neighbors' trust scores based on the number of matched packets, and then upload transactions containing trust scores to their nearest road side units (RSUs). At the second level, the authorized RSUs aggregate the trust scores of each vehicle by a WAM and then use PBFT consensus to maintain a consortium blockchain. However, their applied ad-hoc on-demand vector (AODV) protocol suffers from several security vulnerabilities and challenges that cannot be ignored [113]. Trust update is supported in both time-driven and event-driven ways. Fg is met since continuous trust values are applied. Ic is somehow provided because the TMS sets a blacklist. If a vehicle in the blacklist behaves normally, its trust value is increased until it is removed from the blacklist. Experimental results show that the time for trust aggregation and consensus does not increase significantly with the number of nodes, thus Sc is satisfied. The system can resist attacks on both TM (e.g, bad-mouthing attacks) and on blockchain verification, such that Ro is considered and satisfied. Nevertheless, Ef is not discussed. Su, Ca, HS, Ic, At, Ex, DT, Au, and Pa are not considered or supported.

To reduce the latency of reputation value queries, Dong et al. [99] proposed a hierarchical blockchain-based vehicle reputation management framework by increasing the capacity of the blockchain. The reputation value is calculated by aggregating the subjective recommendations of other vehicles within the same district through a WAM. The first layer of the framework is a PoW-enabled blockchain hierarchy that records only the reputation values of vehicles from the same

district. The second layer of the framework records a district in the first layer and its neighboring ones to facilitate cross-district querying of vehicle reputation values. The coverage area of the hierarchical blockchain is then expanded layer by layer. Cross-district queries are all performed by RSUs. Trust update is supported in an event-driven way. Fg is met by describing trust with a continuous value. Additionally, vehicular network scalability is supported by a layered architecture, while the scalability of blockchain is not discussed. DT is satisfied since the trustworthiness of vehicles providing recommendations is considered. Ro is partially supported because the authors only considered selfish mining attacks against the blockchain. Experimental results show that the broadcast latency and throughput capacity of the blockchain of this scheme is better than those proposed by [114]. But the efficiency of both TM and blockchain is not specified. Ca, HS, Ic, At, Ex, Au, and PP are not supported or considered.

To ensure the privacy of vehicles in vehicular ad-hoc network (VANET) and the credibility of shared messages, Liu et al. [6] designed a BC-TM scheme named BTCPS, consisting of two components. The first component is responsible for the publication and verification of anonymous messages. The second is responsible for TM through a blockchain. When an event occurs, RSUs receive multiple messages from different vehicles. They first evaluate the reputation of each vehicle based on logistic regression, and then use a WAM to determine the credibility of the messages. Next, RSUs create blocks containing reputation data based on a hybrid consensus algorithm of PoW and PBFT. The trust model incorporates the subjective agreement of peers on the messages. Trust update is supported in an event-driven way. The scheme supports Ca as it takes into account changes in vehicle distribution and driving speed. Fg is met by expressing trust with a continuous value. BTCPS only supports the scalability of VANET, thanks to the distributed nature of RSUs. The authors analyzed attacks from compromised RSUs (i.e., miners) and attacks on TM, thus Ro is satisfied. By using group signatures, BTCPS can maintain the reliability of messages in an imperfectly trusted environment without compromising the identity privacy of vehicles. However, Ef is not discussed. HS, Ic, At, Ex, DT, and Au are not supported or considered.

In an SIoT scenario, Azad et al. [100] proposed a TMS for calculating and updating the trustworthiness of devices in a self-enforced manner. The components of the system include users, IoT devices, and a public Bulletin board (PBB) implemented by blockchain. PBB stores users' public keys, and users' submitted ratings to the PBB after interacting with other users' devices. In each iteration, a user calculates a weighted average of the ratings provided by all devices. The overall reputation of the device is then determined based on the positive or negative of the ratings (i.e., $+1$ or -1). Once the reputation value is calculated, the weights of the users are increased if the ratings they provide are in line with the positive or negative of that value. Trust update is supported in an event-driven way. Fg is met by expressing reputation with a continuous score. DT is supported with noninteractive zero-knowledge proof (NIZK) by applying different weights to the feedback from different users. The authors demonstrated that this system can defend against trust-related attacks through theoretical analysis, thus Ro is partially supported. In addition, identity, data, and attribute privacy are preserved by using homomorphic encryption as well as NIZK techniques. Nevertheless, Ef is not discussed. Su, Ca, HS, Ic, At, Ex, Sc, and Au are not supported or concerned.

In IIoT, by grouping multiple IIoT Devices (IIoT-Ds) into IIoT Groups (IIoT-Gs), IIoT-Ds within a group can share information. To prevent more than half of the malicious devices from spreading misinformation, Wu and Ansari [101] designed a new voting mechanism with trust evaluation for access control in blockchain-based IIoT-G. This article employs trust values to assist in access control. The voting results is determined by trust values and feedback according to an equal-weight voting mechanism. In this system, blockchain is not directly used for TM. Instead, it is deployed in IIoT-D to guarantee access control, and each device stores and maintains its own trust-related information. Trust update is supported in a time-driven way. Based on trust evaluation, different devices are assigned different weights in authorization voting, thus DT is satisfied. Ro is partially supported because the authors only considered attacks on TM, e.g., man-in-the-middle attacks. To summarize, this work only achieves the goals of Dy, DT, and Ro, but neglects other criteria. Ef is not discussed, either.

To compensate the shortcomings of traditional TMS in IoT data exchange, Liu et al. [102] proposed a single-domain and multidomain semi-centralized TMS with the aid of blockchain. IoT devices are centrally organized by cloud servers. Those servers maintain a rating data ledger based on a proposed rotation-based consensus protocol within each domain to support cross-domain data exchange. Trust evaluation is aggregated by cloud servers with direct and indirect trust values, and the weights can be dynamically adjusted. The trust calculation incorporates the trustor's beliefs, thus satisfies subjectivity. Trust update is supported in an event-driven way. HS is satisfied because the TMS considers both single domain and multiple domains. Fg is satisfied by expressing trust with a continuous value. Moreover, the authors provided guidance on the setting of dynamic weights so that explainability is supported to some extent. Sc is partially supported because this article only considers the scale change of IoT devices. DT is satisfied since the trustworthiness of recommenders is considered when calculating indirect trust. Au is also satisfied since the blockchain stores all trust related information (e.g., device historical behaviors). Furthermore, the TMS preserves data privacy by encrypting transmitted data. The computation complexity of TM does not exceed $O(n^2)$. However, Ca, Ic, At, and Ro are not supported.

2) IMs: For enabling vehicles to evaluate the trustworthiness of neighboring vehicles in vehicular networks, Yang et al. [103] proposed a blockchain-based decentralized TMS (DTMS). In this system, vehicles use a Bayesian IM to rate received messages based on the distance between a message sender and an event location. Then, vehicles send those ratings to a nearby RSU. The RSU calculates the trust value of vehicles based on the ratings. Then, it packs the values into a block and competes to add the block into a blockchain using a joint PoW and PoS consensus mechanism. However,

the authenticity of the vehicle's identity cannot be guaranteed in this system. In addition, its TM process does not satisfy auditability because the blockchain only stores trust values, which can cause data tampering if a single RSU is subject to malicious attacks to modify its collection [115]. Trust update is supported in an event-driven way. Ca is considered as contextual information (i.e., location) is involved in trust evaluation. Fg is met by using a continuous value to describe trust. A vehicular network can adapt to the change of the number of vehicles. Nevertheless, the scalability of blockchain is not considered, thereby Sc is only partially supported. In addition, the authors only considered trust-related attacks (e.g., bad-mouthing and ballot-stuffing attacks), thus Ro is partially supported. Moreover, specific rating information is not recorded in the blockchain, which saves storage but fails to support Au [104]. To sum up, this work only achieves the goals of Dy, Ca, Fg, Sc, and Ro, but neglects other criteria. Unfortunately, Ef is not discussed.

To alleviate the problem that IoMT and medical smartphone network (MSN) are vulnerable to insider attacks (e.g., compromising sensitive healthcare data), Meng et al. [78] used blockchain to establish a TMS. They divided the MSN into a traditional MSN layer and a chain layer. A central server in the MSN layer receives packet information from the nodes and uses a Bayesian IM to evaluate their trustworthiness. Then, it updates a node blacklist, which is formed based on the node trust values calculated by the server. The blockchain serves as a database to store features of malicious packets uploaded by MSN nodes. The main drawback is that the system relying on the central server suffers from a single point of failure. Trust update is supported in an event-driven way. Fg is met by expressing trust with a continuous value. Moreover, Ic is supported since applying a dynamic blacklist offers an incentive for nodes to behave honestly and normally for being released from it. Furthermore, Sc is partially satisfied with experimental verification on IoT network scalability. Since the authors only considered internal attacks on TM, thus Ro is partially supported. Ef is not discussed. Su, Ca, HS, At, Ex, DT, Au, and PP are unfortunately not supported.

To improve the auditability of reputation values stored in the RSU, Zhang et al. [104] proposed a BC-TMS for IoV. The process of TM starts with a vehicle by determining the trustworthiness of messages by using a Bayesian IM based on the reputation of other vehicles and their distances from an underlying event. After that, the vehicle rates those messages according to its judgment or by visiting the place where the event occurred, and then uploads its ratings to a nearby RSU. After collecting the ratings, the RSU uses a weighted aggregation algorithm to calculate the reputation value of the rated vehicles by considering the reputation of rating senders. Blockchain is maintained by RSUs using a joint PoW and PoS consensus mechanism. Trust update is supported in an event-driven way. Ca is satisfied as contextual information (i.e., distance) is considered in the reputation calculation. Fg is met by describing trust with a continuous value. Ic is supported since the intensity of TM punishment is higher than that of reward intensity. The authors wrote the reputation value update algorithm into a smart contract, which ensures the autonomy of TM. Moreover, the authors analyzed that the memory scalability of the blockchain is considerable by removing redundant information from the block. DT is satisfied because the vehicle reputation serves as a weight to limit the spread of fraud messages. Additionally, all reputation value list and rating information list are stored in the block so that Au is satisfied. Furthermore, this system can defend against attacks on both TM (e.g., malicious rating attacks) and blockchain (i.e., attacks on consensus nodes), indicating Ro is supported. Nonetheless, Ef is not discussed. Su, HS, Ex, and PP are not supported.

To further improve the data security of IoV, Kang et al. [105] proposed a two-stage soft security solution (i.e., miner selection and block verification) based on a DPoS consensus mechanism. The solution uses a multiweight subjective logic model in order to combine trust values at local (i.e., past interactions with miner candidates) and stored on a blockchain (i.e., recommendations from other vehicles) for miner (i.e., RSU) reputation management, and then incents high-reputation miners to participate in block verification. The blockchain stores reputation related information. However, the accuracy of miner reputation calculation is low [116]. Trust update is supported in an event-driven way. Fg is satisfied by expressing trust with a continuous value. Sc is partially supported because the scalability of blockchain is not considered. DT is satisfied since different opinions and recommenders have different weights. The trust-related information (e.g., vehicle sharing data, reputation opinions on RSUs, and miners) stored on the blockchain enables auditing. According to experimental results, this solution can defend the collusion attacks on TM and block validation, thus Ro is supported. The complexity of reputation calculation is $O(n^2)$, while blockchain efficiency is not mentioned. Ca, HS, Ic, At, Ex, and PP are not satisfied.

3) GMs: To accommodate the dynamic security needs of IoT devices, Wang et al. [106] designed a TMS to implement a lightweight attribute-based access control framework for blockchain-empowered IoT. All historical access requests and authorization results are recorded in a Proof-of-Authority (PoA)-based blockchain. The system uses these records to construct a GM. A Markov random walk is performed on the model to calculate the trustworthiness that measures the reliability probability regarding a target device. Trust update is supported in a time-driven way. Fg is met by describing trust with a continuous value. Ic is supported since when bad behavior occurs, punishment is much higher than a reward when normal behavior occurs. Smart contracts are responsible for automatically updating the attributes and trust values of IoT devices, thus At is satisfied. Experimental results prove that the system can well adapt to the scale changes of IoT and blockchain networks, thus Sc is supported. Moreover, DT is satisfied because pretrusted nodes occupy a larger percentage of recommendations than other nodes in trust evaluation. Ro is partially supported since the authors only analyzed attacks against TM, e.g., Sybil attacks and replay attacks. Ef is not mentioned. Su, Ca, HS, Ex, Au, and PP are not supported.

4) GTMs: In order to prevent malicious nodes from sending false scores to maintain robustness among nodes, Esposito et al. [107] proposed a decentralized TM mechanism based on game theory. The mechanism simulates the

TABLE IV
SUMMARY AND COMPARISON OF TRUST VALUE-FREE BC-TMSS

Cat.	Tech.	Ref.	Su	Dy	Ca	Fg	HS	Ic	At	Ex	Sc	DT	Au	Ro	PP	Ef	App.	Limitations
SHB	TC	[117]	○	○	○	-	○	○	●	-	●	-	○	●	Id	○	Tra.	Neglect to evaluate the credibility of messages.
		[118]	○	○	○	-	○	○	○	-	○	-	●	AT	○	○	-	Vulnerable to single point of failures.

●: Meet the criterion; 'Alphabets': Partially meet; ○: Not meet; '-': Not Available. SHB: Secure Hardware-Based; TC: Trusted Computing; Cat.: Category; Tech.: Technique; Su: Subjectivity; Dy: Dynamicity (TD: Time-Driven, ED: Event-Driven); Ca: Context-awareness; Fg: Fine-grainedness; HS: Heterogeneity Support; Ic: Incentive; At: Autonomy; Ex: Explainability; Sc: Scalability (NS: IoT Network Scalability, BS: Blockchain Scalability); DT: Data Trust; Au: Auditability; Ro: Robustness (AT: Attacks on TM, AB: Attacks on Blockchain); PP: Privacy Preservation (Id: Identity, Da: Data, Ar: Attribute); Ef: Efficiency (T: efficiency of TM, B: efficiency of Blockchain); App.: Application (Cit.: City, Hea.: Healthcare, Tra.: Transport, Ind.: Industry, P.S.: Personal and Social life).

interaction between IoT nodes and edge nodes by rejecting scores that may not be realistic. Specifically, the evolved Dempster–Shafer theory is used to combine the collected scores to update the trustworthiness of the nodes by excluding different scores far from the majority. To perform trust calculation, the mechanism uses fuzzy theory to classify trust as none, low, medium, high, and absolutely. The calculation also considers some subjective information (e.g., trustor belief). Besides, a blockchain is maintained by edges nodes for storing reputation scores. A smart contract is deployed to periodically store reputation scores, enabling the autonomy of TM. Trust update is supported in a time-driven way. Ic is satisfied since the payoff structure between nodes resembles a "gift-giving" game. Experimental results show that the mechanism has good scalability in terms of IoT network scale while ignoring the scale of blockchain, so it partially achieves the goal of Sc. This mechanism rejects possibly untrue scores to prevent attacks on TM. However, it lacks robustness evaluation regarding attacks on blockchain, so that Ro is partially satisfied. The performance evaluation of the proposed mechanism is not comprehensive [119]. Ef is not mentioned. Ca, Fg, HS, Ex, DT, Au, and PP are not supported.

5) MLMs: Zhang et al. [108] proposed an AI-based TMS (AIT) for a blockchain-based vehicle network. The TMS performs trust evaluation with two steps, local evaluation and global evaluation. First, vehicles apply a feedforward neural network (FNN) to calculate the local trust levels (LTLs) of nearby vehicles and report them to a local RSU. Then, the RSU aggregates the collected reporting results and also applies an FNN to calculate the global trust levels (GTLs) of vehicles. Finally, the final GTL of each vehicle is the average of the trust levels computed by all RSUs. Blockchain is used to store GTLs of vehicles. Trust update is supported in both time and event-driven ways. Ca is supported since this system takes multiple context information into account. Fg is met by expressing trust with a continuous value. Sc is partially supported since the scalability of the blockchain is ignored. DT is also satisfied because vehicles calculate LTLs by considering the current trust rating of a reporting vehicle. Furthermore, the RSU can track all transaction history of all vehicles located within its direct communication range through the blockchain, indicating that Au is well fulfilled. Ro is partially supported as only attacks on TM are considered, i.e., bad-mouthing attacks and on–off attacks. The efficiency of TM and blockchain is not mentioned. Su, HS, Ic, At, Ex, and PP are not supported.

To build a sustainable smart city, Kumar et al. [109] proposed a trustworthy privacy-preserving secured framework (TP2SF). The framework integrates blockchain and ML algorithms (i.e., XGBoost) to detect suspicious activities in smart city networks for TM, privacy protection, and intrusion detection. Specifically, a TMS calculates a reputation score for each registered IoT node based on transactions and confidence thresholds. A blockchain is maintained by fog nodes, which store reputation scores and trust evidence. Trust update is supported in an event-driven way. Ca is also satisfied because ML algorithms can easily update model parameters in real-time IoT-driven applications of smart city. HS is also supported since the framework can adapt to heterogeneous networks in smart cities. Furthermore, the framework uses fog nodes to accommodate the scalability of the network, while ignoring the scalability of blockchain. The authors considered attacks on TM (e.g., poisoning attacks of ML models) and attacks on blockchain (e.g., 51% attacks), so that Ro is supported. PP is partially supported because two-level privacy protection technology can preserve data and attribute privacy. The first level protects raw data by using enhanced PoW (ePoW) techniques. The second level uses pearson correlation coefficient (PCC) and principal component analysis (PCA) techniques to convert the obtained attributes into a coded format for further protection. However, Ef is not mentioned. Su, Fg, Ic, At, Ex, DT, and Au are not supported.

C. Trust Value-Free BC-TMSs

In this section, we review existing trust value-free BC-TMSs by classify them into two categories: 1) CBs and 2) SHBs. However, the works purely based on certificates do not exist at the moment. This may be because CBs cannot provide sufficient security and flexibility for current complex IoT networks. Table IV summarizes and compares the trust value-free BC-TMSs. Note that Fg, Ex, and DT are not related in this type of BC-TMSs since they regards to trust value evaluation.

1) SHBs: To establish trust in IoV and satisfy the four-way tradeoff of blockchain (i.e., scalability, security, decentralization, and latency), Javaid et al. [117] proposed a scalable blockchain-based protocol using physical unclonable functions (PUFs), certificates, auto-executing smart contracts, and a Dynamic PoW (DPoW) consensus algorithm. PUFs are used for vehicle authentication and trust establishment. However, the protocol does not evaluate the trustworthiness of messages, so a trusted vehicle can broadcast a forged message

TABLE V
SUMMARY AND COMPARISON OF HYBRID BC-TMSS

Cat.	Tech.	Ref.	Su	Dy	Ca	Fg	HS	Ic	At	Ex	Sc	DT	Au	Ro	PP	Ef	App.	Limitations
CB	WAM	[121]	○	ED	●	○	○	●	○	○	NS	○	●	○	Id	T: $O(logn)$	Tra.	Lack of details on how reputation is established.
		[114]	○	ED	○	●	○	○	●	○	NS	●	●	●	Id,Da	○	Ind.	The Ethereum utilized by the system is not well suited for IIoT.
		[7]	○	TD	○	●	○	●	●	○	●	○	●	○	Id,Da	○	Tra.	Only available when malicious vehicles are in the minority.
		[122]	●	ED	○	●	●	○	○	○	NS	○	●	AT	○	○	-	Not a fully decentralized architecture.
		[49]	●	ED	○	●	○	○	●	○	○	●	●	AT	Id,Ar	○	Ind.	Lack of experiments to validate the framework well.
	IM	[89]	○	ED	●	○	○	●	○	○	NS	○	●	AT	Id,Da	○	Tra.	This TMS does not address the location privacy issues.
		[123]	○	TD	○	○	○	●	○	○	○	○	●	AT	Id	○	Tra.	Not a fully decentralized architecture.
SHB (TEE)	WAM	[35]	○	TD	○	●	○	●	○	○	NS	○	○	●	Id,Da	○	Tra.	Lack of explanation of trust model weights.
	MLM	[110]	○	TD	○	●	○	○	●	○	NS	○	●	AB	○	○	-	There are hidden dangers for off-chain trusted workers.
SHB (TC)	WAM	[124]	○	ED	●	●	●	○	○	○	NS	○	○	AT	Id,Da	○	-	The detailed implementation of the model was not presented.
		[125]	●	ED	●	●	●	●	●	○	NS	●	○	○	Id,Ar	○	-	Lack experiments and performance analysis.

●: Meet the criterion; 'Alphabets': Partially meet; ○: Not meet; '-': Not Available. CB: Certificate-Based; SHB: Secure Hardware-Based; TEE: Trusted Execution Environment; TC: Trusted Computing; WAM: Weighted Average Model; IM: Inference Model; MLM: Machine Learning Model; Cat.: Category; Tech.: Technique; Su: Subjectivity; Dy: Dynamicity (TD: Time-Driven, ED: Event-Driven); Ca: Context-awareness; Fg: Fine-grainedness; HS: Heterogeneity Support; Ic: Incentive; At: Autonomy; Ex: Explainability; Sc: Scalability (NS: IoT Network Scalability, BS: Blockchain Scalability; DT: Data Trust; Au: Auditability; Ro: Robustness (AT: Attacks on TM, AB: Attacks on Blockchain; PP: Privacy Preservation (Id: Identity, Da: Data, Ar: Attribute); Ef: Efficiency (T: efficiency of TM, B: efficiency of Blockchain); App.: Application (Cit.: City, Hea.: Healthcare, Tra.: Transport, Ind.: Industry, P.S.: Personal and Social life).

without being detected [120]. Additionally, the blockchain and smart contracts are hosted by RSUs as blockchain miners to manage vehicle registration. DPoW allows the protocol to scale according to the data traffic generated by vehicles. Experimental results indicate that the protocol is scalable regarding the scales of both the vehicular network and the blockchain. Furthermore, the protocol is resistant to attacks on TM (e.g., replay attacks), attacks on entities (e.g., cloning attacks), and attacks on the blockchain (e.g., 51% attacks), indicating that Ro is well supported. The physical properties of PUFs and certificates can preserve identity privacy. This work only supports At, Sc, Ro, and PP. Ef is not mentioned.

To ensure endpoint reliability in IoT, Zhang et al. [118] combined blockchain with trusted network connect protocol (BTNC) for shared authentication, platform verification, and trusted network access. BTNC has two phases: 1) an initialization phase and 2) a trusted network connect (TNC) phase. In the initialization phase, a trusted third party verifies the registration information generated by endpoints, and then constructs a base transaction and eventually includes it in the blockchain. In the TNC phase, the endpoints perform blockchain-based user authentication and platform authentication with each other to gain trust. Then, the update transaction can be constructed and eventually included in the blockchain. However, registration at the trusted third-party authority is vulnerable to a single point of failure. All transaction information generated by endpoints is recorded on blockchain to support the auditability of TM process. BTNC is only resistant to attacks on TM, such as unauthorized users, so it partially supports Ro. This work only supports Au and Ro. Ef is not mentioned.

D. Hybrid BC-TMSs

In this section, we review existing Hybrid BC-TMSs that apply both trust value-based and trust value-free TMSs. Table V summarizes and compares the reviewed works.

To protect the privacy of vehicles while managing trust in VANETs, Lu et al. [121] proposed a blockchain-based anonymous reputation system (BARS). BARS simultaneously maintains three blockchains, i.e., CerBC for storing vehicle certificates, including reputation scores, RevBC for storing revoked public keys, and MesBC for recording all broadcasted messages. The vehicle's reputation score is used to determine the trust level of broadcasted messages based on direct historical interactions and indirect recommendations. However, Feng et al. did not elaborate on how the reputation is established, and BARS cannot prevent malicious behavior in advance [126]. The blockchain with PoW consensus mechanism is maintained by RSU. Trust update is supported in an event-driven way. Ca is satisfied since the relative density of vehicles affects the reputation score. Ic is supported because the system adds incentive and penalty mechanisms in TM. In addition, BARS supports network scalability owing to the distributed nature of RSUs, but it does not consider

that of the blockchains. Besides, all broadcast messages are recorded in MesBC as persistent evidence for evaluating each vehicle's reputation, thus Au is supported. Identity privacy is preserved because the certificate eliminates the linkability between the public key of a vehicle and its real identity. SHA-256-based proof of existence and proof of absence stored on the blockchain are used to find certificates for TM, which can be done with the complexity of both time and space as $O(\log n)$. However, Su, Fg, HS, At, Ex, DT, and Ro are not supported.

Focusing on reputation management for IIoT retail marketing, Liu et al. [114] proposed an anonymous reputation system (ARS-PS) based on a PoS-enabled blockchain. The ARS-PS allows retailers to build reputation by selling products to consumers and aggregating anonymous post-sale reviews. The blockchain maintained by registered retailers ensures that the retailer's reputation building process is transparent to the public. However, the traditional blockchain platform utilized by the system (i.e., Ethereum) cannot provide fast consensus due to the distributed nodes in the IIoT system [127]. Trust update is supported in an event-driven way. Fg is met by expressing reputation with a continuous score. The authors used smart contracts to help automating reputation aggregation and revelation. Moreover, the authors demonstrated that ARS-PS is scalable for IIoT networks through experiments, but ignores the scalability of the blockchain, so that Sc is partially satisfied. In addition, the system ensures that valid reviews originate from different consumers, thus DT is satisfied. Since the review generation and reputation accumulation process is transparent and all retailers and consumers can be publicly verified, Au is supported. Theoretical analysis indicates that ARS-PS is robust against attacks on blockchain as well as trust evaluation, e.g., Sybil attacks and bad-mouthing attacks, thus Ro is fully met. Anonymous identity credentials protect identity privacy and anonymous rating tokens protect data privacy. Ef is not discussed. Su, Ca, HS, Ic, and Ex are not supported or considered.

To address the scalability problem of TM in IoV, Singh et al. [7] proposed an adaptive TMS. It enables event detection and verification between vehicles through smart contract auto-execution and sharded blockchain networks deployed within RSUs. The architecture of system has three important planes: 1) a vehicle plane; 2) a set of RSUs as an edge computing plane (to maintain a blockchain); and 3) a central service plane. A certificate authority issues certificates to ensure communication security and privacy. RSUs collaborate to maintain and update vehicle trust values. However, the proposed TMS is effective for event verification only when malicious vehicles are in minority [128]. Trust update is supported in a time-driven way. Fg is met by describing trust with a continuous value. Ic is satisfied because an incentive mechanism is introduced that rewards well-behaved vehicles. The division of regions and the setup of RSUs as edge nodes make the IoV scalable, and blockchain sharding also improves scalability. In addition, the smart contract contains not only trust-related information but also information, such as reports, addresses, and status of vehicles, thus supporting auditing. Identity and data privacy are preserved by certificates mentioned above. Nevertheless, Ef is not discussed. Su, Ca, HS, Ex, DT, and Ro are not supported or concerned.

To solve the current problem of device identity authentication based on a centralized certificate authority, Hameed et al. [122] proposed a scalable solution for IoT sensor TM with the aid of blockchain and software defined network (SDN). The blockchain is used for data storage and SDN is used for routing network traffic. A trust index is calculated by combining trust history and currently submitted subjective experience values, both of which are stored in the blockchain. Trust update is supported in an event-driven way. Fg is met by expressing trust with continuous index value. The introduction of SDN can solve the problem of IoT network heterogeneity at a controller level, thus HS is satisfied. Experimental results show that the solution has good scalability to the number of IoT nodes and data packets. But there is a lack of experiments to show the scalability of blockchain. In addition, blockchain stores historical trust-related information of IoT devices in the network, so Au is enabled. Ro is partially satisfied because the authors only pointed out that SDN can mitigate attacks on trust (e.g., spoof attacks and DoS attacks). Ef is not discussed. Ca, Ic, At, Ex, DT, and PP are not supported or considered.

To address the problems of traditional supply chain management (e.g., easy data tampering and low trustworthiness), Wu and Zhang [49] proposed a blockchain-enabled supply chain TM framework for smart manufacturing. The framework uses certificates and an improved EigenTrust algorithm [129] to evaluate the trustworthiness of entities (i.e., global trust). The evaluation data sources consist of local trust and subjective recommendation trust. Blockchain provides an open data tracking and storage platform for supply chain networks. Trust update is supported in an event-driven way. Fg is met by expressing trust with a continuous value. The authors introduced smart contracts to restrain malicious behaviors, thus supporting autonomy. Since the trustworthiness of peer nodes determines the trustworthiness of their recommendations, thus DT is satisfied. Moreover, the framework supports auditability of all transactions. However, it can only resist attacks on TM (i.e., coordinated attacks) and thus partially supports Ro. In addition, storing the hashes of original data involved on the chain ensures critical attributes' privacy. And identity privacy is preserved by issuing digital pseudonym identities to nodes. Nevertheless, Ef is not discussed. Ca, HS, Ic, Ex, and Sc are not supported.

To protect the privacy of vehicle location in VANET, Li et al. [89] proposed a BC-TMS. In the process of TM, RSUs use a Dirichlet Distribution-based Bayesian IM to evaluate vehicles behaviors based on query spatial rationality and query frequency rationality. After that, corresponding trust ratings are made based on evaluation results. Moreover, the system maintains two blockchains: a blockchain named CerBC for certificate management, and a blockchain called ReqBC for recording all service query requests. They are maintained by RSUs using HotStuff consensus. However, this TMS does not

address the location privacy issues [130]. Trust update is supported in an event-driven way. Ca is supported since location information is involved in the trust evaluation process. Fg is met by expressing trust with a continuous rating value. Ic is supported because the TMS adopts an incentive model driven by trust. Besides, the authors only analyzed the scalability of the VANET, thus Sc is partially supported. Au is satisfied because all historical trust information of vehicles is recorded on the blockchain. Moreover, the system is only resilient to attacks on TM, e.g., on-off attacks and white-washing attacks, thus Ro is partially supported. It preserves identity privacy of vehicles by means of certificates and data privacy by establishing anonymous cloaking regions. Ef is not mentioned. Su, HS, At, Ex, and DT are not supported.

To overcome the shortcomings of existing authentication mechanisms and TM models for IoV, Yang et al. [123] proposed a TM model supported by blockchain. Vehicles and RSUs are first registered with a certification authority center. Then, the model uses Dirichlet distribution to compute vehicle ratings, applying reputation regression to periodically pack the ratings into blocks, and adopting a punishment revocation mechanism to dynamically adjust the trust status of vehicles. However, this model is not fully decentralized. Trust update is supported in a time-driven way. Ic is supported with a punishment revocation mechanism. Au is satisfied since records verified by a fully trusted cloud are packed and stored on the blockchain for subsequent reputation tracing. Ro is partially supported since the model is only proven to be effective against attacks on TM (e.g., slander attacks). In addition, to prevent identity tracking, each vehicle has multiple pairs of spare keys. However, Ef is not discussed. Su, Ca, Fg, HS, At, Ex, Sc, and DT are not supported.

To break the limitations of traditional public key infrastructure (PKI) technology (e.g., there exist untrusted but legitimate message publishers and single point of failures [131]), Chen et al. [35] proposed a DTMS for intelligent transportation, creatively applying TEE to secure trust evaluation. DTMS has two layers: a bottom service layer supports the operation of message rating and block verification; a top consortium layer maintains trust evaluation and incentives, and block consensus. A global trust credit of a vehicle is a weighted average of the rate on its message rating behavior, the rate on its message sending behavior, and its historical trust credits. The blockchain is used to store the global trust credits. Furthermore, DTMS improves blockchain efficiency by allowing trusted nodes to participate in verification and consensus. However, the weights corresponding to each component in the trust model were not explained [132]. Trust update is supported in a time-driven way. Fg is met by expressing trust with a continuous credit value. DTMS incorporates incentives to stimulate active participation and punish malicious behaviors, thus satisfying Ic. In addition, its layered design enhances the scalability of the system. However, the scalability of the blockchain is not analyzed. Ro is also supported since it uses TEE to resist attacks on TM (e.g., Sybil attacks, bad-mouthing, and ballot-stuffing attacks) and attacks on blockchain (e.g., compromised base stations). Each vehicle registers a unique pseudonym identity into the system to preserve identity privacy. And all transmitted data are encrypted to preserve data privacy. Nevertheless, Ef is not discussed. Su, Ca, HS, At, Ex, DT, and Au are not supported.

To address the risk at the cloud and the edge, Ranathunga et al. [110] proposed a novel cross-layer intelligent trust evaluation model that leverages ML and blockchain for decentralized TM in the IoT ecosystem. The trust evaluation model consists of two parts: 1) off-chain trusted workers and 2) on-chain auto-executed smart contracts. The on-chain smart contract is used to manage IoT assets and trusted workers' identities, record the outputs of trusted workers, as well as calculate the reputations of IoT nodes based on these outputs. The functions of the off-chain trusted worker are executed in the TEE to ensure that related code and data are protected. Trust update is supported in a time-driven way. Fg is met by describing reputation with a continuous score. The authors conducted a preliminary evaluation to verify the performance of the model in terms of scalability, but does not validate blockchain scalability, thus Sc is partially satisfied. In addition, the blockchain records node reputation and the trust related evidence, so Au is supported. Ro is partially supported because the authors only considered attacks on blockchain (e.g., flooding attacks) under simulated scenarios. However, Ef is not mentioned. Su, Ca, HS, Ic, Ex, DT, and PP are not supported.

To overcome the drawback that traditional PKI models rely on a common root of trust and do not fit well into heterogeneous IoT ecosystems, Di Pietro et al. [124] proposed a distributed trust model in combination with reputation scores. The model leverages existing trust domains and bridges them to create end-to-end trust among IoT devices. The bridging is designed with a three-way handshake access control protocol as a secure hardware-based TMS. In addition, the authors defined a built-in reputation mechanism in the blockchain called "obligation chain" that records the entire history of obligation provision performance. Reputation is the average value of on-time performance of obligations. However, the authors did not show detailed model implementation [133]. Trust update is supported in an event-driven way. Ca is satisfied because the model is not dependent on specific scenarios. Fg is met by expressing reputation with a continuous score. HS is supported because the model is specifically proposed for addressing trust between heterogeneous trust domains. Nevertheless, the model meets the goal of IoT network scalability while ignoring blockchain scalability. Moreover, this model only considers attacks on TM (e.g., rating fraud attacks) and ignores attacks on the blockchain, so Ro is partially satisfied. The authors used PKI for hiding real identities to preserve identity privacy and applied encryption for data communications to preserve data privacy. Ef is not discussed. Su, Ic, At, Ex, DT, and Au are not supported.

To achieve cross-platform access control, Tang et al. [125] proposed a blockchain-based trust framework called IoT Passport, which, like [124], treats a platform as a trust domain. The framework is constructed mainly based on various policies that enable platforms to establish arbitrary trust relationships with each other. The trust value is used as an attribute of the IoT device, which is related to the duration of trust between two collaborators, the collaborators' trust in their peers, and

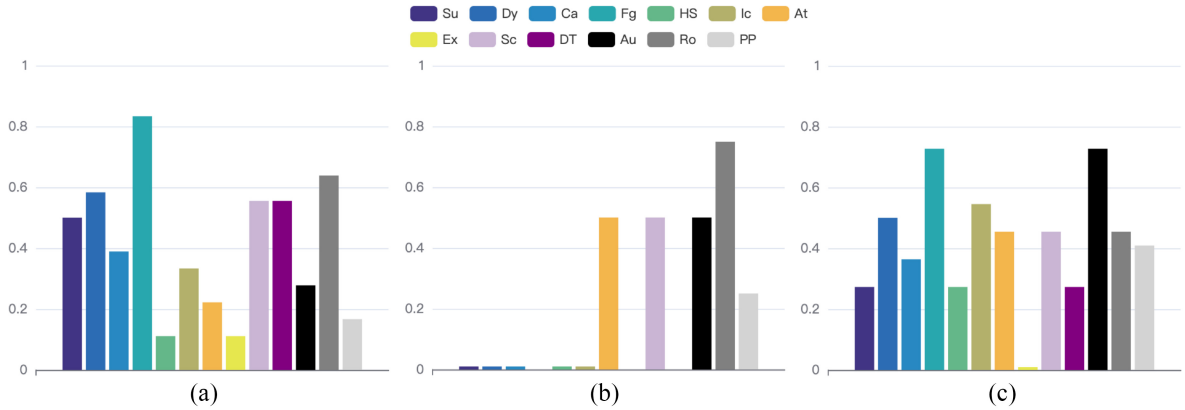

Fig. 5. Statistical bar charts of evaluation criteria satisfaction. Where the vertical coordinate is the percentage of the number of papers that meet the evaluation criteria to the total number of papers in a corresponding category. Fully meet and partially meet are counted as 1 and 0.5, respectively, not meet and not available is counted as 0. (a) Trust value-based. (b) Trust value-false. (c) Hybrid.

the degree of subjective satisfaction. Trust update is supported in an event-driven way. Moreover, Ca is satisfied since the framework is able to adapt to fragmented requirements, changing contexts and arbitrary properties. Fg is met by describing trust with a continuous value. HS is supported by the cross-platform property of the framework. Sc is partially supported since the blockchain scalability is not discussed. DT is satisfied since the credibility of the collaborators is taken into account when aggregating the satisfaction degrees of the collaborators of their peers. Auto-executed smart contracts and proper encryption are utilized to preserve identity privacy and to prevent misuse of user attributes. However, Ef is not discussed. Ic, Ex, DT, Au, and Ro are not supported.

E. Discussion

Fig. 5 shows statistical bar charts of evaluation criteria satisfaction regarding the three types of BC-TMSs. Note that in order to distinguish the two cases: 1) "none of the papers in this category satisfy a criterion" and 2) "this criterion cannot be evaluated in this category," we set the former case to a very small value in the figure for easy observation. Fig. 5(a) presents the statistical results of trust value-based BC-TMSs, which stand at an important position among the three types of BC-TMSs and become a preferred and less error-prone choice of researchers. As one of the basic attributes of trust, subjectivity was satisfied in exactly half of our reviewed works, leaving half of the work choosing objective factors as evidence for trust assessment. Less than half of the reviewed trust value-based BC-TMSs satisfy context-awareness, which shows that most of them are developed for specific scenarios and lack generality. Only two works [102], [109] support heterogeneity, which refers to that an IoT network covers a number of network domains with different types of network structures. This implies that most works support sharing trust evidence and trust evaluation results in a single network domain. However, malicious devices in a multidomain IoT system may keep switching domains to launch white-washing attacks. Besides, auditability and PP are generally neglected, which motivates us to make efforts to research effective solutions. Autonomy is poorly satisfied, requiring researchers to investigate by fully making use of the potential of blockchain. Explainability is even satisfied by only two papers [50], [102], which requests special study as it can enhance the trustworthiness of trust models from a human perspective. According to the figure, the satisfaction of robustness is relatively impressive and in line with the security demands of TMSs. Looking at the details of our reviews, we find that existing works focus on two types of trust-related attacks, i.e., bad-mouthing attacks and ballot-stuffing attacks. This may be because trust value-based trust models mostly take into account peer recommendations. In summary, trust value-based TMSs can obtain fine-grained trust values, and different thresholds can be set to meet diverse security requirements. However, achieving efficient trust calculation and low storage of trust-related information is not a trivial task.

Turning to Fig. 5(b), we do not count fine-grainedness, DT and explainability as they are not applicable to trust value-free BC-TMSs. It is worth noting that the results may be contingent due to few relevant works (only [117] and [118]). This implies that a TMS without trust value evaluation does not adequately enable a trustworthy IoT. The reasons may be as follows. First, the trust relationship considered in the trust value-free BC-TMSs is normally static and objective compared to the trust value-based BC-TMSs, i.e., it cannot be updated frequently once it is determined. Thus, the trust value-free TMSs lack sustainability and are less sensitive to environmental changes. Second, this type of TMSs lacks trust information exchange among network nodes, making the trust relationship within the network relatively loose and fragile. In addition, such TMSs mainly make a binary judgment about trust, i.e., trust and distrust, leading to low flexibility. In summary, this type of TMSs has low flexibility and is insensitive to the change of trust, but is suitable for applying into the IoT scenarios with high privacy requirements.

Looking at Fig. 5(c), the hybrid BC-TMSs integrate the above two systems by making use of the advantages of both. Notably, they pay attention to PP. Thanks to the trust value-free TMSs. The basis of certificate-based TMSs is cryptography, which is essentially suitable for protecting privacy. Besides, as a TMS based on secure hardware, TEE is a secure zone created by a combination of TC and virtualization

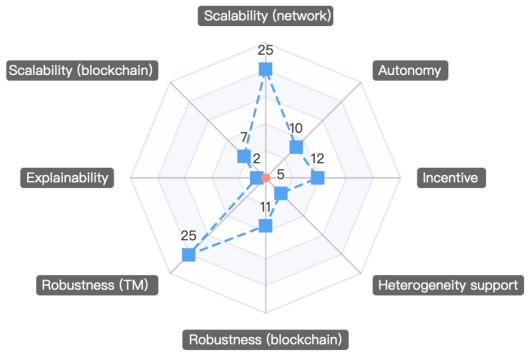

Fig. 6. Radar chart regarding the representative criteria obtained from the statistical results of evaluation criteria satisfaction.

isolation technologies. This zone ensures that computing is not interfered by regular operating systems, which ensures loaded codes (e.g., a trust evaluation algorithm) and data (e.g., trust-related data) are protected in terms of confidentiality and integrity [134]. Similarly, auditability has received attention, probably because hybrid BC-TMSs require additional information to be recorded and thus facilitate the auditing of trust results. However, the satisfaction in terms of all evaluation criteria is still not enough. No works support explainability, which deserves our attention and efforts. In addition, context-awareness, HS, autonomy and DT need to be continuously strengthened. To sum up, the current hybrid BC-TMSs are able to not only leverage trust values to satisfy diverse requirements but also maintain a secure and privacy-preserving environment with the help of sound certificate-based and SHBs.

V. Open Issues and Future Directions

Based on the above in-depth review and the statistical results regarding representative performance evaluation criteria in Fig. 6, in this section, we first analyze the challenges and issues faced by BC-TMSs in IoT. Then, we provide some suggestions in order to guide future research directions.

A. Explainability

1) Open Issues: Explainability is generally neglected by existing studies. This may be because achieving explainability requires relatively cumbersome steps in analysis, justification, and visualization. For example, in a weighted average-based TMS, analysis, and justification are needed on how initial parameters were chosen, how the changes of the parameters affect the final trust evaluation results, and why these occur. In other words, a reasonable explanation needs to be given to make it easy for users to understand. Ignoring explanation not only makes a trust model less convincing but also makes researchers confused on how to optimize the model. Some studies attempt to support explainability by first continuously adjusting experimental parameters and then performing analysis, but this "brute force approach" is sometimes unconvincing [50]. Other studies use mathematical methods to analyze parameter settings, but these methods lack intuitive representation [102]. In general, the existing works have not yet offer sound explainability with regard to trust models.

2) Future Research Directions: From the subjective point of view, it is suggested to encourage researchers to design logically clear ablation experiments and give detailed explanations to facilitate a good understanding of trust models. Besides, since subjectivity is a nature of trust, focusing on user experience and understanding their concerns through questionnaires could be useful in improving the explainability and trustworthiness of trust models. From the objective point of view, improving explainability with the aid of relevant techniques is promising. For example, model-diagnostic techniques for post-hoc explainability could realize trust-related feature visualization, achieve tractability by providing a reference for trust model optimization, and reduce model complexity [135]. These techniques can also be applied into trust models to enhance their trustworthiness.

B. Efficiency

1) Open Issues: Efficiency and energy consumption are overlooked in existing works. IoT devices typically have limited battery storage, while blockchain is a technology with high-energy demands. If too much energy is consumed in the process of TM, it could hinder its practical deployment for IoT. Many studies have only studied the efficiency of TMSs, but ignored the efficiency of blockchain. Nevertheless, the cost of blockchain is generally higher than that of TM. There are many factors that affect blockchain efficiency, the most important of which is the performance of consensus mechanism. The widely used consensus mechanisms, e.g., PoW, have been strongly criticized due to its high and useless energy consumption [136]. In a word, it is of great importance to consider the efficiency of both TM and blockchain, as it affects the practical deployment of BC-TMSs.

2) Future Research Directions: To improve the efficiency of BC-TMSs in IoT, three aspects need further investigation: 1) blockchain; 2) TM; and 3) IoT devices. For blockchain, since its main network architecture is P2P, a fast settlement protocol should be established to allow multiple entities to transact simultaneously [137]. In addition, it is feasible to use lightweight consensus mechanisms, e.g., Proof-of-Trust (PoT) [39], [43], [138], to improve the effectiveness of the system compared to other blockchain systems. Alternatively, designing a blockchain system architecture suitable for IoT could be a good solution for improving the efficiency of BC-TMSs. According to existing research, a fully distributed network architecture is not the most suitable architecture for IoT application scenarios, while a multilayer scalable blockchain architecture (e.g., fog/edge node layer and off-chain layer) could be more effectively compatible with the original functions of IoT while taking the advantages of blockchain. For TM, it is suggested to reduce the times of communications for evaluating trustworthiness, since communication is the most energy-consuming task on the IoT devices [139]. For IoT devices, in addition to improving their power storage and computational capacity, green technologies are highly expected. Besides, parallel processing of big

data (e.g., MapReduce [140] and cloud computing [141]), backscatter communication [142] and 6G technologies [143] should be applied to improve processing, communication and connectivity efficiency.

C. Heterogeneity Support

1) Open Issues: There are relatively few existing BC-TMSs to support IoT network domain heterogeneity. IoT is used in various domains (e.g., smart transportation, advanced manufacturing, and smart cities) due to its inherent heterogeneity to provide diverse and convenient services for our routine life through wireless sensor networks, mobile communication networks, and vehicle networks, etc. [144]. If a TMS cannot support the heterogeneity of network domains, it cannot assist the IoT in achieving the goal of interconnecting everything in the world. Therefore, lacking HS is still a major open issue of BC-TMSs.

2) Future Research Directions: Emerging technologies should be investigated with regard to BC-TMSs to support the heterogeneity of IoT. Network softwarization [145] technology is innovative and attractive. It can separate the software that enables IoT network functions and services from hardware to facilitate the unification of heterogeneous network TM. Moreover, artificial intelligence techniques are worthy of further research for supporting seamless data exchange and cross-domain trust evaluation in heterogeneous networks. For example, federated learning, an emerging learning framework, allows aggregation of heterogeneous data (e.g., trust-related data) by convening the participation of different network domains.

D. Privacy Preservation

1) Open Issues: Privacy is not satisfactorily preserved, which relates not only data, but also identity and its linked attributes. On the one hand, data interaction between devices has become the norm in IoT. However, in the process of data transmission across domains, users' sensitive information is inevitably retained in various information systems, which exacerbates the risk of privacy information leakage and also increases the difficulty of tracing the source of privacy infringement [19]. On the other hand, the data stored on the blockchain are open and transparent. By analyzing the data on the blockchain, it is possible to track user activities and analyze user personal habits. Especially, as the scale of data on the chain grows, the correlation between data may expose personal privacy to a great extent. Meanwhile, if this information is maliciously mined and used, it could pose a serious threat to user privacy [146]. Some papers provided solutions such as using pseudonyms [6], [98]. Nevertheless, the identity of the node in IoT can be leaked from the public address used on the blockchain. There are also papers that use encryption to protect data privacy, such as encrypted transmission of information [102], and encoding trust-related features obtained from collected data [109]. But this increase TMS overhead and increase resource consumption of IoT devices.

2) Future Research Directions: PP in BC-TMSs is a crucially important research topic that urgently requests exploration in the literature. Blockchain optimization could be a promising direction. Some optimized solutions have been proposed by some researchers, such as hybrid coins [147], memory-optimized blockchain data storage schemes [148], and permissioned blockchain usage [47]. However, the privacy of identity, data and attributes of IoT nodes, as well as related access control policies has not yet been well preserved in a holistic way. Additional research is highly needed to be conducted.

E. Scalability

1) Open Issues: The current studies basically consider the scalability of IoT networks, but normally ignore the scalability of the blockchain. Due to the tamper-proofing of blockchain, it is easy to face the problem of insufficient storage resources facing the big data of IoT. So a scalable blockchain becomes very necessary. Some studies improve the memory scalability of blockchain by reducing the stored data in the blockchain [104]. However, from the perspective of auditability, storing as much trust-related data as possible is preferred, which leads to a significant amount of storage overhead and impacts the scalability of blockchain. Therefore, it is necessary to make a tradeoff between scalability and auditability. And novel solutions should be innovated to offer auditability with economic storage consumption.

2) Future Research Directions: To improve the scalability of blockchain, the following technologies become promising [64]: sharding [149], [150], off-chain processing [151], and increasing block size [152], reducing the interval between block generation, as well as reducing data transmission time. In addition, to balance auditability and scalability, it is recommended to store valid trust information and minimize redundancy of storage.

F. Reward and Punishment Mechanisms

1) Open Issues: Reward and punishment mechanisms are not paid much attention in existing works. If a TMS lacks a reward and punishment mechanism, some nodes may become hesitate to participate in TM, but use the services provided by other parties. For example, for trust evaluation, they may not provide recommendations or provide wrong recommendations, which can harm others and disrupt proper functionality of TMS. Moreover, a blockchain system also needs proper incentives to stimulate nodes behave honestly and properly. Because of the lack of centralized control, blockchain network nodes lack motivation and are prone to security problems [153]. Therefore, it is worth a special effort to design an appropriate reward and punishment mechanism in order to incent trusted behaviors of all system entities.

2) Future Research Directions: Incentive mechanisms should be studied to motivate honest and benign behaviors of both IoT system nodes and also blockchain system nodes. First, hybrid incentive mechanisms are expected to be proposed. For example, a combination of a bidding mechanism and a novel time-window-based method [154] can be used to motivate nodes to participate tasks and contribute their resources to improve the sustainability of the system. Second, it is possible to increase the penalty for malicious behavior of

devices to raise the cost of malicious IoT nodes or attackers. This is because it not only conforms to the essential nature of trust (i.e., hard to gain but easy to lose) but also enhances the security of the system. Third, blockchain also needs suitable incentives to meet the requirements of different applications. It is required to address two issues: the reward for proving or mining a block, and the compensation for processing a transaction [147]. In addition, more factors such as long-term interaction between IoT nodes and blockchain consensus nodes (which could be studied by evolutionary game theory [153]), consensus node waiting time cost and transaction processing speed should be considered to accommodate the future market development of IoT and blockchain.

G. Role of Blockchain

1) Open Issues: Existing works do not sufficiently leverage blockchain to help with TM in IoT. The works that combine TM and blockchain can be divided into three categories: 1) only exploit the transparency and tamper-proof nature of blockchain to assist TM without incorporating consensus mechanisms (e.g., [78], [100]); 2) incorporate the consensus mechanism of blockchain into TMSs (e.g., [102], [114]); and 3) add smart contracts to the previous category to make further use of blockchain for trustworthy code execution [106] (e.g., [104], [117]). Each of the three categories has its pros and cons. The first category is intuitive and simple, i.e., only treating the blockchain as a tool for storing trust-related data. Most works in this category still rely on a central authority and thus suffers from a single point of failure, which defeats the initial purpose of introducing blockchain into TM. The second one introduces consensus mechanisms into TMSs in order to improve the sustainability of TMSs. However, the blockchain only works for storing the final trust value and is not involved in the calculation process of that value. The third category performs trust evaluation that is protected by auto-executed smart contracts. However, smart contracts are costly and limited to a certain platform [124]. They are not updatable and vulnerable to several attacks, such as reentrancy and DoS with block gas limit [155]. Therefore, it becomes necessary to address the challenges of the blockchain technology while exploring TM based on blockchain.

2) Future Research Directions: We suggest exploring additional functionalities based on blockchain for TM in IoT. First, it is necessary to make full use of the distributed characteristic of blockchain to make TMSs free from central authorities. Second, blockchain can not only secure the storage of trust-related information but also provide security for trust assessment. Third, it is possible to leverage not only the automatic execution of smart contracts but also their automatic storage of legally binding agreements on the blockchain [156]. Moreover, for the challenge that the irreversibility and non updatability of smart contracts is not applicable to IoT scenarios where flaws or new TM logic emerges, some techniques for upgrading smart contracts should be further investigated. In a word, it is highly recommended to explore additional functions that can be performed by blockchain to achieve reliable and effective TM.

VI. Conclusion

This article presented a systematic review on BC-TMSs in IoT. First, we summarized a set of evaluation criteria that a sound TMS is preferred to satisfy. Then, we proposed a taxonomy of TMSs, and continued with a thorough review on BC-TMSs in IoT by using the proposed criteria as a measure to comment and compare the performance of existing works. Finally, based on the review, we identify a series of open issues and further suggest future research directions accordingly to advance the research on decentralized trustworthy IoT.

References

[1] F. Javed, M. K. Afzal, M. Sharif, and B.-S. Kim, "Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2062–2100, 3rd Quart., 2018.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] M. Stoyanova, Y. Nikoloudakis, S. PanagIoTakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[4] Z. Yan and C. Prehofer, "Autonomic trust management for a component-based software system," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 6, pp. 810–823, Nov./Dec. 2011.

[5] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2127–2162, 4th Quart., 2022.

[6] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020.

[7] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in Internet of Vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2021.

[8] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8599–8622, 2022.

[9] L. Wei, J. Wu, and C. Long, "Blockchain-enabled trust management in service-oriented Internet of Things: Opportunities and challenges," in *Proc. 3rd Int. Conf. Blockchain Technol.*, 2021, pp. 90–95.

[10] Q. Ul Ain Arshad, F. Azam, W. Z. Khan, M. K. Khan, and M. Raza. "Blockchain based decentralized trust management in IoT: Systems, requirements and challenges." Mar. 2022. [Online]. Available: https://www.techrxiv.org/articles/preprint/Blockchain_based_Decentralized_Trust_Management_in_IoT_Systems_Requirements_and_Challenges/19351892

[11] M. K. I. Rahmani et al., "Blockchain-based trust management framework for cloud computing-based Internet of medical things (IoMT): A systematic review," *Comput. Intell. Neurosci.*, vol. 2022, May 2022, Art. no. 9766844.

[12] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. Abd El-Latif, "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[13] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TrustChain: Trust management in blockchain and IoT supported supply chains," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, 2019, pp. 184–193.

[14] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for Internet of Things in smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 716–723, Apr. 2018.

[15] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10452–10473, Jul. 2021.

[16] S. Agrawal and M. L. Das, "Internet of Things—A paradigm shift of future Internet applications," in *Proc. Nirma Univ. Int. Conf. Eng.*, 2011, pp. 1–7.

[17] N. M. Kumar and P. K. Mallick, "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," *Procedia Comput. Sci.*, vol. 132, pp. 109–117, Jun. 2018.

[18] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. Khan, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *J. Netw. Comput. Appl.*, vol. 145, Nov. 2019, Art. no. 102409.

[19] L. Wenqing, D. Wenjie, Z. Xu, and L. Yueming, "The controlled sharing mechanism for private data based on blockchain," in *Proc. IEEE 6th Int. Conf. Data Sci. Cyberspace (DSC)*, 2021, pp. 508–515.

[20] E. Park, A. P. Del Pobil, and S. J. Kwon, "The role of Internet of Things (IoT) in smart cities: Technology roadmap-oriented approaches," *Sustainability*, vol. 10, no. 5, p. 1388, 2018.

[21] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *J. Elect. Comput. Eng.*, vol. 2017, Jan. 2017, Art. no. 9324035.

[22] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2688–2710, 2010.

[23] A. R. Khan et al., "DSRC technology in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) IoT system for intelligent transportation system (ITS): A review," in *Recent Trends in Mechatronics Towards Industry 4.0*. Singapore: Springer, 2022, pp. 97–106.

[24] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. Jäntti, "Reinforcement learning in blockchain-enabled IIoT networks: A survey of recent advances and open challenges," *Sustainability*, vol. 12, no. 12, p. 5161, 2020.

[25] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9326–9337, Dec. 2019.

[26] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. Front. Inf. Technol.*, 2012, pp. 257–260.

[27] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021.

[28] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy Internet of Things: A survey on trust management applications and schemes," *Comput. Commun.*, vol. 160, pp. 475–493, Jul. 2020.

[29] *Internet of Things Global Standards Initiative*, Rec. Y.2060, Int. Telecommun. Union, Geneva, Switzerland, 2012.

[30] L. Gu, J. Wang, and B. Sun, "Trust management mechanism for Internet of Things," *China Commun.*, vol. 11, no. 2, pp. 148–156, Feb. 2014.

[31] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[32] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2018.

[33] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 485–498, Jul.–Sep. 2017.

[34] Z. M. Fadlullah and A.-S. K. Pathan, *Combating Security Challenges in the Age of Big Data: Powered by State-of-the-Art Artificial Intelligence Techniques*. Cham, Switzerland: Springer, 2020.

[35] X. Chen, J. Ding, and Z. Lu, "A decentralized trust management system for intelligent transportation environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 1, pp. 558–571, Jan. 2022.

[36] E. Rutland, *Blockchain Byte*, vol. 2, FINRA. R3 Res., Washington, DC, USA, 2017.

[37] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.

[38] J. H. Khor, M. Sidorov, and P. Y. Woon, "Public blockchains for resource-constrained IoT devices—A state-of-the-art survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11960–11982, Aug. 2021.

[39] W. Feng, Z. Yan, L. T. Yang, and Q. Zheng, "Anonymous authentication on trust in blockchain-based mobile crowdsourcing," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14185–14202, Aug. 2022.

[40] 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, Jun. 2014.

[41] M. T. Lwin, J. Yim, and Y.-B. Ko, "Blockchain-based lightweight trust management in mobile ad-hoc networks," *Sensors*, vol. 20, no. 3, p. 698, 2020.

[42] M. Carbone, M. Nielsen, and V. Sassone, "A formal model for trust in dynamic networks," in *Proc. 1st Int. Conf. Softw. Eng. Formal Methods*, 2003, pp. 54–61.

[43] Z. Yan, L. Peng, W. Feng, and L. T. Yang, "Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–28, 2021.

[44] J. Guo et al., "TROVE: A context-awareness trust model for VANETs using reinforcement learning," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6647–6662, Jul. 2020.

[45] Y. Zhang and Y. Fang, "A fine-grained reputation system for reliable service selection in peer-to-peer networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 8, pp. 1134–1145, Aug. 2007.

[46] Y. Ren, M. Li, and K. Sakurai, "FineTrust: A fine-grained trust model for peer-to-peer networks," *Security Commun. Netw.*, vol. 4, no. 1, pp. 61–69, 2011.

[47] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of Things build our future: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2011–2027, 3rd Quart., 2018.

[48] S. Kharche and P. Dere, "Interoperability issues and challenges in 6G networks," *J. Mobile Multimedia*, vol. 18, no. 5, pp. 1445–1470, 2022.

[49] Y. Wu and Y. Zhang, "An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing," *Adv. Eng. Inform.*, vol. 51, Jan. 2022, Art. no. 101522.

[50] D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, "Decentralized blockchain-based trust management protocol for the Internet of Things," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 1292–1306, Mar./Apr. 2022.

[51] F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira, "Faith in vehicles: A set of evaluation criteria for trust management in vehicular ad-hoc network," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2017, pp. 44–52.

[52] F. G. Mármol and G. M. Pérez, "Security threats scenarios in trust and reputation models for distributed systems," *Comput. Security*, vol. 28, no. 7, pp. 545–556, 2009.

[53] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on Bitcoin's peer-to-peer network," in *Proc. 24th USENIX Security Symp. (USENIX Security)*, 2015, pp. 129–144.

[54] Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula, and Z. Cai, "A survey on blockchain systems: Attacks, defenses, and privacy preservation," *High-Confidence Comput.*, vol. 2, no. 2, Jun. 2022, Art. no. 100048.

[55] S. King and S. Nadal. "PPCoin: Peer-to-peer crypto-currency with proof-of-stake." 2012. [Online]. Available: https://archive.org/details/PPCoinPaper

[56] J. J. Xu, "Are blockchains immune to all malicious attacks?" *Financ. Innov.*, vol. 2, no. 1, pp. 1–9, 2016.

[57] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[58] M. Rosenfeld, "Analysis of Bitcoin pooled mining reward systems," 2011, *arXiv:1112.4980*.

[59] X. Jing, H. Han, Z. Yan, and W. Pedrycz, "SuperSketch: A multi-dimensional reversible data structure for super host identification," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2741–2754, Jul./Aug. 2022.

[60] N. Anita and M. Vijayalakshmi, "Blockchain security attack: A brief survey," in *Proc. 10th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, 2019, pp. 1–6.

[61] W. Guo, "Explainable artificial intelligence for 6G: Improving trust between human and machine," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 39–45, Jun. 2020.

[62] Z. Ying, D. Bourgeois, J. You, M. Zitnik, and J. Leskovec, "GNNExplainer: Generating explanations for graph neural networks," in *Advances in Neural Information Processing Systems*, vol. 32. Red Hook, NY, USA: Curran, 2019.

[63] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, Aug. 2014.

[64] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep./Oct. 2019.

[65] D. Han, Y. Zhu, D. Li, W. Liang, A. Souri, and K.-C. Li, "A blockchain-based auditable access control system for private data in service-centric IoT environments," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3530–3540, May 2022.

[66] J.-C. Fernandez, L. Mounier, and C. Pachon, "A model-based approach for robustness testing," in *Proc. IFIP Int. Conf. Test. Commun. Syst.*, 2005, pp. 333–348.

[67] M. Carbin and M. C. Rinard, "Automatically identifying critical input regions and code in applications," in *Proc. 19th Int. Symp. Softw. Test. Anal.*, 2010, pp. 37–48.

[68] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, "Trust models of Internet of smart things: A survey, open issues, and future directions," *J. Netw. Comput. Appl.*, vol. 137, pp. 93–111, Jul. 2019.

[69] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)," in *Proc. Int. Conf. Netw. Security Appl.*, 2010, pp. 420–429.

[70] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain and trust for secure, end-user-based and decentralized IoT service provision," *IEEE Access*, vol. 8, pp. 119961–119979, 2020.

[71] S. Asiri and A. Miri, "A Sybil resistant IoT trust model using blockchains," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2018, pp. 1017–1026.

[72] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," in *Wireless Sensor and Mobile Ad-Hoc Networks*. New York, NY, USA: Springer, 2015, pp. 217–247.

[73] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, Jun. 2019.

[74] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.

[75] H. L. J. Ting, X. Kang, T. Li, H. Wang, and C.-K. Chu, "On the trust and trust modeling for the future fully-connected digital world: A comprehensive study," *IEEE Access*, vol. 9, pp. 106743–106783, 2021.

[76] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in Internet of Things: Towards secure and privacy-preserving fusion," *Inf. Fusion*, vol. 51, pp. 129–144, Nov. 2019.

[77] T. K. Kim and H. S. Seo, "A trust model using fuzzy logic in wireless sensor network," *World Acad. Sci. Eng. Technol.*, vol. 42, no. 6, pp. 63–66, 2008.

[78] W. Meng, W. Li, and L. Zhu, "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1377–1386, Nov. 2020.

[79] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wireless Netw.*, vol. 24, no. 3, pp. 777–797, 2018.

[80] G. Wang and J. Wu, "FlowTrust: Trust inference with network flows," *Front. Comput. Sci. China*, vol. 5, no. 2, pp. 181–194, 2011.

[81] M. Luecking, C. Fries, R. Lamberti, and W. Stork, "Decentralized identity and trust management framework for Internet of Things," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, 2020, pp. 1–9.

[82] R. O. Andrade and S. G. Yoo, "Cognitive security: A comprehensive study of cognitive science in cybersecurity," *J. Inf. Security Appl.*, vol. 48, Oct. 2019, Art. no. 102352.

[83] R. Rani, S. Kumar, and U. Dohare, "Trust evaluation for light weight security in sensor enabled Internet of Things: Game theory oriented approach," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8421–8432, Oct. 2019.

[84] C. A. Kamhoua, N. Pissinou, and K. Makki, "Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–6.

[85] J. Wang, X. Jing, Z. Yan, Y. Fu, W. Pedrycz, and L. T. Yang, "A survey on trust evaluation based on machine learning," *ACM Comput. Surv.*, vol. 53, no. 5, pp. 1–36, 2021.

[86] X. Jing, Z. Yan, Y. Shen, W. Pedrycz, and J. Yang, "A group-based distance learning method for semisupervised fuzzy clustering," *IEEE Trans. Cybern.*, vol. 52, no. 5, pp. 3083–3096, May 2022.

[87] Z. Hu et al., "SSL-SVD: Semi-supervised learning–based sparse trust recommendation," *ACM Trans. Internet Technol.*, vol. 20, no. 1, pp. 1–20, 2020.

[88] Z. Yan, *Trust Management in Mobile Environments: Autonomic and Usable Models: Autonomic and Usable Models*. Hershey, PA, USA: IGI Global, 2013.

[89] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021.

[90] A. Al-Omary, A. Othman, H. M. AlSabbagh, and H. Al-Rizzo, "Survey of hardware-based security support for IoT/CPS systems," in *Proc. Sustain. Resilience Conf.*, 2018, pp. 52–70.

[91] E. W. Felten, "Understanding trusted computing: Will its benefits outweigh its drawbacks?" *IEEE Security Privacy*, vol. 1, no. 3, pp. 60–62, May/Jun. 2003.

[92] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security Commun. Netw.*, vol. 9, no. 16, pp. 3059–3069, 2016.

[93] J.-E. Ekberg, K. Kostiainen, and N. Asokan, "The untapped potential of trusted execution environments on mobile devices," *IEEE Security Privacy*, vol. 12, no. 4, pp. 29–37, Jul./Aug. 2014.

[94] P. Maene, J. Götzfried, R. De Clercq, T. Müller, F. Freiling, and I. Verbauwhede, "Hardware-based trusted computing architectures for isolation and attestation," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 361–374, Mar. 2018.

[95] A. Lahbib, K. Toumi, A. Laouiti, A. Laube, and S. Martin, "Blockchain based trust management mechanism for IoT," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2019, pp. 1–8.

[96] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," in *Proc. 16th EAI Int. Conf. Mobile Ubiquitous Syst. Comput. Netw. Serv.*, 2019, pp. 190–199.

[97] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, "Trust-based blockchain authorization for IoT," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 2, pp. 1646–1658, Jun. 2021.

[98] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *J. Parallel Distrib. Comput.*, vol. 152, pp. 144–156, Jun. 2021.

[99] W. Dong, Y. Li, R. Hou, X. Lv, H. Li, and B. Sun, "A blockchain-based hierarchical reputation management scheme in vehicular network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[100] M. A. Azad, S. Bag, F. Hao, and A. Shalaginov, "Decentralized self-enforcing trust management system for social Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2690–2703, Apr. 2020.

[101] D. Wu and N. Ansari, "A trust-evaluation-enhanced blockchain-secured industrial IoT system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5510–5517, Apr. 2021.

[102] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A semi-centralized trust management model based on blockchain for data exchange in IoT system," *IEEE Trans. Services Comput.*, early access, Jun. 13, 2022, doi: 10.1109/TSC.2022.3181668.

[103] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[104] H. Zhang, J. Liu, H. Zhao, P. Wang, and N. Kato, "Blockchain-based trust management for Internet of Vehicles," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1397–1409, Jul.–Sep. 2021.

[105] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[106] P. Wang, N. Xu, H. Zhang, W. Sun, and A. Benslimane, "Dynamic access control and trust management for blockchain-empowered IoT," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 12997–13009, Aug. 2022.

[107] C. Esposito, O. Tamburis, X. Su, and C. Choi, "Robust decentralised trust management for the Internet of Things by using game theory," *Inf. Process. Manag.*, vol. 57, no. 6, 2020, Art. no. 102308.

[108] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021.

[109] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101954.

[110] T. Ranathunga, A. McGibney, and S. Rea, "The convergence of blockchain and machine learning for decentralized trust management in IoT ecosystems," in *Proc. 19th ACM Conf. Embedded Netw. Sens. Syst.*, 2021, pp. 499–504.

[111] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.

[112] T. Ranathunga, R. Marfievici, A. McGibney, and S. Rea, "A distributed ledger based platform for automated energy performance assessment," in *Proc. 3rd Int. Conf. Blockchain Comput. Appl. (BCCA)*, 2021, pp. 65–72.

[113] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J.-T. Seo, "An efficient dynamic solution for the detection and prevention of black hole attack in VANETs," *Sensors*, vol. 22, no. 5, p. 1897, 2022.

[114] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3527–3537, Jun. 2019.
[115] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.
[116] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, "Blockchain for smart cities: A review of architectures, integration trends and future research directions," *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102360.
[117] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in Internet of Vehicles with blockchain," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11815–11829, Dec. 2020.
[118] J. Zhang, Z. Wang, L. Shang, D. Lu, and J. Ma, "BTNC: A blockchain based trusted network connection protocol in IoT," *J. Parallel Distrib. Comput.*, vol. 143, pp. 1–16, Sep. 2020.
[119] K. A. Awan, I. U. Din, A. Almogren, H. A. Khattak, and J. J. P. C. Rodrigues, "EdgeTrust—A lightweight data-centric trust management approach for green Internet of edge things," *Wireless Pers. Commun.*, to be published.
[120] O. Alboqomi, T. Gazdar, and A. Munshi, "A new blockchain-based trust management protocol for vehicular ad hoc networks," in *Proc. 4th Int. Conf. Future Netw. Distrib. Syst. (ICFNDS)*, 2020, pp. 1–5.
[121] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust Security Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, 2018, pp. 98–103.
[122] S. Hameed et al., "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology," *IEEE Sensors J.*, vol. 21, no. 6, pp. 8716–8733, Mar. 2021.
[123] Z. Yang, R. Wang, D. Wu, B. Yang, and P. Zhang, "Blockchain-enabled trust management model for the Internet of Vehicles," *IEEE Internet Things J.*, early access, Oct. 29, 2021, doi: 10.1109/JIOT.2021.3124073.
[124] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the Internet of Things," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, 2018, pp. 77–83.
[125] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "IoT passport: A blockchain-based trust framework for collaborative Internet-of-Things," in *Proc. 24th ACM Symp. Access Control Models Technol.*, 2019, pp. 83–92.
[126] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.
[127] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, and K. Xu, "An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4134–4145, Jun. 2020.
[128] A. Roy and S. K. Madria, "BLAME: A blockchain-assisted misbehavior detection and event validation in VANETs," in *Proc. 22nd IEEE Int. Conf. Mobile Data Manag. (MDM)*, 2021, pp. 69–78.
[129] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," in *Proc. 12th Int. Conf. World Wide Web*, 2003, pp. 640–651.
[130] L. Hou, N. Yao, Z. Lu, F. Zhan, and Z. Liu, "Tracking based mix-zone location privacy evaluation in VANET," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10957–10969, Oct. 2021.
[131] L. Axon and M. Goldsmith, "PB-PKI: A privacy-aware blockchain-based PKI," in *Proc. 14th Int. Conf. Security Cryptogr. (SECRYPT)*, vol. 6, 2017, pp. 311–318.
[132] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "A time-aware trust management heuristic for the Internet of Vehicles," in *Proc. IEEE 20th Int. Conf. Trust Security Privacy Comput. Commun. (TrustCom)*, 2021, pp. 1–8.
[133] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.
[134] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 57–64.
[135] A. B. Arrieta et al., "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Inf. Fusion*, vol. 58, pp. 82–115, Jun. 2020.
[136] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf. China-Ireland Int. Conf. Inf. Commun. Technol. (ISSC/CIICT)*, 2014, pp. 280–285.
[137] Y. Lu, "Blockchain and the related issues: A review of current research topics," *J. Manag. Anal.*, vol. 5, no. 4, pp. 231–255, 2018.
[138] W. Feng and Z. Yan, "MCS-chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain," *Future Gener. Comput. Syst.*, vol. 95, pp. 649–666, Jun. 2019.
[139] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 6122–6131, 2016.
[140] A. B. Patel, M. Birla, and U. Nair, "Addressing big data problem using Hadoop and map reduce," in *Proc. Nirma Univ. Int. Conf. Eng. (NUiCONE)*, 2012, pp. 1–5.
[141] Z. Yan, W. Ding, X. Yu, H. Zhu, and R. H. Deng, "Deduplication on encrypted big data in cloud," *IEEE Trans. Big Data*, vol. 2, no. 2, pp. 138–150, Jun. 2016.
[142] P. Wang, Z. Yan, and K. Zeng, "BCAuth: Physical layer enhanced authentication and attack tracing for backscatter communications," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2818–2834, 2022.
[143] Y. Wu, "Ethically responsible and trustworthy autonomous systems for 6G," *IEEE Netw.*, vol. 36, no. 4, pp. 126–133, Jul./Aug. 2022.
[144] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4000–4015, May 2020.
[145] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021.
[146] W. Ding, Z. Yan, and R. H. Deng, "Privacy-preserving data processing with flexible access control," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 363–376, Mar./Apr. 2020.
[147] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[148] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, Mar. 2019.
[149] J. Yun, Y. Goh, and J.-M. Chung, "DQN-based optimization framework for secure sharded blockchain systems," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 708–722, Jan. 2021.
[150] C. Huang et al., "RepChain: A reputation-based secure, fast, and high incentive blockchain system via sharding," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4291–4304, Mar. 2021.
[151] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distrib. Comput.*, vol. 164, pp. 152–167, Jun. 2022.
[152] A. A. Pandey, T. F. Fernandez, R. Bansal, and A. K. Tyagi, "Maintaining scalability in blockchain," in *Proc. Int. Conf. Intell. Syst. Des. Appl.*, 2022, pp. 34–45.
[153] R. Han, Z. Yan, X. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? a survey," *ACM Comput. Surv.*, vol. 55, no. 7, pp. 1–38, 2023.
[154] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, "An efficient collaboration and incentive mechanism for Internet of Vehicles (IoV) with secured information exchange based on blockchains," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1582–1593, Mar. 2020.
[155] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.
[156] Y. I. Alzoubi, A. Al-Ahmad, H. Kahtan, and A. Jaradat, "Internet of Things and blockchain integration: Security, privacy, technical, and design challenges," *Future Internet*, vol. 14, no. 7, p. 216, 2022.

Yijia Liu received the B.S. degree from the School of Computer Science and Technology from Soochow University, Suzhou, China, in 2021. She is currently pursuing the master's degree with the School of Cyber Engineering, Xidian University, Xi'an, China.

Her research interests are in machine learning, IoT, and blockchain.

Jie Wang received the B.S. degree in network engineering from Xidian University, Xi'an, China, in 2020, where he is currently pursuing the Ph.D. degree with the School of Cyber Engineering.

His research interests are in trust management, machine learning, and blockchain.

Zheng Yan (Senior Member, IEEE) received the D.Sc. degree in technology from the Helsinki University of Technology, Espoo, Finland, in 2007.

She is currently a Professor with the School of Cyber Engineering, Xidian University, Xi'an, China. Her research interests are in trust, security, privacy, and security-related data analytics.

Dr. Yan received several awards in recent years, including the Distinguished Inventor Award of Nokia, N2Women: Stars in Computer Networking and Communications, Aalto ELEC Impact Award, the Best Journal Paper Award issued by IEEE Communication Society Technical Committee on Big Data and the Outstanding Associate Editor of 2017 and 2018 for IEEE ACCESS, etc. She served as a General Chair or the Program Chair for numerous international conferences, including IEEE TrustCom 2015 and IFIP Networking 2021. She is a Founding Steering Committee Co-Chair of IEEE Blockchain Conference. She is an Area Editor of IEEE INTERNET OF THINGS JOURNAL and *Information Fusion*, and an Associate Editor of *Information Sciences*, IEEE NETWORK, etc.

Zhiguo Wan (Member, IEEE) received the B.S. degree in computer science from Tsinghua University, Beijing, China, in 2002, and the Ph.D. degree in information security from the National University of Singapore, Singapore, in 2007.

He is a Principal Investigator with Zhejiang Laboratory, Hangzhou, Zhejiang, China. He was a Postdoctoral Researcher with Katholieke University of Leuven, Leuven, Belgium, and an Assistant Professor with the School of Software, Tsinghua University. His main research interests include security and privacy for cloud computing, Internet of Things, and blockchain.

Riku Jäntti (Senior Member, IEEE) received the M.Sc. degree (with distinction) in electrical engineering and the D.Sc. degree (with distinction) in automation and systems technology from Helsinki University of Technology (TKK), Espoo, Finland, in 1997 and 2001, respectively.

He is a Full Professor of Communications Engineering and the Head with the Department of Communications and Networking, School of Electrical Engineering, Aalto University (formerly, known as TKK), Espoo. Prior to joining Aalto, in August 2006, he was a Professor pro tem with the Department of Computer Science, University of Vaasa, Vaasa, Finland. His research interests include radio resource control and optimization for machine type communications, cloud based radio access networks, spectrum and co-existence management, quantum communications, and RF Inference.

Prof. Jäntti is an Associate Editor of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is also a IEEE VTS Distinguished Lecturer (Class 2016).