future internet

MDPI

Review

Blockchain-Enabled Edge Intelligence for IoT: Background, Emerging Trends and Open Issues

Yao Du [1], Zehua Wang [1] and Victor C. M. Leung [1,2,*]

[1] Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC V6T 1Z4, Canada; yaodu@ece.ubc.ca (Y.D.); zwang@ece.ubc.ca (Z.W.)
[2] College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China
* Correspondence: vleung@ieee.org

Abstract: Blockchain, a distributed ledger technology (DLT), refers to a list of records with consecutive time stamps. This decentralization technology has become a powerful model to establish trust among trustless entities, in a verifiable manner. Motivated by the recent advancement of multi-access edge computing (MEC) and artificial intelligence (AI), blockchain-enabled edge intelligence has become an emerging technology for the Internet of Things (IoT). We review how blockchain-enabled edge intelligence works in the IoT domain, identify the emerging trends, and suggest open issues for further research. To be specific: (1) we first offer some basic knowledge of DLT, MEC, and AI; (2) a comprehensive review of current peer-reviewed literature is given to identify emerging trends in this research area; and (3) we discuss some open issues and research gaps for future investigations. We expect that blockchain-enabled edge intelligence will become an important enabler of future IoT, providing trust and intelligence to satisfy the sophisticated needs of industries and society.

Keywords: Internet of Things; blockchain; multi-access edge computing; machine learning

Citation: Du, Y.; Wang, Z.; Leung, V.C.M. Blockchain-Enabled Edge Intelligence for IoT: Background, Emerging Trends and Open Issues. *Future Internet* **2021**, *13*, 48. https://dx.doi.org/10.3390/fi13020048

Academic Editor: Luis Javier Garcia Villalba
Received: 15 January 2021
Accepted: 12 February 2021
Published: 17 February 2021

1. Introduction

Internet of Things (IoT) emerged initially in 1999 in supply chain industries in association with radio-frequency identification (RFID) [1]. The idea was to empower computers to observe, identify, and understand the world without the help of human beings. However, many IoT devices are designed to be battery operated and have a compact physical size; thus, they have very limited energy and computation resources. Such resource-constrained IoT devices are not well-equipped to perform complex processing, such as supporting artificial intelligence (AI) [2]. Although federated learning (FL) can be implemented by a group of IoT devices [3], such computational workload is still too heavy for IoT devices. To overcome this bottleneck, transmitting computational tasks to nearby servers is an attractive solution. Different from traditional cloud computing, such strategy as multi-access edge computing (MEC) delivers computation resources to the edge of the radio access network (RAN). Therefore, computational tasks have no need to travel through the core network, allowing IoT data to be processed and results consumed locally with minimal delay. This mode of computing, while minimizing latency and use of core network communication resources, has its own challenges. For example, security issues and incentives should be taken into considerations. To be specific, the transmitted data may contain private data about personal identity and financial account information. This raises the risk of privacy leakage and malicious attacks. Moreover, nearby servers or computing nodes may need incentives to process tasks for IoT devices. Furthermore, edge servers have limited computation power compared with the cloud. The computing operations also cost storage and energy resources. Therefore, a computing resource trading [4] and data sharing [5] framework or platform is needed to motivate edge servers. As a distributed ledger technology (DLT), blockchain has emerged as a potential solution for the above issues, due to its nature of data transparency, distributed operation, and reliability. It is

timely to comprehensively survey the application of blockchain to enable edge intelligence in support of IoT applications.

1.1. Related Surveys

There exist several surveys on related research areas. Table 1 summarizes these surveys and compare them with this review.

Table 1. Summary of the existing surveys and tutorials with their primary focus.

Reference	AI	MEC	Recent Advances	Trends	Research Gaps
ElMamy et al. [6]	✗	✓	✗	✗	✗
Tariq et al. [7]	✗	✓	✗	✗	✗
Jameel et al. [8]	✓	✗	✓	✗	✗
Liu et al. [9]	✓	✓	✗	✓	✗
Kumari et al. [10]	✓	✗	✗	✓	✗
Salah et al. [11]	✓	✗	✗	✗	✗
Tahir et al. [12]	✓	✓	✗	✗	✗
Nguyen et al. [13]	✓	✓	✗	✗	✗
Xiong et al. [14]	✗	✓	✗	✗	✗
Yang et al. [15]	✗	✓	✗	✗	✗
Sekaran et al. [16]	✗	✓	✗	✗	✗
Fernandez Carames et al. [17]	✓	✓	✗	✗	✗
Chamola et al. [18]	✗	✓	✗	✗	✗
Queiroz et al. [19]	✓	✓	✗	✗	✗
Mollah et al. [20]	✓	✓	✗	✗	✗
Our Review	✓	✓	✓	✓	✓

ElMamy et al. [6] surveyed the usage of DLT to mitigate multiple cyber-threats in Industry 4.0. This survey classified the most important cyber-attacks into four classes, including scanning, local to remote, power of root, and denial of service. Tariq et al. [7] reviewed security issues around fog-enabled IoT. They considered blockchain as the key to address fog computing security issues. However, these works do not consider the capability of blockchain as an enabler of AI at the edge.

For AI enabled by blockchain, there exist several literature reviews. Jameel et al. [8] surveyed the application of reinforcement learning in blockchain-enabled industrial IoT networks. They pointed out that machine learning (ML) algorithms, such as Q-learning, can improve the performance of the network, in terms of block time minimization and transaction throughput enhancement. Furthermore, Liu et al. [9] gave a two-way convergence of blockchain and ML. On one hand, blockchain can endow ML with the features of security and trust. On the other hand, ML can be used as a tool to optimize blockchain networks. Kumari et al. [10] studied existing blockchain-based AI approaches for energy cloud management, to address security and privacy issues using blockchain and AI. Furthermore, Salah et al. [11] gave a comprehensive review of blockchain applications for AI. The relationship between AI and blockchain in the IoT-enabled ecosystem was discussed. However, MEC has not been considered in these works.

Additionally, MEC is a key technology of emerging fifth-generation (5G) networks. Multiple surveys on blockchain solutions in 5G networks exist, centered around security challenges in 5G systems. In addition, Tahir et al. [12] discussed blockchain applications in 5G networks. They gave a comprehensive survey on the integration of blockchain with 5G networks and beyond. In this review, the transparency, auditability, and distributed properties of blockchains were considered to address issues, such as security, resources management, and energy efficiency. The paper identified three major challenges associated with MEC, including identity authentication, privacy, and trust management. Then, it introduced some blockchain-based solutions to meet these challenges. While this survey covered a lot of topics, blockchain-enabled mobile edge intelligence was not studied thoroughly in this survey. By contrast, Nguyen et al. [13] gave a brief survey of blockchain-

enabled federated approach. This ML architecture is empowered by the decentralization feature of blockchain.

Furthermore, Xiong et al. [14] studied the motivation for the integration of MEC and blockchain. Computational heavy tasks (e.g., proof of work) in the blockchain system are offloaded to MEC servers. They focused on using edge computing to enabling mobile blockchains. However, the use of blockchains to enable efficient and secure MEC was not considered. Additionally, Yang et al. [15] surveyed the collaboration of edge computing and blockchain. They claimed that blockchain could extend the capability of edge computing, in terms of reliable access and control of the network and computation resources. Different from this comprehensive survey, in the present work we focus on blockchain-enabled distributed and decentralized ML. In addition, we analyze the emerging trend and open issues in this research area.

A survey on blockchain-enabled MEC for IoT automation was presented by Sekaran et al. [16]. This review focused on the integration of blockchain with IoT. More importantly, computational loads and delays were considered and investigated. Applications of blockchain for 6G-enabled IoT were further investigated and classified in this paper. Besides, Fernandez Carames et al. [17] studied the collaboration of blockchain, IoT, and edge computing for higher education. Different from other review articles that mainly focus on academic research, it gave a detailed road map of the smart campus implementation. This could be helpful for researchers to understand how blockchain-enabled edge computing works in a realistic IoT application scenario, such as autonomous driving [21]. As for the Internet of vehicles (IoV), blockchain-enabled MEC platforms could be applied for information-exchange and trust. Moreover, Chamola et al. [18] surveyed the integration of IoT, AI, and blockchain to deal with the coronavirus disease 2019 (COVID-19) pandemic. Queiroz et al. [19] investigated blockchain solutions for different layers in edge computing, including fog layer, edge layer, static multi-layer, and dynamic multi-layer. Applicable ML algorithms were also discussed in this paper. However, this survey mainly focused on the IoV domain and did not cover other areas comprehensively. Mollah et al. [20] focused on the blockchain-enabled intelligent transportation systems (ITS). Blockchain-empowered applications, including edge computing and AI, were investigated in this article, and the challenges and opportunities of blockchain-based applications in ITS were discussed.

The literature search strategy of this paper is described as follows: We searched for literature published since 2016, first with the keywords: blockchain, MEC, and IoT, and then with the keywords: blockchain, machine learning, and IoT. We combined the two data sets and eliminated duplicates. The selections of papers from the combined dataset were based on the co-citation frequency, node centrality in the literature graph, and the impact of the publishers. We explored the summary table of CiteSpace [22], a literature mining software that groups research papers in clusters, and selected the top-ranked articles in each cluster.

1.2. Contributions and Organization

In this review, we present a comprehensive survey of blockchain-enabled edge intelligence in the IoT domain. The main contributions are listed as follows:

- We review and analyze the literature related to blockchain-enabled edge intelligence, aiming at giving new researchers in this area some basic ideas and the big picture.
- In this paper, we not only summarize the technical contributions of related papers but also illustrate and provide some insights on the technical trends.
- We identify some open issues and research gaps in this research area, and discuss future research opportunities from the perspectives of the social layer, data layer, and technical layer.

The rest of this survey paper is organized as follows. In Section 2, we introduce some background about blockchain, MEC, and AI. Section 3 mines the literature to identify emerging trends. Then, we point out some research gaps and discuss some potential research questions in Section 4. Finally, we conclude this paper in Section 5.

2. Background

In this section, we provide some basic background of blockchain technology, MEC, and AI. Clarifications and comparisons are given to facilitate understanding. To be specific, we first introduce blockchain fundamentals to give readers a basic idea. We focus on the part of blockchain technology that is related to this survey and leave out the rest of the blockchain fundamentals, such as consensus algorithm details, Merkle tree, transaction architectures, and digital signatures, for brevity. Next, MEC is introduced. We focus on its definition and the integration of blockchain and MEC. Finally, blockchain-enabled AI is discussed. We aim at illustrating how this integration works in the IoT domain.

2.1. Blockchain Fundamentals

Blockchain refers to a set of records that are sequentially chained together using cryptography. Blockchains could be classified into two major types: public and permissioned chains. On the one hand, a public chain is like the Internet. Each user of this record system can find this chain and get access to it. On the other hand, a permissioned chain only allows authenticated entities to read and add to the records. Additionally, a consortium blockchain is a hybrid type between public and permissioned chain, but more like a private chain. It is permissioned and supervised by a predetermined group of entities.

The chain architecture in Figure 1 guarantees the immutability of blockchain records. Once a block exists in this chain, one cannot change anything in previous blocks. A conventional database is like a single screenshot of information, but the blockchain is like a chain of timestamped screenshots. There is a degree of freedom and continuity in time, allowing the blockchain to track the history of this record system.

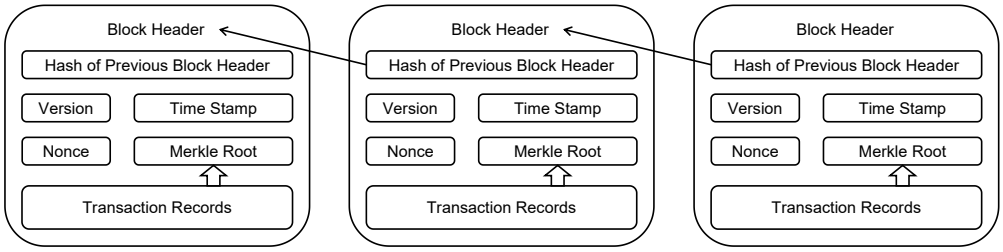


Figure 1. The chain architecture of the blockchain.

Generally speaking, a blockchain uses "consensus" to add new data records (not replace them). However, traditional databases use "permission" to manage data. It has centralized administration and maintenance. In the Bitcoin system, which is the most well-known application of public blockchain, proof-of-work (PoW) is used to reach this consensus. PoW is a kind of mathematical "puzzle". The secret of this puzzle (e.g., Nonce) is hard to find but easy to be verified. The process of finding the nonce is called "mining" [23]. The first miner who discovers the secret can add the block to the longest chain and gets a reward in the form of a Bitcoin. In this decentralized system, full duplicates of transaction records are located at different networked miners. The verification and confirmation of each transaction are processed based on the consensus algorithm. No single third entity could fully control the process in this peer-to-peer network. In contrast, a distributed system also processes transactions in different locations, but it may still be under the control of a single entity. That is the main difference between distributed and decentralized systems. To reiterate, blockchain is a decentralized system, shifting the authority of governance from a centralized third party to individual entities in this record system.

Different from the Bitcoin network, Ethereum [24] embraces the smart contract, a kind of executable scripts stored on the blockchain [25]. Instead of PoW, Ethereum uses Proof-of-stake (PoS) as its consensus mechanism. This consensus strategy chooses block validators at random, with the ones having more stakes gaining more chances to be selected. This frees blockchain nodes from meaningless and energy-consuming mining.

2.2. Integration of MEC and DLT

Several terms are used in the literature to describe the computing collaboration among the end-user, the nearby server, and the cloud. They include fog computing [26], edge computing [27], and MEC [28]. Compared with the "cloud", the "fog" is closer to the "ground" (e.g., the IoT data source). It refers to the extended part of cloud computing, including distributed resources, wired and wireless data transmissions, and intermediate layers between edge and cloud. Edge computing, however, focuses on the task of executing using edge nodes in the RAN outside of the core network. Furthermore, mobile edge computing is a form of edge computing that includes the data caching and computation offloading strategies within the mobile network [29]. Moreover, recent interests in MEC reflect the practical situation with multi-technology RANs in edge computing [30]. It covers access points, hot spots, routers, etc., to establish an edge network. In this review, we use the acronym "MEC" to stand for multi-access edge computing, which also encompasses mobile edge computing. The relationships among fog computing, edge computing, and MEC are, thus, illustrated in Figure 2.

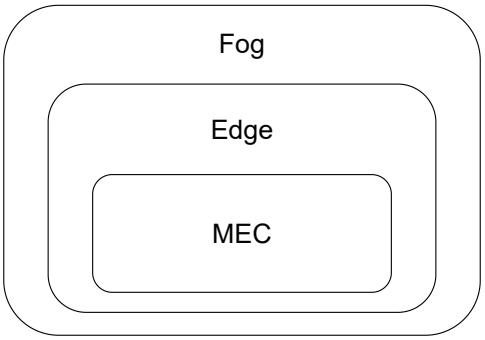


Figure 2. The relationships among different phrases.

In general, the integration between blockchain and MEC is mutually beneficial [15]. On one hand, blockchain introduces security, privacy, and trust to MEC [31,32]. Efficient control and incentive of cooperation among edge devices and servers are securely enabled by blockchain. On the other hand, MEC improves the scalability of blockchain in a distributed and efficient manner by delivering computing and cache resources to the blockchain-enabled IoT systems. For example, blockchain mining requires a high computational capability in the PoW process, which imposes great challenges for IoT devices. The reason why IoT devices should actively mine is that a global consensus is required for transaction validation. Different from a distributed IoT system, a blockchain-enabled IoT system decentralize the authority to each IoT device. In other words, there is no single third party that could help IoT devices make a global decision. Therefore, the PoW mechanism needs to be in place to confirm and secure the integrity and validity of transactions. Fortunately, MEC can be introduced as a solution to this issue. By offloading computational tasks to an MEC server, resource-constrained IoT devices can use PoW to reach consensus for decentralized applications.

Nguyen et al. [33] discussed the privacy leakage issue in blockchain-MEC integration. In this article, mobile users act as miners in the blockchain system. Data processing tasks and mining tasks are offloaded from users to nearby MEC servers. The privacy level of this process is modeled and formulated. Furthermore, blockchain was introduced as a strong security mechanism for MEC systems in vehicular networks [34]. In addition, Reference [35] introduced a blockchain-based trust mechanism for MEC systems. By establishing a reputation system for the edge nodes, the miner in the blockchain network was, thus, selected in a trusted manner.

Additionally, blockchain-enabled payment systems for the video streaming industry were developed with an incentive mechanism for MEC servers [36]. Furthermore, the flexibility and scalability of block size could be significantly improved by MEC. However,

not every edge device could have enough cryptocurrency to buy the offloading service. Therefore, Zhang et al. [37] proposed a loan strategy for this purpose. Although the mining task could be executed on MEC servers, competition exists among IoT devices. The reason is that the resources of edge servers are still limited compared to relatively numerous IoT devices. To deal with this issue, Zhao et al. [38] solved the computation resources allocation problem in the MEC-assisted public blockchain network. Moreover, this strategy could protect the blockchain system from 51% attack [39] because the attacker with the majority stake in this system would try to preserve and secure this kind of cryptocurrency, but not to destroy it.

2.3. Blockchain-Enabled AI

Traditional AI solutions, including deep learning and reinforcement learning, require the centralized governance of data. A single learner should gather data and computing resources for learning machines and agents before the training exercise. This centralized architecture leads to several issues, such as single points of failure and personal data leakage [40]. As mentioned above, blockchain is a decentralized and distributed record system. This characteristic is very suitable for deploying AI solutions in distributed IoT systems. Moreover, collaboration and trusted data sharing among learning machines could be realized by blockchain technology. In this review, we focus on introducing smart contract-based AI, especially the federated AI solution.

In a nutshell, smart contract [25] is a powerful tool to enable distributed and decentralized ML for IoT systems. As illustrated in Figure 3, this kind of predefined and self-verified scripts, including learning algorithms and models, can be deployed at each distributed learning device in a decentralized manner. Furthermore, only learning parameters are shared and verified by blockchain transactions, while sensitive IoT data are not accessible to any third parties. This guarantees the secure sharing of the learning experience and gives the self-governance of data to each entity, which is the basic idea of blockchain-based FL. Thus, blockchain and smart contact together enable a global platform for collaborating ML in a distributed and decentralized manner.

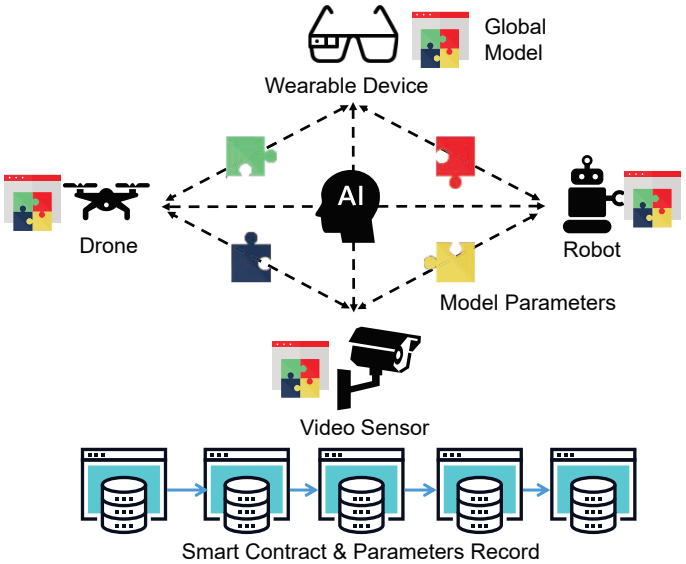


Figure 3. Blockchain-based artificial intelligence (AI) for the Internet of Things (IoT).

Blockchain was introduced to manage the reputation of learning devices [41–45]. To be specific, Kang et al. [42] proposed effective incentive mechanisms for reliable FL. Consortium blockchain was further introduced by them for reputation management. Moreover, blockchain-enabled reward systems were considered in Reference [4,46–50]. Furthermore, the blockchain-enabled data integrity and sources validation could be realized by deep learning with convolutional neural networks [51], giving the trustworthiness of training

data quality. Moreover, Ma et al. [52] investigated data noise and the decentralized solution for data cleaning with edge intelligence.

Lu et al. [40] gave a secure data sharing architecture for decentralized and secure learning strategies to solve the privacy issue in ML. Moreover, the computing work in the blockchain consensus process was used for FL. Furthermore, Qu et al. [46] introduced poisoning attacks in decentralized ML. Likewise, Kang et al. [42] and Ramanan and Nakayama [53] proposed reliable FL strategies by removing the centralized model aggregator in ML. Plus, Yin et al. [54] investigated a blockchain-based federated deep learning in the IoT domain. This strategy was motivated by multiparty secure computation, which was also investigated in Reference [55]. Besides, Liu et al. [56] used smart contracts in the self-defense of FL. Membership inference and poisoning attacks were, thus, prevented in this way.

3. Emerging Trends and Visions

In this section, we aim at providing research directions and identifying emerging trends in this area. We first discuss emerging research directions and related works in this area, including blockchain-enabled IoT communications, blockchain-based IoT security, decentralized ML in IoT, and blockchain-enabled incentive mechanisms in IoT. Then, recent advances are selected and listed for future exploration. Finally, we summarize and illustrate different trends according to the timeline.

3.1. Blockchain-Enabled IoT Communications

- *5G and beyond*: Although the 5G network improves services for IoT communications [57], it may not be capable of enabling new IoT applications, including telemedicine, haptic communication, bio-IoT, etc. Khan et al. [58] provided some future directions for IoT communication in 6G systems. In terms of blockchain-enabled edge intelligence, there are multiple research directions related to IoT communications. For 5G and beyond, Lu et al. [59] discussed blockchain and FL particularly. Potential application scenarios were listed in this paper, including intelligent transportation, mobile networks, network data analysis, etc. Moreover, IoT automation could be realized by 6G-enabled MEC. Sekaran et al. [16] pointed out research challenges in terms of IoT-enabled 6G devices. Furthermore, Nguyen et al. [13] discussed the function of blockchain in 5G and beyond networks in-depth.
- *Decentralized D2D*: For blockchain-enabled edge intelligence, device-to-device (D2D) communication is a feasible solution for data sharing and collaboration. Furthermore, blockchain gives the feature of decentralization to D2D. Particularly, Seng et al. [60] investigated ultra-dense wireless networks (UDNs). A decentralized computation offloading platform was proposed to coordinate tasks among devices and edge servers. Furthermore, Zhang et al. [47] studied cache sharing for data delivery. To assist MEC based offloading for inter-domain traffic, they proposed a blockchain-enabled market to motivate both D2D and MEC nodes. Plus, a partial Practical Byzantine Fault Tolerance protocol was proposed to minimize latency and guarantee the confidence level of the D2D sharing.
- *Edge Computing*: The tradeoff between limited resources and required latency is a major challenge for edge computing. To deal with this issue, Wu et al. [61] considered the collaboration of edge and cloud. They proposed an energy-efficient IoT task offloading algorithm for blockchain-enabled edge computing. Additionally, Xu et al. [62] studied crowd-intelligence. An ecosystem was designed for trustless and hybrid human-machine crowd-intelligence. Zhang et al. [63] further investigated edge service migration. A blockchain-based secure edge service migration, namely Falcon, was proposed to extend the service scalability and flexibility. Furthermore, Chuang et al. [64] presented a trust-aware IoT data economic system (TIDES). The trading process in MEC systems was entirely based on the smart contract. Furthermore, Feng et al. [65] optimized the allocation of limited radio and computational resources. The schedul-

ing of block producers was considered in this resource allocation. Furthermore, fast transaction writing and maximum mining revenue should be considered separately according to different IoT device requirements. A blockchain-based offloading strategy was given for the above scenarios in MEC systems [66].

- *Edge Caching*: Content caching is a popular solution to the ever-increasing IoT data traffic. Liu et al. [67] gave the offloading mode selection and caching strategy for wireless blockchain networks. A novel MEC-enabled wireless blockchain framework was further given for computation offloading and content caching [68]. Besides, ultra-reliable communication is a popular trend. Sharma et al. [69] used neural-blockchain for ultra-reliable caching in drone networks. Additionally, Cui et al. [70] implemented FL for content caching in edge computing. A novel compressed algorithm of the FL approach, namely CREAT, was proposed for this edge caching case.
- *Distributed Network Function Virtualization*: As a fundamental technology of software-defined industrial IoT [71,72], network function virtualization (NFV) has emerged in blockchain-enabled edge intelligence recently. Distributed NFV offers a flexible way for large scale IoT networks management. Fu et al. [73] proposed a blockchain-based framework to reach consensus across different management and orchestration systems. Furthermore, a novel distributed software-defined network (SDN) architecture was proposed to control fog nodes at the network edge [74].

Table 2 summarizes the literature on IoT communications and their related research directions.

Table 2. Research directions and related literature on IoT communications.

Directions	Ref.	Contributions
5G and Beyond	[12]	Provide proof-of-concept for blockchain applications in 5G and beyond networks.
	[13]	Investigate the potential of blockchain in 5G and beyond network for IoT.
	[16]	Suggest guidelines toward blockchain enabled IoT with 6Gcommunication.
	[59]	Propose blockchain-enabled learning framework for 5G beyondscenarios.
Decentralized D2D	[60]	Propose decentralized platform design for D2D computationcoordination in UDNs.
	[47]	Optimize the decentralized D2D sharing and design the consensus for transactions execution.
Edge Computing	[61]	Propose an energy-efficient IoT task offloading algorithm for blockchain-enabled edge computing.
	[62]	Design a trustless hybrid human-machine ecosystem for industrial IoT based on crowd-intelligence.
	[63]	Propose a novel service migration framework for flexible edge service.
	[64]	Propose a trust-aware data trading system for MEC.
	[65]	Design the joint resources allocation for blockchain-enabled MEC systems.
	[66]	Propose a blockchain-based offloading strategy in MEC scenarios
Edge Caching	[67]	Propose caching strategy for wireless blockchain networks.
	[68]	Design an MEC-enabled wireless blockchain framework.
	[69]	Propose an ultra-reliable drone-caching approach enabled by neural-blockchain.
	[70]	Propose edge caching solutions based on FL.
Distributed NFV	[73]	Propose a distributed NFV framework for management and orchestration based on the MEC-enabled blockchain.
	[74]	Propose a novel distributed network architecture for fog nodes based on SDN.

3.2. Blockchain-Based IoT Security

No technology is perfect, neither is blockchain. The vulnerabilities of blockchain technology have drawn the attention of both industries and academics [75]. For example, a smart contract developer may make errors, and the related vulnerability could cause a

hard fork in the blockchain system. Moreover, consensus mechanisms have the risk of 51% vulnerability, which may cause malicious manipulations of transaction records. Therefore, researchers and system designers should consider security issues while investigating blockchain-based IoT systems.

- *Authentication*: Authentication based on public-key cryptography is an effective solution to the security issue in IoT systems. A group signature scheme was proposed for block validation in MEC [76]. Moreover, the authentication of FL nodes was given in the Internet of health things [77]. The participating nodes were authenticated by the smart contract in the proposed FL framework. Furthermore, Lin et al. [78] investigated the authenticity of emergency levels in healthcare cases. The delay of the MEC network was also optimized by them.
- *Data Security*: With the immutability of data records, blockchain has a nature of data security. Therefore, this topic was considered in most literature in this research area. For example, Kang et al. [79] gave a secure data sharing scheme based on the consortium blockchain and smart contracts for vehicular networks.
- *Data Privacy*: In public blockchain systems, participants are anonymous because they are just hashes of public keys. Different from a public blockchain in which all records are visible to everyone, a permissioned or private blockchain, such as the Hyperledger Fabric, only allows authenticated entities to access the data on the blockchain. Furthermore, the zero-knowledge proof is another technique to make a transaction without revealing participants' information. It has been implemented to Zcash, a privacy-protecting digital currency. For data privacy in IoT systems, IoT devices are normally linked to human activities, storing sensitive data owned by individuals. Zyskind et al. [80] introduced blockchain to protect personal data. Nguyen et al. [33] considered privacy level for blockchain users in MEC systems. Furthermore, the privacy of the MEC network topology also needs protection. Yang et al. [81] constructed an MEC system without exposing topology privacy. Lu et al. [40] further investigated privacy-preserved data sharing for industrial IoT. FL was used to deal with IoT data leakage. Moreover, Arachchige et al. [82] proposed a privacy-preserving framework, namely PriModChain.
- *Data Integrity*: Reliable data acquisition requires data integrity. Islam and Shin [83] proposed a UAV-assisted data acquisition scheme based on blockchain technology. The data were encrypted with the help of a UAV. In addition, Kumar et al. [84] presented a novel framework called 'BlockEdge', which used blockchain to provide data integrity in a decentralized manner. Furthermore, client data can be verified to ensure integrity. Zhang et al. [85] proposed a platform architecture to detect the failure in industrial IoT. The Merkle tree was used in this platform.

Table 3 summarizes the literature on IoT security and the related research directions.

Table 3. Research directions and related literature on IoT security.

Directions	Ref.	Contributions
Authentication	[76]	Design a group signature scheme for MEC based on blockchain.
	[77]	Propose an authentication framework for participating FL nodes.
	[78]	Optimize the MEC network delay with authenticity priorities.
Data Security	[79]	Propose a secure data sharing scheme based on consortium blockchain.
Data Privacy	[33]	Propose an MEC-based blockchain network and maximize the privacy levels.
	[81]	Employ blockchain for topology protection in MEC.
	[40]	Design a secure data sharing architecture based on FL for industrial IoT.
	[82]	Propose a novel privacy-preserving framework for ML in industry 4.0.
Data Integrity	[83]	Propose a UAV-based scheme to achieve integrity in IoT data acquisition.
	[84]	Propose a novel blockchain and edge framework to ensure data integrity in Industry 4.0.
	[85]	Design a verifiable data architecture for device failure detection in industrial IoT.

3.3. Blockchain-Enabled Incentive Mechanisms in IoT

- *Energy Trading*: On one hand, most IoT and other edge devices are energy-constrained. On the other hand, IoT devices generate and own a huge amount of data, containing valuable information. Therefore, knowledge and energy trading between edge servers and edge nodes is a research trend in this area. Lin et al. [4] proposed a novel edge intelligence framework using wireless power transfer. By exploring the permissioned blockchain, the energy and knowledge trading was secured in the proposed framework. Furthermore, Kang et al. [86] designed a peer-to-peer energy trading model. An incentive mechanism was proposed for discharging electrical vehicles to boost the electric power grid. A pricing platform was further given based on a consortium blockchain. Additionally, the FL-based power management was investigated by Wang et al. [87]. They proposed an AI-enabled, blockchain-based electric vehicle integration system, named AEBIS, for smart grid. The overall supply power could be balanced by demand-side devices.
- *Entities Collaboration*: Motivated by the mining reward process, collaboration design among different entities in IoT systems emerges as a popular direction in this research area. Liu et al. [88] motivated the collaboration among content owners, transcoders, and receivers by the proposed framework in MEC-enabled video steaming. Besides, Zhao et al. [44] proposed an FL-enabled crowdsourcing framework for smart home systems, in which collaboration was motivated by the reward. Furthermore, a new proof of business consensus protocol was developed by Hu et al. [89] to guarantee the incentive in blockchain-enabled federated slicing. Moreover, Ridhawi et al. [90] studied the composition process in content delivery networks. Participants were rewarded by fog entities for solving this process in multimedia service delivery.
- *Auction Mechanism*: MEC servers require incentives to execute the tasks offloaded from IoT devices. However, trustworthiness should be considered in this research direction. Sun et al. [91] proposed double auction mechanisms to motivate MEC servers. Moreover, a blockchain was used to prevent record tampering from malicious edge servers.

Table 4 summarizes the literature on incentive mechanisms in IoT and the related research directions.

Table 4. Research directions and literature related to incentive mechanism in IoT.

Directions	Ref.	Contributions
Energy Trading	[4]	Propose a novel knowledge and energy trading frame work based on permissioned blockchain.
	[86]	Propose a peer-to-peer energy trading model based on the consortium blockchain.
	[87]	Propose a novel power management platform based on the blockchain and FL for smart grid.
Entities Collaboration	[88]	Design an incentive mechanism based on blockchain to enable collaboration in MEC-enabled video steaming.
	[44]	Propose an incentive mechanism to award entities in FL crowdsourcing for smart home systems.
	[89]	Develop a new proof of business consensus protocol to incentive entities in federated network slicing.
	[90]	Propose a blockchain-enabled service composition solution.
Auction Mechanism	[91]	Propose double auction mechanisms to motivate MEC servers in cross-server resource allocation.

3.4. Decentralized ML in IoT

- *Neural Networks*: Using neural networks in the Internet of medical things is a popular trend. However, medical data are privacy-sensitive and vulnerable to malicious attacks. Połap et al. [92] proposed a federated approach for blockchain-based neural networks in Internet of medical things. It guaranteed distributed and local data storage for patients.
- *Deep Reinforcement Learning*: This learning approach was widely used in academic research. However, most papers just applied deep reinforcement learning (DRL) mechanically for optimization purposes. Another trend is to explore its potential for IoT, especially in mobile blockchain applications. Gao et al. [93] gave a task scheduling approach based on DRL to maximize the mining reward and minimize the cost. Moreover, a DRL approach was presented for blockchain-enabled MEC [94]. Cooperative task offloading was investigated in this paper. Furthermore, Zhuang et al. [95] investigated routing control in blockchain-enabled MEC. A novel DRL-based approach was given for adaptive network routing. Moreover, Yu et al. [96] investigated DRL and FL jointly. They proposed an intelligent ultra-dense edge computing framework and used DRL to make the offloading decision and to allocate resources. Furthermore, Jiang et al. [97] proposed a video analytics framework and DRL solutions to reduce the latency of the MEC system in the Internet of autonomous vehicles. Additionally, a framework was proposed for blockchain-enabled MEC. The adaptive resource allocation was given based on DRL approaches [98]. Furthermore, Asheralieva and Niyato [99] investigated deep Q-learning and Bayesian deep learning for the decision making in blockchain-based MEC.
- *FL*: Learning in a federated way is not a new topic. However, blockchain-enabled FL emerges as a popular research trend. Its decentralized framework gives privacy and security in the learning process. Hua et al. [100] proposed a blockchain-enabled FL for heavy-haul railways and implemented asynchronous collaborative learning in this federated system. Committee consensus was further devised for blockchain-enabled FL to reduce the cost of computing and increase security [101]. Moreover, cognitive computing has emerged as a new trend in Industry 4.0 networks [102]. A decentralized method was proposed for cognitive computing based on blockchain-enabled FL. Furthermore, Shen et al. [103] investigated the unintended property leakage problem. They proposed a novel property inference attack to exploit this issue in FL. Plus, Souza et al. [104] proposed a distributed and federated approach

named as DFedForest, which was based on random forest algorithms and blockchain technologies. Additionally, a decentralized deep learning method called DDLPF was proposed for IoT applications [105]. DDLPF is a decentralized deep learning paradigm with privacy-preservation and fast few-shot learning. The meta-learning, FL, and blockchain techniques were jointly investigated in this paper.

Table 5 summarizes the literature on ML in IoT and the related research directions.

Table 5. Research directions and literature related to ML in IoT.

Directions	Ref.	Contributions
Neural Networks	[92]	Design a federated approach for neural networks in the Internet of medical things.
DRL	[93]	Propose a DRL-based solution for task scheduling in the mobile blockchain.
	[94]	Proposed a cooperative computation offloading strategy based on DRL for blockchain-enabled MEC.
	[95]	Propose a DRL-based routing control for blockchain-based MEC.
	[96]	Propose DRL-based strategies for offloading and resources management in ultra-dense edge networks.
	[97]	Propose DRL solutions for MEC-enabled video analytics on the Internet of autonomous vehicles.
	[98]	Propose a framework for edge nodes to reach consensus and allocate resources by DRL approaches.
	[99]	Develop a learning approach for decision making based on deep Q-learning in blockchain-based MEC.
FL	[100]	Propose a blockchain-enabled FL method in haul railway control system.
	[101]	Devise an innovative committee consensus mechanism for blockchain-enabled FL.
	[102]	Propose a cognitive computing paradigm based on FL and blockchain.
	[103]	Propose a novel property inference attack to evaluate the property leakage in blockchain-enabled FL for intelligence edge computing.
	[104]	Design a novel and decentralized FL method based on forest algorithms and blockchain.
	[105]	Propose a practical decentralized deep learning approach for IoT applications based on the FL and blockchain.

3.5. Recent Advances

In this part, we select and introduce some recent advances related to blockchain-enabled edge intelligence. These topics are not fully investigated yet, but a few high-quality works have already been done. We aim at highlighting these new topics for researchers who wish to glimpse the latest research trends in this area. In addition, these advances further support that blockchain-enabled edge intelligence could be a game-changer across different industries.

- *Video Streaming*: Traditional video streaming requires centralized governance of data, which leads to centralized and low-profit video processing. Moreover, this centralized management and distribution of a large volume of video content require substantial data storage and communication bandwidth at a huge cost. In addition, video streams have to be converted into several versions to meet the different requirements of downloaders, by a process called video transcoding [106] that is a computation task with

a heavy workload. By exploiting blockchain-enabled edge intelligence, transcoding tasks can be offloaded to MEC servers and user privacy is also secured. This approach was proposed by Liu et al. [107], and smart contracts were further implemented to enable self-organized video streaming. Lui et al. [36] further proposed an adaptive block size scheme in Reference [36], together with an autonomous content delivery market based on smart contracts. The authors further developed incentive mechanisms to facilitate collaboration among content providers, transcoders, and downloaders in Reference [88].

- *Tactile Internet*: Ultra-low delay communication is the main feature of the tactile Internet, which could be brought into reality With the help of 5G and beyond networks. This has motivated multiple research works and applications, such as haptic communications [108] and real-time telesurgery [109,110]. By bringing computing and caching resources close to end devices, MEC becomes the key to realize the above delay-sensitive application. A few papers have investigated the blockchain-enabled tactile Internet incorporating MEC. For example, Hassija et al. [111] proposed a blockchain-based mobile data offloading scheme to deal with the efficiency and scalability issues in tactile Internet. Furthermore, drone-based tactile Internet was studied in Reference [112]. A blockchain-based security framework was introduced to replace heavy security algorithms for resource-constrained drones.
- *Digital Twins*: Real-world physical components can be virtualized into the digital world. This real-time simulation is like a man in a mirror. All replicas of the same physical component are called digital twins (DTs) [113]. Furthermore, blockchain was investigated in this paper to ensure transparency, trust, and security across different industries. Moreover, blockchain-enabled low-latency FL was proposed for edge association in DTs wireless network [114]. The time cost and learning accuracy were balanced by exploring multi-agent reinforcement learning optimization. Furthermore, Lu et al. [115] explored empowering FL with permissioned blockchain to improve communication security and data privacy protection in DTs edge networks.

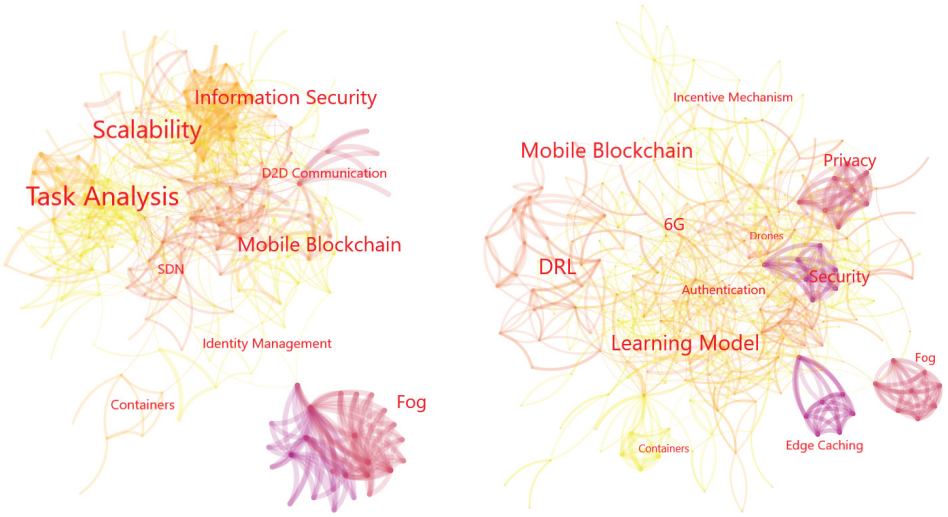
3.6. Summery of Topics and Trends

In the following, we summarize hot topics and research trends based on the previous mining of peer-viewed articles in the institute of electrical and electronics engineers (IEEE) Explore and Web of Science databases, including early accessed papers. Further, we visualize hot topics based on co-citation and co-word graphs. Finally, we illustrate multiple emerging trends according to the timeline.

Keywords could be a strong tool to classify different topics related to blockchain-enabled edge intelligence. In this subsection, we use CiteSpace [22], a data mining tool empowered by ML algorithms, to classify hot topics for readers. The purpose of this data mining is to offer an intuitive vision of this research area.

Particularly, we use the log-likelihood ratio (LLR) algorithm to identify popular topics for researchers. Before we give the illustration, the two graph types are explained as follows: (1) Co-citation relationship: the correlation of two paper exists when they are cited in the same paper. This relationship gets stronger when more co-citations occur. (2) Co-word relationship: keywords in the same paper have certain correlations. If the co-occurring of two keywords happens frequently, then the co-word relationship between these two keywords is strong.

The light color of a link means the co-citation exists recently. The dark color means the correlation between this literature pair occurs early. The font size of each topic represents its co-citation and co-word frequencies in Figure 4a,b, respectively. Readers could visualize the big picture of the research area from these figures.



(**a**) Co-citation graph (**b**) Co-word graph

Figure 4. Illustration of emerging trends. (**a**) Co-citation graph. (**b**) Co-word graph.

Based on the above data mining and classification, we propose some emerging trends according to the timeline in Figure 5. The selected topics have occurred in the existing literature frequently. One can see that we slice the related topics according to the years of publications. In addition, more and more topics and related works emerge as time goes by. This means the surveyed research area is evolving and becoming more popular.

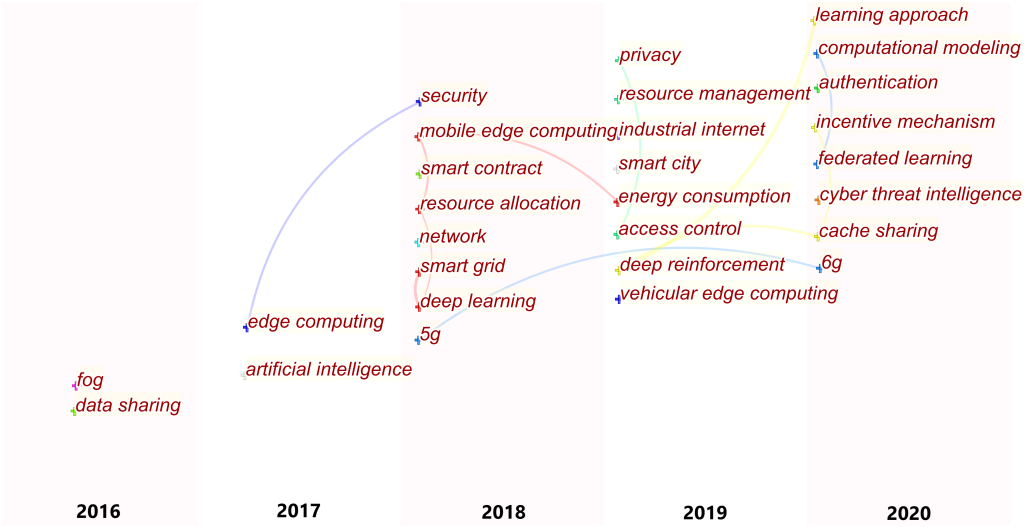


Figure 5. Emerging trends according to timeline.

As we can see from the above picture, there are multiple links between pairs of hot topics. A link between two topics means that they are correlated. For example, 5G-related blockchain-enabled edge intelligence was a hot topic in 2018. It evolved and became 6G in 2020. In addition, deep learning was a hot topic in 2018, but it evolved to deep reinforcement learning in 2019, and finally updated to FL in 2020. Moreover, privacy and access control were two correlated topics in 2019. Additionally, blockchain-enabled mobile edge computing mainly focused on resource allocation in 2018 and then there were more works related to energy consumption and privacy issues in 2019. This makes sense because IoT devices are energy-constrained, especially for those in industrial IoT systems [116].

4. Open Issues and Discussions

In this section, we sum up some open issues for blockchain-enabled edge intelligence. We first discuss blockchain-enabled trust in three layers, namely the social layer, data layer, and technical layer. We aim to help readers understand this research area from different perspectives but not limited to the technical domain. Next, we list and describe some challenges and research gaps in this area, including selfish learning, fork issues, and transaction rejection. Finally, we raise three research questions by discussing some unresolved issues and conflicts in this research area.

4.1. Trust Layers for Edge Intelligence

Blockchain-enabled trust could be considered in different layers for researchers and developers from different research areas. We further extend the description of blockchain trust layers [117] for blockchain-enabled edge intelligence as follows:

- *Social Layer*: the layer at which task publishers (e.g., IoT devices or human users), workers (e.g., edge nodes or servers), and blockchain platforms (e.g., smart contracts, decentralized applications) could interact with each other and make transactions on resources and information. In this layer, interactions among entities could include reputation establishment [118], resources marketing [119], paid collaboration, identity management, and the regulation of training strategies.
- *Data Layer*: the layer at which information records in blockchain are managed by self-governance. The recorded data could include learning model parameters, IoT data, reputation records, published tasks, transaction records, and the history of global learning models. This layer concerns with learning quality, data integrity, privacy, protection, the architecture of blockchain transactions, and the lifecycle of records.
- *Technical Layer*: the layer at which strategies are implemented to realize the functions of edge intelligence. Platforms (e.g., Hyperledger Fabric) and mathematical foundations are included in this layer. Such strategies could include learning algorithms, consensus mechanisms, incentive mechanisms, zero-knowledge proofs, secure multi-party computation, contribution evaluation frameworks, optimization algorithms, etc.

4.2. Challenges and Research Gaps

Although blockchain has many advantages according to our literature review, it is not perfect for edge intelligence in IoT. To realize the blockchain-enabled edge intelligence, there are still many research gaps in this area. We list some major challenges as follows:

- *Selfish Learning*: In the Bitcoin system, selfish mining [120] may cause serious security and fairness issues. Selfish miners refer to a group of miners who collude to increase their reward. Minority groups or individuals could not compete with the selfish group because of their limited computing resources. This could further lead to the centralization of mining operations. Motivated by selfish mining, selfish learning attacks are attacking blockchain-enabled edge intelligence systems, where edge nodes exchange learning experiences and get the reward according to their contributions [121]. In such attacks, edge nodes collude in an FL scenario and accumulate model contributions. In this case, the selfish group will always win and get a reward. Moreover, other normal learning nodes tend to join in this selfish group for mining rewards. Furthermore, individuals can become selfish too. A single learning node may not powerful enough to win, so it just hides, waits, and accumulates its model contribution for future rewards. This could cause delays and decrease the quality of the global learning model.
- *Fork Issues*: Forks occur when the software of different mining nodes become misaligned. When edge nodes are not in agreement with the same learning model or algorithm, an alternative chain (i.e., a forked chain) emerges. Two potential conditions may cause a fork in a blockchain-enabled edge intelligence system. On one hand, the computing capability of MEC servers, which are close to the task publisher (i.e., the IoT device) geographically, is limited and relatively weak. A malicious attacker can deploy a powerful rogue MEC server close to the target task publisher. As the

requirement of low-latency in edge intelligence is met with fast consensus mechanisms in blockchain systems, the mining puzzle could be very easily solved by this powerful rogue server. With malicious intentions in mind, this rogue node could start a fork to attack the global learning model. On the other hand, the global model could also fork accidentally if two learning nodes contribute the most and equally to the global learning model in the same iteration, as both model contributions are recorded at nearly the same time.

- *Transaction Rejection*: Edge nodes are resource-constrained, especially for IoT devices. Although there are several research works related to incentive mechanisms for IoT devices and edge servers, transaction rejection is still an unresolved problem. Most papers take the success of blockchain transactions for granted because miners are assumed to have a strong desire to record the transaction into a block for a reward. However, blockchain nodes could always refuse to participate in mining if the predefined reward is not good enough because solving computational puzzles costs a lot of energy. As resource-constrained devices, edge nodes may not spend their energy and join in the blockchain system because they have difficulty in recharging. In such cases, transactions are always rejected, and the consensus of a global learning model is hard to realize.

4.3. Cross-Layer Research Questions

As discussed in the above section, topics and research trends are focused on different layers of blockchain-enabled trust. For example, decision-making in the social layer; security and privacy issues in the data layer; and mathematical foundation and mechanisms in the technical layer. However, there are some conflicts in the existed literature that cut across these layers. We briefly summarize them into three research questions:

- *Question 1*: How to design a balanced framework for blockchain-enabled edge intelligence?
  This is a common issue that exists in most decentralized systems. The Zooko's Triangle [122] points out that it is highly unlikely to have a decentralized system with both security and human-readability. Thus, we could further acknowledge that efficiency, security, and decentralization are three angles in the Zooko's triangle of blockchain-enabled edge intelligence. Researchers should keep this conflict in mind when they use blockchains to enable edge intelligence. For example, either the decentralization level or security level might be sacrificed when they maximize the transaction speed in edge systems. Thus, a trade-off exists among these factors.
- *Question 2*: How to establish standard criteria to verify a high-quality training model for edge intelligence?
  Deep learning models or parameters are shared and traded in decentralized ML, such as FL. However, there is no general criterion for evaluating and verifying recorded models or parameters. Each paper has its own method that may not be readily compared with that implemented in another article. Furthermore, it might not be a good idea to simply use accuracy or the loss function to verify the quality of the ML model because it could cost a lot of energy and time for training a very accurate model, which might not be preferable for energy-constrained devices in some low-latency cases.
- *Question 3*: How to reduce the complexity of blockchain strategies for edge intelligence?
  Different from other devices, edge or IoT devices are resource-constrained. Blockchain strategies presented in most papers are not suitable for the blockchain-enabled edge intelligence because most proposed algorithms, such as zero-knowledge proof for privacy preservation, are too complicated for edge nodes to execute. Researchers should keep this in mind when they develop their own strategies in the scenario of blockchain-enabled edge intelligence.

5. Conclusions

In this review, we have given a thorough literature survey on blockchain-enabled edge intelligence. To help researchers and readers in understanding this area, we have first given some basic knowledge about blockchain, MEC, and AI. Furthermore, research trends and directions have been introduced by exploring literature mining. We have presented a vision of research trends, as well as the hot topics, in this area. Additionally, video streaming, tactile Internet, and digital twins (DTs) have been highlighted and introduced for their cutting-edge applications. Finally, we have discussed some open issues and research gaps, including selfish learning, fork issues, and transaction rejection.

Funding: This work was supported by Blockchain@UBC, the Natural Sciences and Engineering Research Council of Canada (CREATE Grant 528125 and Grant RGPIN-2019-06348), and the Guangdong Pearl River Talent Recruitment Program (Grant 2019ZT08X603).

Acknowledgments: We thank the editor and reviewers for their constructive comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ashton, K. That 'Internet of Things' Things. *RFID J.* **2009**, *22*, 97–114.
2. Deng, S.; Zhao, H.; Fang, W.; Yin, J.; Dustdar, S.; Zomaya, A.Y. Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. *IEEE Internet Thing. J.* **2020**, *7*, 7457–7469. [CrossRef]
3. Kim, H.; Park, J.; Bennis, M.; Kim, S. Blockchained On-Device Federated Learning. *IEEE Commun. Lett.* **2020**, *24*, 1279–1283. [CrossRef]
4. Lin, X.; Wu, J.; Bashir, A.K.; Li, J.; Yang, W.; Piran, J. Blockchain-Based Incentive Energy-Knowledge Trading in IoT: Joint Power Transfer and AI Design. *IEEE Internet Thing. J.* **2020**, 1–14. [CrossRef]
5. Rivera, A.V.; Refaey, A.; Hossain, E. A Blockchain Framework for Secure Task Sharing in Multi-Access Edge Computing. *IEEE Netw.* **2020**, 1–8. [CrossRef]
6. ElMamy, S.B.; Mrabet, H.; Gharbi, H.; Jemai, A.; Trentesaux, D. A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0. *Sustainability* **2020**, *12*, 9179. [CrossRef]
7. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. *Sensors* **2019**, *19*, 1788. [CrossRef]
8. Jameel, F.; Javaid, U.; Khan, W.U.; Aman, M.N.; Pervaiz, H.; Jantti, R. Reinforcement Learning in Blockchain-Enabled IIoT Networks: A Survey of Recent Advances and Open Challenges. *Sustainability* **2020**, *12*, 5161. [CrossRef]
9. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C.M. Blockchain and Machine Learning for Communications and Networking Systems. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1392–1431. [CrossRef]
10. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166. [CrossRef]
11. Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and Open Research Challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
12. Tahir, M.; Habaebi, M.H.; Dabbagh, M.; Mughees, A.; Ahad, A.; Ahmed, K.I. A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities. *IEEE Access* **2020**, *8*, 115876–115904. [CrossRef]
13. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [CrossRef]
14. Xiong, Z.; Zhang, Y.; Niyato, D.; Wang, P.; Han, Z. When Mobile Blockchain Meets Edge Computing. *IEEE Commun. Mag.* **2018**, *56*, 33–39. [CrossRef]
15. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1508–1532. [CrossRef]
16. Sekaran, R.; Patan, R.; Raveendran, A.; Al-Turjman, F.; Ramachandran, M.; Mostarda, L. Survival Study on Blockchain Based 6G-Enabled Mobile Edge Computation for IoT Automation. *IEEE Access* **2020**, *8*, 143453–143463. [CrossRef]
17. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, fog and edge computing enabled smart campuses and universities. *Appl. Sci.* **2019**, *9*, 4479. [CrossRef]
18. Chamola, V.; Hassija, V.; Gupta, V.; Guizani, M. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access* **2020**, *8*, 90225–90265. [CrossRef]
19. Queiroz, A.; Oliveira, E.; Barbosa, M.; Dias, K. A Survey on Blockchain and Edge Computing Applied to the Internet of Vehicles. Available online: https://arxiv.org/ftp/arxiv/papers/2011/2011.13676.pdf (accessed on 12 February 2021).

20. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.Y.; Koh, L.H. Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey. Available online: https://arxiv.org/pdf/2007.06022.pdf (accessed on 12 February 2021).
21. Jiang, X.; Yu, F.R.; Song, T.; Ma, Z.; Song, Y.; Zhu, D. Blockchain-Enabled Cross-Domain Object Detection for Autonomous Driving: A Model Sharing Approach. *IEEE Internet Thing. J.* **2020**, *7*, 3681–3692. [CrossRef]
22. Chen, C.; Song, M. Visualizing a field of research: A methodology of systematic scientometric reviews. *PLoS ONE* **2019**, *14*, e0223994. [CrossRef]
23. Kiayias, A.; Koutsoupias, E.; Kyropoulou, M.; Tselekounis, Y. Blockchain Mining Games. In Proceedings of the 2016 ACM Conference on Economics and Computation, Maastricht, The Netherlands, 24–28 July 2016; pp. 365–382.
24. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
25. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
26. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 17 August 2012.
27. Satyanarayanan, M. The Emergence of Edge Computing. *Computer* **2017**, *50*, 30–39. [CrossRef]
28. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile Edge Computing: A Survey. *IEEE Internet Thing. J.* **2018**, *5*, 450–465. [CrossRef]
29. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K.B. A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2322–2358. [CrossRef]
30. Porambage, P.; Okwuibe, J.; Liyanage, M.; Ylianttila, M.; Taleb, T. Survey on Multi-Access Edge Computing for Internet of Things Realization. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2961–2991. [CrossRef]
31. Rahman, A.; Hossain, M.S.; Loukas, G.; Hassanain, E.; Rahman, S.S.; Alhamid, M.F.; Guizani, M. Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications. *IEEE Access* **2018**, *6*, 72469–72478. [CrossRef]
32. Guan, Z.; Lyu, H.; Li, D.; Hei, Y.; Wang, T. Blockchain: A distributed solution to UAV-enabled mobile edge computing. *IET Commun.* **2020**, *14*, 2420–2426. [CrossRef]
33. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Privacy-Preserved Task Offloading in Mobile Blockchain with Deep Reinforcement Learning. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 2536–2549. [CrossRef]
34. Shrestha, R.; Nam, S.Y.; Bajracharya, R.; Kim, S. Evolution of V2X Communication and Integration of Blockchain for Security Enhancements. *Electronics* **2020**, *9*, 1338. [CrossRef]
35. Xiao, L.; Ding, Y.; Jiang, D.; Huang, J.; Wang, D.; Li, J.; Vincent Poor, H. A Reinforcement Learning and Blockchain-Based Trust Mechanism for Edge Networks. *IEEE Trans. Commun.* **2020**, *68*, 5460–5470. [CrossRef]
36. Liu, M.; Teng, Y.; Yu, F.R.; Leung, V.C.M.; Song, M. A Mobile Edge Computing (MEC)-Enabled Transcoding Framework for Blockchain-Based Video Streaming. *IEEE Wirel. Commun.* **2020**, *27*, 81–87. [CrossRef]
37. Zhang, Z.; Hong, Z.; Chen, W.; Zheng, Z.; Chen, X. Joint Computation Offloading and Coin Loaning for Blockchain-Empowered Mobile-Edge Computing. *IEEE Internet Thing. J.* **2019**, *6*, 9934–9950. [CrossRef]
38. Zhao, N.; Wu, H.; Chen, Y. Coalition Game-Based Computation Resource Allocation for Wireless Blockchain Networks. *IEEE Internet Thing. J.* **2019**, *6*, 8507–8518. [CrossRef]
39. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, D. Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1977–2008. [CrossRef]
40. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4177–4186. [CrossRef]
41. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Zhang, J. Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory. *IEEE Internet Thing. J.* **2019**, *6*, 10700–10714. [CrossRef]
42. Kang, J.; Xiong, Z.; Niyato, D.; Zou, Y.; Zhang, Y.; Guizani, M. Reliable Federated Learning for Mobile Networks. *IEEE Wirel. Commun.* **2020**, *27*, 72–80. [CrossRef]
43. Rehman, M.H.u.; Salah, K.; Damiani, E.; Svetinovic, D. Towards Blockchain-Based Reputation-Aware Federated Learning. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on ComputerCommunications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 183–188.
44. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet Thing. J.* **2020**. [CrossRef]
45. Passerat-Palmbach, J.; Farnan, T.; McCoy, M.; Harris, J.D.; Manion, S.T.; Flannery, H.L.; Gleim, B. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain 2020), Rhodes Island, Greece, 2–6 November 2020; pp. 550–555.
46. Qu, Y.; Gao, L.; Luan, T.H.; Xiang, Y.; Yu, S.; Li, B.; Zheng, G. Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing. *IEEE Internet Thing. J.* **2020**, *7*, 5171–5183. [CrossRef]
47. Zhang, R.; Yu, F.R.; Liu, J.; Huang, T.; Liu, Y. Deep Reinforcement Learning (DRL)-Based Device-to-Device (D2D) Caching with Blockchain and Mobile Edge Computing. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 6469–6485. [CrossRef]

48. Somy, N.B.; Kannan, K.; Arya, V.; Hans, S.; Singh, A.; Lohia, P.; Mehta, S. Ownership Preserving AI Market Places Using Blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain 2019), Atlanta, GA, USA, 14–17 July 2019; pp. 156–165.
49. Ouyang, L.; Yuan, Y.; Wang, F.Y. Learning Markets: An AI Collaboration Framework Based on Blockchain and Smart Contracts. *IEEE Internet Thing. J.* **2020**. [CrossRef]
50. Toyoda, K.; Zhao, J.; Zhang, A.N.S.; Mathiopoulos, P.T. Blockchain-Enabled Federated Learning with Mechanism Design. *IEEE Access* **2020**, *8*, 219744–219756. [CrossRef]
51. Lugan, S.; Desbordes, P.; Brion, E.; Tormo, L.X.R.; Legay, A.; Macq, B. Secure Architectures Implementing Trusted Coalitions for Blockchained Distributed Learning (TCLearn). *IEEE Access* **2019**, *7*, 181789–181799. [CrossRef]
52. Ma, L.; Pei, Q.; Zhou, L.; Zhu, H.; Wang, L.; Ji, Y. Federated Data Cleaning: Collaborative and Privacy-Preserving Data Cleaning for Edge Intelligence. *IEEE Internet Thing. J.* **2020**. [CrossRef]
53. Ramanan, P.; Nakayama, K. BAFFLE: Blockchain Based Aggregator Free Federated Learning. In Proceedings of 2020 IEEE International Conference on Blockchain (Blockchain 2020), Rhodes Island, Greece, 2–6 November 2020; pp. 72–81.
54. Yin, B.; Yin, H.; Wu, Y.; Jiang, Z. FDC: A Secure Federated Deep Learning Mechanism for Data Collaborations in the Internet of Things. *IEEE Internet Thing. J.* **2020**, *7*, 6348–6359. [CrossRef]
55. Wang, Q.; Guo, Y.; Wang, X.; Ji, T.; Yu, L.; Li, P. AI at the Edge: Blockchain-Empowered Secure Multiparty Learning With Heterogeneous Models. *IEEE Internet Thing. J.* **2020**, *7*, 9600–9610. [CrossRef]
56. Liu, Y.; Peng, J.; Kang, J.; Iliyasu, A.M.; Niyato, D.; El-Latif, A.A.A. A Secure Federated Learning Framework for 5G Networks. *IEEE Wirel. Commun.* **2020**, *27*, 24–31. [CrossRef]
57. Zhang, K.; Zhu, Y.; Maharjan, S.; Zhang, Y. Edge Intelligence and Blockchain Empowered 5G Beyond for the Industrial Internet of Things. *IEEE Netw.* **2019**, *33*, 12–19. [CrossRef]
58. Khan, L.U.; Yaqoob, I.; Imran, M.; Han, Z.; Hong, C.S. 6G Wireless Systems: A Vision, Architectural Elements, and Future Directions. *IEEE Access* **2020**, *8*, 147029–147044. [CrossRef]
59. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for 5G Beyond. *IEEE Netw.* **2020**, *35*, 219–225.
60. Seng, S.; Li, X.; Luo, C.; Ji, H.; Zhang, H. A D2D-assisted MEC Computation Offloading in the Blockchain-Based Framework for UDNs. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; IEEE: New York City, NY, USA, 2019.
61. Wu, H.; Wolter, K.; Jiao, P.; Deng, Y.; Zhao, Y.; Xu, M. EEDTO: An Energy-Efficient Dynamic Task Offloading Algorithm for Blockchain-Enabled IoT-Edge-Cloud Orchestrated Computing. *IEEE Internet Thing. J.* **2020**, *8*, 2163–2176. [CrossRef]
62. Xu, J.; Wang, S.; Bhargava, B.K.; Yang, F. A Blockchain-Enabled Trustless Crowd-Intelligence Ecosystem on Mobile Edge Computing. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3538–3547. [CrossRef]
63. Zhang, X.; Wu, W.; Yang, S.; Wang, X. Falcon: A Blockchain-Based Edge Service Migration Framework in MEC. *Mob. Inf. Syst.* **2020**, *2020*, 8820507. [CrossRef]
64. Chuang, I.H.; Huang, S.H.; Chao, W.C.; Tsai, J.S.; Kuo, Y.H. TIDES: A Trust-Aware IoT Data Economic System with Blockchain-Enabled Multi-Access Edge Computing. *IEEE Access* **2020**, *8*, 85839–85855. [CrossRef]
65. Feng, J.; Yu, F.R.; Pei, Q.; Du, J.; Zhu, L. Joint Optimization of Radio and Computational Resources Allocation in Blockchain-Enabled Mobile Edge Computing Systems. *IEEE Trans.Wirel. Commun.* **2020**, *19*, 4321–4334. [CrossRef]
66. Liu, W.; Cao, B.; Zhang, L.; Peng, M.; Daneshmand, M. A Distributed Game Theoretic Approach for Blockchain-based Offloading Strategy. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
67. Liu, M.; Yu, F.R.; Teng, Y.; Leung, V.C.M.; Song, M. Joint Computation Offloading and Content Caching for Wireless Blockchain Networks. In Proceedings of the IEEE Infocom 2018—IEEE Conference on Computer Communications Workshops (Infocom Wkshps), Honolulu, HI, USA, 15–19 April 2018; IEEE: New York City, NY, USA, 2018; pp. 517–522.
68. Liu, M.; Yu, F.R.; Teng, Y.; Leung, V.C.M.; Song, M. Computation Offloading and Content Caching in Wireless Blockchain Networks with Mobile Edge Computing. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11008–11021. [CrossRef]
69. Sharma, V.; You, I.; Jayakody, D.N.K.; Reina, D.G.; Choo, K.R. Neural-Blockchain-Based Ultrareliable Caching for Edge-Enabled UAV Networks. *IEEE Trans. Ind. Inform.* **2019**, *15*, 5723–5736. [CrossRef]
70. Cui, L.; Su, X.; Ming, Z.; Chen, Z.; Yang, S.; Zhou, Y.; Xiao, W. CREAT: Blockchain-assisted Compression Algorithm of Federated Learning for Content Caching in Edge Computing. *IEEE Internet Thing. J.* **2020**. [CrossRef]
71. Luo, J.; Chen, Q.; Yu, F.R.; Tang, L. Blockchain-Enabled Software-Defined Industrial Internet of Things with Deep Reinforcement Learning. *IEEE Internet Thing. J.* **2020**, *7*, 5466–5480. [CrossRef]
72. Luo, J.; Yu, F.R.; Chen, Q.; Tang, L. Blockchain-Enabled Software-Defined Industrial Internet of Things with Deep Recurrent Q-Network. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
73. Fu, X.; Yu, F.R.; Wang, J.; Qi, Q.; Liao, J. Performance Optimization for Blockchain-Enabled Distributed Network Function Virtualization Management and Orchestration. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6670–6679. [CrossRef]
74. Sharma, P.K.; Chen, M.; Park, J.H. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access* **2018**, *6*, 115–124. [CrossRef]

75. Hasanova, H.; Baek, U.j.; Shin, M.g.; Cho, K.; Kim, M.S. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *Int. J. Netw. Manag.* **2019**, *29*, e2060. [CrossRef]
76. Zhang, S.; Lee, J. A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing. *IEEE Internet Thing. J.* **2020**, *7*, 4557–4565. [CrossRef]
77. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef]
78. Lin, D.; Hu, S.; Gao, Y.; Tang, Y. Optimizing MEC Networks for Healthcare Applications in 5G Communications with the Authenticity of Users' Priorities. *IEEE Access* **2019**, *7*, 88592–88600. [CrossRef]
79. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks. *IEEE Internet of Thing. J.* **2019**, *6*, 4660–4670. [CrossRef]
80. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
81. Yang, H.; Liang, Y.; Yuan, J.; Yao, Q.; Yu, A.; Zhang, J. Distributed Blockchain-Based Trusted Multidomain Collaboration for Mobile Edge Computing in 5G and Beyond. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7094–7104. [CrossRef]
82. Arachchige, P.C.M.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S.; Atiquzzaman, M. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6092–6102. [CrossRef]
83. Islam, A.; Shin, S.Y. BUAV: A Blockchain Based Secure UAV-Assisted Data Acquisition Scheme in Internet of Things. *J. Commun. Netw.* **2019**, *21*, 491–502. [CrossRef]
84. Kumar, T.; Harjula, E.; Ejaz, M.; Manzoor, A.; Porambage, P.; Ahmad, I.; Liyanage, M.; Braeken, A.; Ylianttila, M. BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks. *IEEE Access* **2020**, *8*, 154166–154185. [CrossRef]
85. Zhang, W.; Lu, Q.; Yu, Q.; Li, Z.; Liu, Y.; Lo, S.K.; Chen, S.; Xu, X.; Zhu, L. Blockchain-based Federated Learning for Device Failure Detection in Industrial IoT. *IEEE Internet Thing. J.* **2020**. [CrossRef]
86. Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3154–3164. [CrossRef]
87. Wang, Z.; Ogbodo, M.; Huang, H.; Qiu, C.; Hisada, M.; Abdallah, A.B. AEBIS: AI-Enabled Blockchain-Based Electric Vehicle Integration System for Power Management in Smart Grid Platform. *IEEE Access* **2020**, *8*, 226409–226421. [CrossRef]
88. Liu, M.; Yu, F.R.; Teng, Y.; Leung, V.C.M.; Song, M. Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing. *IEEE Trans.Wirel. Commun.* **2019**, *18*, 695–708. [CrossRef]
89. Hu, Q.; Wang, W.; Bai, X.; Jin, S.; Jiang, T. Blockchain Enabled Federated Slicing for 5G Networks with AI Accelerated Optimization. *IEEE Netw.* **2020**, *34*, 46–52. [CrossRef]
90. Ridhawi, I.A.; Aloqaily, M.; Boukerche, A.; Jaraweh, Y. A Blockchain-Based Decentralized Composition Solution for IoT Services. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
91. Sun, W.; Liu, J.; Yue, Y.; Wang, P. Joint Resource Allocation and Incentive Design for Blockchain-Based Mobile Edge Computing. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 6050–6064. [CrossRef]
92. Połap, D.; Srivastava, G.; Jolfaei, A.; Parizi, R.M. Blockchain Technology and Neural Networks for the Internet of Medical Things. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 508–513.
93. Gao, Y.; Wu, W.; Nan, H.; Sun, Y.; Si, P. Deep Reinforcement Learning based Task Scheduling in Mobile Blockchain for IoT Applications. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–7.
94. Feng, J.; Yu, F.R.; Pei, Q.; Chu, X.; Du, J.; Zhu, L. Cooperative Computation Offloading and Resource Allocation for Blockchain-Enabled Mobile-Edge Computing: A Deep Reinforcement Learning Approach. *IEEE Internet Thing. J.* **2020**, *7*, 6214–6228. [CrossRef]
95. Zhuang, Z.; Wang, J.; Qi, Q.; Liao, J.; Han, Z. Adaptive and Robust Routing with Lyapunov-Based Deep RL in MEC Networks Enabled by Blockchains. *IEEE Internet Thing. J.* **2020**. [CrossRef]
96. Yu, S.; Chen, X.; Zhou, Z.; Gong, X.; Wu, D. When Deep Reinforcement Learning Meets Federated Learning: Intelligent Multi-Timescale Resource Management for Multi-access Edge Computing in 5G Ultra Dense Network. *IEEE Internet Thing. J.* **2020**. [CrossRef]
97. Jiang, X.; Yu, F.R.; Song, T.; Leung, V.C.M. Intelligent Resource Allocation for Video Analytics in Blockchain-Enabled Internet of Autonomous Vehicles with Edge Computing. *IEEE Internet Thing. J.* **2020**. [CrossRef]
98. Guo, F.; Yu, F.R.; Zhang, H.; Ji, H.; Liu, M.; Leung, V.C.M. Adaptive Resource Allocation in Future Wireless Networks with Blockchain and Mobile Edge Computing. *IEEE Trans.Wirel. Commun.* **2020**, *19*, 1689–1703. [CrossRef]
99. Asheralieva, A.; Niyato, D. Distributed Dynamic Resource Management and Pricing in the IoT Systems with Blockchain-as-a-Service and UAV-Enabled Mobile Edge Computing. *IEEE Internet Thing. J.* **2020**, *7*, 1974–1993. [CrossRef]
100. Hua, G.; Zhu, L.; Wu, J.; Shen, C.; Zhou, L.; Lin, Q. Blockchain-Based Federated Learning for Intelligent Control in Heavy Haul Railway. *IEEE Access* **2020**, *8*, 176830–176839. [CrossRef]
101. Li, Y.; Chen, C.; Liu, N.; Huang, H.; Zheng, Z.; Yan, Q. A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus. *IEEE Netw.* **2020**, 1–8.

102. Qu, Y.; Pokhrel, S.R.; Garg, S.; Gao, L.; Xiang, Y. A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks. *IEEE Trans. Ind. Inform.* **2020**, *35*, 234–241 [CrossRef]
103. Shen, M.; Wang, H.; Zhang, B.; Zhu, L.; Xu, K.; Li, Q.; Du, X. Exploiting Unintended Property Leakage in Blockchain-Assisted Federated Learning for Intelligent Edge Computing. *IEEE Internet Thing. J.* **2020**. [CrossRef]
104. Souza, L.A.C.d.; Rebello, G.A.F.; Camilo, G.F.; Guimarães, L.C.B.; Duarte, O.C.M.B. DFedForest: Decentralized Federated Forest. In Proceedings of 2020 IEEE International Conference on Blockchain (Blockchain 2020), Rhodes Island, Greece, 2–6 November 2020; pp. 90–97.
105. Wu, Y.; Mendis, G.J.; Wei, J. DDLPF: A Practical Decentralized Deep Learning Paradigm for Internet of Things Applications. *IEEE Internet Thing. J.* **2020**. [CrossRef]
106. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C.M. Resource Allocation for Video Transcoding and Delivery Based on Mobile Edge Computing and Blockchain. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, UAE, 9–13 December 2018; pp. 1–6.
107. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C.M. Decentralized Resource Allocation for Video Transcoding and Delivery in Blockchain-Based System with Mobile Edge Computing. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11169–11185. [CrossRef]
108. Antonakoglou, K.; Xu, X.; Steinbach, E.; Mahmoodi, T.; Dohler, M. Toward Haptic Communications Over the 5G Tactile Internet. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3034–3059. [CrossRef]
109. Gupta, R.; Thakker, U.; Tanwar, S.; Obaidat, M.S.; Hsiao, K.F. BITS: A Blockchain-driven Intelligent Scheme for Telesurgery System. In Proceedings of the 2020 International Conference on Computer, Information and Telecommunication Systems (CITS), Hangzhou, China, 5–7 October 2020; pp. 1–5.
110. Qadri, Y.A.; Nauman, A.; Zikria, Y.B.; Vasilakos, A.V.; Kim, S.W. The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1121–1167. [CrossRef]
111. Hassija, V.; Chamola, V.; Gupta, V.; Chalapathi, G.S.S. A Blockchain based Framework for Secure Data Offloading in Tactile Internet Environment. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1836–1841.
112. Hassija, V.; Saxena, V.; Chamola, V. A Blockchain-based Framework for Drone-Mounted Base Stations in Tactile Internet Environment. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 261–266.
113. Yaqoob, I.; Salah, K.; Uddin, M.; Jayaraman, R.; Omar, M.; Imran, M. Blockchain for Digital Twins: Recent Advances and Future Research Challenges. *IEEE Netw.* **2020**, *34*, 290–298. [CrossRef]
114. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Low-latency Federated Learning and Blockchain for Edge Association in Digital Twin empowered 6G Networks. *IEEE Trans. Ind. Inform.* **2020**. [CrossRef]
115. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Communication-efficient Federated Learning and Permissioned Blockchain for Digital Twin Edge Networks. *IEEE Internet Thing. J.* **2020**, *8*, 2276–2288. [CrossRef]
116. Yang, L.; Li, M.; Si, P.; Yang, R.; Sun, E.; Zhang, Y. Energy-Efficient Resource Allocation for Blockchain-Enabled Industrial Internet of Things with Deep Reinforcement Learning. *IEEE Internet Thing. J.* **2020**, *8*, 2318–2329. [CrossRef]
117. Lemieux, V.L.; Hofman, D.; Batist, D.; Joo, A. Blockchain Technology for Recordkeeping. 2019. Available online: http://armaedfoundation.org/wp-content/uploads/2019/06/AIEF-Research-Paper-Blockchain-Technology-Recordkeeping.pdf (accessed on 17 February 2020).
118. Asheralieva, A.; Niyato, D. Reputation-Based Coalition Formation for Secure Self-Organized and Scalable Sharding in IoT Blockchains with Mobile-Edge Computing. *IEEE Internet Thing. J.* **2020**, *7*, 11830–11850. [CrossRef]
119. Fan, S.; Zhang, H.; Zeng, Y.; Cai, W. Hybrid Blockchain-Based Resource Trading System for Federated Learning in Edge Computing. *IEEE Internet Thing. J.* **2020**, *8*, 2252–2264. [CrossRef]
120. Eyal, I.; Sirer, E.G. Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 436–454.
121. Qiu, C.; Yao, H.; Wang, X.; Zhang, N.; Yu, F.R.; Niyato, D. AI-Chain: Blockchain Energized Edge Intelligence for Beyond 5G Networks. *IEEE Netw.* **2020**, *34*, 62–69. [CrossRef]
122. Zooko, W.O. Names: Decentralized, Secure, Human-Meaningful: Choose Two. 2003. Available online: https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html (accessed on 12 February 2021).