An Internet of Things Edge Intelligence Powered by Blockchain

Galiveeti Poornima[1] and Pallavi R[2]

[1]School of CSE&IS, Presidency University
[2]School of CSE&IS, Presidency University

Abstract

Blockchain, a decentralized and immutable distributed ledger technology (DLT), encompasses a sequential arrangement of records accompanied by chronological timestamps. Utilizing decentralization technology has emerged as a potent paradigm for fostering trust within entities lacking inherent trustworthiness, thereby reliably enabling verification. Driven by the recent progress in multi-access edge computing (MEC) and artificial intelligence (AI), the integration of blockchain with edge intelligence has emerged as a developing technological paradigm within the realm of the Internet of Things (IoT). In this scholarly discourse, we shall comprehensively examine the functioning of blockchain-enabled edge intelligence within the Internet of Things (IoT) domain. Our primary objective is to elucidate the intricacies of this technological framework while concurrently discerning the current trends.

Furthermore, we shall endeavor to proffer unresolved matters that warrant further scholarly investigation. To provide a more precise elucidation, we shall give the reader a foundational understanding of Distributed Ledger Technology (DLT), Multi-access Edge Computing (MEC), and Artificial Intelligence (AI). Secondly, we shall thoroughly examine extant scholarly literature to discern nascent patterns and developments within this particular domain of inquiry. Lastly, we shall engage in a discourse about unresolved quandaries and cavities in the existing body of research, thereby delineating potential avenues for future investigations. Integrating blockchain technology with edge intelligence is anticipated to become a pivotal facilitator for the Internet of Things (IoT) in the foreseeable future. This amalgamation holds the potential to instill trust and intelligence, thereby effectively catering to the intricate requirements of various industries and society at large.

1 Introduction

The concept of the Internet of Things (IoT) first surfaced in the year 1999 within the realm of supply chain industries, specifically in conjunction with the utilization of radio-frequency identification (RFID) technology [1]. The underlying concept entailed endowing computational systems with the capacity to autonomously perceive, discern, and comprehend the surrounding environment without human intervention. Nevertheless, many Internet of Things (IoT) devices are specifically engineered to operate on battery power and possess a diminutive physical form factor. Consequently, these devices are inherently constrained by their severely restricted energy and computational capabilities. Resource-limited Internet of Things (IoT) devices exhibit inadequate capabilities to execute intricate computational tasks, including the facilitation of artificial intelligence (AI) [2]. While it is true that federated learning (FL) can indeed be executed by a collective assemblage of Internet of Things (IoT) devices [3], it is worth noting that the computational burden associated with this process remains excessively onerous for IoT devices. Transmitting computational tasks to proximate servers is an appealing resolution to surmount this bottleneck. In contrast to conventional cloud computing, the multi-access edge computing (MEC) approach entails providing computational resources at the periphery of the radio access network (RAN). Hence, computational tasks do not necessitate traversal across the core network, thereby enabling the processing of Internet of Things (IoT) data and the consumption of results to occur locally with negligible latency.

The present computational paradigm, which aims to reduce latency and utilize core network communication resources, is challenging. The consideration of security issues and incentives is of paramount importance in this context. In a more precise manner, the data being transmitted can encompass sensitive information about personal identities and financial account details. The circumstance above gives rise to an increased susceptibility to privacy breaches and malevolent intrusions. Furthermore, it is imperative to consider providing incentives to nearby servers or computing nodes to efficiently process tasks assigned by Internet of Things (IoT) devices. In addition, it is worth noting that edge servers exhibit a relatively constrained computational capacity when juxtaposed with their cloud counterparts. In addition to their computational functions, it is imperative to acknowledge that computing operations incur storage and energy resources expenses. Hence, it is essential to establish a framework or platform for computing resource trading [4] and data sharing [5] to incentivize the utilization of edge servers. Blockchain, as a distributed ledger technology (DLT), has surfaced as a prospective resolution for the concerns above, owing to its inherent attributes of data transparency, distributed operation, and dependability. The present moment presents a suitable occasion to undertake a comprehensive examination of the utilization of blockchain technology in facilitating edge intelligence to bolster Internet of Things (IoT) applications.

2 Literature Survey

In their study, ElMamy et al. [6] conducted a comprehensive survey on utilizing Distributed Ledger Technology (DLT) to address and mitigate various cyber threats within the context of Industry 4.0. The present survey has categorized the most significant cyber-attacks into four distinct classes: scanning, local to remote, power of root, and denial of service. In their scholarly work, Tariq et al. [7] comprehensively examined the various security concerns that arise in the context of fog-enabled Internet of Things (IoT) systems. The researchers regarded blockchain technology as a pivotal solution for mitigating the security challenges associated with fog computing. Nevertheless, it is imperative to note that the works above fail to consider the inherent potential of blockchain technology in facilitating artificial intelligence (AI) at the edge.

Many scholarly works have been conducted within the realm of artificial intelligence (AI) facilitated by blockchain technology, specifically in literature reviews. The investigation conducted by Jameel et al. [8] examined the utilization of reinforcement learning within the context of blockchain-enabled industrial Internet of Things (IoT) networks. The authors highlighted the potential of machine learning (ML) algorithms, specifically Q-learning, to enhance network performance by minimizing block time and improving transaction throughput. Moreover, Liu et al. [9] presented a convergence of blockchain and machine learning in a bidirectional manner. From a scholarly perspective, the integration of blockchain technology has the potential to bestow upon machine learning (ML) the invaluable attributes of security and trust. Conversely, machine learning (ML) can serve as a valuable instrument for optimizing blockchain networks. In their seminal work, Kumari et al. [10] conducted a comprehensive investigation into the various extant methodologies of blockchain-based artificial intelligence (AI) frameworks employed in energy cloud management. The primary objective of their study was to proactively tackle the pressing concerns surrounding security and privacy by harnessing the synergistic potential of blockchain technology and AI algorithms. In addition, Salah et al. [11] extensively examined the various applications of blockchain in the context of artificial intelligence. The discourse revolved around the interplay between artificial intelligence (AI) and blockchain technology within the Internet of Things (IoT)-)-enabled ecosystem. Nevertheless, the inclusion of MEC needs to be considered in the studies above.

Moreover, Mobile Edge Computing (MEC) assumes a pivotal role as a fundamental technology in the realm of burgeoning fifth-generation (5G) networks. Numerous surveys about blockchain solutions within the context of 5G networks have been conducted, primarily focusing on the security challenges within 5G systems. Furthermore, the scholarly work undertaken by Tahir et al. [12] delved into an extensive analysis of the various applications of blockchain technology within the context of 5G networks. A comprehensive survey was conducted to examine the integration of blockchain technology with 5G networks and its potential implications for future advancements. This review examines blockchains' attributes, namely transparency, audibility, and distributed nature, to address security, resource management, and energy efficiency concerns. The scholarly article has successfully delineated three obstacles inherently linked to Mobile Edge Computing (MEC): identity authentication, privacy, and trust management. Subsequently, a series of blockchainions were introduced to address the challenges effectively. Although this comprehensive survey encompassed a wide range of topics, it is worth noting that the examination of blockchain-enabled mobile edge intelligence needed to be conducted sufficiently exhaustively within the scope of this survey. In contrast, the scholarly work by Nguyen et al. [13] provides a concise overview of a federated approach that leverages blockchain technology. The machine learning architecture in question derives its capabilities from the inherent decentralization characteristic of blockchain technology.

Moreover, the scholarly work by Xiong et al. [14] examined the underlying incentives driving the convergence of Mobile Edge Computing (MEC) and blockchain technology. In the blockchain system, computationally intensive tasks, such as proof of work, are delegated to Mobile Edge Computing (MEC) servers. The researchers directed their attention toward using edge computing to facilitate the implementation of mobile blockchains. Nevertheless, incorporating blockchain technology to reduce the optimization of efficient and secure Mobile Edge Computing (MEC) must be considered. In addition, the collaborative investigation of the integration of edge computing and blockchain was conducted by Yang et al. [15]. The proponents posited that integrating blockchain technology could augment the efficacy of edge computing by enhancing the dependability of network accessibility and facilitating improved governance over computational resources. In contrast to the comprehensive survey, the present study focuses on blockchain-enabled distributed and decentralized machine learning. Furthermore, we analyze the developing trend and the unresolved matters within this realm of research.

Sekaran et al. [16] presented a scholarly investigation of the utilization of blockchain-enabled Mobile Edge Computing (MEC) to automate Internet of Things (IoT) systems. The present analysis centers on amalgamating blockchain technology with the Internet of Things (IoT). The investigation primarily focused on carefully considering and examining computational loads and delays. This paper delved into a comprehensive exploration and categorization of the various applications of blockchain technology within the context of the 6G-enabled Internet of Things (IoT). Furthermore, the scholarly work by Fernandez Carames et al. [17] delved into examining the synergistic integration of blockchain technology, the Internet of Things (IoT), and edge computing within higher education. In contrast to extant review articles that predominantly focus on scholarly investigations, the present paper offers a comprehensive exposition delineating the intricate trajectory of smart campus implementation. This study benefits researchers seeking to understand the operational mechanics of blockchain-enabled edge computing within a practical Internet of Things (IoT) application scenario, specifically about autonomous driving [18]. Utilizing blockchain-enabled Mobile Edge Computing (MEC) platforms presents a promising avenue for applying information exchange and trust within the Internet of Vehicles (IoV). Furthermore, the scholarly work conducted by Chamola et al. [19] encompassed a comprehensive examination of the amalgamation of Internet of Things (IoT), Artificial Intelligence (AI), and blockchain technology as a means to address the global health crisis known as the coronavirus disease 2019 (COVID-19) pandemic. The study by Queiroz et al. [20] explored blockchain solutions about various layers within edge computing. These layers encompassed the fog, edge, static, and dynamic multi-layer. The present paper also discusses machine learning algorithms that can be effectively employed in practical applications. Nevertheless, it is imperative to acknowledge that the scope of this survey primarily centered around the Internet of Vehicles (IoV) domain, thus potentially limiting its comprehensive coverage of other pertinent areas. The study by Mollah et al. (2020) focused on integrating blockchain technology within intelligent transportation systems (ITS). This article delved into examining applications empowered by blockchain technology, encompassing edge computing and artificial intelligence. Furthermore, it thoroughly explored the challenges and opportunities in blockchain-based applications within Intelligent Transportation Systems (ITS).

3 Recent Technologies

We begin by elucidating blockchain technology's fundamental principles to provide readers with a foundational understanding. The present investigation centers on the specific aspects of blockchain technology that pertain to this survey while deliberately excluding other essential elements of blockchain, such as intricate details regarding consensus algorithms, Merkle tree structures, transaction architectures, and digital signatures, to maintain conciseness. Subsequently, the introduction of MEC is undertaken. Our primary focus revolves around elucidating the fundamentals of the subject matter, namely the precise delineation of its definition and the intricate amalgamation of two distinct technological domains, blockchain and Mobile Edge Computing (MEC). Therse pertains to integrating blockchain technology with artificial intelligence (AI). Our objective is to elucidate the mechanics of this integration within the Internet of Things (IoT) domain.

3.1 Fundamentals of Blockchain

The term ”blockchain” denotes a collection of records that are systematically interconnected through the utilization of cryptographic techniques. Blockchains can be categorized into two primary classifications: public and permission. From a particular perspective, a public chain resemblance nice to the Internet. Everyone utilizing this record system can locate and obtain entry to the chain above. In contrast, a permissioned blockchain permits authenticated entities to access and contribute to the records. Moreover, it is worth noting that a consortium blockchain can be characterized as a hybrid variant that lies on the continuum between public and permissioned chains, albeit leaning more toward the attributes of a private chain. The system operates within a permissioned framework and is subject to oversight by a pre-established consortium of entities.

The term ”blockchain” denotes a collection of records that are systematically interconnected through the utilization of cryptographic techniques. Blockchains can be categorized into two primary classifications: public and permission. From a particular perspective, a public chain resembles the Internet. Every individual utilizing this particular record system possesses the capability to locate and obtain access to the chain above. In contrast, a permissioned blockchain exclusively

The architectural design depicted in Figure **??** ensures the preservation of immutability within the blockchain records. Once a block has been established within this chain, any modifications to preceding blocks are rendered immutable. A conventional database can be likened to a singular snapshot encapsulating information, whereas the blockchain can be analogously conceived as a sequential series of timestamped photos. The blockchain possesses a certain degree of autonomy and temporal coherence, enabling it to effectively trace the historical trajectory of the record above system.

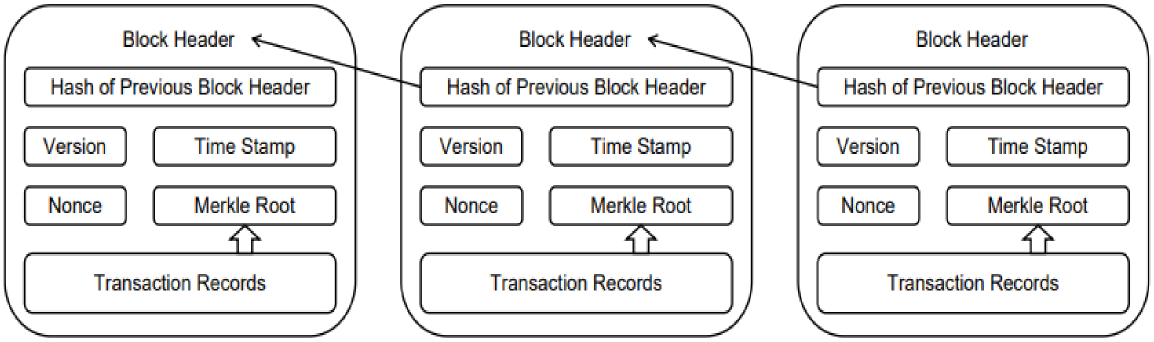

Figure 1: Blockchain Architecture

In a broad sense, it can be posited that a blockchain employs a mechanism known as ”consensus” to append novel data entries rather than supplanting existing ones. Traditional databases use the concept of ”permission” as a means of data management. The system exhibits a centralized framework for both administration and maintenance. In the context of the widely recognized application of public blockchain, namely the Bitcoin system, it is imperative to note that the consensus mechanism employed is the proof-of-work (PoW). Proof of Work (PoW) can be classified as a mathematical problem that requires a solution to validate a transaction or block in a decentralized network. The enigma inherent in this particular puzzle, Nonce, is characterized by its elusive nature, rendering it arduous to unearth. However, once discovered, its validity can be readily easily ascertained. Determining the Nonce is commonly called ”mining” in the literature [21].

The initial miner who successfully uncovers the undisclosed information possesses the prerogative to append the block to the most extensive sequence of blocks, thereby meriting a remuneration in the form of a unit of the digital currency known as Bitcoin. Within the framework of this decentralized system, it is imperative to acknowledge that complete replicas of transaction records are strategically situated across various networked miners. The consensus algorithm conducts the processing of verification and confirmation for each transaction. The absolute dominion over the operational dynamics within this peer-to-peer network eludes any singular external entity. In contradistinction, a distributed system, albeit executing transactions across disparate locations, may nevertheless remain subject to the dominion of a solitary entity. The principal distinction between distributed and decentralized systems lies therein. In recapitulation, blockchain represents a decentralized framework that effectively redistributes the locus of governance from a centralized intermediary to discrete entities within the record-keeping system.

In contrast to the Bitcoin network, Ethereum [22] incorporates the concept of smart contracts, which are executable scripts stored on the blockchain [23]. In contrast to using Proof-of-Work (PoW), Ethereum has adopted the employment of Proof-of-Stake (PoS) as its prevailing consensus mechanism. The consensus strategy employs a random selection process for block validators, wherein individuals with higher stakes are likelier to be chosen. The liberation of blockchain nodes from the burdensome and resource-intensive process of mining is achieved by eliminating futile activities and reducing energy consumption.

3.2 Blockchain-AI

Conventional artificial intelligence (AI) methodologies, such as deep learning and reinforcement learning, necessitate centralized data administration. Before engaging in the training exercise, an individual learner must procure data and computing resources essential for training machines and agents in the realm of learning. Adopting a centralized architecture gives rise to many concerns, including but not limited to the vulnerability of single points of failure and the potential compromise of personal data [24]. As previously indicated, blockchain technology embodies a decentralized and distributed ledger system. The characteristic above exhibits a high degree of compatibility with implementing artificial intelligence (AI) solutions within distributed Internet of Things (IoT) designs. Furthermore, the potential for fostering collaboration and facilitating secure data sharing among learning machines can be actualized by utilizing blockchain technology. This review aims to introduce the utilization of intelligent contract-based artificial intelligence (AI), particularly emphasizing the federated AI solution.

In brief, using intelligent contracts [23] presents a formidable mechanism for facilitating the implementation of distributed and decentralized machine learning within the Internet of Things (IoT) systems. As depicted in Figure 2, the type above of pre-established and self-validated scripts, encompassing both learning algorithms and models, can be effectively implemented on individual distributed learning devices in a decentralized fashion. In addition, it is essential to note that within this framework, solely the learning parameters undergo the process of sharing and verification through blockchain transactions. Conversely, it is crucial to emphasize that the sensitive data generated by Internet of Things (IoT) devices remain inaccessible to any external entities or third parties. The proposition above ensures the reliable dissemination of the educational encounter. It bestows each entity the autonomy to govern their data, exemplifying the fundamental concept of blockchain-based federated learning. The convergence of blockchain technology and smart contracts has facilitated the establishment of a worldwide framework that fosters collaborative machine learning in a distributed and decentralized fashion.

Blockchain technology was introduced to manage and uphold the reputation of learning devices effectively, as evidenced by scholarly works [25, 26, 27, 28, 29]. In their seminal work, Kang et al. [26] put forth a comprehensive framework comprising efficient incentive mechanisms to foster federated learning (FL) reliability. The individuals above introduced the consortium blockchain to enhance reputation management. Furthermore, the utilization of blockchain technology to facilitate reward systems has been explored in the scholarly works referenced [4, 30, 31, 32, 33, 34]. Moreover, establishing data integrity and validating sources through the utilization of deep learning techniques, specifically convolutional neural networks [35], can effectively ensure the reliability and credibility of the training data. Furthermore, the scholarly work by Ma et al. [36] delved into the intricate realm of data noise and its implications on the decentralized solution for data cleaning, employing the cutting-edge concept of edge intelligence.

The authors, Lu et al. [24], proposed an architecture for secure data sharing in the context of decentralized and secure learning strategies. Their work aimed to address the privacy concerns associated with machine learning. Furthermore, the utilization of computational resources within the blockchain consensus mechanism has been employed in the Federated Learning (FL) context. In addition, the authors Qu et al. [30] have introduced the concept of poisoning attacks within decentralized machine learning. Similarly, Kang et al. [26] and Ramanan and Nakayama [37] have put forth credible federated

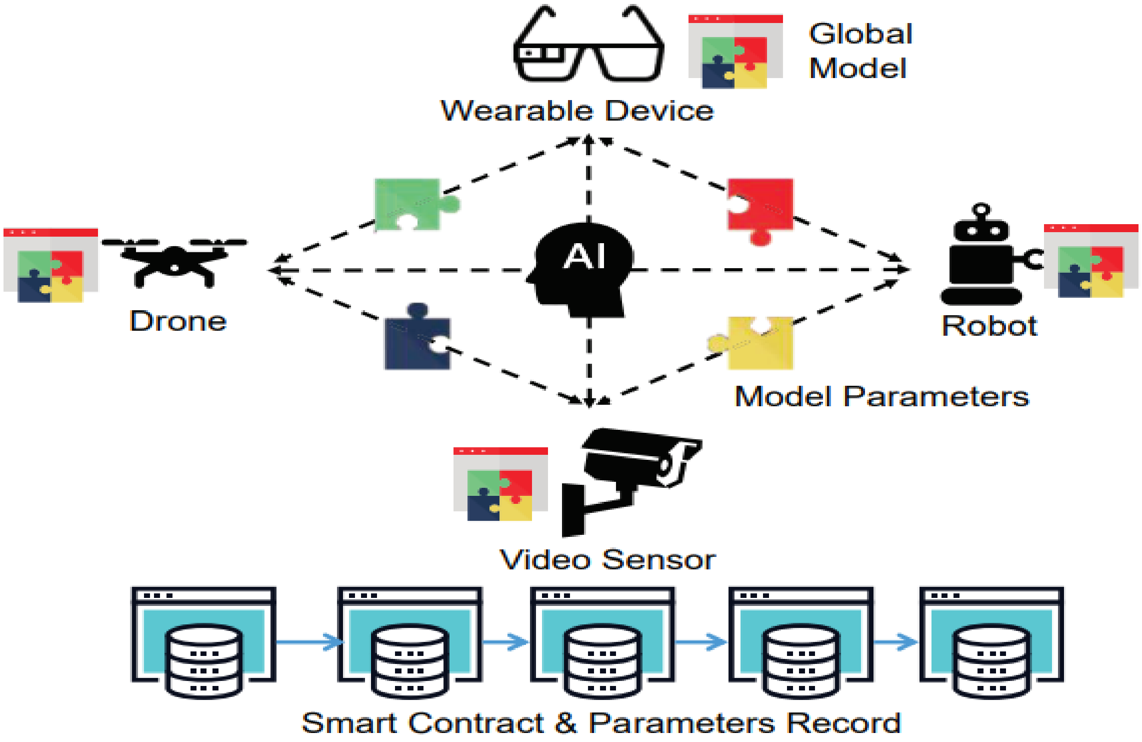

Figure 2: AI for the IoT using blockchain

knowledge (FL) approaches through the elimination of the centralized model aggregator within the realm of machine learning (ML).

Furthermore, the study by Yin et al. [38] delved into exploring a blockchain-based federated deep learning approach within the Internet of Things (IoT) domain. The impetus behind this particular strategy was derived from the study of multiparty secure computation, a subject also explored in the scholarly work referenced [39]. Moreover, using smart contracts in federated learning (FL) has been studied by Liu et al. [40] to enhance self-defense mechanisms. In this manner, membership inference and poisoning attacks were prevented.

3.3 MEC-DLT integration

In the existing body of literature, various terminologies have been employed to delineate the collaborative computational processes involving the end user, the proximate server, and the cloud infrastructure. The concepts above encompass fog computing [41], edge computing [42], and multi-access edge computing (MEC) [43]. In contrast to the ethereal nature of the ”cloud,” the concept of ”fog” computing exhibits a closer proximity to the terrestrial realm, specifically about the source of Internet of Things (IoT) data. The term ”edge computing” pertains to the expanded cloud computing domain, encompassing distributed resources, wired and wireless data transmissions, and intermediate layers between the edge and the cloud. On the other hand, the concept of edge computing centers its attention on the execution of tasks by utilizing edge nodes situated within the Radio Access Network (RAN), which exists outside the core network. Moreover, it is worth noting that mobile edge computing represents a variant of edge computing encompassing data caching and computation offloading techniques within the mobile web, as elucidated by reference [44].

Furthermore, the contemporary scholarly pursuits in Mobile Edge Computing (MEC) are indicative of the pragmatic circumstances surrounding the deployment of multi-technology Radio Access Networks (RANs) within the realm of edge computing, as evidenced by the citation [28]. The subject matter encompasses a range of components, such as access points, hot spots, routers, and other related elements, all utilized to establish an edge network. In the present analysis, we employ the acronym ”MEC” as an abbreviation for multi-access edge computing, which also encompasses mobile edge computing. The interconnections and interdependencies between fog computing, edge computing, and multi-access edge computing (MEC) are visually depicted in Figure 3.

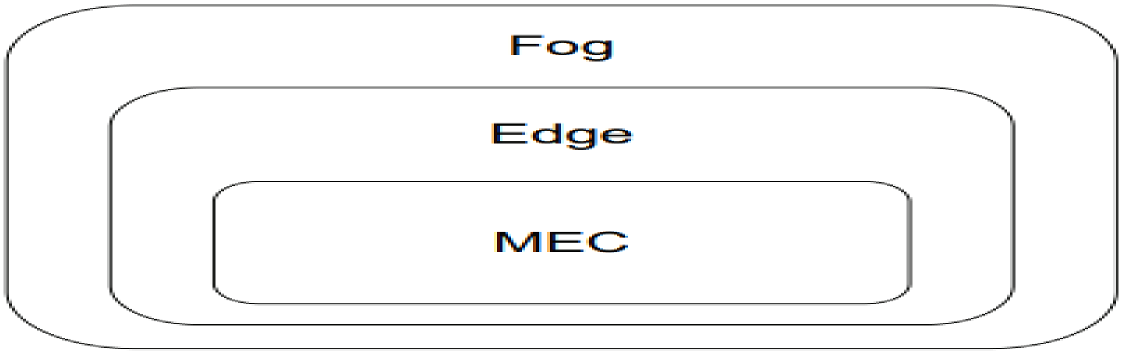

Figure 3: Relationships between phrases.

The symbiotic relationship between blockchain and Mobile Edge Computing (MEC) is widely acknowledged [15]. Blockchain, in its essence, bestows upon the realm of Mobile Edge Computing (MEC) a trifecta of paramount attributes, namely security, privacy, and trust [45, 46]. The secure facilitation of efficient control and incentivization of cooperation between edge devices and servers is made possible through blockchain technology. In contrast, the utilization of Mobile Edge Computing (MEC) presents a viable solution for enhancing the scalability of blockchain technology within the context of distributed and efficient operations. This is achieved by providing computing and cache resources to IoT systems integrated with blockchain capabilities. An illustrative instance pertains to the necessity of a substantial computational capacity in the Proof of Work (PoW) mechanism for blockchain mining, thereby presenting formidable obstacles for Internet of Things (IoT) devices. The rationale behind the active mining of IoT devices lies in establishing a global consensus to validate transactions. In contrast to a distributed Internet of Things (IoT) system, a blockchain-enabled IoT system exhibits the characteristic of decentralizing authority to individual IoT devices. The absence of a singular intermediary entity capable of facilitating a universal determination for Internet of Things (IoT) devices is evident. Hence, the Proof of Work (PoW) mechanism must be implemented to ascertain and safeguard the integrity and legitimacy of transactions effectively. The introduction of MEC is a viable solution to the issue above. By leveraging the computational capabilities of Mobile Edge Computing (MEC) servers, Internet of Things (IoT) devices with limited resources can employ Proof of Work (PoW) mechanisms to achieve consensus in the context of decentralized applications.

Nguyen et al. thoroughly examined the privacy leakage issue in integrating blockchain and mobile edge computing (MEC) in their seminal work [47]. Within this scholarly article, it is posited that individuals who utilize mobile devices assume the role of miners within the blockchain system. The delegation of data processing tasks and mining tasks from users to proximate Mobile Edge Computing (MEC) servers is observed. The level of privacy in this particular process has been meticulously modeled and formulated. Moreover, blockchain technology was introduced as a robust security mechanism for Mobile Edge Computing (MEC) systems within the context of vehicular networks, as indicated by reference [48]. Furthermore, a blockchain-based trust mechanism for Mobile Edge Computing (MEC) systems was introduced by Reference [49]. Establishing a reputation system for the edge nodes in the blockchain network facilitated the selection of the miner in a manner that engendered trust.

Furthermore, the video streaming industry has witnessed the development of payment systems that leverage blockchain technology, enabling enhanced functionality. These systems have been designed to incorporate an incentive mechanism for Mobile Edge Computing (MEC) servers [50]. Moreover, the enhancement of block size flexibility and scalability can be substantially augmented by utilizing Mobile Edge Computing (MEC). Nevertheless, it should be noted that not all edge devices possess an adequate amount of cryptocurrency to procure the offloading service. Henceforth, Zhang et al. [51] have posited a loan strategy to fulfill this objective. While it is possible to carry out the mining task on MEC servers, it is essential to acknowledge the presence of competition within IoT devices. The rationale behind this observation lies in the inherent limitation of resources that edge servers possess compared to the relatively abundant number of Internet of Things (IoT) devices. The computation resources allocation problem in the MEC-assisted public blockchain network was addressed by Zhao et al. [52]. Furthermore, the implementation of this particular approach has the potential to safeguard the integrity of the blockchain system against a 51% attack [53]. It is worth noting that an assailant possessing a majority stake within the said system would be inclined to uphold and fortify the cryptocurrency above rather than dismantle it.

4 New Ideas

Within this particular section, our primary objective is to furnish research directions and discern the emergence of trends within this specific domain. In this discourse, we examine nascent avenues of research and the corresponding scholarly contributions within this domain. These encompass the realms of blockchain-facilitated Internet of Things (IoT) communications, IoT security fortified by blockchain technology, decentralized machine learning (ML) within the IoT framework, and the incentivization mechanisms in IoT that are empowered by blockchain. Subsequently, contemporary advancements are meticulously chosen and cataloged for subsequent investigation. In conclusion, we shall succinctly encapsulate and elucidate various patterns and tendencies by the chronological sequence.

4.1 IoT Security with Blockchain

It is imperative to acknowledge that no technology can be deemed flawless, including the blockchain. The vulnerabilities inherent in blockchain technology have garnered significant attention from various industries and scholars [54]. In the context of innovative contract development, it is plausible for a developer to inadvertently introduce errors, thereby engendering vulnerabilities that have the potential to instigate a hard fork within the blockchain system. Furthermore, it is imperative to acknowledge that consensus mechanisms inherently possess a susceptibility to a 51%

- ***Authentication :*** IoT security can be effectively addressed with public-key cryptography-based Authentication. The MEC block validation scheme used group signatures [55]. In IoT, FL nodes were authenticated [56]. In the FL framework, the intelligent contract established nodes. Lin et al. [57] examined whether healthcare emergency levels were authentic. Additionally, they optimized MEC network delay.

- ***Data Security:*** With immutable data records, blockchain provides data security. Most literature in this field considered this topic. Kang et al. [58] proposed a consortium blockchain and intelligent contract-based vehicular network protocol for secure data sharing.

- ***Data Privacy:*** Participants are anonymous in public blockchain systems as they are just hashes of public keys. The Hyperledger Fabric is a permissioned or private blockchain that only authenticated entities can access. Another way to transact without revealing participant information is the zero-knowledge proof. It was added to the privacy-protecting cryptocurrency Zcash. To protect data privacy in IoT systems, devices attached to human activities store sensitive personal data. Zyskind et al. [59] introduced blockchain for personal data protection. MEC blockchain users' privacy was considered by Nguyen et al. [47]. Pr note that MEC network topology privacy is also essential. The MEC system by Yang et al. [60] protected topology privacy. Lu et al. [24] assessed industrial IoT privacy-preserved data sharing. FL addresses IoT data leakage. The privacy-preserving framework PriModChain was proposed by Arachchige et al. [61].

- ***Data Integrity:*** Credible data acquisition requires integrity. Islam and Shin [62] proposed a blockchain-based UAV-assisted data acquisition protocol. The data were encrypted with a UAV. Kumar et al. [63] also introduced "BlockEdge," a decentralized blockchain framework for data integrity. Finally, client data can be verified for integrity. Zhang et al. [64] proposed a platform architecture for industrial IoT failure detection. Platform used Merkle tree.

4.2 ML decentralized in IoT

- ***Neural Networks:*** Integrating neural networks into the Internet of Medical Things is a growing trend. Medical records are private and vulnerable to hackers. Połap et al. [65] suggested a federated approach for blockchain-based neural networks in IoMT. Insured distributed and local patient data storage.

- ***Deep Reinforcement Learning:*** This learning method was standard in academia. However, most papers mechanically use deep reinforcement learning (DRL) for optimization. Exploring its IoT potential, especially in mobile blockchain apps, is another trend. Gao et al. [66] used DRL to schedule mining tasks to maximize reward and minimize cost. DRL was also proposed for blockchain-enabled MEC [67]. This paper examined cooperative task offloading. Zhuang et al. [68] examined blockchain-enabled MEC routing control. A new DRL-based method was introduced for adaptive network routing. Yu et al. [69] studied DRL and FL together. They proposed an intelligent ultra-dense edge computing framework using DRL for offloading and resource allocation. Jiang et al. [70] suggested a video analytics framework and DRL solutions to reduce MEC system latency in the Internet of autonomous vehicles. A blockchain-enabled MEC framework was also proposed. Based on DRL, adaptive resource allocation was given [71]. Additionally, Asheralieva and Niyato [72] examined deep Q-learning and Bayesian deep learning for blockchain-based MEC decision-making.

- ***Federated Learning:*** Federation-based learning has been introduced previously. Blockchain-enabled FL research is widespread. Its decentralized framework ensures learning privacy and security. Hua et al. [73] implemented asynchronous collaborative learning in their blockchain-enabled FL for heavy-haul railways. A committee consensus was developed for blockchain-enabled FL to lower computing costs and enhance security [74]. Industry 4.0 networks now use cognitive computing [75]. The proposed decentralized cognitive computing method uses blockchain-enabled FL. Additionally, Shen et al. [76] examined the issue of unintended property leakage. They devised a new property inference attack to exploit FL. Souza et al. [77] proposed DFedForest, a distributed and federated approach based on random forest algorithms and blockchain technologies. DDLPF, a decentralized deep learning method, was proposed for IoT [78]. DDLPF is a fast, decentralized deep learning paradigm that prioritizes privacy and few-shot learning.

5 conclusion

This review comprehensively examines the existing literature on integrating blockchain technology with edge intelligence. We have initially provided a foundational understanding of blockchain, MEC, and AI to facilitate comprehension for researchers and readers alike. In addition, the exploration of literature mining has contributed to identifying and introducing research trends and directions. In this discourse, we have expounded upon a comprehensive perspective on the trajectory of research trends within this particular domain. Additionally, we have elucidated the salient subjects currently occupying the forefront of scholarly inquiry. The user's text needs to be more sufficient to respond.

References

[1] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] S. Deng, H. Zhao, W. Fang, J. Yin, S. Dustdar, and A. Y. Zomaya, "Edge intelligence: The confluence of edge computing and artificial intelligence," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7457–7469, 2020.

[3] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1279–1283, 2019.

[4] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang, and M. J. Piran, "Blockchain-based incentive energy-knowledge trading in iot: Joint power transfer and ai design," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14685–14698, 2020.

[5] A. V. Rivera, A. Refaey, and E. Hossain, "A blockchain framework for secure task sharing in multi-access edge computing," *IEEE Network*, vol. 35, no. 3, pp. 176–183, 2020.

[6] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, “A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0,” *Sustainability*, vol. 12, no. 21, p. 9179, 2020.

[7] N. Tariq and M. Asim, “Feras al-obeidat, muhammad zubair farooqi, thar baker, mohammad hammoudeh, and ibrahim ghafir. the security of big data in fog-enabled iot applications including blockchain: a survey,” *Sensors*, vol. 19, no. 8, p. 1788, 2019.

[8] 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.

[9] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, “Blockchain and machine learning for communications and networking systems,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020.

[10] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, “Blockchain and ai amalgamation for energy cloud management: Challenges, solutions, and future directions,” *Journal of Parallel and Distributed Computing*, vol. 143, pp. 148–166, 2020.

[11] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for ai: Review and open research challenges,” *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[12] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad, and K. I. Ahmed, “A review on application of blockchain in 5g and beyond networks: Taxonomy, field-trials, challenges and opportunities,” *IEEE Access*, vol. 8, pp. 115876–115904, 2020.

[13] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for 5g and beyond networks: A state of the art survey,” *Journal of Network and Computer Applications*, vol. 166, p. 102693, 2020.

[14] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When mobile blockchain meets edge computing,” *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[15] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: A survey, some research issues and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[16] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda, “Survival study on blockchain based 6g-enabled mobile edge computation for iot automation,” *IEEE access*, vol. 8, pp. 143453–143463, 2020.

[17] T. M. Fernández-Caramés and P. Fraga-Lamas, “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,” *Applied Sciences*, vol. 9, no. 21, p. 4479, 2019.

[18] X. Jiang, F. R. Yu, T. Song, Z. Ma, Y. Song, and D. Zhu, “Blockchain-enabled cross-domain object detection for autonomous driving: A model sharing approach,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3681–3692, 2020.

[19] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, “A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact,” *Ieee access*, vol. 8, pp. 90225–90265, 2020.

[20] A. Queiroz, E. Oliveira, M. Barbosa, and K. Dias, “A survey on blockchain and edge computing applied to the internet of vehicles,” in *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–6, IEEE, 2020.

[21] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, “Blockchain mining games,” in *Proceedings of the 2016 ACM Conference on Economics and Computation*, pp. 365–382, 2016.

[22] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[23] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[24] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[25] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10700–10714, 2019.

[26] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.

[27] M. H. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Towards blockchain-based reputation-aware federated learning," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 183–188, IEEE, 2020.

[28] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2020.

[29] J. Passerat-Palmbach, T. Farnan, M. McCoy, J. D. Harris, S. T. Manion, H. L. Flannery, and B. Gleim, "Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data," in *2020 IEEE international conference on blockchain (Blockchain)*, pp. 550–555, IEEE, 2020.

[30] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5171–5183, 2020.

[31] R. Zhang, F. R. Yu, J. Liu, T. Huang, and Y. Liu, "Deep reinforcement learning (drl)-based device-to-device (d2d) caching with blockchain and mobile edge computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6469–6485, 2020.

[32] N. B. Somy, K. Kannan, V. Arya, S. Hans, A. Singh, P. Lohia, and S. Mehta, "Ownership preserving ai market places using blockchain," in *2019 IEEE international conference on blockchain (Blockchain)*, pp. 156–165, IEEE, 2019.

[33] L. Ouyang, Y. Yuan, and F.-Y. Wang, "Learning markets: An ai collaboration framework based on blockchain and smart contracts," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14273–14286, 2020.

[34] K. Toyoda, J. Zhao, A. N. S. Zhang, and P. T. Mathiopoulos, "Blockchain-enabled federated learning with mechanism design," *Ieee Access*, vol. 8, pp. 219744–219756, 2020.

[35] S. Lugan, P. Desbordes, E. Brion, L. X. R. Tormo, A. Legay, and B. Macq, "Secure architectures implementing trusted coalitions for blockchained distributed learning (tclearn)," *Ieee Access*, vol. 7, pp. 181789–181799, 2019.

[36] L. Ma, Q. Pei, L. Zhou, H. Zhu, L. Wang, and Y. Ji, "Federated data cleaning: Collaborative and privacy-preserving data cleaning for edge intelligence," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6757–6770, 2020.

[37] P. Ramanan and K. Nakayama, "Baffle: Blockchain based aggregator free federated learning," in *2020 IEEE international conference on blockchain (Blockchain)*, pp. 72–81, IEEE, 2020.

[38] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "Fdc: A secure federated deep learning mechanism for data collaborations in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6348–6359, 2020.

[39] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu, and P. Li, "Ai at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9600–9610, 2020.

[40] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. Abd El-Latif, "A secure federated learning framework for 5g networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 24–31, 2020.

[41] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13–16, 2012.

[42] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[43] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: a survey. ieee internet things j 5: 450–465," 2018.

[44] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE communications surveys & tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[45] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE access*, vol. 6, pp. 72469–72478, 2018.

[46] Z. Guan, H. Lyu, D. Li, Y. Hei, and T. Wang, "Blockchain: A distributed solution to uav-enabled mobile edge computing," *IET Communications*, vol. 14, no. 15, pp. 2420–2426, 2020.

[47] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2536–2549, 2020.

[48] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of v2x communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, 2020.

[49] L. Xiao, Y. Ding, D. Jiang, J. Huang, D. Wang, J. Li, and H. V. Poor, "A reinforcement learning and blockchain-based trust mechanism for edge networks," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5460–5470, 2020.

[50] M. Liu, Y. Teng, F. R. Yu, V. C. Leung, and M. Song, "A mobile edge computing (mec)-enabled transcoding framework for blockchain-based video streaming," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 81–87, 2020.

[51] Z. Zhang, Z. Hong, W. Chen, Z. Zheng, and X. Chen, "Joint computation offloading and coin loaning for blockchain-empowered mobile-edge computing," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9934–9950, 2019.

[52] N. Zhao, H. Wu, and Y. Chen, "Coalition game-based computation resource allocation for wireless blockchain networks," *IEEE internet of things journal*, vol. 6, no. 5, pp. 8507–8518, 2019.

[53] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[54] H. Hasanova, U.-j. Baek, M.-g. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, vol. 29, no. 2, p. e2060, 2019.

[55] S. Zhang and J.-H. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4557–4565, 2019.

[56] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach," *Ieee Access*, vol. 8, pp. 205071–205087, 2020.

[57] D. Lin, S. Hu, Y. Gao, and Y. Tang, "Optimizing mec networks for healthcare applications in 5g communications with the authenticity of users' priorities," *Ieee Access*, vol. 7, pp. 88592–88600, 2019.

[58] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE internet of things journal*, vol. 6, no. 3, pp. 4660–4670, 2018.

[59] G. Zyskind, O. Nathan, *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE security and privacy workshops*, pp. 180–184, IEEE, 2015.

[60] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, "Distributed blockchain-based trusted multidomain collaboration for mobile edge computing in 5g and beyond," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7094–7104, 2020.

[61] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial iot systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.

[62] A. Islam and S. Y. Shin, "Buav: A blockchain based secure uav-assisted data acquisition scheme in internet of things," *Journal of Communications and Networks*, vol. 21, no. 5, pp. 491–502, 2019.

[63] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage, I. Ahmad, M. Liyanage, A. Braeken, and M. Ylianttila, "Blockedge: blockchain-edge framework for industrial iot networks," *IEEE Access*, vol. 8, pp. 154166–154185, 2020.

[64] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, "Blockchain-based federated learning for device failure detection in industrial iot," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5926–5937, 2020.

[65] D. Połap, G. Srivastava, A. Jolfaei, and R. M. Parizi, "Blockchain technology and neural networks for the internet of medical things," in *IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pp. 508–513, IEEE, 2020.

[66] Y. Gao, W. Wu, H. Nan, Y. Sun, and P. Si, "Deep reinforcement learning based task scheduling in mobile blockchain for iot applications," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, IEEE, 2020.

[67] J. Feng, F. R. Yu, Q. Pei, X. Chu, J. Du, and L. Zhu, "Cooperative computation offloading and resource allocation for blockchain-enabled mobile-edge computing: A deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6214–6228, 2019.

[68] Z. Zhuang, J. Wang, Q. Qi, J. Liao, and Z. Han, "Adaptive and robust routing with lyapunov-based deep rl in mec networks enabled by blockchains," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2208–2225, 2020.

[69] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, "When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5g ultradense network," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2238–2251, 2020.

[70] X. Jiang, F. R. Yu, T. Song, and V. C. Leung, "Intelligent resource allocation for video analytics in blockchain-enabled internet of autonomous vehicles with edge computing," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14260–14272, 2020.

[71] F. Guo, F. R. Yu, H. Zhang, H. Ji, M. Liu, and V. C. Leung, "Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1689–1703, 2019.

[72] A. Asheralieva and D. Niyato, "Distributed dynamic resource management and pricing in the iot systems with blockchain-as-a-service and uav-enabled mobile edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1974–1993, 2019.

[73] G. Hua, L. Zhu, J. Wu, C. Shen, L. Zhou, and Q. Lin, "Blockchain-based federated learning for intelligent control in heavy haul railway," *IEEE Access*, vol. 8, pp. 176830–176839, 2020.

[74] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Network*, vol. 35, no. 1, pp. 234–241, 2020.

[75] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2964–2973, 2020.

[76] M. Shen, H. Wang, B. Zhang, L. Zhu, K. Xu, Q. Li, and X. Du, "Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2265–2275, 2020.

[77] L. A. C. de Souza, G. A. F. Rebello, G. F. Camilo, L. C. Guimarães, and O. C. M. Duarte, "Dfedforest: Decentralized federated forest," in *2020 IEEE International conference on blockchain (blockchain)*, pp. 90–97, IEEE, 2020.

[78] Y. Wu, G. J. Mendis, and J. Wei, "Ddlpf: A practical decentralized deep learning paradigm for internet-of-things applications," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9740–9752, 2020.