IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Blockchain-Enabled Federated Learning for UAV Edge Computing Network: Issues and Solutions

CHAOYANG ZHU[1,4], XIAO ZHU[2,4], JUNYU REN[1,4], AND TUANFA QIN[3,4]

[1]School of Electronic and Information *Engineering*, South China University of Technology, Guangzhou 510641, China
[2]School of Electronic Information Engineering,Guangxi Vocational Technical Institute of Industry,Nanning,530001,China
[3]School of Computer and Electronic Information, Guangxi University, Nanning 530004, China
[4]Guangxi Key Laboratory of Multimedia Communications and Network Technology, Guangxi University, Nanning 530004, China

Corresponding author: Tuanfa Qin(tfqin@gxu.edu.cn).

This work was supported in part by the National Natural Science Foundation of China under grant no. 61761007, 61563004, and in part by the Natural Science Foundation of Guangxi Zhuang Autonomous Region under grant no. 2016GXNSFAA380222.

ABSTRACT Unmanned aerial vehicles (UAVs) extend the traditional ground-based Internet of Things (IoT) into the air. UAV mobile edge computing (MEC) architectures have been proposed by integrating UAVs into MEC networks during the current novel coronavirus disease (COVID-19) era. UAV mobile edge computing (MEC) shares personal data with external parties (such as edge servers) during intelligent medical analytics. However, this technique raises privacy concerns about patients' health data. More recently, the concept of federal learning (FL) has been set up to protect mobile user data privacy. Compared to traditional machine learning, federated learning requires a decentralized distribution system to enhance trust for UAVs. Blockchain technology provides a secure and reliable solution for FL settings between multiple untrusted parties with anonymous, immutable, and distributed features. Therefore, blockchain-enabled FL provides both theories and techniques to improve the performance of intelligent UAV edge computing networks from various perspectives. This survey begins by discussing the current state of research on blockchain and FL. Then, compare the leading technologies and limitations. Second, we will discuss how to integrate blockchain and FL into UAV edge computing networks and the associated challenges and solutions. Finally, we discuss the fundamental research challenges and future directions.

INDEX TERMS Unmanned aerial vehicles, Mobile Edge Computing, Federated Learning, Blockchain, Privacy

I. INTRODUCTION

UNMANNED aerial vehicles (UAVs), commonly known as drones or remote-controlled aircraft, have been widely used in the past few decades due to their excellent mobility and low cost [1]. Furthermore, in recent years, advances in drone manufacturing technology and lower manufacturing costs have led to a surge in enthusiasm for both civilian and commercial applications, making them more accessible for the public to use [2].

The Internet of Things (IoT) network architecture is evolving rapidly to cover various fields and applications [3]. UAVs have been deployed as air-ground equipment to address processing and storage requirements at the IoT networks [4]. However, there are substantial disadvantages to using UAVs, such as their inability to fly in inclement weather and the controller's requirement for visual line of sight (LOS) [5]. Most significantly, limited battery capacity and computing capabilities are viewed as their primary constraints. Furthermore, due to the UAV's limited computational capability, complicated algorithms requiring high CPU and GPU power cannot be run onboard. Additionally, processing and memory management of this massive amount of data on UAVs have been identified as critical issues, especially when utilizing artificial intelligence (AI) to extract and exploit helpful information [6].

Mobile Edge Computing (MEC) is an emerging technology proposed by the European Telecommunications Standards Institute (ETSI) in 2014 [7].It is capable of resolving the aforementioned issues effectively. Mobile edge computing can process complex data on the local side of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

ground base station, which is then forwarded to more capable marginal servers. [8]. As a result, UAVs can perform more complex tasks while the compute-intensive tasks are offloaded to the ground base station server. This will shorten the task's duration, but it will also reduce the drone's energy consumption, allowing it to fly for longer. However, widely used task offloading techniques such as matching theory rely on precise knowledge of global state information (GSI), which is incompatible with large-scale scenarios involving incomplete information. [9].

Future UAV-assisted MEC networks require a distributed learning approach that allows modeling without requiring raw data publication. The federated learning (FL) framework proposed by Google makes sense [10]. FL uses many mobile devices and a central computing server to perform machine learning. FL updates the parameters locally and then aggregates the model to create a shared model. Thus, FL seems like a promising solution for UAV-assisted MEC networks that maintains privacy during data analysis. For example, the author [11] designed an intelligent task offloading scheme based on federated reinforce learning to cope with such a rapidly changing scene. UAVs potentially provide many services in modern IoT interconnection, such as smart cities, smart farming, and intelligent transportation [12].

Despite the numerous benefits mentioned previously, FL continues to face challenges [13]. On the one hand, a single central node controls the entire algorithmic model due to the gradient aggregation mechanism used in FL. As a result, we must address data security concerns in order for all participants to have confidence in the central node and provide transparent information. Furthermore, FL systems currently lack adequate and transparent procedures for evaluating contributions and compensating training nodes to ensure continuous active training. Finally, an efficient distributed system must detect and prevent honest but curious training workers. Combining the UAV network with cutting-edge technology, such as blockchain, significantly improves user data security [14] [15].

Blockchain technology is a viable alternative solution for addressing the security and privacy concerns associated with MEC networks assisted by UAVs. The author provides a blockchain-based AI-empowered pandemic scenario supervision scheme [16]. A swarm of AI-enabled drones autonomously monitors pandemic outbreaks, reducing human involvement to the bare minimum. Blockchain is a distributed ledger technology that enables unmanned aerial vehicles to securely store data in the form of transactions. Also, blockchain technology enables FL to overcome the above issues. The blockchain combines consensus, and incentive mechanisms to secure data storage and traceability [17]. It can avoid single points of failure and extend FL to large-scale untrusted users on the UAV network. BCFL can also create an effective incentive mechanism by offering rewards proportional to the data sample, allowing mobile devices to provide large numbers of training samples.

However, UAVs network are always scattered throughout the UAV-assisted MEC networks. Due to the open nature of UAV communication and the MEC paradigm, it will be challenging to protect security during data analytics using traditional blockchain and FL methods. Therefore, how to protect data transmission security to the maximum extent possible is a critical issue that must be resolved.

While numerous researchers address various aspects of the data sharing problem in BCFL paradigms, there is no systematic examination of UAV-assisted MEC networks. This article discusses a novel paradigm for integrating blockchain and federated learning technology. We examined related works focusing on network structure design, performance enhancement, and consensus mechanisms in order to provide a comprehensive picture of UBFL-related research.

A. COMPARISON AND OUR CONTRIBUTIONS

Several federated learning systems have been proposed in the literature. For example, the works in [19] present the key FL concept and its enabling protocols and challenges in FL design and implementation. The survey in [20] discusses security and privacy in FL systems. It describes possible solutions for evaluations of malicious threats in FL networks. The integration of FL in mobile edge networks is investigated in [21], where challenges in FL implementation are explored, such as communication costs, resource allocation, and privacy and security. Meanwhile, FL and Internet-of-Things (IoT) are explored in [22], by providing a survey on the technical issues in FL designs, such as sparsification, robustness, privacy, scalability, and a brief discussion of FL applications in the IoT. Moreover, researchers present an overview of the FL applications in industrial IoT [23]. Although the focus is based on the characteristics and fundamentals of FL, the discussion of FL usage in UAV network is limited. The work mainly discusses the FL architecture and models, with a brief introduction to the FL in UAV informatics [24].

Although FL or blockchain in edge computing has been extensively studied in the literature, there is currently no review study on blockchain enabling federated learning in UAV edge computing networks. In order to fill this research gap, we conducted an extensive investigation of the UAV-enabled edge computing network, which integrates with FL and blockchain to achieve intelligence and security as described in this paper. The UBFL (Blockchain-enabled and Federated Learning MEC network supported by UAVs) architecture is described. Then we focus on the critical design issues and technical problems of UBFL in edge computing, including communication cost, resource allocation, incentive learning, security, and privacy protection. Finally, the possible research challenges and future research directions are proposed. The comparison between the related works and our paper is summarized in Table.1. To this end, the main contributions of this paper are as follows:

- The basic principles of FL and blockchain are summarized, and a UBFL architecture suitable for UAV edge computing networks is proposed.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

TABLE 1. Existing surveys on BCFL-related topics and our new contributions.

References	Key topic	Recent Advances in BC and FL				Taxonomy	Highlights
		Resource management	Security and privacy	Incentive mechanism	Communication Cost		
[18]	BC concept	✗	✗	✗	✗	None	A discussion of the architectures, algorithms, and data processing methods in BC systems.
[19]	FL concept	✓	✓	✗	✗	None	A survey of the FL concepts, technologies and associated learning approaches.
[20]	Security and privacy in FL	✗	✓	✗	✗	None	A review on the security and privacy issues in FL systems.
[21]	BC in edge networks	✓	✗	✓	✗	None	A survey on the integration of BC in mobile edge networks.
[22]	BCFL for IoT	✓	✓	✓	✗	None	A survey on the use of BCFL in IoT networks.
[23]	BCFL for IIoT	✓	✓	✗	✗	The discussion of FL in UAV is very limited.	A survey on the combination of BCFL and IIoT, mostly focusing on technical issues in FL implementation.
[24]	BCFL for UAV B5G	✗	✗	✗	✗	The discussion of FL in UAV is very limited.	A study on the FL architectures and models, with a very short introduction to MEC.
Our work	UBFL for UAV edge computing	✓	✓	✓	✓	A holistic taxonomy is presented.	A comprehensive survey on the use of UBFL in UAV edge computing, from motivations, requirements to UBFL designs and applications in a wide range of UAV domains edge computing.

- We talked about technical issues in the UBFL architecture, like how to communicate, how to allocate resources, how to learn, and how to protect privacy and security.
- We summarize the existing solutions to the problems of UBFL in the UAV edge network.
- Finally, we outline the main research challenges and discuss possible future directions for using UBFL in mobile edge computing.

B. STRUCTURE OF THE SURVEY

The remainder of this paper is organized as follows: Section II presents the structure of UAV mobile edge intelligence computing. In Sections III and IV, we describe the research status, advantages, and disadvantages of FL and blockchain. A generic UBFL architecture is also proposed, where the network components and working concepts are presented. The design and some critical use cases of UFBL implementation in edge computing are discussed in Section V. In contrast, technical issues in the UBFL architecture, such as communication costs, resource allocation, incentive learning, security, and privacy protection, are discussed in Section VI. The key research challenges and future directions are discussed in Section VII. Finally, Section VIII concludes the paper. Table.2 is the list of abbreviations in the paper. The architecture of the survey is shown in Fig.1.

II. UAV EDGE INTELLIGENT COMPUTING NETWORK

The UAV edge computing network combines edge computing technology with unmanned aerial vehicles (UAVs) [25]. The UAV can be a user node that submits computation-intensive tasks to the ground base station's edge server, or it can be an aerial edge server that supports many ground user nodes, as shown in Fig.2.

TABLE 2. List of abbreviations.

Item	Description
UAVs	Unmanned aerial vehicles
IoT	Internet of Things
MEC	Mobile Edge Computing
MEC Server	Mobile Edge Computing Server
UAV-MEC	UAV-assisted Mobile edge computing network
LoS	Line-of-sight
AI	Artificial Intelligence
ML	Machine Learning
FL	Federated Learning
BC	Blockchain
BCFL	Blockchain-enabled Federated Learning
UBFL	Blockchain-enabled and Federated Learning UAV-assisted MEC network
GBS	Ground Base Station
TFF	Tensor Flow Federated
GAN	Generative Adversarial Networks
PoW	Proof of Work
POS	Proof of Stake
DPOS	Delegated Proof of Stake
BFT	Byzantine Fault Tolerance
P2P	Peer to Peer

In contrast to conventional edge computing, UAV-assisted edge intelligent computing uses intelligent methods to address issues such as offloading strategy and resource management in UAV networks. In addition, it provides computing services for intelligent apps operated by UAV users [26]. Combining machine learning with the UAV edge computing network can give this architecture great power [27]. Based on the wireless channel state, ground node distribution, and onboard information about the vehicle, the UAV can make the best decisions, such as where to land. On the other hand, it can also provide computing and unloading services for many people in one place quickly and easily with its mobile ability. Its mobile capabilities can also provide computing

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

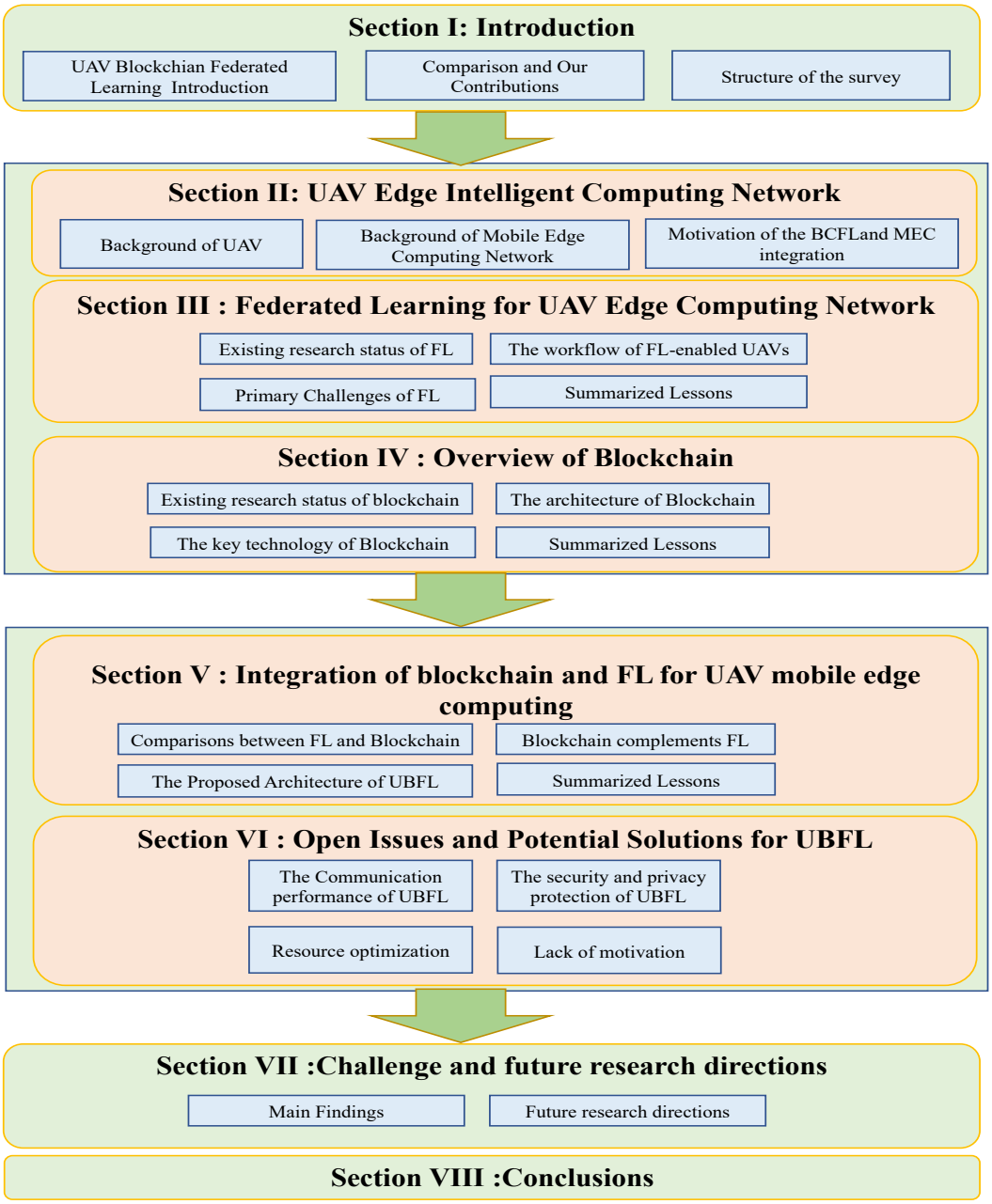

FIGURE 1. The structure of the survey.

and offloading services for many people in one place quickly and easily. As the user node, the ground base station provides computing service support for the UAV; the edge intelligent computing scenario is oriented to the UAV network. Multiple UAVs jointly perform tasks and are connected with the base station as a MEC server through an air-to-air. The base station server is by UAVs that do not need much power.

After completing task processing, the edge server will return the results to the UAV. This way can reduce the energy consumption of UAVs and task processing time delays, thereby prolonging the life of the UAVs and improving the user experience [28].

However, the edge server of the ground base station needs to collect data from multiple UAV nodes, which increases the data privacy league of UAV nodes. As users attach importance to privacy protection, such algorithms are facing significant privacy challenges [29]. Because of the increasing data volume in the UAV-MEC network and the growing concern about data privacy 5G beyond wireless networks [30], centralized artificial intelligence training on cloud-base server may not be appropriate [31]. We will go through this in-depth in the following section.

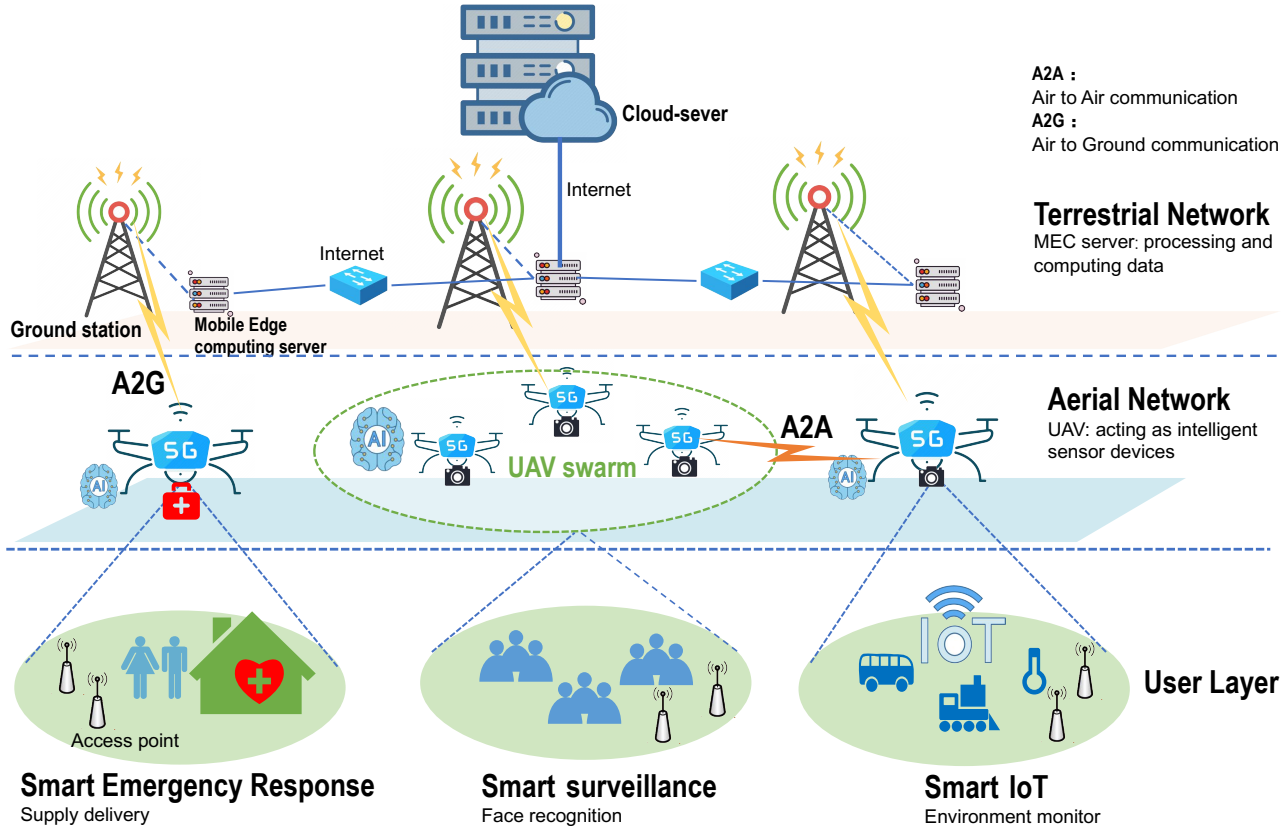

FIGURE 2. The architecture of UAV edge intelligent computing network.

III. FEDERATED LEARNING FOR UAV EDGE COMPUTING NETWORK

Current AI and deep learning technologies face two significant challenges: data islands and privacy security [32]. Faced with these obstacles, federated learning (FL) emerges as a promising paradigm for protecting device privacy by enabling devices to train AI models locally without transmitting raw data to a server.

A. EXISTING RESEARCH STATUS OF FL

Federated learning, first proposed by Google in 2016 [10], [33], establishes a sharing paradigm between mobile terminals and servers to utilize large-scale data while protecting user privacy effectively. Compared to traditional machine learning techniques, federated learning improves learning efficiency, addresses the issue of data islands, and protects local data privacy. However, the majority of this disparate data is unbalanced in reality. As a result, a practical and realistic strategy for data distribution optimization was developed in [34]. After that, many studies were conducted to improve the federated learning model. For example, [35] offered two strategies to reduce communication use during training. Furthermore, [13] fixes the primary federated learning mechanism by sharing the model's bias towards some participants, thus assuring fairness between participants in compressed federated learning. Finally, in [36], the author presented the single sample/small sample exploratory learning approach.

B. THE WORKFLOW OF FL-ENABLED UAVS NETWORK

As shown in Fig.3, federated learning typically consists of multiple participants and a server component. First, participants train shared models aggregated by servers and distributed to participants. The training process for federated learning is divided into three steps [37]:

- **Step 1 : Task initialization**
  Before the training begins, the server determines the training's tasks and objectives, selects the devices to participate in federated learning, and then sends the shared model to the selected devices.
- **Step 2: Local training and upadates**
  Each device trains the local model using private data. The purpose of training is to identify the best local model. After training, upload the model parameters to the server in preparation for the next step. Each client k trains a local model on its own dataset $\mathbf{d}_k$ and calculates an update w_k by minimizing a loss function $\mathcal{F}(\mathbf{w}_k)$:

$$\mathbf{w}_k^* = \arg\min \mathcal{F}(\mathbf{w}_k), k \in \mathcal{K}. \quad (1)$$

  Here, the loss function can be different for different FL algorithms [28]. For example, with a set of input-output pairs $\{x_i, y_i\}_{i=1}^K$, the loss function $\mathcal{F}$ of a linear regression FL model can be defined as: $\mathcal{F}(\mathbf{w}_k) = \frac{1}{2}(x_i^T \mathbf{w}_k -$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

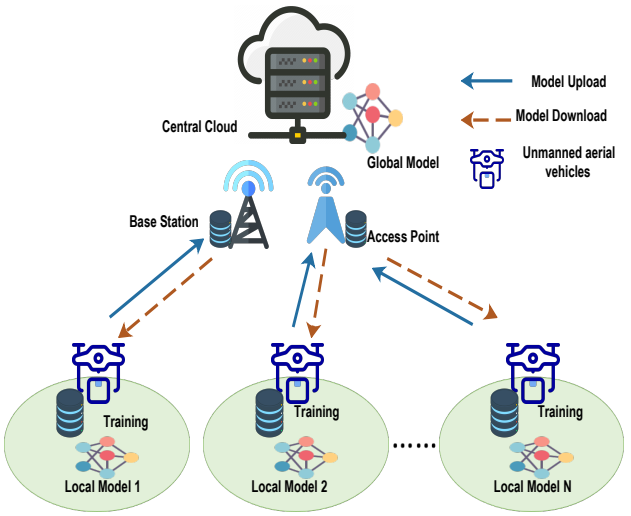

FIGURE 3. A Cloud-based FL-enabled UAV Network Architecture.

$y_i)^2$. Then, each client k uploads its computed update $\mathbf{w}_k$ to the server for aggregation.

- **Step 3: Global aggregation and download**
  The server collects data from all participants and aggregates model parameters. By averaging the local model parameters, the federated learning server obtains the next round of shared global model. The goal is to identify the most effective global model. As a result, the server computes a new version of the global model. By solving the following optimization problem:

$$\mathbf{w}_G = \frac{1}{\sum_{k\in\mathcal{K}} |D_k|} \sum_{i=1}^{K} |D_k| \, \mathbf{w}_k \tag{2}$$

$$(P1): \min_{\mathbf{w}_{i\in\mathcal{K}}} \frac{1}{K} \sum_{i=1}^{K} \mathcal{F}(\mathbf{w}_i) \tag{3}$$

Subject to (C1): $\mathbf{w}_1 = \mathbf{w}_2 = \cdots \mathbf{w}_i = \mathbf{w}_G$

Here, the loss function F reflects the accuracy of the FL algorithm, the accuracy of an FL-based object classification task. The constraint (C1) This ensures that all clients and the server share the same learning model over the FL task after each training. After the derivation of the model, the server broadcasts the new global update $\mathbf{w}_G$ to all clients for optimizing the local models in the next learning round. The FL process is iterated until the global loss function converges or the desired accuracy is achieved.

While several of the FL benefits are addressed in [38], we add the following after reviewing a collection of publications on numerous UAVs:

1) User privacy protection. Federated learning data is only stored locally and is not shared among participants, ensuring user data privacy and meeting the requirements of General Data Protection Regulations.
2) Model adaptation for large-scale data. Large-scale training data can help to improve training model quality. Federated learning can ensure that the trained model's effect is not harmed. At the same time, it can reduce the amount of equipment needed for training while increasing the model's training speed [39].
3) Improve the data source's flexibility. With the technical support of federated learning, some data sources that cannot participate in training due to specific factors can store data locally and participate in the overall model's training to improve the model's generalization effect [40].

C. PRIMARY CHALLENGES OF FL

Several studies in recent years have revealed that FL still has issues [41]. This section discusses some of the challenges that federated learning faces. The majority of prior research indicates that the following critical issues must be addressed in order to increase the efficiency of FL communication:

1) **Single point of failure:** Federated learning generally requires a central server to aggregate local models. If this central server fails, the local model update will be inaccurate [42].
2) **Communication performance:** Federated learning creates global models by combining local models on a central server. Network latency is caused by communication with the central server [10]. Concurrently, federated learning must upload iterative transmission parameters to a server. When multiple models are sent at the same time, the central server may cause network congestion due to bandwidth and other resource constraints like user count and training iterations.
3) **Lack of rewards:** Federated learning uses participant resources to train a global model, potentially addressing the data privacy issue of machine learning. In such a promising paradigm, a lack of training data and other resources will decline performance. Thus, it is critical to encourage more participants to contribute their valuable resources to federated learning [43].

Apart from communication efficiency, communication security during local updates transmission is another problem to be resolved. The authors provided various security and privacy open issues in FL as below [34]:

1) Poisoning attack. Malicious participants can upload failures of training samples or models for machine learning failure prediction. Simultaneously, a malicious client will upload an incorrect mask gradient to the central server via the intervention of the local model, which will harm the global model. The FL cannot audit malicious trainers. If these false parameters are aggregated into the entire model without verification, it will have a direct impact on the model's quality and may even fail the entire federated learning process [44].
2) Malicious devices can pollute storage models. An attacker can also extract data from a shared model [45]. Even if training resources are held locally, the FL

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

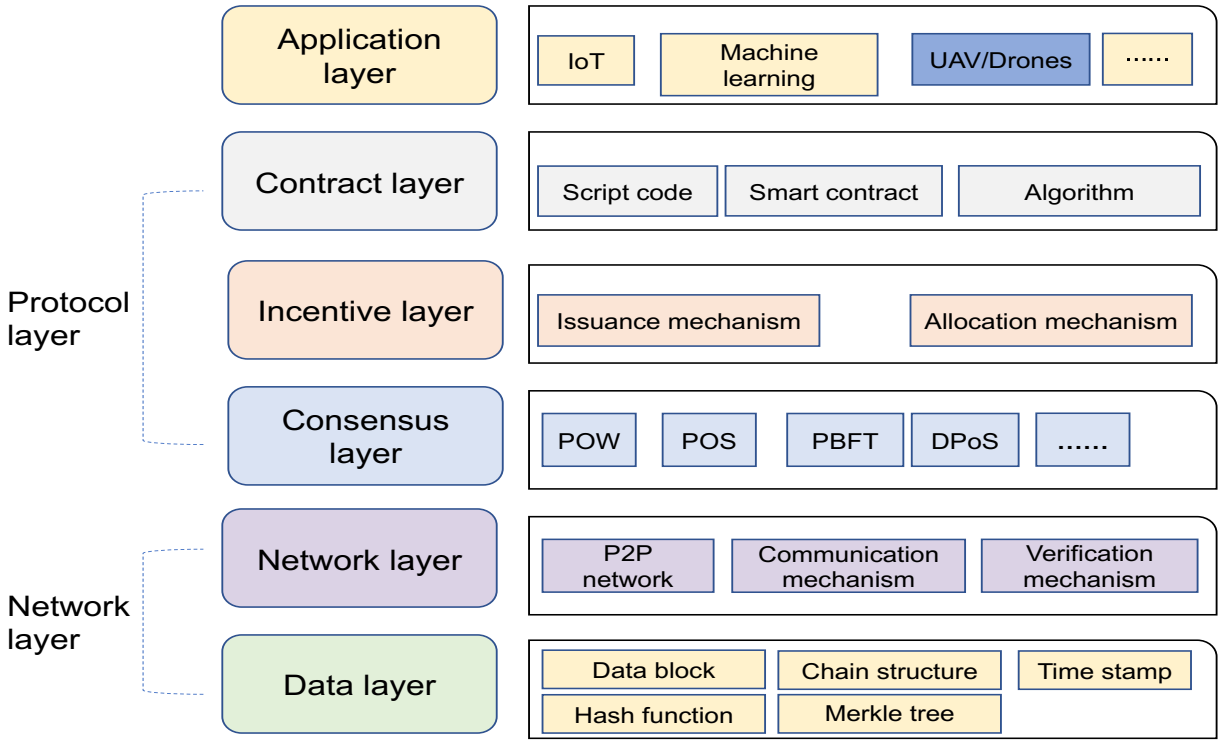

FIGURE 4. The architecture of Blockchain.

framework can violate data privacy. Therefore, the confidentiality of transmission and storage parameters must be enhanced. Based on the changes of federated learning gradient parameters in each round, malevolent users can deduce sensitive data from users. An intermediate gradient can also extract meaningful information. Malicious center servers can also use generative adversarial networks to steal data [46].

3) There is a lack of trust between participants in federated learning because they come from different organizations or institutions. In light of the lack of confidence, how to develop a safe and dependable cooperation mechanism is an urgent challenge that needs to be solved in practice [47].

D. SUMMARIZED LESSONS

The majority of existing FL training algorithm use offline learning protocols [48].

Before being selected as a worker by the server, the remote device collects and stores training data. Therefore, it is aware of the local data size$\mathbf{N}_{local}$. When uploading the gradient, data size $\mathbf{N}_{local}$ can be sent as a hyperparameter to the server in a single communication round. Thus, the global model gradient average can be calculated by Eq.(2).

However, communication in UAVs network alway in real time. Online federated training is a potential solution for UAVs network in the futrue IoT networks [49].

IV. AN OVERVIEW OF BLOCKCHAIN

Blockchain, a distributed append-only public ledger technology, was initially intended for cryptocurrencies. However, the Genesis Block was released in January 2009, marking the first application based on blockchain technology. The World Economic Forum forecasted and studied the application of blockchain in the financial scene in 2018 [50].

A. EXISTING RESEARCH STATUS OF BLOCKCHAIN

Blockchain technology has gained popularity for its capacity to improve distributed systems' security, reliability, and robustness. This technology has profited in finance, remote sensing, data analysis, and healthcare. The author surveys blockchain protocols for IoT networks and presents an overview of blockchain applications in IoT, such as Internet of Vehicles, Internet of Energy, Internet of Cloud, and Edge computing [51] [52].

The following blockchain technologies are mostly employed in the current IoT application [53]:

1) **Identity Management:** Blockchain uses hash address and permission authentication to secure participating nodes.
2) **Distributed Ledger:** The Consensus Method and Point-to-Point Transmission ensure the data consistency of each node in a distributed ledger.
3) **Data logging:** The data on the blockchain is transparent, traceable, and tamper-proof thanks to asymmetric encryption (such as the elliptic curve) and hash algorithms.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

4) **Incentive mechanism:** Blockchain employs incentives like digital currency to keep participants motivated to keep it running.
5) **Consensus mechanism:** The consensus mechanism ensures data security and dependability among dispersed nodes in the blockchain. Using the consensus technique, each participant authenticates the data, reducing the danger of data tampering and ensuring data consistency.

B. THE ARCHITECTURE OF BLOCKCHAIN

The structure of blockchain consists network layer, data layer, consensus layer, control layer, and application layer as shown in Fig.4.

- **Network layer:** The blockchain Network layer is divided into two layers: data and network [54]. The data layer is the system's data structure design ledger. It defines a blockchain's components. The primary chain is made up of identical blocks of the same size. Timestamps and hash algorithms connect blocks chronologically and secure transaction data. The network layer decentralizes data exchange between blockchain and accounting nodes [55]. A blockchain network is a peer-to-peer network, meaning there is no central server and users exchange information. Each node can receive and transmit data.
- **Protocol layer:** Three critical components comprise the protocol layer: consensus, incentive, and contract. According to [56], the consensus layer distributes the billing nodes' workload. The incentive layer is responsible for developing a compensation system for accounting nodes, with the goal of encouraging them to participate in blockchain security verification. The contract layer is composed of scripting code, algorithmic methods, and intelligent contracts [57].
- **Application layer:** The application layer is dedicated to developing blockchain solutions for a variety of applications and industries. Numerous blockchain use cases and scenarios are included in the application layer. Recently, there are several works attempting to apply blockchain into UAV-assisted MEC networks.

C. THE KEY TECHNOLOGY OF BLOCKCHAIN

A blockchain consists of four components: encryption, distributed storage, a consensus mechanism, and a smart contract. The consensus process is the principal technology of Blockchain, and smart contracts are explored in depth below [58]:

1) Consensus algorithm:

Nodes in the blockchain system can join and depart at will. Most systems employ P2P networks to transmit data to better interact with the blockchain system. A P2P network node performs network routing, block data validation, distribution, and node discovery. The blockchain's consensus algorithm includes a fine selection of specific packaging nodes and an acceptable economic incentive mechanism [54]. Blockchain consensus algorithms include Proof of Work, Proof of Stake, and Delegated Proof of Stake, Byzantine Fault Tolerance Algorithm (BFT). Table.3 summary consensus in Blockchain. The working principles and application domains of each consensus method are described below.

- **PoW (proof of work):** The PoW mechanism was first used in Bitcoin to choose packing nodes based on processing capability. The SHA256 mathematical challenge is tough to solve but easy to verify. The first node to solve the problem obtains the next block and the bitcoin reward generated by the system. Pow-based blockchains, like Bitcoin, are highly decentralized. Consensus approaches using competing processing power can sustain 50% attacks. PoW uses probabilistic blocks. The more blocks a block has, the more definite it is. So, a transaction must be confirmed for at least 1 hour to be considered final by the Bitcoin system.
- **PoS (proof of stake):** The PoS algorithm is proposed as a PoW solution to significant energy waste, and nodes can quickly join or leave the blockchain system. In a PoS system, block confirmation is still probabilistic, requiring multiple nodes to validate the block. The authors analyzed the complexity, contending that identifying accounting rights based on rights and interests can effectively reduce resource waste, block time, and transaction processing time [56]. Experienced currency users are more likely to choose the next block and earn the reward. In this way, users with economic interests can ensure the blockchain's efficacy while avoiding PoW's excessive energy usage [65].
- **BFT (Byzantine fault tolerance):** The Byzantine general problem can only be addressed using the BFT algorithm if the number of Byzantine nodes does not exceed 1/3 of the total number of nodes. An oral protocol and a written protocol make up the original BFT algorithm. In the oral protocol, the nodes must communicate the received "command" to one another before determining the outcome based on the information provided by each node. Written protocols that demand signature verification of sent data prevent Byzantine nodes from modifying the received data arbitrarily, resulting in a more reliable result [66].
- **DPoS (Delegated proof of stake):** Compared to the accounting methods PoW and PoS consensus, DPoS can be seen as a "democratic centralism" accounting method that can better tackle problems like energy waste and mining pools that threaten decentralization. The PoS board decision is equivalent to the DPoS consensus. Each node in the system can have rights and interests, representing the vote to grant a wish before accounting. In additonally, the node will enter the board based on the defined schedule for package settlement and manufacturing new blocks. It can also compensate for the fact

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

TABLE 3. A Comparative analysis of blockchain consensus algorithms.

References	Consensus	Efficiency	power consumption	Double spend resistance	Application	TPS/ips	Blockchain
[59]	PoW	Low	High	strong	Eth,Bitccoin	7,15	public
[60]	POS	High	Low	Weak	Peercoin	70	public
[61]	PoS + PoW	High	High	strong	PPcoin	10	public
[62]	PBFT	Medium	Low	strong	Fabric v0.6.0	200∼100	Consortium
[63]	DBFT	Medium	Low	strong	Eos v2.0,NEO	1 000	Consortium
[64]	DPoS	Low	Low	Medium	Eos v1.0	3 600	public

that people interested in bookkeeping do not wish to participate in bookkeeping: a consensus algorithm designed to be efficient, decentralized, and customizable [67].

Since there is no optimal consensus algorithm for all aspects of the blockchain system at the moment. Additionally, decentralization application enables users to participate actively in the consensus process, validate consensus, and ensuring the system's security and increasing its availability. Therefore, a blockchain system can be stable only if the flow of resources, user interaction, and participation are completely guaranteed.

2) **Smart Contract:**

Smart contracts define the terms and conditions agreed upon by all parties. The contracts' events can only be executed automatically when the relevant conditions are met, overcoming the problem of single-point failure in the centralized group-buying pricing and reputation evaluation mechanisms. On a blockchain, smart contracts are digital versions of traditional contracts. Like traditional computer programs, blockchain smart contracts have interfaces that can receive and respond to external messages, as well as process and store them [68]. As a result, smart contracts must be executed in a sandbox. The environment effectively isolates the contract working environment from the host system, improving intelligent contract security. Most common blockchain platforms use virtual machines and containers to create sandboxes where contract code can be executed separately.

D. SUMMARIZED LESSONS

Blockchains require more computing power to maintain consistent records among participants. Traditional consensus authentication mechanisms like proof of work have improved blockchain security, but their high computational overhead has become a bottleneck, slowing down block output speed. Improving blockchain transaction authentication efficiency will improve computing efficiency and create an intelligent blockchain. The idea of an intelligent contract expands the use of blockchain, but its intelligence must be improved. Further research is needed to realize a blockchain-based network's edge intelligence.

V. INTEGRATION OF BLOCKCHAIN AND FL FOR UAV MOBILE EDGE COMPUTING

Federated learning aims to create new value by enabling privacy protection technologies where data is available and invisible and improving user service quality by utilizing data from all parties. On the other hand, blockchain aims to ensure that transaction records cannot be tampered with, use consensus algorithms and distributed technologies to solve the problem of double payments in a decentralized network, and eventually achieve digital value representation and transfer. Given the issues mentioned above with blockchain and federated learning, blockchain and federated learning characteristics are examined. The following sections go over how to integrate and supplement blockchain and federated learning.

A. COMPARISONS BETWEEN FEDERATED LEARNING AND BLOCKCHAIN

Federated learning deals with the problem of data privacy through computation. The issue of untrusted data storage is addressed by blockchain. Both are complementary technologies that, like federated research, can be used to solve the problem of witnesses. In the traditional federated study framework, a trusted third-party server is used. For example, privacy protection is critical to conducting a federated study based on blockchain technology and realizing centralized or weak decentralization. In-depth analysis revealed many similarities and differences between the learning and chain blocks; a detailed comparison of the two technologies is provided below.

1) **Similarities:**

- Each node in the deployment structure is distributed independently.
- Each node's status is equal, and there is no centralized node.
- There is a risk of data privacy leakage. As a result, private data should be securely encrypted before performing transactions in federated learning and blockchain.

2) **Difference:**

- Category: The chain of blocks can be as simple as

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

TABLE 4. Potential benefits of UBFL architecture compared to our work.

References	Characteristics	Basic UAV Networks	UAV MEC Networks	Our Approach
[69]	Communication range	Limited range that depends on the used technology	Extended range based on MEC infrastructure	Extended range based on MEC infrastructure
[70]	QoS	Fair data delivery speed with limited throughput	Very fast data delivery with high throughput and reliability level	Very fast data delivery with high throughput and reliability level
[71]	Identity verification	No UAV identity verification	No UAV identity verification	UAV identity is checked so not any drone can participate in the mission
[72]	Data security	N/A	N/A	Data is stored in UBFL that provides security
[73]	Privacy	N/A	N/A	Data is stored in UBFL that provides privacy
[74]	Trust	N/A	N/A	Trust is provided since all participant's identities are verified
[75]	Decentralization	Centralized system	Centralized System	Decentralized System
[76]	Resource management	Basic, depends on the used technology	MEC resource management	managing MEC resources using Federated learning
[77]	Power efficiency	N/A	N/A	UBFL provide UAVs power efficiency
[78]	Scalability	N/A	N/A	Better scalability using Federated learning

a distributed database; FL is a distributed machine learning modeling and training system.

- Mechanism for problem-solving: Federated learning can solve the challenges of data isolation and data privacy to meet the goal of multi-party joint modeling. Blockchain seeks to solve most of the existing system's centralized, trust, and tampering problems.
- Data storage: All nodes in the blockchain keep a copy of the same data. Federated learning parties only have their data, not that of other parties [79].
- Validation: The participants verify each new transaction on the blockchain via a consensus algorithm, ensuring trust and anonymity against malicious attacks. Authentication is not required for the client to update the gradient to the server in FL [80].

B. BLOCKCHAIN COMPLEMENTS FEDERATED LEARNING

Both federated learning and blockchains require multiple parties to participate in creating a trusted network based on consensus. However, in terms of application goals, federated learning focuses on value creation, whereas Blockchain focuses on value representation and transfer [81]. Table.4 summarizes the potential BCFL integration solutions in the literature. Blockchain enables FL in two ways:

1) Blockchain is a reliable identity and identification system. Using the Blockchain's permission system and identity management, untrusted users can join a secure and trusted cooperation mechanism. Blockchain offers data security sharing. It is visible, traceable, tamper-proof, and forgery-proof. The distributed ledger feature of Blockchain naturally maintains the consistency of model parameter data among various participants in federated learning.
2) Taking advantage of the tamper-proof and decentralized qualities of Blockchain, rewards will be granted to the active client who exchanges data information. The more clients are involved in federated learning, the more accurate the model findings become. Model training is completed, and reward resources are written into the Blockchain according to each participant's input amount and quality [82]. Using the open and transparent nature of Blockchain will increase participation and improve participant cooperation.

C. THE PROPOSED ARCHITECTURE: UBFL

A BC-based FL-enabled UAV MEC network (UBFL) is presented in this subsection. We first introduce the UBFL architecture, arising from the integration of Blockchain and FL. Then, we present the training workflow of UBFL. Fig.5 presents the schematics of the proposed architectural design.

1) Architecture of UBFL

The client utilizes the Blockchain to establish a decentralized, federated training platform and store private data in a blockchain in the proposed architecture. It is considered that the global server is MEC-assisted to address the computational constraints of UAVs. The UBFL network is split into two layers: the user layer and the edge service layer. UAV mobile terminals make up the majority of the user layer. Base stations with Mobile Edge Computing (MEC) servers and specific storage and computing capabilities comprise the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

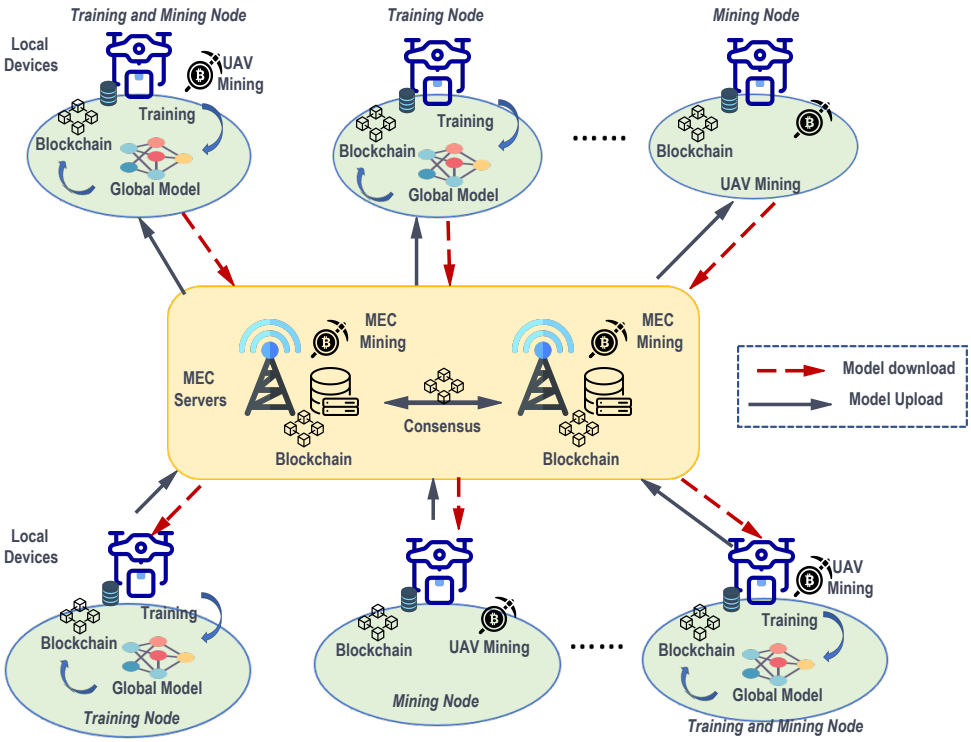

FIGURE 5. The conceptual of UBFL architecture.

edge service layer. The MEC server calculates and updates the global model.

The first relevant research focused on the creation of UBFL was proposed by [83]. The UBFL's main idea is to use Blockchain technology to solve problems like private exchanges and reward mechanisms. However, as seen in Fig.5, all subsequent research followed the same basic design framework. To be more specific, the Blockchain serves as a central database for the decentralized and private FL system. As a result, the main goal is to recompense clients based on the quality of their contributions while also protecting the privacy of the underlying data set and warding off malevolent attackers. Table.5 summarize existing solutions integrated with Blockchain and federated learning in a UAV-assisted MEC network. We will outline the main characteristics of the architecture.

2) UBFL training workflow

The illustration of a single communication round of UBFL systems is shown in Fig.6. In classical FL (see Fig.3), the global model is calculated by the base station of the MEC server and updated. However, in our UBFL architecture, global model calculations are performed directly on the UAVs in a decentralized manner via blockchain [84]. In the UBFL network, local training is performed using UAVs, and the data collected by UAVs can be used to train model parameters. The overall process is as follows:

- Local training: According to the data collected locally by sensing, the participating UAV users searched for local model parameters using an algorithm based on gradient descent to minimize the loss function.
- Upload parameters: UAV transmits the model parameters and computing time T to MEC server through wireless network. The MEC server stores them in the form of transactions.
- Model broadcasting and verification: The MEC server adds its digital signature to the model and broadcasts to other MEC server.
- Mining and Block validation: Upon receiving the local models from the other server, each MEC server uses consensus algorithm to mine current block.The current server block, if verified, is added to local ledgers of MEC.
- Global model download and aggregation: UAV downloads the gradient updates from MEC server. Each UAV aggregate the global model with other gradient upload as follow function:

$$w_i^{(t,l)} = w_i^{(t-1,l)} - \frac{\beta}{N_i}\left(\left[\nabla f_k\left(w_i^{(t-1,l)}\right) - \nabla f_k\left(w^{(l)}\right)\right] + \nabla f\left(w^{(l)}\right)\right) \tag{4}$$

In the UBFL architecture, each drone computes and exchanges training updates via a blockchain ledger running on the edge network, effectively performing global model aggregation on a local device without the need for a central server. The blockchain service runs on the MEC server, receiving and storing model parameters uploaded by UAVs

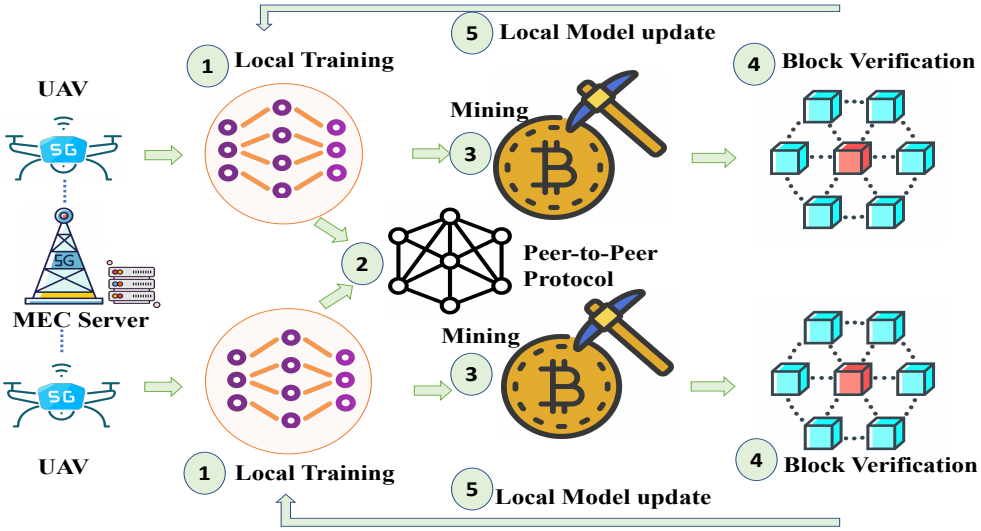

FIGURE 6. Illustration of UBFL training workflow.

and authenticating them via consensus protocols [85]. On the other hand, UBFL eliminates network latency associated with communicating with a central server.

D. SUMMARIZED LESSONS

To facilitate comprehension of the various UBFL structural variants, we classify UBFL frameworks into three categories. We leverage their organizational structure to develop customized UBFL structures to meet specific requirements. The UBFL makes use of blockchain and FL to bolster system security and build a more intelligent mechanism. However, its inefficiency impairs the overall performance of the system and has an effect on future applications. The flexibly coupled UBFL is recommended when the FL network is not suitable for running on a blockchain but requires a blockchain to aid in its learning process, such as for increased model accuracy or data sharing. The following section discusses the major UBFL technologies and solutions. We propose that UBFL's safety and dependability be evaluated in light of the computing requirements and environments in which it is used. If an aggregator-free system is required, the fully connected UBFL framework is recommended.

VI. OPEN ISSUES AND POTENTIAL SOLUTIONS FOR UBFL

In this section, we manipulate blockchain to do reputation management to restrain participants' behaviors. In this situation, the loosely coupled UBFL will be a good choice. Resource constraints and communication latency are impediments to the efficient operation of UBFL and must be addressed regardless of the architecture. We introduce technical work related to the UBFL architecture in a UAV edge computing network. We will introduce the key technologies of the UBFL architecture, including its communication performance and secure privacy protection.

A. THE COMMUNICATION PERFORMANCE

1) Communication Costs

Problem definition: Communication costs are vital issues that need attention in a BCFL system. In most current BCFL system schemes, transmission is analyzed by combining training delay, miner communication delay, and mining delay. However, in the application of edge computing, communication costs are concentrated on edge computation delay and parameter transmission delay. Table.5 summarizes the communication cost problem and solution.

Solution: Some recent work has been involved to solve the problem. In References [86], a new edge association algorithm for edge networks based on digital twins is proposed. The authors further discussed the impact of unreliable communication between the user and the MEC server may reduce communication latency and improve the reliability of the edge computing plane. A blockchain platform is used to run the Delegated Proof of Stake (DPoS) consensus mechanism to establish a decentralized training network for FLchain edge computing.

When determining the optimum block arrival rate, both communication and consensus latency are considered. These findings and insights highlight significant results and insights about adaptive BFL design. The online delay minimization algorithm optimizes the delay by considering frame size, block size, and block arrival rate. It is demonstrated that taking communication and consensus delays into account while determining an acceptable FLchain training delay increases overall model learning performance [85].

A gradient compression scheme was designed to generate sparse but significant gradients to reduce communication overhead without compromising accuracy, improving the communication efficiency of the blockchain-enabled FL [87]. Moreover, it further strengthens the privacy preservation of training data. The security analysis and numerical results

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

TABLE 5. The Potential Solution for Communication Cost of UBFL

Solved problem	Solution	Reference	Application scenarios
Low-latency	a new edge association algorithm	[86]	digital twin empowered 6G
Management overheads	a three-layer architecture and specifical communication protocols	[87]	fog computing supported Internet of Vehicles
Communication delay	A distributed learning framework	[88]	5G networks
System delay	FLchain architecture	[83]	Industrial Internet of Things
end-to-end delay	local on-board machine learning (oVML) model autonomous vehicles	[89]	autonomous vehicles
Latency overhead	Hybrid architecture	[90]	6G networks
Latency overhead	Hierarchical architecture	[91]	5G Industrial Internet of Things

indicate that the proposed schemes can achieve decentralized FEL security, scalable, and communication-efficient.

Discussion: In the UBFL architecture, each drone user computes and exchanges his training updates through a blockchain ledger running on top of the edge network, performing global model aggregation on a local device without needing a central server. While eliminating network costs (such as latency) associated with communicating with a central server, the use of the blockchain introduces new costs associated with block mining. Therefore, the communication problem of UBFL needs to consider the training delay, update communication delay, and block mining delay on the equipment at the same time.

B. THE SECURITY AND PRIVACY PROTECTION

Establishing security and privacy protection mechanisms is critical for blockchain-based federated learning systems. Using blockchain technology to govern the data source method of data information transmission between nodes can eliminate a single point of failure. Moreover, they are incredibly effective against attacks, especially in decentralized, federated learning systems. The summary for security and privacy protection of UBFL is shown in Table.6.

1) Poisoning attacks

Problem definition: The UBFL design is vulnerable to data or model poisoning threats [87]. An attacker manipulates the local training process, hyper-parameters, and model weight before submitting the aggregation. To compromise classifications, an attacker can employ data poisoning to inject a backdoor into an aggregate detection model. It was an attempt to poison the training data by introducing malicious data into the ordinarily normal training data set, which is more successful than just training data poisoning.

Solution: In References [99], a hybrid BCFl framework that uses smart contracts to detect and punish attackers with fines automatically. The authors analyzed the communication efficiency and design am attacker detection algorithm.

The authors in Reference [107] analyzed a two-phase learning stage. The first phase is a numerical evaluation, preventing the malicious devices from being selected. For the second phase, researchers devised a participant-selection algorithm that enables the FL server to select the appropriate group of devices for each round of FL training. The researchers believe that the study can shed new light on the joint research of blockchain and federated learning.

Discussion: To summarize, attackers can train local models to replace global models and adjust parameter values to manipulate the training outcome during model transmission. As a result, many researchers are researching ways to detect attacks on blockchain-based federated learning systems.

Adjusting mining difficulty without affecting training performance also reduces the risk of poisoning attacks. As a result, blockchain mining and local data training should consider the attack model. An adversary miner, for example, could manipulate data blocks. Defensive miners use witch attacks to double trade, making mining inefficient.

2) Single point failure

Problem definition: FL relies on a central server, which makes global model updates problematic. So all local model updates are subject to subsequent local model updates' accuracy. Since bandwidth constraints, sending multiple models simultaneously may overload the central server [108].

Solution: In order to improve Federated Learning security, the author proposes a blockchain network called FLchain (FL) [109]. Each local model parameter is a block on the specific channel ledger. In addition, the paper introduces the concept of "the global model state trie," which is stored and updated on the blockchain network from mobile device updates. Quantitive Analysis FLchain outperforms traditional FL schemes by ensuring provenance. Furthermore, they maintain the auditable characteristics of the FL model.

FLChain replaces the traditional FL parameter server, requiring on-chain consensus. It is not easy to motivate and deter distributed trainers. An honest trainer can profit proportionally from a well-trained model, while the malicious can be quickly detected and severely punished [93]. The author created DDCBF to speed up the querying of blockchain-documented data. Finally, the author builds a model of our work and calculates its costs.

In References [110], Consortium chains typically use con-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

TABLE 6. Summary for security and privacy protection in UBFL

Solved problem	Framework	Blockchain type	Consensus mechanism
Single point failure, lack of motivation	BlockFL [92]	Public	PoW
Single point failure, lack of motivation	FLChain [93]	Public	-
Single point failure	FLChain [94]	Public	PBFT/PoW
Poison attack, lack of motivation	RFL [95]	Consortium	PBFT
Single point failure, lack of motivation, privacy leakage	DeepChain [96]	Public	Blockwise-BA
Single point failure, privacy leakage	FedBC [97]	-	-
Single point failure, lack of motivation	BC-FL [98]	Public	Pow
Single point failure, poison attack, lack of motivation	BlockFLA [99]	Public & private	PoW & PBFT
Single point failure	Chain FL [100]	Private	PoA
Poison attack	PSFL [44]	-	-
Single point failure, poison attack	BFEL [101]	Public & consortium	DPoS/PBFT & PoV
Single point failure, poison attack, privacy leakage	Biscotti [102]	public	PoF
Single point failure, poison attack	VFChain [103]	Public	Algorand
Single point failure	BLADE-FL [104]	Public	PoW
Single point failure, poison attack, lack of motivation	BFLC [105]	Public	Committee
Single point failure, poison attack, lack of motivation	VBFL [106]	Public	PoS

sensus mechanisms to keep the chain from being manipulated by a small number of malicious nodes. In the case of PBFT (Practical Byzantine Fault Tolerance), as long as the number of misbehaving nodes is less than 1/3 of the total number of nodes, the regular operation of the blockchain will not be affected.

Discussion: The FL center server can be replaced with distributed blockchain nodes to resolve single-point failures. In addition, miner nodes can exchange the model updates of a local device. The qualitative evaluation shows that FLchain is robust. Traditional FL schemes are preferred as they ensure provenance and maintain auditable aspects of the FL model in an immutable manner.

3) Privacy leakage

Problem definition: Although all participants exchange gradient information and will not expose their original data to the outside world, there is still a risk that the original data will be counter derived only based on the open gradient update process.

Solution: A blockchain-based decentralized, federated learning framework can avoid the centralized structure's privacy and failure risks. An open-source deep learning framework named DeepChain was created to address these issues. DeepChain also provides a blockchain-based value-driven incentive mechanism to force participants to behave appropriately [96]. Meanwhile, DeepChain ensures participant data privacy and training process suitability. The article implements a DeepChain prototype and tests it on a real dataset in various settings, with promising results.

We also note that secure multi-party computation and homomorphic encryption show good promise without seeing each other's plaintext. [111]. The UAV can match encrypted cipher-text operations with plaintext operations using homomorphic encryption. However, there is no third-party authority to manage the private key in the system, making homomorphic encryption challenging to use directly. Furthermore, using the same homomorphic encryption key across all nodes does not protect privacy. However, it solves the problem of key distribution and management without a central node and enables the use of homomorphic encryption in gradient operation and privacy protection. [108].

Discussion: Differential privacy, homomorphic encryption, and other technologies are still the most beneficial for BCFL. With Laplacian noise, for example, the possibility of noise removal is greatly reduced, and differential privacy is achieved. Homomorphic encryption improves the security of outsourced storage and computing in federated learning. It is possible to effectively encrypt data before sharing it on the blockchain, which is important when dealing with personal and private data.

C. RESOURCE OPTIMIZATION

Problem definition: Since the UAV network having constrained computing and communication resources, incorporating blockchain and FL into the UAV edge computing application presents new challenges. Although MEC computational offloading strategies can improve UAV computing performance, the communication efficiency of UBFL becomes a key challenge in large-scale IoT scenario [117]. Given the future application, one can use optimization theory to optimize the task allocation and resource allocation.

Solution: A potential solution to this difficult problem could involve in [118]. The author proposes a decentralized

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

TABLE 7. The Comparison of Some Prominent Incentive Mechanisms for BCFL

Ref.	blockchain type	Resource	Incentive Mechanism	Protocol/sheme	Problem type
[93]	public	Data resources	Reputation-based and Contract theory	Incentive	self-interested
[112]	consortium	Data resources	reputation-based	worker selection, attack detection	self-interested, malicious
[113]	public	Training resources	Bayesian Nash Equilibrium theory	Incentive	self-interested, malicious
[114]	-	Data resources	Pricing-base	Incentive, audit	self-interested
[115]	public	Training resources	rewards-based	incentive, punish-ing	self-interested, malicious
[116]	-	Data resources	smart contract	incentive, audit	self-interested, malicious

FL framework by integrating blockchain into FL, namely BLADE-FL. In a round of the proposed BLADE-FL, each client broadcasts its trained model to other clients, competes to generate a block based on the received models, and then aggregates the models from the generated block before its local training in the next round. The work considers the learning performance of BLADE-FL and develops an upper bound on the global loss function. A lightweight blockchain platform based on DPoS consensus has been widely used to support model updates and block mining in federated learning [119]. Additionally, considering the rate at which local devices learn, the rate at which models arrive, and the rate at which blocks are generated across the entire blockchain-based federated learning system is an effective way to address future resource allocation issues between miners and local devices.

Discussion: Resource allocation is critical in UBFL systems to ensure optimal data training resource use. Deep reinforcement learning is widely used to implement resource allocation strategies for blockchain-based federated learning systems. In particular, the deep neural network model is used to decompose the problem and solve the sub-problems. To improve the efficiency of the integration scheme, the literature [120] proposes an asynchronous aggregation scheme and uses reinforcement learning authorized by digital twin to schedule relay users and allocate spectrum resources.

D. LACK OF MOTIVATION

FL has no incentive to attract sufficient distributed training data and computation power. A few of the techniques used in FL incentive mechanisms are Stackelberg game [121]. Blockchain are used to improve FL traning node selection, contribution evaluation, and robustness. We compare prominent research on design goals and main incentive mechanisms in BCFL, shown in Table.7.

Problem definition: FL has assumed that participants' mobile devices are trustworthy volunteers. This assumption precludes the use of traditional FL methods in UAV networks. There are two types of workers in the Fl training: self-interested individuals who are hesitant to contribute their computing resources unconditionally in the absence of economic incentives, and malicious individuals who send corrupt updates to disrupt the learning process [115]. Incentive mechanisms for participating in training and worker selection schemes for reliable federated learning have not been explored yet.

Solution: The authors in Reference [93] presented FLChain replace traditional FL parameter server. Furthermore, although blockchain-enabled FL has been proposed to give workers reward, any rigorous reward policy design has not been discussed. The author design a repeated competition schemes for FL [122].

The scheme proposed in [113], the author design a reputation-based worker selection scheme combining reputation with contract theory to motivate high-reputation mobile devices with high-quality data to participate in model learning. The final goal of the incentive mechanism is to improve FL performance. A incentive mechanism based on Bayesian game theory used to address challenges in UAV-aided wireless networks is provided in Reference [114]. Model predicte accuracy are also considered.

Discussion: Most of the incentive mechanisms proposed in this section aim to increase model training participation and thus the robustness of the entire blockchain-based federated learning system. As well as model updating verified and audited by blockchain, federated learning training now has some unique functions for the incentive mechanism to achieve security. However, the ledger network ensures fairness in the federated learning process by collecting gradients and updating parameters. The cost of verifying gradient updating has not been fully considered in existing studies. The future incentive scheme should encourage more user to join FL, thus improving its performance. The proposed incentive scheme should also be lightweight, as resource-constrained

nodes are reluctant to perform expensive computations.

VII. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

In this section, we describe potential prospective research directions that we believe would be fascinating to work on and study in the future. The study directions are grouped according to the high-level challenges that they are supposed to address.

A. ENERGY-AWARE COMMUNICATION

Artificial intelligence techniques will be expanded in UAV communication systems over the next decade. Using the UBFL architecture, it is possible to perform global model aggregation on a local device without the need for a central server. While the blockchain does away with the need for a central server, it does so at the expense of additional costs associated with block mining. To reduce UBFL's energy consumption, two UBFL costs must be considered: training and block mining [123]. Due to the fact that the UAV communication system is a more complex multi-dimensional network than current terrestrial communication networks, it is expected that energy-consumption, connectivity, and stable operation will need to be improved in the future.

B. PRIVACY ENHANCEMENT MODEL AGGREGATION

The survey results indicate that privacy and secrecy strategies are critical for UBFL interaction and proper functioning. Scientific innovation will drive future inter- and intra-UAV communication technology. There are significant security and privacy concerns associated with ensuring FL convergence. Numerous data aggregation strategies have been proposed recently to maintain the UBFL network's security and privacy. However, the limited processing power of the intelligent sensor renders the scheme unsuitable for the bright UAV environment. In References [124], the author proposes attack-proof strategy as a potential technology for UBFL in model aggregation. However, how to devise the appropriate Privacy enhancement data aggregation technique still needs further exploration by the research community.

C. FULLY DECENTRALIZE AND ROBUSTNESS TRAINING

Traditional synchronous FL systems are centralized, which may cause a straggler effect in the decentralized network. The straggler effect occurs when wireless model updates are delayed during FL training. Synchronization FL global aggregation occurs following each worker's parameter update. UAV network and connectivity issues cause many worker dropouts during training. A realistic technique to minimize the straggler impact is to select a subset of participating UAVs for each global iteration. Due to the decentralized nature of UBFL, any device can act as an aggregator. After each round, a portion of UAV dworker is chosen. UBFL uses a mini-batch SGD optimizte algorithm to reduce the device workload [78]. Asynchronous FL also allows participants to join mid-way through a training round. This is more representative of real-world FL settings and can help ensure FL scalability. However, while many efforts have been made to support centralized algorithms against the straggler problem, decentralized algorithms have received little attention.Due to the guaranteed convergence, synchronous FL remains the most popular [34]. UAVs integrated with 5G and IoT technologies will have great economic and stability implications for smart cities in the near future. It is critical to consider the training strategy's robustness in the presence of massive data distributed according to decentralize application.

D. HETEROGENEITY DATA COLLECTTION

Communication between heterogeneous nodes with varying levels of computing power and bandwidth will become the primary constraint on UAV-enabled Internet of Things. Current research on UAV edge computing networks ignores nodes from heterogeneous networks. As a result, how to establishing a flexible coordination mechanism among numerous heterogeneous nodes is worth exploring.

VIII. CONCLUSION

This survey outlines the UBFL architecture of blockchain-enabled federated learning in UAV edge computing networks. We first introduced the latest developments in federated learning technology, especially blockchain technology.

To discover the UBFL architecture in UAV edge computing, we introduce how blockchain technology can enhance and solve critical issues related to federated learning, i.e., communication cost, resource allocation, security, and privacy protection. Finally, we have outlined the key research challenges and possible directions toward fully realizing the UBFL architecture.

Our review shows that the basic architecture for federated learning using blockchain is still in its infancy. There are many challenges in areas related to privacy protection, security, smart contracts, scalability and performance issues, and consensus protocols and incentive mechanism design. This survey opens up a new way to realize UAVs' scalable and secure edge intelligence in the next-generation wireless network.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (No. 61761007) and the Scientific Research Project of Guangxi University Xingjian College of Science and Liberal Arts (No. Y2021ZK03).

REFERENCES

[1] I. A. Ridhawi, O. Bouachir, M. Aloqaily, and A. F. M. Boukerche, "Design guidelines for cooperative uav-supported services and applications," *ACM Computing Surveys (CSUR)*, vol. 54, pp. 1 – 35, 2022.

[2] Y. Zeng, R. Zhang, and T. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 36–42,.

[3] L. YANG, H. YAO, and J. WANG, "Multi-uav enabled load-balance mobile edge computing for iot networks[j," *IEEE Internet of Things Journal*, vol. 2020, no. 99, p. 1.

[4] A. Islam, A. Al Amin, and S. S. Y, "Fbi: A federated learning-based blockchain-embedded data accumulation scheme using drones for internet of things[j," *IEEE Wireless Communications Letters*.

[5] Y. Zeng, J. Lyu, and R. Zhang, "Cellular-connected uav: Potential, challenges, and promising technologies," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 120–127,.

[6] A. Fakhreddine, C. Bettstetter, S. Hayat, R. Muzaffar, and D. Emini, "Handover challenges for cellular-connected uavs," in *Proceedings of the 5th Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, Seoul, Korea, pp. 9–14.

[7] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450 465,.

[8] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A survey on mobile edge networks: Convergence of computing caching and communications," *IEEE Access*, vol. 5, pp. 6757–6779,.

[9] F. Zhou, R. Hu, Z. Li, and Y. Wang, "Mobile edge computing in unmanned aerial vehicle networks," *IEEE Wireless Communications*, vol. 27, no. 1, pp. 140–146,.

[10] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *AISTATS*, 2017.

[11] R. Wang, Y. Cao, A. Noor, T. A. Alamoudi, and R. Nour, "Agent-enabled task offloading in uav-aided mobile edge computing," *Computer Communications*, vol. 149, pp. 324–331, 2020.

[12] H. Shakhatreh, "Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48 572–48 634,.

[13] S. Niknam, H. Dhillon, and J. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEECommun. Mag*, vol. 58, no. 6, pp. 46–51,.

[14] E. J. D. Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys (CSUR)*, vol. 53, pp. 1 – 27, 2020.

[15] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90 478–90 494, 2020.

[16] A. Islam, T. Rahim, M. Masuduzzaman, and S. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using internet of drone things," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 166–173,.

[17] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale internet of things data storage and protection," *IEEE Transactions on Services Computing*, vol. 12, no. 5, pp. 762–771, 2018.

[18] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*.

[19] D. Nguyen, M. Ding, P. Pathirana, A. Seneviratne, J. Li, and H. Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*.

[20] V. Mothukuri, R. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Future Gener. Comput. Syst*, vol. 115, pp. 619–640,.

[21] Q. L. Wang, Y. F. Guo, X. F. Wang, T. X. Ji, L. X. 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.

[22] W. S. Zhang, Q. H. Lu, Q. Y. Yu, Z. T. Li, Y. Liu, S. K. Lo, S. P. Chen, X. W. Xu, and L. M. Zhu, "Blockchain-based federated learning for device failure detection in industrial iot," *Ieee Internet of Things Journal*, vol. 8, no. 7, pp. 5926–5937, 2021.

[23] P. Y. Zhang, H. Sun, J. Y. Situ, C. X. Jiang, and D. L. Xie, "Federated transfer learning for iiot devices with low computing power based on blockchain and edge computing," *Ieee Access*, vol. 9, pp. 98 630–98 638, 2021.

[24] Y. L. Lu, X. H. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for 5g beyond," *Ieee Network*, vol. 35, no. 1, pp. 219–225, 2021.

[25] S. H. Alsamhi, F. A. Almalki, F. Afghah, A. Hawbani, A. V. Shvetsov, B. Lee, and H. B. Song, "Drones' edge intelligence over smart environments in b5g: Blockchain and federated learning synergy," *Ieee Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 295–312, 2022.

[26] Z. P. Cheng, Z. B. Gao, M. H. Liwang, L. F. Huang, X. J. Du, and M. Guizani, "Intelligent task offloading and energy allocation in the uav-aided mobile edge-cloud continuum," *Ieee Network*, vol. 35, no. 5, pp. 42–49, 2021.

[27] Y. J. Dong, Z. Hassan, J. L. Cheng, J. Hossain, and V. C. M. Leung, "An edge computing empowered radio access network with uav-mounted fso fronthaul and backhaul: Key challenges and approaches," *Ieee Wireless Communications*, vol. 25, no. 3, pp. 154–160, 2018.

[28] X. Cao, J. Xu, and R. Zhang, "Mobile edge computing for cellularconnected uav: Computation offloading and trajectory optimization," in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC*, pp. 1–5,.

[29] P. MACH and Z. BECVAR, "Mobile edge computing: a survey on architecture and computation offloading[j," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1628–1656.

[30] L. Barbieri, S. Savazzi, M. Brambilla, and M. Nicoli, "Decentralized federated learning for extended sensing in 6g connected vehicles," *Vehicular Communications*, vol. 33, 2022.

[31] J. R. Wang, K. Y. Liu, and J. P. Pan, "Online uav-mounted edge server dispatching for mobile-to-mobile edge computing," *Ieee Internet of Things Journal*, vol. 7, no. 2, pp. 1375–1386, 2020.

[32] O. Hireche, C. Benzaid, and T. Taleb, "Deep data plane programming and ai for zero-trust self-driven networking in beyond 5g," *Computer Networks*, vol. 203, 2022.

[33] J. Konecný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *ArXiv*, vol. abs/1610.05492, 2016.

[34] W. Lim, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Commun. Surveys Tuts*, vol. 22, no. 3,pp, pp. 2031–2063,.

[35] N. Tran, W. Bao, A. Zomaya, M. Nguyen, and C. Hong, "Federated learning over wireless networks: Optimization model design and analysis," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr*, pp. 1387–1395.

[36] Z. Du, C. Wu, T. Yoshinaga, K.-L. Yau, Y. Ji, and J. Li, "Federated learning for vehicular internet of things: Recent advances and open issues," *IEEE Open J. Comput. Soc*, vol. 1, pp. 45–61,.

[37] B. Brik, A. Ksentini, and M. Bouaziz, "Federated learning for uavs-enabled wireless networks: Use cases, challenges," *and open problems.IEEE Access*, vol. 8, pp. 53 841–53 849.

[38] L. Kong, X.-Y. Liu, H. Sheng, P. Zeng, and G. Chen, "Federated tensor mining for secure industrial internet of things," *IEEE Trans. Ind. Informat*, vol. 16, no. 3, pp. 2144–2153,.

[39] 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 Things J*, vol. 7, no. 7, pp. 6348–6359,.

[40] J. Ren, H. Wang, T. Hou, S. Zheng, and C. Tang, "Federated learning-based computation offloading optimization in edge computingsupported internet of things," *IEEE Access*, vol. 7, pp. 69 194–69 201,.

[41] X. Wang, C. Wang, X. Li, V. Leung, and T. Taleb, "Federated deep reinforcement learning for internet of things with decentralized cooperative edge caching," *IEEE Internet Things J*, vol. 7, no. 10, pp. 9441–9455,.

[42] Y. Liu, J. T. Nie, X. D. Li, S. H. Ahmed, W. Y. B. Lim, and C. Y. Miao, "Federated learning in the sky: Aerial-ground air quality sensing framework with uav swarms," *Ieee Internet of Things Journal*, vol. 8, no. 12, pp. 9827–9837, 2021.

[43] J. W. Kang, Z. H. Xiong, D. Niyato, S. L. Xie, and J. S. 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. 10 700–10 714, 2019.

[44] Z. M. Chen, H. Y. Cui, E. S. Wu, and X. Yu, "Dynamic asynchronous anti poisoning federated deep learning with blockchain-based reputation-aware solutions," *Sensors*, vol. 22, no. 2, 2022.

[45] Z. Du, C. Wu, T. Yoshinaga, K.-L. Yau, Y. Ji, and J. Li, "Federated learning for vehicular internet of things: Recent advances and open issues," *IEEE Open J. Comput. Soc*, vol. 1, pp. 45–61,.

[46] M. Shen, H. Wang, B. Zhang, L. H. Zhu, K. Xu, Q. Li, and X. J. 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, 2021.

[47] 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. 181 789–181 799, 2019.

[48] W. Wu, L. He, W. Lin, R. Mao, C. Maple, and S. A. Jarvis, "Safa: A semi-asynchronous protocol for fast federated learning with low overhead," *IEEE Transactions on Computers*, vol. 70, pp. 655–668, 2021.

[49] Y. Chen, Y. Ning, M. Slawski, and H. Rangwala, "Asynchronous online federated learning for edge devices with non-iid data," *2020 IEEE International Conference on Big Data (Big Data)*, pp. 15–24, 2020.

[50] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE Network*, vol. 33, no. 3, pp. 10–17,.

[51] J. Xie, H. Tang, T. Huang, F. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys Tutorials*.

[52] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Vehicular Communications*, vol. 23, p. 100249, 2020.

[53] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[54] X. Wang, X. Zha, W. Ni, R. Liu, Y. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," *Computer Communications*.

[55] S. Rathore, B. W. Kwon, and J. H. Park, "Blockseciotnet: Blockchain-based decentralized security architecture for iot network," *Journal of Network and Computer Applications*, vol. 143, pp. 167–177.

[56] W. Wang, D. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 32 822 370,.

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

[58] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial," *IEEE Internet of Things Journal*, 2021.

[59] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[60] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[61] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT express*, vol. 6, no. 2, pp. 93–97, 2020.

[62] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[63] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "Distributed consensus protocols and algorithms," *Blockchain for Distributed Systems Security*, vol. 25, p. 40, 2019.

[64] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information processing systems*, vol. 14, no. 1, pp. 101–128, 2018.

[65] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18,.

[66] Z. H. Li, H. F. Yu, T. Y. Zhou, L. Luo, M. C. Fan, Z. L. Xu, and G. Sun, "Byzantine resistant secure blockchained federated learning at the edge," *Ieee Network*, vol. 35, no. 4, pp. 295–301, 2021.

[67] S. Zhang and J.-H. Lee, "Double-spending with a sybil attack in the bitcoin decentralized network," *IEEE Transactions on Industrial Informatics*.

[68] A. Dorri, S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot//2017," in *IEEE/ACM Second International Conference on InternetofThings Design and Implementation (IoTDI). IEEE*, vol. 2017, pp. 173–178.

[69] M. Ali, H. Karimipour, and M. Tariq, "Integration of blockchain and federated learning for internet of things: Recent advances and future challenges," *Computers & Security*, vol. 108, p. 102355, 2021.

[70] S. H. Alsamhi, F. A. Almalki, F. Afghah, A. Hawbani, A. V. Shvetsov, B. Lee, and H. Song, "Drones' edge intelligence over smart environments in b5g: Blockchain and federated learning synergy," *IEEE Transactions on Green Communications and Networking*, 2021.

[71] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," *Ad Hoc Networks*, vol. 120, p. 102574, 2021.

[72] H. Lee and J. Kim, "Trends in blockchain and federated learning for data sharing in distributed platforms," in *2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2021, pp. 430–433.

[73] 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. 205 071–205 087, 2020.

[74] 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.

[75] J. Li, Y. Shao, K. Wei, M. Ding, C. Ma, L. Shi, Z. Han, and V. Poor, "Blockchain assisted decentralized federated learning (blade-fl): Performance analysis and resource allocation," *IEEE Transactions on Parallel and Distributed Systems*, 2021.

[76] D. Saraswat, A. Verma, P. Bhattacharya, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain-based federated learning in uavs beyond 5g networks: A solution taxonomy and future directions," *IEEE Access*, 2022.

[77] M. Aloqaily, I. Al Ridhawi, and M. Guizani, "Energy-aware blockchain and federated learning-supported vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[78] Y. Xu, Z. Lu, K. Gai, Q. Duan, J. Lin, J. Wu, and K.-K. R. Choo, "Besifl: Blockchain empowered secure and incentive federated learning paradigm in iot," *IEEE Internet of Things Journal*, 2021.

[79] C. Ma, J. Li, M. Ding, L. Shi, T. Wang, Z. Han, and H. V. Poor, "When federated learning meets blockchain: A new distributed learning paradigm," *ArXiv*, vol. abs/2009.09338, 2020.

[80] M. Aloqaily, O. Bouachir, A. Boukerche, and I. Al Ridhawi, "Design guidelines for blockchain-assisted 5g-uav networks," *Ieee Network*, vol. 35, no. 1, pp. 64–71, 2021.

[81] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned uav networks: Challenges, solutions, and comparisons," *Computer Communications*, vol. 151, pp. 518–538, 2020.

[82] L. H. Yin, J. Y. Feng, S. X. Lin, Z. Q. Cao, and Z. Sun, "A blockchain-based collaborative training method for multi-party data sharing," *Computer Communications*, vol. 173, pp. 70–78, 2021.

[83] 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.

[84] K.-R. M. F. Sattler, S. Wiedemann and W. Samek, "Robust and communication-efficient federated learning from non-iid data," *IEEE Trans. Neural Netw. Learn. Syst*, vol. 31, no. 9, pp. 1–14,.

[85] S. R. Pokhrel, "Federated learning meets blockchain at 6g edge: A drone-assisted networking for disaster response," in *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, pp. 49–54.

[86] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6g networks," *IEEE Trans. Ind. Informat*, vol. 17, no. 7, pp. 5098–5107,.

[87] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," *IEEE Trans. Intell. Transp. Syst*, vol. 19, no. 8, pp. 2627–2637,.

[88] Y. C. Wan, Y. Y. Qu, L. X. Gao, and Y. Xiang, "p privacy-preserving blockchain-enabled federated learning for b5g-driven edge computing," *Computer Networks*, vol. 204, 2022.

[89] S. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans.Commun*, vol. 68, no. 8, pp. 4734–4746,.

[90] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[91] Y. Liu, J. L. Peng, J. W. 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.

[92] U. Majeed, L. U. Khan, A. Yousafzai, Z. Han, B. J. Park, and C. S. Hong, "St-bfl: A structured transparency empowered cross-silo federated learning on the blockchain framework," *Ieee Access*, vol. 9, pp. 155 634–155 650, 2021.

[93] X. Bao, C. Su, Y. Xiong, W. Huang, and Y. Hu, "Flchain: A blockchain for auditable federated learning with trust and incentive," in *2019 5th International Conference on Big Data Computing and Communications (BIGCOM*, pp. 151–159,.

[94] U. Majeed and C. S. Hong, "Flchain: Federated learning via mec-enabled blockchain network," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. IEEE, 2019, pp. 1–4.

[95] S. Rahmadika, M. Firdaus, S. Jang, and K. H. Rhee, "Blockchain-enabled 5g edge networks and beyond: An intelligent cross-silo federated

learning approach," *Security and Communication Networks*, vol. 2021, 2021.

[96] J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1,.

[97] X. Wu, Z. Wang, J. Zhao, Y. Zhang, and Y. Wu, "Fedbc: Blockchainbased decentralized federated learning," in *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA*, pp. 217–221,.

[98] Z. Y. Li, J. Liu, J. L. Hao, H. M. Wang, and M. Xian, "Crowdsfl: A secure crowd computing framework based on blockchain and federated learning," *Electronics*, vol. 9, no. 5, 2020.

[99] H. B. Desai, M. S. Ozdayi, and M. Kantarcioglu, "Blockfla: Accountable federated learning via hybrid blockchain architecture," in *Proceedings of the eleventh ACM conference on data and application security and privacy*, 2021, pp. 101–112.

[100] C. Korkmaz, H. Kocas, A. Uysal, A. Masry, O. Ozkasap, and B. Akgun, "Chain fl: Decentralized federated machine learning via blockchain," in *2020 Second International Conference on Blockchain Computing and Applications (BCCA*, pp. 140–146,.

[101] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain," *IEEE Access*, vol. 7, pp. 178 082–178 093, 2019.

[102] M. Shayan, C. Fung, C. Yoon, and I. Beschastnikh, "Biscotti: A blockchain system for private and secure federated learning," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 7, pp. 1513–1525,.

[103] Z. Peng, J. Xu, X. Chu, S. Gao, Y. Yao, R. Gu, and Y. Tang, "Vfchain: Enabling verifiable and auditable federated learning via blockchain systems," *IEEE Transactions on Network Science and Engineering*, pp. 1–1,.

[104] J. Li, Y. Shao, K. Wei, M. Ding, C. Ma, L. Shi, Z. Han, and V. Poor, "Blockchain assisted decentralized federated learning (blade-fl): Performance analysis and resource allocation," *IEEE Transactions on Parallel and Distributed Systems*, 2021.

[105] H. Liu, S. P. Zhang, P. F. Zhang, X. Q. Zhou, X. B. Shao, G. G. Pu, and Y. Zhang, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *Ieee Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073–6084, 2021.

[106] H. Chen, S. A. Asif, J. Park, C.-C. Shen, and M. Bennis, "Robust blockchained federated learning with model validation and proof-of-stake inspired consensus," *arXiv preprint arXiv:2101.03300*, 2021.

[107] K. Zhang, H. Huang, S. Guo, and X. Zhou, "Blockchain-based particpant selection for federated learning," in *International Conference on Blockchain and Trustworthy Systems*. Springer, 2020, pp. 112–125.

[108] Y. Qu, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet Things J*, vol. 7, no. 6, pp. 5171–5183,.

[109] U. Majeed and C. Hong, "Flchain: Federated learning via mecenabled blockchain network," in *Proc. 20th Asia–Pac. Netw. Oper. Manag. Symp. (APNOMS*, pp. 1–4.

[110] V. Mothukuri, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and K. K. R. Choo, "Fabricfl: Blockchain-in-the-loop federated learning for trusted decentralized systems," *Ieee Systems Journal*.

[111] X. Yin, Y. Zhu, and J. Hu, "A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions," *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–36, 2021.

[112] K. Toyoda, J. Zhao, A. N. S. Zhang, and P. T. Mathiopoulos, "Blockchain-enabled federated learning with mechanism design," *Ieee Access*, vol. 8, pp. 219 744–219 756, 2020.

[113] 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. 10 700–10 714, Dec. 2019.

[114] J. Weng, J. Weng, H. Huang, C. Cai, C. Wang, and IEEE, "FedServing: A Federated Prediction Serving Framework Based on Incentive Mechanism," 2021.

[115] Z. B. Zhang, D. J. Dong, Y. H. Ma, Y. L. Ying, D. W. Jiang, K. Chen, L. D. Shou, and G. Chen, "Refiner: A reliable incentive-driven federated learning system powered by blockchain," *Proceedings of the Vldb Endowment*, vol. 14, no. 12, pp. 2659–2662, 2021.

[116] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-Based Incentive," *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, vol. 18, no. 5, pp. 2438–2455, Sep. 2021.

[117] Y. Zhou, C. H. Pan, P. L. Yeoh, K. Z. Wang, M. Elkashlan, B. Vucetic, and Y. H. Li, "Secure communications for uav-enabled mobile edge computing systems," *Ieee Transactions on Communications*, vol. 68, no. 1, pp. 376–388, 2020.

[118] J. Li, Y. M. Shao, K. Wei, M. Ding, C. A. Ma, L. Shi, Z. Han, and H. V. Poor, "Blockchain assisted decentralized federated learning (blade-fl): Performance analysis and resource allocation," *Ieee Transactions on Parallel and Distributed Systems*, vol. 33, no. 10, pp. 2401–2415, 2022.

[119] R. Wang and W. T. Tsai, "Asynchronous federated learning system based on permissioned blockchains," *Sensors*, vol. 22, no. 4, 2022.

[120] Y. H. Liu, Y. Y. Qu, C. H. Xu, Z. C. Hao, and B. Gu, "Blockchain-enabled asynchronous federated learning in edge computing," *Sensors*, vol. 21, no. 10, 2021.

[121] R. Zeng, C. Zeng, X. Wang, B. Li, and X. Chu, "A comprehensive survey of incentive mechanism for federated learning," *arXiv preprint arXiv:2106.15406*, 2021.

[122] K. Toyoda and A. N. Mang, "Mechanism Design for An Incentive-aware Blockchain-enabled Federated Learning Platform," C. Baru, J. Huan, L. Khan, X. Hu, R. Ak, Y. Tian, R. Barga, C. Zaniolo, K. Lee, and Y. Ye, Eds., 2019, pp. 395–403.

[123] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019.

[124] B. Jia, X. S. Zhang, J. W. Liu, Y. Zhang, K. Huang, and Y. Q. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot," *Ieee Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4049–4058, 2022.

CHAOYANG ZHU received the MS degree in communication and information system from Guangxi University , Nanning, China, in 2008. He is currently pursuing the PhD degree in information and communication engineering with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. His current research interests include UAV wireless network, mobile Edging Computing, federated learning, blockchain, and privacy protect of IOT.

XIAO ZHU received the MS degree in communication and information system from Guilin University of Electronic Science and Technology, Guilin, China, in 2008. She is currently pursuing the PhD degree in information and communication engineering with the School of Electronic and Information Engineering, Harbin Institute of Technology, ShenZhen, China. Her current research interests include UAV wireless network, Moblie Edging Computing, federated learning, blockchain, and privcy protect of IOT.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3174865, IEEE Access

JUNYU REN received the MS degree in communication and information system from Guilin University of Electronic Science and Technology, Guilin, China, in 2005. She is currently pursuing the PhD degree in information and communication engineering with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. Her current research interests include wireless body area network, Internet of Things, fog computing, blockchain, and trust management.

TUANFA QIN received the PhD degree from Nanjing University, Nanjing, China,in 1997. Since 1991, he has been with the School of Computer, Electronic and Information, Guangxi University, Nanning, China, where he became an associate professor in 1997 and a professor in 2000. He is also the laboratory director of Guangxi Key Laboratory of Multimedia Communications and Network Technology. He has authored more than 200 academic papers and participated in writing 2 monographs. He has obtained 12 authorized Chinese invention patents in the field of communication, and 7 utility model patents, and more than 20 copyrights of computer software registration. He has sponsored over 5 projects of National Natural Science Foundation of China, over 2 National Innovation Fund Projects for small and medium-sized enterprises, and over more than 10 provincial and ministerial projects. His general research interests include wireless body area network and wireless multimedia communication.