Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey

Dun Li1 · Dezhi Han1 · Tien-Hsiung Weng4 · Zibin Zheng2 · Hongzhi Li3 · Han Liu1 · Arcangelo Castiglione3 · Kuan-Ching Li4

Accepted: 24 October 2021 / Published online: 20 November 2021
© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

Abstract
Federated learning (FL) is a promising decentralized deep learning technology, which allows users to update models cooperatively without sharing their data. FL is reshaping existing industry paradigms for mathematical modeling and analysis, enabling an increasing number of industries to build privacy-preserving, secure distributed machine learning models. However, the inherent characteristics of FL have led to problems such as privacy protection, communication cost, systems heterogeneity, and unreliability model upload in actual operation. Interestingly, the integration with Blockchain technology provides an opportunity to further improve the FL security and performance, besides increasing its scope of applications. Therefore, we denote this integration of Blockchain and FL as the Blockchain-based federated learning (BCFL) framework. This paper introduces an in-depth survey of BCFL and discusses the insights of such a new paradigm. In particular, we first briefly introduce the FL technology and discuss the challenges faced by such technology. Then, we summarize the Blockchain ecosystem. Next, we highlight the structural design and platform of BCFL. Furthermore, we present the attempts ins improving FL performance with Blockchain and several combined applications of incentive mechanisms in FL. Finally, we summarize the industrial application scenarios of BCFL.

Keywords Blockchain · Federated learning · Smart Contract · Incentive mechanism · Industrial Applications

1 Introduction

The quality and security of data are the keys to the development of machine learning and artificial intelligence (AI). However, rich data is often privacy sensitive and large scale, which will hinder traditional methods to log into a data center and train there. Besides, most of the data and resources needed for effective training of machine learning models are owned by a few large technology companies, which is detrimental to privacy protection and further leads to centralization problems. Thus, a novel, distributed learning approach that allows large-scale joint modeling without publishing raw data becomes imperative. In this context, Federated learning (FL) proposed by Google (Konečný et al. 2016; Aledhari et al. 2020; Konečný et al. 2016; McMahan et al. 2017) has recently received great attention at both the research and application levels.

Specifically, FL is an emerging machine learning technology consisting of many mobile devices and a central storage server. This technology allows distributed model training using local datasets from large-scale nodes, such as mobile
devices. FL updates the parameters without uploading the original training data and then builds a shared model by aggregating the locally computed updates (Xu et al. 2020). A typical example is the FedAVG algorithm, which is based on the iterative model averaging proposed in McMahan et al. (2017). This method is robust and allows to generate imbalanced and independent, and constant distribution non-IID data distributions. The basic design structure of FL is shown in Fig. 1. Based on this, FL offers promising privacy protection for mobile devices while ensuring high learning performance.

However, despite the many benefits mentioned above, FL still faces serious challenges. The gradient aggregation mechanism used for FL makes the entire algorithmic model dependent on the control of a central node. So we need to address two trust issues: one is to ensure that there is a central node that all participants trust, and the other is to ensure that information about the operations of the central node is transparent. First of all, FL relies on centralized databases and remains at risk of distributed denial of service DDoS attacks and privacy breaches. Again, currently, FL systems do not have suitable and transparent contribution evaluation mechanisms and incentive mechanisms to ensure continuous active training of training nodes. Finally, an effective distributed system needs to identify and prevent malicious nodes. However, the current FL system does not provide adequate mechanisms to implement these operations.

Interestingly, Blockchain technology provides an opportunity to address the above challenges of FL. More precisely, through the combination of chain structure, tree structure, and graph structure, the Blockchain ensures secure storage and data traceability (Liang et al. 2020). Besides, through the consensus mechanism of proof-of-work (POW), Blockchain realizes the untamperability of data. In more detail, due to the validation process of Blockchain local training results, the proposed BCFL framework can avoid the single point of failure (SPOF) and extend its federation scope to untrusted users in the public network. In addition, by providing rewards proportional to the size of the training samples, BCFL can realize effective incentives and thus facilitate the union of more devices with a large number of training samples. Therefore, the Blockchain can be seen as a perfect complement for FL, providing it with improved interoperability, privacy, security, reliability, and scalability (Liang et al. 2021).

Although many papers involve different aspects of the BCFL paradigm, there is no systematic investigation on this paradigm. In this article, we present a survey on a new paradigm for integrating Blockchain and FL. This survey denotes such a synthesis of Blockchain and FL as Blockchain-based federated learning (BCFL) framework. To present a complete picture of BCFL-related studies, we surveyed the related works focusing on structure design, performance enhancement attempts, incentive mechanism design, and industrial applications of BCFL, in a period ranging from 2016 to 2021. Given the previous work, we aim to (i) provide a conceptual introduction to FL and Blockchain technology, (ii) provide a systematic analysis of the potential of incorporating Blockchain into FL, and (iii) discuss the specific applications of BCFL in depth.

In detail, the main contributions of this paper are summarized as follows.

- We provide an overview of the definition, architectural design, and deployed platform for Blockchain and FL convergence.
- We provide a systematic survey on the studies dedicated to improving the performance of FL by integrating block FL systems.
- We survey the existing studies on effective incentive mechanisms for training nodes using Blockchain.
- We summarize the current feasible applications for BCFL in industrial applications.

The rest of this article is organized as follows. We first introduce the related work in Sect. 2. Section 3 then introduces the background and fundamentals of FL and Blockchain. Subsequently, Sect. 4 presents the convergence architecture and deployment platform of BCFL. Section 5 then summarizes the attempts to make appropriate improvements to the BCFL. Section 6 discusses the transparent contribution recognition and effective reward for clients in BCFL. Section 7 next summarizes the feasible application of BCFL. Finally, Sect. 8 concludes the paper.
Blockchain ecosystem in Section 3.2.

Particular, the works proposed in Konečný et al. (2016), McMahan et al. (2017), Kairouz et al. (2019), Yang et al. (2019), Bonawitz et al. (2019), Yu et al. (2021), Li et al. (2020), Gu et al. (2019), Li et al. (2019), Mothukuri et al. (2021), Liang et al. (XXXX), comprehensively introduced the relevant information of FL works proposed in Zheng et al. (2017), Kumar and Jaiswal (2020), Zhou et al. (2020), Saleh (2020), Li et al. (2020), Hewa et al. (2021), Liang et al. (2019), Xiao et al. (2020) summarized the main information concerning the structure and characteristics of Blockchain. In this work, we take Yang’s work (Yang et al. 2019) and Zheng’s work (Zheng et al. 2017) as baselines and organize the closely related research. As Fig. 2 shows, Yang’s work is associated with more highly cited articles, and Zheng’s work links more paper groups.

In conclusion, the technological development of FL has attracted much attention, and the related research has shown an explosive growth trend. However, as Table 1 shows, there is no existing survey related to the combination of Blockchain and FL in the literature. To fill this gap, we propose in this work the first survey that performs a thorough investigation of the relevant studies published in recent years on BCFL. Again, we systematically present the structural designs, deployed platforms, performance improvement, node incentive mechanisms, and the industrial applications of BCFL. Finally, based on the related works, Table 2 defines a list of acronyms and the definitions used in this survey.

3 Background

In this section, we provide all the background necessary to understand better and follow this paper. More precisely, we briefly introduce FL integration in Sect. 3.1 and present Blockchain ecosystem in Section 3.2.

3.1 Federated learning integration

FL refers to the calculation process that enables the data owner $F_i$ to perform model training and obtain the model $M_{FED}$ without giving their data $D_i$, while ensuring that the gap between the effect $V_{FED}$ of the model $M_{FED}$ and the effect $V_{SUM}$ of the model $M_{SUM}$ is small enough. This calculation can be expressed as follows.

$$\omega_i^t = \arg\min_{\omega_i^t} F(\omega_i^t)$$

$$F(\omega_i^t) = \frac{1}{|D_i|} \sum_{j \in D_i} f_j(\omega_i^t)$$

Where $|D_i|$ is an arbitrarily small positive value, $1 \leq i \leq n$, and $n$ is the number of participants to the system.

3.1.1 Taxonomy of FL

The basis of FL is the data matrix. As shown in Fig. 3, based on the different distribution patterns of sample space and feature space of data, FL can be divided into three categories: horizontal federated learning (HFL), vertical federated learning (VFL), and federated transfer learning (FTL) which divide the dataset horizontally (i.e., user dimension), longitudinally (i.e., feature dimensions), and non-dimensionally, respectively.

3.1.2 The workflow of FL

FL systems generally consist of data holders and central servers. The amount of local data or the number of features of each data holder may not be enough to support successful model training. Therefore, support from other data holders is required. Figure 4 illustrates the FL process for the client-server architecture.

In a typical cooperative modeling process of FL, the training of local data by the data holders occurs only locally to protect data privacy. Next, the gradients generated by the iterations are used as interaction information after desensitization and uploaded to a third-party trusted server instead of local data, waiting for the server to return the aggregated parameters to update the model. In detail, the steps of FL can be summarized as follows.

- **Step 1.** System Initialization. First, the central server sends the modeling task and seeks to participate in the client.
- **Step 2.** Local Calculation. After the joint modeling task is opened and the system parameters are initialized, each data holder will be required to perform local calculations according to the data locally first.

![Image: The loosely related researches of Yang’s work and Zheng’s work](Image)
| Category                                      | Ref. no | Author(s)          | Topic                                      | Published |
|-----------------------------------------------|---------|--------------------|--------------------------------------------|-----------|
| **Fundamental architecture, algorithm, and model** |         |                    |                                            |           |
| Konečný et al. (2016,?); McMahan et al. (2017) |         | Mcmahanet al.      | Concept and applications                    | 2017.6-9  |
| Kairouz et al. (2019)                         |         | Kairouz et al.     | Advances and open problems                  | 2019.1    |
| Yang et al. (2019)                            |         | Yang et al.        | Concept and applications                    | 2019.2    |
| Bonawitz et al. (2019)                        |         | Bonawitz et al.    | System design                               | 2019.3    |
| Li et al. (2020)                              |         | Tian Li et al.     | Challenges, methods, and future directions  | 2019.8    |
| Gu et al. (2019)                              |         | Gu et al.          | Distributed machine learning                | 2019.9    |
| Li et al. (2019)                              |         | Qinbin Li et al.   | Data privacy and protection                 | 2019.11   |
| Mothukuri et al. (2021)                       |         | Mothukuri et al.   | Security and privacy                        | 2020.10   |
| Shen et al. (2020)                            |         | Sheng Shen et al.  | Data privacy and security                   | 2020.10   |
| Lo et al. (2020)                              |         | SK Lo et al.       | A Software engineering perspective         | 2020.12   |
| Lyu et al. (2020)                             |         | Lyu et al.         | Threats                                    | 2020.3    |
| Bellavista et al. (2021)                      |         | Bellavista et al.  | Deployment environments                     | 2021.2    |
| Zhan et al. (2021)                            |         | Yufeng Zhan et al. | Incentive mechanism design                  | 2021.3    |
| Kulkarni et al. (2020)                        |         | Kulkarni et al.    | Personalization techniques                  | 2020.3    |
| Jin et al. (2020)                             |         | Yilan Jin et al.   | Utilizing unlabeled data                    | 2020.5    |
| Hu et al. (2020)                              |         | Sixu Hu et al.     | Benchmark suite                             | 2020.10   |
| **Performance improvement**                   |         |                    |                                            |           |
| **Embeding technology, and application**       |         |                    |                                            |           |
| Cui et al. (2018)                             |         | Cui et al.         | FL for Internet of things                   | 2018.6    |
| Lim et al. (2020)                             |         | Bryan Lim et al.   | FL in Mobile edge networks                  | 2020.2    |
| Du et al. (2020)                              |         | Du et al.          | FL for Vehicular internet of things         | 2020.4    |
| Saputra et al. (2020)                         |         | Saputra et al.     | FL for Electric vehicle networks            | 2020.4    |
| Aledhari et al. (2020)                        |         | Aledhari et al.    | Enabling technologies, protocols, and applications | 2020.8    |
| Tan et al. (2020)                             |         | Tan et al.         | FL in Vehicular networks                    | 2020.8    |
| Wahab et al. (2021)                           |         | Wahab et al.       | FL in Communication and networking systems  | 2021.2    |
3.1.3 Applications of FL

Currently, FL has been integrated with other emerging technologies by many scholars to enable industrial applications, such as the efficiency improvement of mobile and wireless communication (Konecný et al. 2016; Sattler et al. 2020; Reisizadeh et al. 2020; Li et al. 2020; Niknam et al. 2020), edge computing (Wang et al. 2019; Doku et al. 2021; Lu et al. 2020; Fantacci and Picano 2020; Wang et al. 2019; Li et al. 2020; Lim et al. 2020), health care (Rieke et al. 2020; Bogdanova et al. 2020; Zerka et al. 2020), Internet of Things (Savazzi et al. 2020; Yang et al. 2020; Yuan et al. 2020; Qolomany et al. 2020; Briggs et al. 2020; Lim et al. 2020; Gao et al. 2020; Kamel and Mougy 2020; Imteaj and Amini 2019), Internet of Vehicles (Samarakoon et al., 2020; Hsu et al., 2020; Du et al., 2020), anomaly detection (Nguyen et al. 2019; Weinger et al. 2020), smart city (Jiang et al. 2020), financial fraud identification (Fan et al. 2020), visual object detection (Liu et al. 2020) and fog computing (Zhou et al. 2020; Cai et al. 2020). It can be seen that FL is prominent in industrial applications for privacy-sensitive data and the processing of non-IID data. Practical industrial-scale applications are not yet sufficient, but theoretical preparations are relatively well established.

3.1.4 Open-source frameworks of FL

There are currently a few open-source frameworks for researchers and developers to build FL systems. A summary of such frameworks is listed in Tab 3.

Table 2 The summary of acronyms and definitions

| Acronym | Definition |
|---------|------------|
| FL | Federated learning |
| HFL | Horizontal federated learning |
| VFL | Vertical federated learning |
| FTL | Federated transfer learning |
| BCFL | The integration of Blockchain and federated learning |
| AI | Artificial intelligence |
| DDoS | Distributed denial of service |
| SPOF | Single point of failure |
| PoW | Proof of work |
| PoS | Proof of stake |
| DPoW | Delayed proof-of-work |
| DPoS | Delegated proof-of-stake |
| PBFT | Practical byzantine fault tolerance |
| dBFT | Delegated byzantine fault tolerance |
| PooL | Verify the pooling |
| IoV | Internet of vehicles |
| IoT | Internet of things |
| DTWN | Digital twin wireless network |
| 5G | 5th Generation mobile networks |
| 6G | 6th Generation mobile networks |

Fig. 4 The workflow of FL

3.2 Blockchain ecosystem

3.2.1 Overview of Blockchain

Blockchain is essentially a decentralized distributed database. All the interactive records (transactions) generated in the system are linked into chains as blocks and stored in each section in time. Furthermore, each transaction is guaranteed by cryp-
tography and PoW algorithms that cannot be tampered with or forged, so each node in the system can achieve secure peer-to-peer transactions. As Fig. 5 shows, a block consists of a block header containing metadata and some transaction records. These blocks are linked by the hash pointer of the block header to form a complete ledger, which is the narrow definition of Blockchain. More precisely, from the bottom to the top, the Blockchain is composed of the data layer, incentive mechanism, consensus layer, network layer, and application layer (Zheng et al. 2017; Fan et al. 2021; Zheng et al. 2018; Lu 2018; Liang et al. 2019).

Based on different application scenarios and designed systems, the Blockchain is generally divided into public chain, consortium chain, and private chain. Table 4 presents the comparison of three different types of Blockchain. Generally, different types of Blockchain are selected according to the requirements of different business scenarios (Liang et al. 2021). However, in a broad sense, only the public chain can meet the original design intention of the Blockchain.

### 3.2.2 Consensus mechanism

The most fundamental consensus mechanism of Blockchain is the proof-of-work (PoW). A node chooses to store the hash value of a specific block in the current block and then mines it. Once successfully linked, it means that the node accepts the transactions of this block and all previous blocks linked by this block. In addition to PoW, there are many other types of consensus mechanisms. Table 5 lists several typical consensus mechanisms and gives a comparative explanation.

### 3.2.3 Smart contract

The smart contract can digitally verify the negotiated or executed contracts and allow trusted transactions without a third party. Besides, these transactions are traceable, and irreversible (Huang et al. 2019). Thus, the success of Ethereum has contributed to the realization of smart contracts. As shown in Fig. 6, it includes transaction processing and preservation mechanism and a complete state machine for accepting and processing various smart contracts. Smart contracts bring great versatility and adaptability to the Blockchain. It is because of the smart contract functionality that various algorithms, including FL, can be deployed on the Blockchain.

### 4 Structure design of BCFL

This section outlines the main characteristics of the Blockchain-based federated learning (BCFL) framework. More precisely, in Sect. 4.1, we first introduce the BCFL architecture arising from the integration of Blockchain and FL. Then, we present the design of data storage and the deployed platform of BCFL in Sects. 4.2 and 4.3, respectively.

### 4.1 Architecture of BCFL

The first related research focused on the construction of BCFL has been proposed by Kim et al. (2018). The main concept underlying the BCFL is to solve the issues on private exchange and reward mechanisms by using Blockchain (Hieu et al. 2020). Subsequent related studies, such as Mugunthan et al. (2020), Kang et al. (2020), Ma et al. (2020), and Majeed and Hong (2019), have also built some contributions on this foundation, but only introducing some small-scale improve-
ments. Besides, to make an intuitive display, a demo of BCFL has been proposed by Zhang et al. (2020). However, these follow-up studies all adopted this basic design structure, as shown in Fig. 7.

Specifically, the Blockchain mainly serves as a central database for the FL system, which is fully decentralized and privacy-protected. Therefore, the main goal is to reward the clients according to the quality of their contributions while

![Fig. 6 Smart contract](image)

**Table 4** Taxonomy of Blockchain systems

| Blockchain     | Participants  | Characteristics       | TPS               |
|----------------|---------------|-----------------------|-------------------|
| Public         | Anyone        | Decentralized         | 3–20 data writes per second |
| Consortium     | Authorized nodes | Partially centralized | 1000 data writes per second |
| Private        | Authorized nodes | Centralized          | 1000 data writes per second |

**Table 5** The summary of Consensus in Blockchain

| Consensus | Merits                                                                 | Weakness                                                                 |
|-----------|------------------------------------------------------------------------|--------------------------------------------------------------------------|
| PoW       | Complete centralization, nodes free access                             | Waste of energy and difficult to reduce the confirmation time of blocks  |
|           | Simple algorithm                                                        | Prone to forking and need to wait for multiple forks to reach consistency |
|           | The cost of destruction is huge (destroyer exceed 50%)                 |                                                                         |
| PoS       | Low performance requirements for nodes                                 | No final consistency, need checkpoint mechanism to compensate and finality|
|           | Short consensus time                                                    |                                                                         |
| DPoW      | Significantly reduce the number of nodes involved in validation        | Sacrifices the concept of decentralization, not suitable for public chains |
| DPoS      | Energy conservation                                                    | Slightly more centralized, e.g., participants with high equity can vote to make themselves a validator. |
| Rapidity  | High consensus efficiency for high frequency trading                   |                                                                         |
| PBFT      | High consensus efficiency for high frequency trading                   | The existence of cryptocurrency and the incentive mechanism will create a Matthew effect making the poor poorer and the rich richer in the community |
|           | The system will stop when only 33% of the nodes are left running       |                                                                         |
| dBFT      | Highly fault-tolerant with bookkeeping done by multiple nodes          | The system will not be able to provide services when more than one-third of the bookkeepers stop working |
|           | Every block has finality                                                |                                                                         |
|           | The algorithm has a strict mathematical proof that it will not bifurcate|                                                                         |
| PooS      | No cryptocurrency required                                              | Less decentralized                                                       |
|           | Second-level consensus verification                                     |                                                                         |
protecting the privacy of the underlying dataset and fending off malicious adversaries.

### 4.2 Data storage

As with any distributed system, FL bears the privacy leakage challenge. For BCFL, the Blockchain plays a pivotal role in solving this problem (Liang et al. 2020). Indeed, the decentralized functioning of Blockchain enables to make FL fault-tolerant (Shayan et al. 2021), and can help to avoid attacks effectively. More precisely, to better solve the security problem of data storage, many studies try to make further improvements based on ordinary Blockchain. For example, a new ring decentralization algorithm (Hu et al. 2020), and an innovative committee consensus mechanism (Li et al. 2021) was shown to be feasible solutions for improving decentralized FL performance and reducing consensus computation, respectively. In summary, the Blockchain data storage model can protect the privacy of a single client update and maintain the large-scale performance of the global model.

### 4.3 Deployed platform

In BCFL, the functions of the Blockchain layer need to be implemented with the support of a platform. Different Blockchain platforms have different characteristics. For example, public chains provide stable performance, consortium chains provide robust security, and private chains provide more customization features. From a careful analysis of the literature, the current BCFL mainly adopts four platforms: Ethereum, Hyperledger Fabric, EOS, and Custom Blockchain. The features comparison of these platforms is shown in Table 6.

#### 4.3.1 Ethereum

As the earliest programmable Blockchain, Ethereum is Turing-Complete (Buterin XXXX). The work proposed by Nagar (2019) deploys the BCFL platform using an unlicensed side chain, using a technique proposed by layer 2 extension. Moreover, based on smart contracts in Ethereum, Mugunthan et al. (2020) proposes the BlockFlow architecture, which initially realizes accountable and privacy-preserving FL through a novel contribution scoring procedure. Similarly, Baffile (Ramanan et al. 2020) and ChainFL (Korkmaz et al. 2020) are both Ethereum-based FL systems, which use smart contracts to coordinate round partitioning, model aggregation, and update tasks in FL.

#### 4.3.2 Hyperledger Fabric

As an open-source project, Fabric is initiated by the Linux Foundation and maintained by several corporate organizations. Zhang et al. (2020) demonstrate FL training neural network model on FL client’s physical distribution dataset. The underlying communication between the server and the client uses the new Blockchain-based protocol on the secure data exchange system.

#### 4.3.3 EOS

The Enterprise Operating System (EOS) is a Blockchain-based operating system designed for commercial distributed applications (Grigg XXXX). For example, an EOS-based FL framework is proposed in Martinez et al. (2019), in which the model owner $O$ has the total liability of payment for the device and producer work, as opposed to devices $D$ needing to pay for their transactions.

#### 4.3.4 Custom Blockchain

Although there are many well-established public chains or consortium chains on the market, many researchers still choose to load FL systems with Custom Blockchains. The main reason is that the Custom Blockchain allows better flexibility, programmability, and extensibility. In particular, the work of Kim et al. (2020) proposes BlockFL, an architecture based on a Custom Blockchain in which local learning model updates are exchanged and validated. Similarly, Lu et al. (2020) propose a system consisting of a dual-module containing a permission Blockchain module and a FL module.

### 5 Model improvement in BCFL

FL is essentially a kind of machine learning. Therefore, its learning performance, efficiency, and security are important aspects to take into account. For this reason, several studies have been proposed to make appropriate improvements to the BCFL and enhance the above model performance. Table
Table 6  The summary of Deployed Platform for BCFL

| Platform          | Blockchain type | Consensus | Identity     | Recent studies                      | Refs.                         |
|-------------------|-----------------|-----------|--------------|------------------------------------|-------------------------------|
| Ethereum          | Public          | PoW, PoS | Anonymity    | BlockFLow, BAFFLE, Chain FL        | Nagar (2019), Mugunthan et al. (2020), Ramanan et al. (2020), Korkmaz et al. (2020) |
| Hyperledger Fabric| Consortium      | SOLO, Kafka | Known identity | DEMO                               | Zhang et al. (2020)            |
| EOS               | Consortium      | DPoS, BFT | Known identity | BlockFL                           | Martinez et al. (2019)         |
| Custom Blockchain | Private         | PBFT      | Known identity | BlockFL*, Secure-DataSharing      | Kim et al. (2020), Lu et al. (2020) |

The table summarizes the current effective attempts to improve the BCFL.

5.1 Performance improvement

FL is a distributed machine learning method that supports local storage of data. In this method, the client implements training through interactive gradient values. Therefore, the underlying idea for improving the accuracy of the model is similar to classical machine learning.

5.1.1 Fault tolerant enhancement

ChainFL proposed in Korkmaz et al. (2020) achieves encouraging results on the Modified National Institute of Standards and Technology database digit recognition task (MNIST) and Canadian Institute for Advanced Research image classification task (CIFAR-10). Such results demonstrate that the BCFL model can enhance the system fault tolerance without losing the corresponding model performance compared to the traditional FL model.

5.1.2 Solving non-IID issues

The ID labels of data samples have a significant impact on the accuracy of machine learning models. To address the problem that user-generated data samples across devices are likely to become non-IID, Jeong et al. (2018) proposed federated augmentation (FAug), a data augmentation scheme that collectively trains generative models on each device to enhance the local data to generate IID datasets.

5.2 Efficiency tracking and improvement

For industrial areas such as languages and games, large-scale computations still have high demands on overall algorithm performance (Ogiela and Ogiela 2009). Thus, the tracking and measurement of the algorithm’s efficiency are therefore crucial.

5.2.1 Replace oracle service with chaincode

The efficiency of the database will have an appreciable impact on the efficiency of FL. Again, the smart contract function in the Blockchain can replace the oracle service to achieve the data access function. The work of Drungilas et al. (2021) uses chaincode in Hyperledger structures instead of oracle services in the database and compares the runtime of functions executed using either chaincode or oracle services, demonstrating that negligible differences between implementations justify the flexible choice of model.

5.2.2 Setting weight parameter

Blockchain allows the performance of algorithms to be securely stored and recorded, and in particular, the long-term trend of FL can be tracked, depicting the overall situation and future dynamics of algorithm efficiency during operation. Therefore, weights based on each client’s local learning accuracy and weights based on each client’s frequency of participation can be used to achieve higher stability and faster convergence times to target accuracy. For instance, Kim and Hong (2019) propose a local learning weighting method for node recognition. This method selects nodes according to the participation frequency and data and weights to achieve fast convergence and stable learning accuracy.
5.3 Security improvement

Existing schemes have proven that the Blockchain-based decentralized control mechanism of Blockchain can effectively prevent risks such as SPOF (Liu et al., 2020; Kim and Kim, 2020; Firdaus and Rhee, 2021; Dwivedi et al., 2021; Ruggeri et al., 2020), DDoS attacks (Li et al., 2019; Saad et al., 2019; Rodrigues et al., 2017; Houda et al., 2019; Elisa et al., 2020), and poisoning attacks (Liang et al., 2019; Barański and Konorski, 2020; Rathore et al., 2019). However, the considerable computing power and storage cost of standard solutions are still critical challenges.

5.3.1 Re-encryption algorithms

Another possibility to achieve low-cost security improvements is to use re-encryption algorithms (Han et al. 2020). For example, the work by Li et al. (2020) proposes a crowdsourcing framework called CrowdSFL, in which a re-encryption algorithm based on the ElGamal cryptosystem is designed to ensure that interaction values and other information are not exposed to other participants outside the workflow. In this way, users can realize crowdsourcing with less overhead and higher security.

5.3.2 Improved consensus

As mentioned in Sect. 4.2, the consensus mechanism in the Blockchain can better ensure the security and privacy of FL’s data storage. Therefore, the appropriate improvement of the consensus mechanism can make FL more suitable for different scenarios and data. A reliable worker selection scheme for FL tasks proposed in Kang et al. (2020) introduces the concept of reputation as a metric to identify trusted and reliable workers in joint to prevent unreliable updates.

6 Incentive mechanism in BCFL

FL participants pay for computational resources. However, the training and commercialization of models are not instantaneous, and therefore, there is some delay before the federation reimburses participants. In this section, we outline the incentive mechanism underlying the BCFL. More precisely, in Sect. 6.1, we summarize the current attempts to apply Blockchain technology in handling lazy clients, while in Sects. 6.2 and 6.3 we assess the client contribution and compelling motivation, respectively.

6.1 Handling lazy clients

Basic FL does not take into account the identification of lazy clients and lacks incentives for influential learning clients.
Some studies have already begun to try the node incentive of FL, such as Ng et al. (2020), Khan et al. (2020). However, since there is no actual token mechanism design, these studies mainly focus on documentation, detection, and simulation. In contrast, Block-FL’s incentive mechanism deals with lazy nodes more practically. Typically, the works of Li et al. (2020) and Li et al. (2021) propose and evaluate the learning performance of Blade-FL with bounds that are convex concerning the total number of rounds $K$ and optimize the computational resource allocation to minimize the upper bound.

### 6.2 Assessing client contribution

To sustain the long-term engagement of the high-quality data owners (especially enterprises), the FL system needs to provide appropriate incentives based on the accurate evaluation of computational contributions. The systems in FL can be synchronous or asynchronous, depending on whether they use communication or not. In practice, the system functionality of FL can be well realized only if the computational work of the participating nodes is reasonably and well evaluated. The current, reliable methods mainly include a joint learning framework based on Blockchain protocol (Ma et al. 2021) and a new measurement standard based on verification error (Martinez et al. 2019). Similarly, some of these methods introduce the concept of competition to prevent workers from deviating from the protocol (Ogiela et al. 2016), rewarding only those who contribute (Toyoda et al. 2020).

### 6.3 Effective motivation

Based on the contribution score assessment, part of the BCFL model attempts to incentive highly reputable mobile devices with high-quality data to participate in FL (Kang et al. 2019). The peer-to-peer payment system is a natural profit allocation mechanism in the Blockchain. Taking inspiration from that mechanism, the work of Liu et al. (2020) proposes a support vector machine-based profit allocation framework based on the proof of Shapley protocol. On the other hand, the framework proposed in Cai et al. (2020) is based on evaluating the fractions of the dataset for the corresponding share rewards and a framework of reasonable contribution scores generated by both protocols.

### 7 Industrial applications of BCFL

Due to the strong adaptability exhibited by BCFL, there is an increasing trend of its wide application. This section mainly studies the industrial applications of BCFL. As shown in Table 8, we divide these applications into nine areas and summarize the benefits and improvements brought by the corresponding research.

#### 7.1 Data processing in health care

The health care industry is in a prominent position in using data to create value and improve human health. However, it has been proved that the traditional methods used to alleviate the privacy problems of health data are insufficient to protect personal interests. For this reason, it is easy to guess that medical data is highly privacy sensitive. BCFl can be an effective solution to mitigate the problems mentioned above since it can perfectly meet the data processing requirements in the field of medical and health care. In particular, BCFl not only completes the modeling requirements of physical therapy data but also avoids privacy leaks on relevant data. For instance, a new agent model based on BCFL is proposed in Dp et al. (2021), as a real-time medical data processing system. Again, to strengthen the privacy of health care data, the model proposed in Passerat-Palmbach et al. (2019) adopts the integration of unique privacy protection technology based on a protocol composed of protected hardware components and the native Ethereum cryptographic toolkit. Finally, the work of Passerat-Palmbach et al. (2020) also uses a similar model, and on this basis, it strengthens the incentive mechanism of data operation.

#### 7.2 Anomaly detection in network security

Open networks and service sharing scenarios are complex and varied, leading to serious security challenges (Li et al. 2021). In the FL setting, adversaries have more opportunities to poison a local machine learning model with malicious training samples, thus affecting the results of FL and evading detection. However, the work of Preuveneers et al. (2018) shows that audit machine learning models using an anomaly detection algorithm that detects incremental updates recorded on a Blockchain ledger can effectively prevent attacks. For the same purpose, the framework proposed by Desai et al. (2020) uses smart contracts to detect and punish attackers through fines automatically.

#### 7.3 Device failure and anomaly detection in IoT

Device fault detection is one of the most critical issues in the industrial Internet of Things (IIoT). However, in traditional IoT device fault detection, client devices need to upload raw data to a central server for model training, which carries the risk of leakage of sensitive business data (Zhao et al. 2021). Given the sensitivity, massive volume, fragmentation, and security of multi-party data computation in IoT environment, the works of Yin et al. (2020), and Rahman et al. (2020) both propose a BCFL-based learning approach for device
| Application domains                              | Applicable data                                      | Benefits                                                      | Related studies                                                                 |
|-------------------------------------------------|------------------------------------------------------|---------------------------------------------------------------|--------------------------------------------------------------------------------|
| Data processing in Health care                  | Covid-19 data                                        | Data security, auditability, and incentives                   | Dp et al. (2021); Passerat-Palmbach et al. (2019, 2020); Kumar et al. (2020); Kuo and Ohno-Machado (2018); Aich et al. (2021) |
|                                                 | Transaction Metadata                                 | Addressing data heterogeneity                                 |                                                                                    |
|                                                 | Medical data                                         | Model robustness                                             |                                                                                    |
| Anomaly detection in network security           | Automatic encoder for anomaly detection              | Data Auditability                                            | Preuveneers et al. (2018); Desai et al. (2020)                                    |
| Device failure and anomaly detection in IoT     | The movement data                                    | High testing accuracy                                        | Zhao et al. (2021); Yin et al. (2020); Rahman et al. (2020); Zhang et al. (2021) |
|                                                 |                                                      | High communication efficiency                                |                                                                                    |
|                                                 |                                                      | Complete privacy and anonymity                               |                                                                                    |
| Internet of vehicles For Trustworthy Vehicular Networks | Train running data Vehicle localization application data | High quality parameter collection                            | Otoum et al. (2020); Pokhrel (2020); Chai et al. (2020); Pokhrel and Choi (2020); Hua et al. (2020) |
|                                                 |                                                      | High test accuracy                                           |                                                                                    |
|                                                 |                                                      | High communication efficiency                                |                                                                                    |
|                                                 |                                                      | Anti-attack                                                  |                                                                                    |
| 5G & 6G secure communication                    | LP solver with GMI Communication network data        | System reliability and security                              | Liu et al. (2020); Hu et al. (2020); Lu et al. (2021); Rahmadika et al. (2021) |
|                                                 |                                                      | Improved data privacy                                        |                                                                                    |
|                                                 |                                                      | Incentives and fairness                                      |                                                                                    |
| Intelligent Edge Computing                      | MovieLens datasets CASIA-WebFace                     | High communication efficiency                                | Rehman et al. (2020); Cui et al. (2020); Shen et al. (2021)                      |
|                                                 |                                                      | Bandwidth optimization                                       |                                                                                    |
|                                                 |                                                      | Privacy protection                                           |                                                                                    |
| Fog Computing                                   | Fog servers data                                     | Decentralized Privacy                                        | Qu et al. (2020)                                                                 |
|                                                 |                                                      | Poisoning Attack Proof                                       |                                                                                    |
|                                                 |                                                      | High Efficiency                                              |                                                                                    |
| Cognenve Computing                              | CIFAR-10 dataset                                    | Advanced validation                                          | Qu et al. (2021)                                                                 |
|                                                 |                                                      | Fast convergence                                              |                                                                                    |
| Defence framework for sustainable society       | “Airplane,” “Bird,” “Drone,” and “Ship” from the different sources | Advanced validation                                          | Sharma et al. (2020)                                                            |
|                                                 |                                                      | Privacy protection                                           |                                                                                    |
fault detection in IoT. In particular, to solve the data heterogeneity problem in IoT fault detection, Zhang et al. (2021) proposed a novel centroid distance weighted federated averaging (CDW_FedAvg) algorithm. In detail, this algorithm effectively enhances the applicability and model accuracy by taking the distance between positive and negative classes of each client dataset as the basis for calculation.

7.4 Internet of vehicles for trustworthy vehicular networks

On the Internet of Vehicles (IoV), sharing data between vehicles for collaborative analysis can improve the driving experience and service quality (Xu et al. 2021). However, efficiency, security, and privacy issues have become obstacles for data providers to participate in the data sharing process (Meng et al. 2021; Pokhrel and Choi 2020; Zou et al. 2021). Fortunately, the BCFL framework is a suitable solution to the contradiction between large-scale data sharing and privacy protection. More precisely, the fundamental applications of BCFL deal with using the validation and consensus mechanisms within the Blockchain to secure IoV data and jointly ensuring trustworthy shared training for mutual machine learning models on decentralized end devices (Otoum et al. 2020). In detail, such operations are carried out by adapting instant block validation at the Blockchain level (Pokhrel 2020) and assessing the trustworthiness of vehicle observations during data collection (Chai et al. 2020). On this basis, the work of Pokhrel and Choi (Pokhrel and Choi 2020) uses the consensus mechanism of Blockchain to manage data without any centralized training or coordination. Meanwhile, the characteristics of controllable networks and BCFL parameters (such as retransmission limit, block size, block arrival rate, and frame size) can better capture their impact on system-level performance. Finally, some researchers have deployed SVM (Hua et al. 2020), and DRL algorithms to improve the efficiency.

7.5 5G and 6G for secure communication

In recent years, a large number of new applications requiring different network services have emerged. To secure FL in 5G communication, the main current solutions are Blockchain authorization (Liu et al. 2020) and decentralized federated slicing architecture (Hu et al. 2020). Furthermore, the work of Lu et al. (2021) proposed a digital twin wireless network (DTWN) scheme which moved real-time data processing and computing to the edge plane by merging digital twins into wireless networks.

7.6 Intelligent edge computing

Edge computing architecture can quickly process the data collected by the Internet of Things (IoT) Zou et al. (2021). Based on the concept of Blockchain reputation perception for fine-grained FL, the model proposed in Rehman et al. (2020) can ensure credible collaborative training in mobile edge computing systems. Again, the work of Cui et al. (2020) proposes to apply a compression algorithm of FL, assisted by the Blockchain, to predict the content caching of files. On the other hand, as shown in Shen et al. (2021), a new attribute inference attack is proposed. This attack exploits the unexpected attribute leakage of FL aided by Blockchain in intelligent edge computing.

7.7 Fog computing

As an extension of cloud computing and the foundation of IoT, fog computing is experiencing rapid growth. Indeed, fog computing has the potential to alleviate some thorny issues, such as network congestion, latency, and local autonomy. However, privacy concerns and consequent inefficiencies are slowing down the performance of fog computing (Huang et al. 2019). FL-Block proposed in Qu et al. (2020) modifies the structure of the fog server by storing global updates on the Blockchain to secure the global updates, allowing the end devices to maintain the global model and coordinates based on distributed consensus.

7.8 Cognitive computing

Cognitive computing is used to teach a computer to think like a human brain, not just to develop an artificial system. In particular, with the success of AlphaGo and other AI algorithms, cognitive computing has also ushered in a vast development. In this context, the work of Qu et al. (2021) introduces a BCFL-based customized reward system to promote public equipment to participate in high-performance industries by deploying Blockchain as the underlying architecture.

7.9 Sustainable society

Defense organizations and armed forces are crucial elements for the protection and survival of a nation. However, ensuring these elements requires robust networks and computing power to coordinate intelligence and information processing efficiently. Moreover, given the highly classified nature of national data, Sharma et al. (2020) propose a distributed computational defense framework for a sustainable society using Blockchain technology and FL features. In particular, the proposed framework enables us to infer battlefield states while protecting the privacy of sensitive data.
8 Conclusions and future research directions

This paper presents a survey on the applicability and integration of Blockchain with federated learning FL. More precisely, we denote this integration as the Blockchain-based federated learning (BCFL) framework and provide a comprehensive survey of issues related to BCFL implementation. In this paper, we first provide a basic description of the definitions and ecosystems characterizing Blockchain and FL. Then, we present the structure design of BCFL as a whole and summarize the feasible deployment platforms. Next, we discuss the model improvement of FL through the introduction of Blockchain. After that, we survey the research related to Blockchain incentives as an element to improve FL systems. Finally, we summarize the full range of possible applications of BCFL in the industry.

In conclusion, the combination of Blockchain and FL is an auspicious research direction, as it can better ensure data security and privacy in the case of abundant data. In addition, this combination makes it possible for more application scenarios to adopt this distributed learning model that does not need to share raw data for joint modeling.

This survey aims to provide a clear view on this topic to ensure that more and more researchers would start working on it. Future research directions could deepen and develop the following aspects:

1. This paper does not use a cross-referencing and quantitative measure to quantify the overall trends in relevant research. Therefore, future research could consider introducing these elements as a supplement.
2. Future studies may consider summarizing and classifying the related works from a broader range of perspectives to uncover additional research information relevant to BCFL.
3. BCFL may be applied to increasingly more industrial fields. Consequently, some research efforts may consider more application effects in different industrial fields and make more comparative studies.

Funding This research is supported by the National Natural Science Foundation of China under Grants 61873160 and 61672338 and the Natural Science Foundation of Shanghai under Grant 21ZR1426500.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Aich S, Sinai NK, Kumar S, Ali M, Choi R, Joo MI, Kim H (2021) Protecting personal healthcare record using blockchain and federated learning technologies. In: 2021 23rd International conference on advanced communication technology (ICACT), pp. 109–112
Azedhari M, Razzak R, Parizi RM, Saeed F (2020) Federated learning: a survey on enabling technologies, protocols, and applications. IEEE Access 8:699–725
Barański S, Konorski J (2020) Mitigation of fake data content poisoning attacks in ndn via blockchain. In: 2020 30th International telecommunication networks and applications conference (ITNAC), pp. 1–6
Bellavista P, Foschini L, Mora A (2021) Decentralised learning in federated deployment environments: a system-level view. ACM Comput Surveys (CSUR) 54(1):1–38
Bogdanova A, Attoh-Okine N, Sakurai T (2020) Risk and advantages of federated learning for health care data collaboration. ASCE-ASME J Risk Uncertain Eng Syst, Part A: Civil Eng 6:04020031
Bonawitz K, Eichner H, Grieskamp W, Huba D, Ingerman A, Ivanov V, Kiddon C, Konečný J, Mazzocchi S, McMahan HB et al. (2019) Towards federated learning at scale: system design. arXiv preprint arXiv:1902.01046
Briggs C, Fan Z, Andráš P (2020) A review of privacy preserving federated learning for private iot analytics. ArXiv, https://arxiv.org/abs/2004.11794
Buterin V “Ethereum/wiki, github. [online]. available:,” https://github.com/ethereum/wiki
Cai L, Lin D, Zhang J, Yu S (2020) Dynamic sample selection for federated learning with heterogeneous data in fog computing. In: ICC 2020–2020 IEEE International conference on communications (ICC), pp. 1–6
Cai H, Rueckert D, Passerat-Palmbach J (2020) 2CP: decentralized protocols to transparently evaluate contributivity in blockchain federated learning environments. ArXiv, https://arxiv.org/abs/2011.07516
Chai H, Leng S, Chen Y, Zhang K (2020) A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Trans Intell Transport Syst. https://doi.org/10.1109/TITS.2020.3002712
Cui L-Z, Su, Ming Z, Chen Z, Yang S, Zhou Y, Xiao W (2020) Create: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing. In: IEEE Internet Things J, pp. 1–1
Cui L, Yang S, Chen F, Ming Z, Lu N, Qin J (2018) A survey on application of machine learning for internet of things. Int J Mach Learn Cybern 9(8):1399–1417
Desai H, Ozdayi MS, Kantarcioglu M (2020) BlockFLA: Accountable federated learning via hybrid blockchain architecture. In: Proceedings of the eleventh ACM conference on data and application security and privacy
Doku R, Rawat D (2021) Mitigating data poisoning attacks on a federated learning-edge computing network. In: 2021 IEEE 18th Annual consumer communications and networking conference (CCNC), pp. 1–6, 2021
Dp A, Gsb C, Ky D (2021) Agent architecture of an intelligent medical system based on federated learning and blockchain technology. J Inf Secur Appl 58(11):102748
Drungilas V, Vaiciukynas E, Jurgeaitis M, Butkien R, Cepioniene L (2021) Towards blockchain-based federated machine learning: smart contract for model inference. Appl Sci 11(3):1010
Du Z, Wu C, Yoshinaga T, Yau K-LA, Ji Y, Li J (2020) Federated learning for vehicular internet of things: recent advances and open issues. IEEE Open J Comput Soc 1:45–61
Blockchain for federated learning toward... 4439

Ma C, Li J, Ding M, Shi L, Wang T, Han Z, Poor H (2020) When federated learning meets blockchain: a new distributed learning paradigm. ArXiv, https://arxiv.org/abs/2009.09338

Martinez I, Francis S, Hafid A (2019) Record and reward federated learning contributions with blockchain. In: 2019 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC), pp. 50–57

McMahan B, Moore E, Ramage D, Hampson S, Arcas BAy (2017) Communication-efficient learning of deep networks from decentralized data. In: Artif Intell Stat PMLR, pp. 1273–1282

Meng X, Xu J, Liang W et al (2021) A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for internet of vehicles. Comput Electr Eng 95:107431

Mohukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G (2021) A survey on security and privacy of federated learning. Future Gener Comput Syst 115:619–640

Mugunthan V, Rahaman R, Kagal L (2020) BlockFlow: an accountable and privacy-preserving solution for federated learning. ArXiv, https://arxiv.org/abs/2007.03856

Nagar A (2019) Privacy-preserving blockchain based federated learning with differential data sharing. ArXiv, https://arxiv.org/abs/1912.04859

Ng KL, Chen Z, Liu Z, Yu H, Liu Y, Yang Q (2020) A multi-player game for studying federated learning incentive schemes. In: IICAI

Nguyen TD, Marchal S, Mettinen, Fereidooni H, Asokan N, Sadeghi AR (2019) Diot: A federated self-learning anomaly detection system for IoT. In: 2019 IEEE 39th International conference on distributed computing systems (ICDCS), pp. 756–767

Niknam S, Dhillon HS, Reed JH (2020) Federated learning for wireless communications: motivation, opportunities, and challenges. IEEE Commun Magaz 58:46–51

Ogiela L, Ogiela U (2009) Secure information splitting using grammar schemes. New challenges in computational collective intelligence. Springer, Berlin, Heidelberg, pp. 327–336

Ogiela L, Ogiela M, Ogiela U (2016) Efficiency of strategic data sharing and management protocols. In: 2016 10th International conference on innovative mobile and internet services in ubiquitous computing (IMIS), pp. 198–201

Otoum S, Ridhawi IA, Moutfah H (2020) Blockchain-supported federated learning for trustworthy vehicular networks. In: GLOBECOM 2020–2020 IEEE Global communications conference, pp. 1–6

Passerat-Palmbach J, Farnan T, McCoy M, Harris J, Manion ST, Flannery H, Gleim N (2020) Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In: IEEE international conference on blockchain (Blockchain). Passerat-Palmbach J, Farnan T, Miller R, Gross M, Flannery H, Gleim B (2019) blockchain-orchestrated federated learning architecture for healthcare consortia. ArXiv, https://arxiv.org/abs/1910.12603

Pokhrel S (2020) WITHDRAWN: towards efficient and reliable federated learning using blockchain for autonomous vehicles. Comput Netw. https://doi.org/10.1016/j.comnet.2020.107431

Pokhrel S, Choi J (2020) Federated learning with blockchain for autonomous vehicles: analysis and design challenges. IEEE Trans Commun 68:4734–4746

Pokhrel S, Choi J (2020) Improving TCP performance over WiFi for internet of vehicles: a federated learning approach. IEEE Trans Vehic Technol 69:6798–6802

Preuveneers D, Rimmer V, Tsingenopoulos I, Spooren J, Joosen W, Ilie-Zador E (2018) Chained anomaly detection models for federated learning: an intrusion detection case study. Appl Sci 8:2663

Qolomyan B, Ahmad K, Al-Fuqaha A, Qadir J (2020) Particle swarm optimized federated learning for industrial IoT and smart city services. In: GLOBECOM 2020–2020 IEEE global communications conference, pp. 1–6

Qu Y, Gao L, Luan TH, Xiang Y, Yu S, Li B, Zheng G (2020) Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J 7:5171–5183

Qu Y, Pokhrel S, Garg S, Gao L, Xiang Y (2021) A blockchained federated learning framework for cognitive computing in industry 4.0 networks. IEEE Trans Ind Inf 17:2964–2973

Rahmada S, Firdaus M, Jang S, Rhee K (2021) Blockchain-enabled 5g edge networks and beyond: an intelligent cross-silo federated learning approach. Secur Commun Netw 2021:1–14

Rahman M, Hossain MS, Islam MS, Alrajeh N, Muhammad G (2020) Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access 8:71–87

Ramanan PN, Nayakama K, Sharma R (2020) Baffle: blockchain based aggregator free federated learning. In: 2020 IEEE International Conference on Blockchain (Blockchain), pp. 72–81

Rathore S, Pan Y, Park JH (2019) Blockdeepnet: a blockchain-based secure deep learning for IoT network. Sustainability 11:3974

Rehman MHU, Salah K, Damiani E, Svetinovic D (2020) Towards blockchain-based reputation-aware federated learning. In: IEEE INFOCOM 2020–IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 183–188

Reisizadeh A, Mokhtari A, Hassani H, Jadbabaie A, Pedarsani R (2020) FedPAQ: A communication-efficient federated learning method with periodic averaging and quantization. ArXiv, https://arxiv.org/abs/1909.13014

Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, Bakas S, Galtier M, Lindman B, Maier-Hein KH, Oruslin S, Sheller MJ, Summers RM, Trask A, Xu D, Baust M, Cardoso MJ (2020) The future of digital health with federated learning. NPJ Digit Med 3:1–7

Rodrigues BB, Bocek TM, Lareida A, Hausheer D, Rafati S, Stiller B (2017) A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. FIP International conference on autonomous infrastructure, management and security. Springer, Cham, pp. 16–29

Ruggeri A, Celesti A, Fazio M, Galletta A, Villari M (2020) BCB-X3DH: a blockchain based improved version of the extended triple diffie-hellman protocol. In: 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 73–78

Ryf tel T, Trask A, Dahl M, Wagner B, Mancuso J, Rueckert D, Passerat-Palmbach J (2018) A generic framework for privacy preserving deep learning. ArXiv, https://arxiv.org/abs/1811.04017

Saad M, Spaulding J, Njilla LL, Kamhoua CA, Shetty S, Nyang D, Mohaisen A (2019) Exploring the attack surface of blockchain: a systematic overview. ArXiv, https://arxiv.org/abs/1904.03487

Sahle F (2020) Blockchain without waste: proof-of-stake. Inf Syst Ecol

Samarakoon S, Bennis M, Saad W, Debhab M (2020) Distributed federated learning for ultra-reliable low-latency vehicular communications. IEEE Trans Commun 68:1146–1159

Saputra YM, Nguyen DN, Hoang DT, Vu TX, Dutkiewicz E, Chatzinotas S (2020) Federated learning meets contract theory: energy-efficient framework for electric vehicle networks. arXiv preprint arXiv:2004.01828

Sattler F, Wiedemann S, Müller K, Samek W (2020) Robust and communication-efficient federated learning from non-iid data. IEEE Trans Neural Netw Learn Syst 31:3400–3413

Savazzi S, Nicolli M, Rampa V (2020) Federated learning with cooperating devices: a consensus approach for massive IoT networks. IEEE Internet Things J 7:4641–4654

Sharma P, Park JH, Cho K (2020) Blockchain and federated learning-based distributed computing defense framework for sustainable society. Sustainable Cities Soc 59:102220
