TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 10/31 pp135–147
DOI: 10.26599/TST.2024.9010034
Volume 30, Number 1, February 2025

Quantifying Bytes: Understanding Practical Value of Data Assets in Federated Learning

Minghao Yao, Saiyu Qi*, Zhen Tian, Qian Li, Yong Han, Haihong Li, and Yong Qi

Abstract: The data asset is emerging as a crucial component in both industrial and commercial applications. Mining valuable knowledge from the data benefits decision-making and business. However, the usage of data assets raises tension between sensitive information protection and value estimation. As an emerging machine learning paradigm, Federated Learning (FL) allows multiple clients to jointly train a global model based on their data without revealing it. This approach harnesses the power of multiple data assets while ensuring their privacy. Despite the benefits, it relies on a central server to manage the training process and lacks quantification of the quality of data assets, which raises privacy and fairness concerns. In this work, we present a novel framework that combines Federated Learning and Blockchain by Shapley value (FLBS) to achieve a good trade-off between privacy and fairness. Specifically, we introduce blockchain in each training round to elect aggregation and evaluation nodes for training, enabling decentralization and contribution-aware incentive distribution, with these nodes functionally separated and able to supervise each other. The experimental results validate the effectiveness of FLBS in estimating contribution even in the presence of heterogeneity and noisy data.

Key words: Federated Learning (FL); blockchain; fairness

1 Introduction

Due to the extensive use of deep learning and the Internet of Things (IoT), inference and collection based on users' data assets have raised the concerns of privacy protection. Generally, data assets hold immense potential value[1–5], which plays a pivotal role as a vital business resource in today's internet-driven era. The data assets often comprise a vast amount of user information, including personal health data, online shopping records, browsing histories, and even the trade secrets of enterprise users[6–11]. All of these data constitute the invisible assets of each human. The legal landscape for enhancing privacy and security is steadily maturing[12–14], but there is still a need for advanced technical methods to protect the security of data assets to facilitate their usage.

The owners of data assets aim to quantify and establish transparency around their data. This enables them to harness the value of their assets while safeguarding against potential malicious exploitation. Effectively managing, protecting, and leveraging data assets is essential for individuals, institutions, and society. But we have to face two unavoidable questions: How to protect our data assets from breaches? How to maximize their value? Unfortunately, privacy protection and value realization of data assets are contradictory issues. When data assets are protected, it becomes challenging to fully

• Minghao Yao, Saiyu Qi, Zhen Tian, Yong Han, Haihong Li, and Yong Qi are with School of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China. E-mail: minghao_yao@stu.xjtu.edu.cn; saiyu-qi@xjtu.edu.cn; zhentian@stu.xjtu.edu.cn; han_yong@stu.xjtu.edu.cn; li_haihong@stu.xjtu.edu.cn; qiy@xjtu.edu.cn.
• Qian Li is with School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China. E-mail: qianlix@xjtu.edu.cn.
* To whom correspondence should be addressed.
Manuscript received: 2023-10-27; revised: 2024-01-05; accepted: 2024-02-03

exploit their value. Similarly, to fully realize the value of data assets, privacy must be infringed upon. In this case, new technical methods are needed to strike a balance between privacy protection and value realization.

Federated Learning[15] (FL), as an emerging machine learning paradigm, provides a solution to this issue. FL adopts a client-server architecture. Clients train local models on their own data and upload the trained models to the server. Upon receiving local models, the server aggregates them and returns the aggregated global model to the clients. On the one hand, this approach to some extent maintains a balance between privacy protection and value realization. Clients upload local models instead of their data, thus avoiding the exposure of raw data. On the other hand, the central server can use these local models to train a more powerful global model, realizing the value of the client's data assets. However, FL still has two challenges.

- **Privacy protection**: During training, clients rely on a trusted centralized server for model aggregation, but a malicious server could breach privacy by analyzing model parameters, posing significant privacy concerns[16−19]. The presence of malicious servers and the lack of server supervision also complicate assessing individual node contributions, making it challenging to evaluate their impact on the global model. Additionally, as FL is typically initiated by the server, individual clients often lack flexibility in task selection and initiating independent FL tasks.
- **Value estimation**: Clients often possess data assets of varying quantity and quality but may receive the same global model, raising concerns about fairness in both contributions and rewards[20−22]. This occurs primarily due to (1) Noise introduced into data, resulting from data storage and network constraints, and inevitable errors in data labeling due to human limitations, causing unfairness; (2) The presence of free-riders who seek to benefit from the global model without contributing valuable information by providing dummy data and labels. These challenges can reduce client motivation for participating in FL tasks.

This paper presents FL and Blockchain by Shapley value (FLBS), a decentralized FL contribution estimation approach that enables model aggregation and client contribution evaluation without a central server. Compared to usual FL methods under client-server architecture, better results have been achieved in terms of privacy protection and value realization of client data assets, while ensuring model performance. This decentralized approach leverages blockchain technology, enabling clients to control the behavior of nodes in each round using smart contracts on the blockchain to ensure security and transparency. Furthermore, it utilizes the Shapley value from cooperative game theory as the basis for contribution assessment, allocating rewards and recording them on the blockchain, thus ensuring fairness and traceability of the results.

The contributions of this paper are as follows:

(1) We introduce a decentralized FL approach where clients can autonomously initiate training tasks on the blockchain, offering incentives to engage other clients. Smart contracts randomly select aggregation and evaluation nodes each round, operating independently and mutually supervising to earn rewards. Clients can join tasks on the blockchain, receiving rewards corresponding to their data asset contributions to the model.

(2) We propose a blockchain-based contribution-aware mechanism that calculates the Shapley value of participating clients in each round through evaluation nodes, which assess contributions and receive corresponding rewards. Moreover, historical contributions can be traced on the blockchain. Experimental results demonstrate that our approach performs well with noisy and heterogeneous data.

(3) We present a comprehensive set of contribution-aware methods for decentralized FL. Due to the convenience of client participation and the fairness of contribution assessment, both large institutions and individual devices can initiate or join tasks and receive rewards. We implement the corresponding FLBS framework and conduct experiments to validate its effectiveness.

In summary, our decentralized FL approach empowers clients to participate securely and fairly in FL, even in the absence of a central server, thereby safeguarding their data assets and promoting participation in collaborative learning.

2 Related Work

In this section, we review and discuss prior research and developments in the field related to FL. We aim to provide context for our own work by highlighting the key findings, methodologies, and contributions of existing studies.

2.1 FL

The concept of FL was first introduced by Google as a decentralized machine learning approach[23]. Its main idea is to distribute model training to local devices or servers where the data resides, rather than centralizing the data storage in one place. Each local device, typically mobile devices, sensors, cloud servers, etc., can independently train a model and then transmit its updates to a central server. The central server continuously collects model updates from clients and aggregates them using aggregation rules, such as Federated Averaging (FedAvg), to obtain the updated model. FL not only addresses the problem of data silos but also provides a degree of privacy and security, making it a method to tackle challenges related to limited training data and data sharing restrictions. It has witnessed rapid development in both academia and industry[24−26].

FL effectively leverages the computational resources of various participants to train local models, thereby reducing the computational burden on the central server. Most importantly, it possesses inherent privacy-preserving properties, as individual participants do not need to share their raw data. Instead, they only conduct model training on nodes with decentralized data storage. This effectively prevents malicious servers from directly accessing sensitive data, reducing the potential privacy leakage risks during data transmission and solving the issue of high communication costs, as it does not require transmitting raw data from client devices to the central server. FL, as a new paradigm for distributed machine learning, has given rise to a series of promising applications, including medical decision-making[27−29], recommendation services[30, 31], and spatiotemporal systems[32−34]. Tech giants like Google and Apple have already made beneficial attempts to implement FL on mobile phones.

The architecture of FL determines that the more clients with high-quality data participate in the training, the better the results will be. However, ensuring that participants receive contributions matching their data assets and attracting more clients to join the training task remains a challenging issue[35].

2.2 Fairness

Due to the participation of multiple stakeholders and the heterogeneity of customer data distribution, FL systems face challenges related to accountability[36] and fairness[37, 38]. The basic FL framework is unable to address the issues arising from varying data quality and heterogeneous data distribution among multiple organizations. For most deep learning methods, data is a critical driver of their performance. Therefore, designing a system that incentivizes rational agents to contribute their fair share of data and maximizes the accuracy of the resulting model while improving collaboration is a key challenge in the practical application and long-term development of FL[39].

In anticipation of other clients sharing their data, rational agents may be inclined to engage in harmful behaviors such as free-riding[40], where they do not provide data but still benefit from improved models. To motivate more data owners to participate, service providers can incentivize by fairly assessing each data owner's contribution to the FL training process and offering corresponding rewards and compensation, thereby encouraging broader participation[41−43]. This approach helps build a fair and incentivized FL ecosystem, attracting more data holders to actively participate and collectively drive model performance improvements.

Contribution assessment of FL participants is an active subfield[44−48], aiming to estimate the value of each FL participant by assessing their impact on the global model performance without exposing the sensitive local data of each participant. Kang et al.[49] proposed measuring the value of a participant's own data or related variants as their contribution, aiming to identify and quantify each individual's contribution to the project or task. However, it does not consider the value gain that an individual participant brings to the FL collective. Wang et al.[50] considered the value loss of the data when removing a participant from the entire FL group as their contribution, following the leave-one-out approach widely used in machine learning tasks[51].

Shapley value, as a classic data evaluation scheme[52], was introduced in 1953 to solve the cooperative game problem[53], which has been widely used to evaluate the contributions of participants in FL, known as Federated Shapley Value (FedSV)[54−57]. FedSV retains the desirable properties of the Shapley value. The main idea is to enumerate all possible combinations of participants and calculate the marginal gain in data assert value brought by including a participant in the federation as their contribution. FL is a classical collaborative computing scene, we need a high-quality dataset to take part in model training. The

Shapley value approach is intuitive, easy to understand, and ensures fairness in assessing individual contributions to the project. It is the most widely applied method in the current FL contribution assessment.

However, these fairness analysis algorithms typically require a fixed server to distribute learning tasks and perform model parameter computations on the server side to determine client contributions. This approach is not conducive to attracting more clients to participate and is susceptible to malicious attacks. Therefore, exploring new paradigms for FL has become an important topic in recent years.

2.3 Blockchain

In client-server architecture of FL, centralized data collection and model aggregation are typically reliant on a single entity, such as an MEC server[58]. However, due to the centralization of the FL framework and the untrustworthiness of clients, traditional FL solutions are susceptible to attacks from malicious clients and servers. Once the server is compromised, it can lead to a single point of failure, disrupting the entire FL system. Furthermore, the performance bottleneck of a single service node cannot meet the scalability requirements.

To address these issues, the introduction of Secure Multi-party Computation (SMC)[59, 60] offers an alternative decentralized solution. However, the interactive nature of SMC imposes a heavy communication burden on clients. Blockchain[61], as a shared and tamper-resistant ledger with distributed storage of transaction records and collective maintenance as its technological features, provides a new perspective for credible, secure, and traceable verification of client privacy data asset management.

The integration of FL with blockchain is currently a hot topic of research, a classic approach is the FL platform proposed by Toyoda and Zhang in 2019[62]. Blockchain FL can eliminate the threat of single points of failure and malicious servers. Ramanan and Nakayama[63] proposed BAFFLE, a blockchain-based FL solution[63]. It uses Smart Contracts (SC) to aggregate local models. Kim et al.[64] introduced BlockFL, where local model updates are exchanged and verified through smart contracts deployed in the blockchain. It attracts potential high-quality data providers by offering incentives proportional to the size of the training data. However, these approaches do not consider the computational and communication overhead of blockchain network nodes.

Blockchain-based solutions have also emerged to address the auditability issues in FL. Bao et al.[65] introduced FLChain to construct an auditable decentralized FL system, capable of detecting malicious nodes and rewarding honest trainers. Zhang et al.[66] proposed a blockchain-based FL approach for fault detection in IoT devices and maintaining client data responsibility. Kang et al.[67] developed a reliable worker selection scheme based on blockchain for reputation management of trainers to prevent unreliable model updates.

Our work primarily focuses on the valuation of client data assets, aiming to provide new perspectives for the future of decentralized FL paradigms. While some research areas may overlap, they often overlook the impact of client data quality on fairness. Furthermore, many of these solutions tend to emphasize the outcomes and efficiency of technical frameworks, thereby neglecting certain security concerns.

3 Overview of FLBS

FLBS offers a novel solution for FL based on the blockchain while rewarding participants according to their contributions to the global model. The method finds relevance in various scenarios, benefiting both large organizations and personnel in their decision-making processes. For instance, hospitals can utilize this technology to initiate FL tasks on the blockchain, encouraging other hospitals to share their data assets, ultimately enhancing diagnostic accuracy and reliability. Furthermore, FLBS extends its applicability to cross-device scenarios, allowing clients to engage in FL tasks on the blockchain. This not only enables personalized services based on client habits but also provides them with rewards for their data asset contributions.

Considering the decentralized nature of blockchain, storing large machine learning models directly on it faces inherent limitations. Currently, efficient distributed storage methods include keeping only data description information on the blockchain or leveraging the InterPlanetary File System (IPFS) protocol. The IPFS protocol supports distributed peer-to-peer file storage and transmission. It stores files and application data on multiple devices, ensuring faster, more stable, and secure network access. Each data block is distinguished by a distinct hash value, and

these hash values can be recorded on the blockchain, forming data fingerprints. In the context of blockchain FL, client model parameters are locally stored, with smart contracts managing these models.

Figure 1 illustrates the workflow of FLBS, which comprises two primary components: aggregation and evaluation. In each training round, aggregation nodes and evaluation nodes are selected randomly. The aggregation nodes amalgamate upload models based on optimal contribution combinations and subsequently upload the aggregated model to the blockchain. Similarly, the evaluation nodes upload clients' historical contributions to the blockchain. These two types of nodes operate independently while also being able to verify results mutually, can effectively defend against attacks from malicious nodes, ensuring the transparency and traceability of the entire process. Meanwhile, the client nodes selected only upload their local model instead of data sets, which can guarantee the privacy of FLBS.

The overall process is as follows:

(1) Initialization: Clients launch FL tasks on the blockchain via smart contracts, specifying reward tokens and a public dataset. Other clients have the option to decide whether they want to participate in the FL training task.

(2) Node selection: Smart contracts are employed to select the nodes for training, aggregation, and evaluation in this round. The aggregation and evaluation nodes do not partake in the training task but receive compensation for their contributions through the aggregation and evaluation of local models.

(3) Local training: Clients train their local models using the initial global model and their local data. They then call IPFS to obtain a token representing their local model parameters and send this token to the evaluation nodes.

(4) Model evaluation: Evaluation nodes use the obtained tokens to call the IPFS protocol and retrieve local models from all training nodes. By calculating the utility values between different model combinations, they select the most suitable combination and upload the corresponding model tokens and contributions for this round's training to the blockchain.

(5) Model aggregation: Aggregation nodes use model tokens on the blockchain to retrieve models via IPFS and perform model aggregation locally to generate a new global model. They then upload the

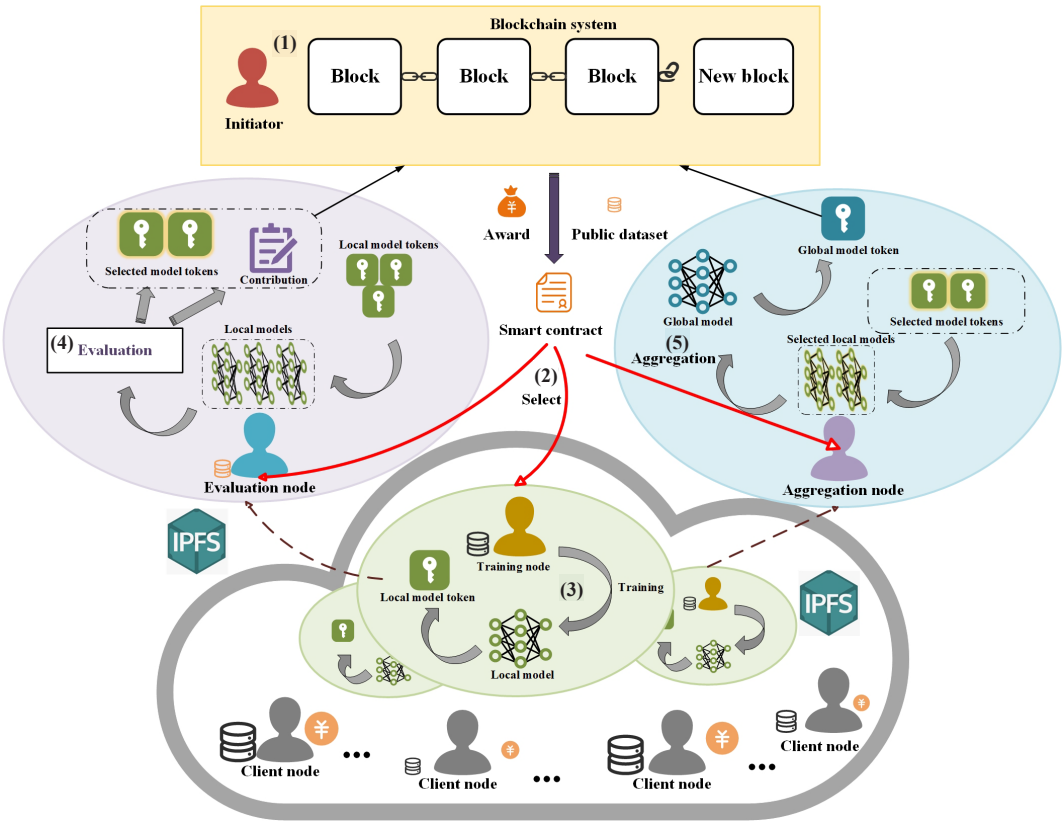


Fig. 1 Overview of FLBS.

token representing the new global model to the blockchain. Return to the Node Selection Phase for a new iteration.

(6) Completion phase: When the final training round concludes, the smart contract consolidates the contributions of each node on the blockchain for each round and distributes tokens based on their contributions.

4 Algorithm Description

In this section, we will provide a detailed explanation of the computational intricacies and operational workflow of the FedAvg algorithm. Furthermore, we will elucidate the design details of FLBS.

4.1 Design of FedAvg

Suppose there are $N = \{1, 2, \ldots, n\}$ clients participating in training task, The global objective function $F(\omega)$ of FL is to aggregate the i-th client's objective function $F_i(\omega)$ on their model parameter ω as follows:

$$F(\omega) = \frac{1}{N}\sum_{i=1}^{n} F_i(\omega) \tag{1}$$

Then we extend the optimization objective to the perspective of clients i, which has dataset D_i, and the data point $P_i = \{1, 2, \ldots, p\}$. The local objective is always defined as follows:

$$\min_{\omega} F_i(\omega) = \frac{1}{p}\sum_{\xi \in D_i} \ell\left(f(\omega); \xi\right) \tag{2}$$

which can minimize the i-th client's loss function ℓ which can measure the error between the model's predicted output $f(\omega)$ and the actual label ξ during training. To improve the distributed optimization problem described in Eq. (1), the FedAvg process is as follows, there are $T = \{1, 2, \ldots, t\}$ collaborative training rounds in total.

(1) The FedAvg framework starts with the initialization of a global model ω_0 on a central server.

(2) In each round t, a subset $K = \{1, 2, \ldots, k\}$ of clients is selected to participate as the probability P_k. This selection can be random or based on certain strategies.

(3) The selected client k performs local training using the current global model ω_t. This local training process typically consists of multiple local iterations to train the client's model. After each local iteration, a local model ω_{t+1}^k update is generated.

(4) After completing local training, K clients upload their local model updates $\{\omega_t^1, \omega_t^2, \ldots, \omega_t^k\}$ to the central server. These updates are typically the differences in model parameters, indicating how the model should be adjusted to fit the client's data.

(5) The central server collects model updates from different clients. These model updates are aggregated to create a new global model ω_{t+1}.

(6) The generated global model becomes the starting point for the next round $t+1$ of training. After this global model update, the entire training process proceeds to the next round, starting with client selection.

(7) The above steps are iterated multiple times until a predefined stopping condition is met, such as a certain number of training rounds or model performance convergence.

In this paper, our objective is to minimize Eq. (1), and it is possible to acquire the contributions of each client in each round.

4.2 Design of FLBS

Fairness plays a pivotal role in evaluating FL, which can incentivize more clients to join the process. When participants believe their contributions will be treated fairly, they are more motivated to cooperate actively. The FedAvg method falls short in accurately evaluating the quality of client data assets, thereby posing challenges in providing precise incentives to participants. The FLBS framework seeks improvement by incorporating the Shapley value from cooperative game theory to better gauge the contribution of data assets.

Cooperative game theory is a concept aimed at achieving common goals through collaboration among multiple participants, which shares some similarities with the optimization objectives of FL. The Shapley value, within the realm of cooperative game theory, serves as a concept employed to ascertain the equitable distribution of gains derived from collaboration among multiple participants. It quantifies the contribution of each client to the cooperative game and provides a fair way to distribute the gains.

Let $K = \{1, 2, \ldots, k\}$ represent the set of selected clients, participating in the training round $T = \{1, 2, \ldots, t\}$. Next, these clients generate all power sets $\mathcal{S} \subseteq K$, which range from the empty set to the full. These power sets represent different combinations of clients to consider when calculating Shapley values. $\upsilon(\mathcal{S})$ can acquire the performance of the model

collaboratively trained by clients in $\mathcal{S}$ as utility score.

Marginal contribution $\Phi_i^t(v)$ represents the impact of a specific client i on a particular outcome when added to a client combination in round t,

$$\Phi_i^t(v)=\begin{cases}\dfrac{1}{|\mathcal{S}|}\displaystyle\sum_{\mathcal{S}\subseteq K\setminus\{i\}}\dfrac{1}{\binom{N-1}{|\mathcal{S}|}}\left[v(\mathcal{S}\cup\{i\})-v(i)\right], & i\in K;\\ 0, & i\notin K\end{cases}\tag{3}$$

Then we can use marginal contributions to compute the Shapley value for each selected client. Finally, all clients can calculate the cumulative sum of values across all rounds as follows:

$$\Phi_i(v)=\sum_{t=1}^{T}\Phi_i^t(v)\tag{4}$$

These assigned Shapley values can be utilized for different applications, such as adjusting model weights or feature selection in FL.

The design details of FLBS are depicted in Algorithm 1. In each round t, smart contracts on the blockchain select the nodes participating in training and the nodes responsible for aggregation and contribution evaluation. Nodes participating in training in each round utilize gradient update $\nabla F_i(\omega^t)$ by the model ω^t from the previous round and upload local models ω_i^t. The contribution assessment node utilizes U to evaluate the performance of different client combinations M by sampling all local model combinations π in the k-th iteration through the Monte Carlo method, in which truncation is applied to combinations that do not exceed the threshold δ. It selects node combinations with relatively better model performance and assesses the contribution values of each node in this round. The aggregation node updates models as Eq. (1) from the selected combinations and uploads global model ω^t to the blockchain.

Algorithm 1 FLBS algorithm

Input: number of clients N, number of total rounds T, initialized model ω_0, learning rate η

Output: final global model ω and clients' contribution set Φ

for training round $t=1,2,\ldots,T$ **do**
  Select clients:
  $\omega_i^{t+1}\leftarrow\omega^t-\eta\nabla F_i(\omega^t)$; // client i acquire global ω^t
  Evaluation node:
  $\Phi_i^t=0, k=0$;
  while convergence criteria not meet **do**
    $k=k+1$;
    for j in $N=\{1,2,\ldots,n\}$ **do**
      if $|v_N-v_{j-1}^k|\leqslant\delta$ **then**
        $v_j^k=v_{j-1}^k$;
      else
        $M=\{\pi^k[1],\pi^k[2],\ldots,\pi^k[j]\}$;
        $v_j^k\leftarrow U(\sum_{i\in M}\frac{|D_i|}{\sum_{i\in M}|D_i|}\omega_i^t)$;
      $\Phi_{\pi^k[j]}^{t+1}\leftarrow\frac{1}{k}((k-1)\Phi_{\pi^k[j]}^{t+1}+(v_j^k-v_{j-1}^k))$;
return ω and Φ;

5 Experiment

In this section, we will conduct experiments to validate FLBS using standard datasets and artificially noised datasets.

5.1 Experiment setting

5.1.1 Dataset

Canadian Institute For Advanced Research 10 (CIFAR-10) is a widely used computer vision dataset comprising 10 distinct categories of color images. Each category contains 6000 images, resulting in a total of 60 000 images. This dataset is commonly employed for training and testing image classification algorithms and deep learning models.

In this paper, we initially preprocess the CIFAR-10 dataset by introducing Dirichlet coefficients ($\alpha=1$) to create Non-Independently and Identically Distributed (Non-IID) dataset. This step is taken to evaluate the effectiveness of FLBS on datasets with non-identical and non-uniform data distributions among clients.

Additionally, we artificially introduce noise to the dataset to simulate real-world scenarios where data may be noisy. We randomly select 20% of the nodes and add Gaussian noise to 10% of their data, multiplying their data quality by a noise coefficient. Then, we select 20% of the nodes and apply noise to their labels, randomly mapping 10% of their existing labels to other labels.

These scenarios aim to evaluate the algorithm's performance under various noise conditions, allowing us to assess its robustness and suitability for handling real-world noisy data.

5.1.2 Network architecture

ResNet-20 is a specific model within the ResNet[68] model series, and it is one of the relatively smaller variants of ResNet. ResNet-20 consists of 20 layers of convolutional layers, comprising residual blocks, and it is considered a shallow model within the ResNet series.

In summary, ResNet-20 is selected for experimentation because of its favorable properties in image classification tasks, its efficiency in training, and

its lightweight nature, which is particularly advantageous in scenarios involving minimal communication and aggregation overhead.

5.1.3 Training setup

In our experiments, the number of clients $N = 50$, and the number of clients selected per round $K = 5$, mini-batch size $B = 64$, learning rate $\eta = 0.01$, and total number of training rounds $T = 1000$.

5.2 Baselines

(1) FedAvg: It is one of the most broadly used algorithms in FL, and its primary idea is to train a global model by communicating and aggregating local model parameters among clients.

(2) FedFa: It introduces a dual-momentum gradient optimization scheme[69], which accelerates the model's convergence speed. Additionally, it proposes an algorithm that combines training accuracy and training frequency information to measure the weights, aiding clients in participating in server aggregation with fairer weights.

(3) FedFV: This method is designed to address fairness in FL[70]. It aims to reduce potential conflicts between clients before averaging gradients. The algorithm initially utilizes cosine similarity to detect gradient conflicts and then iteratively eliminates such conflicts by modifying the direction and magnitude of the gradients.

5.3 Global model performance

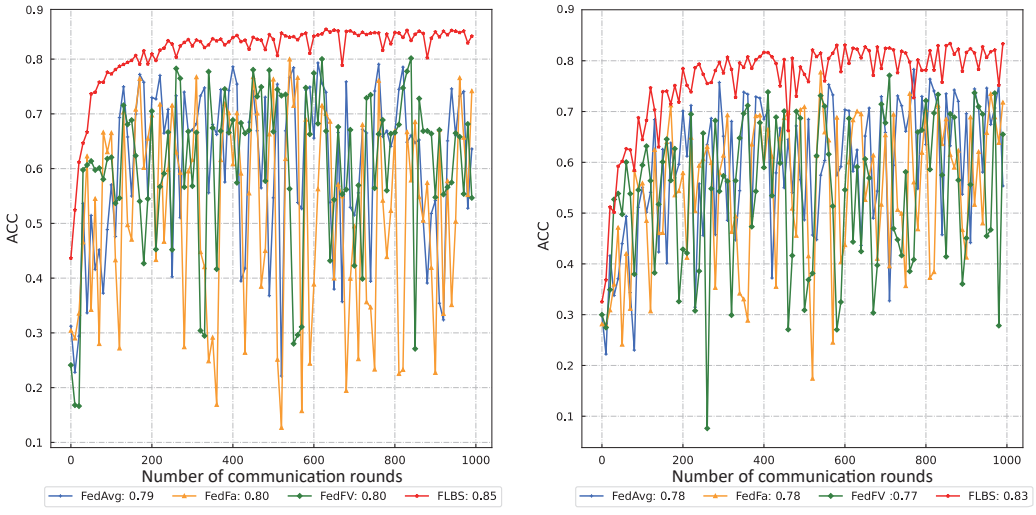
In this experiment, our main objective is to assess how our algorithm's accuracy is affected when noise is intentionally added to both IID and Non-IID datasets. Our goal is to determine whether FLBS could attain improved accuracy in scenarios where clients involved in the training possess noisy data, ultimately delivering advantages to these clients in terms of model performance.

Figure 2 illustrates a comparison of accuracy between FLBS and three other algorithms: FedAvg, FedFa, and FedFV. We test these methods under the condition that data and label noise are introduced into subsets of clients' IID and Non-IID datasets. The x-axis represents training rounds, while the y-axis represents global model accuracy (ACC). It is evident that FLBS consistently outperforms other algorithms in terms of accuracy and exhibits relatively lower variance between rounds. This is due to FLBs's ability to select relatively optimal combinations of clients from the current round, excluding clients with poor data quality from the combinations.

5.4 Fairness

In this experiment, our focus is to explore the relationship between the data asset quality distribution among clients and the contribution distribution under different algorithms. We aim to investigate whether FLBS could provide fair assurances for client contributions when some clients contain noise data. Due to space limitations, this paper primarily discusses scenarios under Non-IID data.

Kullback-Leibler (KL) divergence, also known as relative entropy, is a metric used to measure the difference between two probability distributions. KL



(a) IID noise case (b) Non-IID noise case

Fig. 2 Global model test accuracy (the maximum accuracy of each method is shown in the legend).

divergence quantifies the information loss when one distribution is used to approximate another. It can be employed to acquire the similarity or dissimilarity between two probability distributions. KL divergence reflects the goodness of fit between two distributions, and in this paper, we use KL divergence as a metric to assess the distribution of data quality and data contributions under different noise conditions. The formula for KL divergence for discrete probability distributions is as follows:

$$\mathrm{KL}(P\|Q) = \sum P(x) \log \frac{P(x)}{Q(x)} \tag{5}$$

where $\mathrm{KL}(P\|Q)$ represents the KL divergence from distribution Q to distribution P. $P(x)$ is the true probability distribution, and $Q(x)$ is the probability distribution used to approximate $P(x)$. A KL divergence closer to 0 indicates that the distributions P and Q are closer to each other.

The KL divergence between the result of FLBS and the data quality in different scenarios is shown in Fig. 3. The horizontal axis represents the different noise scenarios applied to heterogeneous data, ranging from left to right as IID&No noise, IID&Noise, Non-IID&No Noise, and Non-IID&Noise. The vertical axis represents the KL divergence between client contributions and data quality. A smaller KL divergence indicates a closer alignment between data quality and contribution perception distributions. In comparison to the Fedavg whose contribution only depends on dataset size, FLBS more effectively illustrates the relationship between contributions and data quality. Even when compared to the fairness-evaluable FedFa, FLBS still exhibits strong perceptual performance.

The experiments demonstrate that FLBS can perceive the impact of client data assets on the global model's contributions. It can incentivize client participation through contribution-based rewards, attracting more participants to engage in the training task.

5.5 Validation dataset

In this experiment, our primary focus is to investigate the impact of the data upload method employed in our testing dataset on model accuracy. Since evaluation nodes need to test the performance of the combined model, a small dataset must be accessible to clients. When selected as evaluation nodes, they are required to assess the contributions of clients participating in the current round. This dataset needs to have the characteristics of low space occupancy and high testing accuracy.

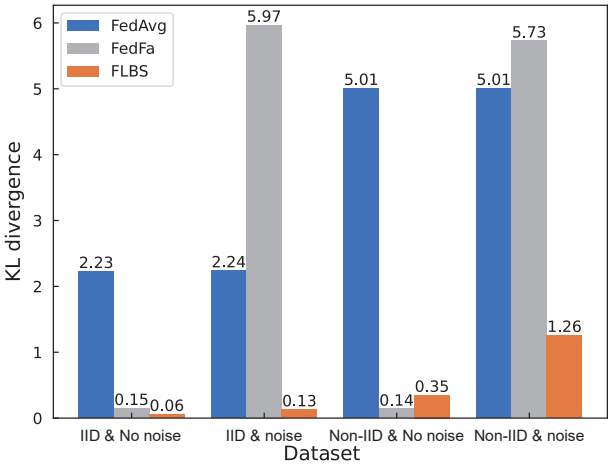


Fig. 3 Fairness: The extent to which client contributions, as computed by FedAvg, FedFa, and FLBS, align with the actual quality of data assets.

There are two methods for uploading the dataset:

(1) Initiator uploads testing set: In this approach, the initiator of the training process, who aims to obtain a well-performing FL model, uploads a testing set to evaluate the overall model accuracy and assess client contributions.

(2) Extraction from participant data: Participants are selected to train with the hope of acquiring a better global model. In this method, participants extract a small portion of their data, with the utmost respect for privacy, to construct a testing dataset. This approach is reasonable while minimizing privacy infringement.

Figure 4 provides insights into how clients, both with and without noisy data, respond to variations in data upload methods and dataset sizes in both IID and Non-IID scenarios. Experiments are conducted for different magnitudes of both upload methods in IID scenarios, including initiator uploads with 500, 2500, 5000, and 10 000 data points, as well as participant data extraction forming testing sets of 500, 2500, and 5000 data points (comprising 1%, 5%, and 10% of participants' data, respectively). The test results indicate that, whether in IID or Non-IID scenarios, for both noise-free and noisy datasets, the initiator upload method outperforms the data extraction method in terms of accuracy.

Furthermore, as the size of the testing dataset increases, model accuracy decreases, which eventually stabilizes. This phenomenon is due to the risk of

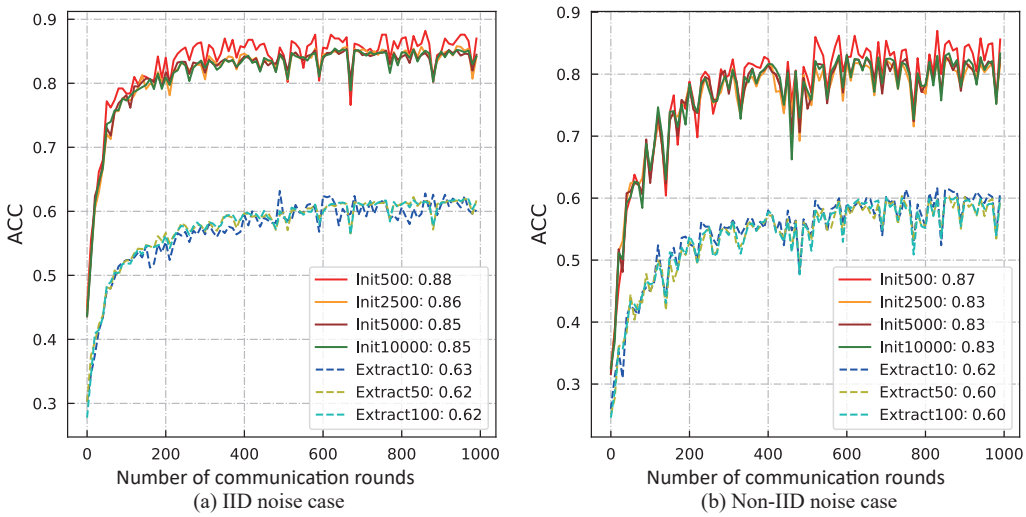


Fig. 4 Impact of data acquisition patterns on global model performance (the maximum test accuracy of each model is shown in the legend).

overfitting when the dataset is too small. Overfitting occurs when the model learns the noise or specific features of the training data rather than the general patterns that can be applied to new data. This can result in the model performing well on small testing datasets but poorly on larger or more diverse datasets. As the testing dataset size grows, overfitting diminishes, and increasing the dataset size further does not significantly affect accuracy. Therefore, uploading a relatively small testing dataset can prevent overfitting while reducing the cost of data upload and download.

6 Conclusion

In this paper, we have discussed the origins and evolution of the question concerning the valuation of our data assets, summarizing relevant developments in recent years. Research in the realm of a fair assessment of data assets in decentralized FL has been relatively limited. To bridge this gap, we have introduced a decentralized FL framework, denoted as FLBS, and conducted experimental evaluations using client data assets of varying quality. The results indicate that FLBS provides a robust assessment of clients' data asset contributions without the need for a central server, particularly in scenarios involving heterogeneous and noisy data. Meanwhile, FLBS has some nature like scalability and fairness which can stimulate more participants to contribute their data in the model training phase. And our method can also as a base framework to accommodate other FL and blockchain algorithms.

Our research represents a significant advancement in this emerging and critical field. FLBS decentralizes various processes and functionalities of FL to individual clients, enabling a fair and transparent assessment of their contributions. This allows clients to understand the value of their data assets, thereby motivating them to actively participate in training tasks.

Furthermore, numerous intriguing avenues for future exploration lie ahead. It would be valuable to explore alternative contribution assessment algorithms beyond Shapley values. Additionally, further research can be conducted to investigate additional properties and criteria for fairness in FL, expanding our understanding and capabilities in this domain.

Acknowledgment

This work was supported by the Natural Science Basic Research Program of Shaanxi Program (No. 2024JC-JCQN-67), the Fundamental Research Funds for the Central Universities (Nos. xzy012022083 and xxj032022012), the Shaanxi Province QinChuangYuan "Scientist + Engineer" Team Building Project (No. 2022KXJ-054), the National Key Research and Development Program of China (No. 2023YFB2703800), the National Natural Science Foundation of China (No. 62206217), and the China Postdoctoral Science Foundation (Nos. 2022M722530 and 2023T160512).

References

[1] H. T. Tseng, N. Aghaali, and N. Hajli, Customer agility and big data analytics in new product context, *Technol.*

Forecast. Soc. Change, vol. 180, p. 121690, 2022.

[2] Y. Chen, K. Sherren, M. Smit, and K. Y. Lee, Using social media images as data in social science research, *New Media Soc.*, vol. 25, no. 4, pp. 849–871, 2023.

[3] A. T. Tomczyk, D. Buhalis, D. X. F. Fan, and N. L. Williams, Pricepersonalization: Customer typology based on hospitality business, *J. Bus. Res.*, vol. 147, pp. 462–476, 2022.

[4] X. Chen, J. Sun, and H. Liu, Balancing web personalization and consumer privacy concerns: Mechanisms of consumer trust and reactance, *J. Consum. Behav.*, vol. 21, no. 3, pp. 572–582, 2022.

[5] C. Barrett, Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection? *Scitech Lawyer*, vol. 15, no. 3, pp. 24–29, 2019.

[6] M. Nasr, R. Shokri, and A. Houmansadr, Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning, in *Proc. 2019 IEEE Symp. Security and Privacy*, San Francisco, CA, USA, 2019, pp. 739–753.

[7] Z. Liu, Y. Chen, Y. Zhao, H. Yu, Y. Liu, R. Bao, J. Jiang, Z. Nie, Q. Xu, and Q. Yang, Contribution-aware federated learning for smart healthcare, in *Proc. Thirty-Sixth AAAI Conf. Artificial Intelligence*, Vancouver, Canada, 2022, pp. 12396–12404.

[8] Q. Guo, Y. Qi, S. Qi, and D. Wu, Dual class-aware contrastive federated semi-supervised learning, arXiv preprint arXiv: 2211.08914, 2022.

[9] Q. Yang, Y. Liu, T. Chen, and Y. Tong, Federated machine learning: Concept and applications, *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, p. 12, 2019.

[10] J. P. Bharadiya, Machine learning and AI in business intelligence: Trends and opportunities, *Int. J. Comput.*, vol. 48, no. 1, pp. 123–134, 2023.

[11] A. Matala, Reviewing the performance of local governments in managing corporate social responsibility program, *AKADEMIK J. Mahas. Human.*, vol. 2, no. 2, pp. 55–63, 2022.

[12] R. N. Zaeem and K. S. Barber, The effect of the GDPR on privacy policies: Recent progress and future promise, *ACM Trans. Manag. Inf. Syst.*, vol. 12, no. 1, p. 2, 2021.

[13] E. Goldman, An introduction to the California consumer privacy act (CCPA), Santa Clara Univ. Legal Studies Research Paper, 2020, http://dx.doi.org/10.2139/ssrn.3211013.

[14] S. Wachter, Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR, *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 436–449, 2018.

[15] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, Communication-efficient learning of deep networks from decentralized data, in *Proc. 20th Int. Conf. Artificial Intelligence and Statistics*, Fort Lauderdale, FL, USA, 2017, pp. 1273–1282.

[16] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, Membership inference attacks against machine learning models, in *Proc. 2017 IEEE Symp. Security and Privacy*, San Jose, CA, USA, 2017, pp. 3–18.

[17] M. Fredrikson, S. Jha, and T. Ristenpart, Model inversion attacks that exploit confidence information and basic countermeasures, in *Proc. 2015 22nd ACM SIGSAC Conf. Computer and Communications Security*, Denver, CO, USA, 2015, pp. 1322–1333.

[18] L. Melis, C. Song, E. De Cristofaro, and V. Shmatikov, Exploiting unintended feature leakage in collaborative learning, in *Proc. 2019 IEEE Symp. Security and Privacy*, San Francisco, CA, USA, 2019, pp. 691–706.

[19] D. Wu, S. Y. Qi, Y. Qi, Q. Li, B. W. Cai, Q. Guo, and J. X. Cheng, Understanding and defending against White-box membership inference attack in deep learning, *Knowl.-Based Syst.*, vol. 259, p. 110014, 2023.

[20] Y. Sarikaya and O. Ercetin, Motivating workers in federated learning: A stackelberg game perspective, *IEEE Netw. Lett.*, vol. 2, no. 1, pp. 23–27, 2020.

[21] J. Lin, M. Du, and J. Liu, Free-riders in federated learning: Attacks and defenses, arXiv preprint arXiv: 1911.12560, 2019.

[22] N. Ding, Z. Fang, and J. Huang, Incentive mechanism design for federated learning with multi-dimensional private information, in *Proc. 2020 18th Int. Symp. Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks* (*WiOPT*), Volos, Greece, 2020, pp. 1–8.

[23] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, Federated learning: Strategies for improving communication efficiency, arXiv preprint arXiv: 1610.05492, 2016.

[24] Q. Guo, Y. Qi, S. Qi, D. Wu, And Q. Li, FedMCSA: Personalized federated learning via model components self-attention, *Neurocomputing*, vol. 560, p. 126831, 2023.

[25] Q. Guo, D. Wu, Y. Qi, S. Qi, and Q. Li, FLMJR: Improving robustness of federated learning via model stability, in *Proc. 2022 27th European Symp. Research in Computer Security*, Copenhagen, Denmark, 2022, pp. 405–424.

[26] R. S. Antunes, C. A. Da Costa, A. Küderle, I. A. Yari, and B. Eskofier, Federated learning for healthcare: Systematic review and architecture proposal, *ACM Trans. Intellig. Syst. Technol.*, vol. 13, no. 4, p. 54, 2022.

[27] N. Rieke, J. Hancox, W. Li, F. Milletarì, H. R. Roth, S. Albarqouni, S. Bakas, M. N. Galtier, B. A. Landman, K. Maier-Hein, et al., The future of digital health with federated learning, *NPJ Digit. Med.*, vol. 3, no. 1, p. 119, 2020.

[28] I. Dayan, H. R. Roth, A. Zhong, A. Harouni, A. Gentili, A. Z. Abidin, A. Liu, A. B. Costa, B. J. Wood, and C. S. Tsai, et al., Federated learning for predicting clinical outcomes in patients with COVID-19, *Nat. Med.*, vol. 27, no. 10, pp. 1735–1743, 2021.

[29] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology, *Fut. Generat. Comput. Syst.*, vol. 129, pp. 380–388, 2022.

[30] L. Yang, B. Tan, V. W. Zheng, K. Chen, and Q. Yang, Federated recommendation systems, in *Federated Learning*: *Privacy and Incentive*, Q. Yang, L. Fan, and H. Yu, eds. Cham, Switzerland: Springer, 2020, pp. 225–239.

[31] C. Niu, F. Wu, S. Tang, L. Hua, R. Jia, C. Lv, Z. Wu, and G. Chen, Billion-scale federated learning on mobile clients: A submodel design with tunable privacy, in *Proc. 26th Ann. Int. Conf. Mobile Computing and Networking*,

London, UK, 2020, p. 31.
[32] C. Meng, S. Rambhatla, and Y. Liu, Cross-node federated graph neural network for spatio-temporal data modeling, in *Proc. 2021 27th ACM SIGKDD Conf. Knowledge Discovery & Data Mining*, Singapore, 2021, pp. 1202–1211.
[33] Y. Zhu, Y. Liu, J. J. Q. James, and X. Yuan, Semi-supervised federated learning for travel mode identification from GPS trajectories, *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2380–2391, 2022.
[34] Y. Liu, J. J. Q. Yu, J. W. Kang, D. Niyato, and S. Y. Zhang, Privacy-preserving traffic flow prediction: A federated learning approach, *IEEE Intern. Things J.*, vol. 7, no. 8, pp. 7751–7763, 2020.
[35] S. P. Karimireddy, W. Guo, and M. I. Jordan, Mechanisms that incentivize data sharing in federated learning, in *Proc. Workshop on Federated Learning*: *Recent Advances and New Challenges* (*in Conjunction with NeurIPS 2022*), New Orleans, LA, USA, arXiv preprint arXiv:2207.04557, 2022.
[36] S. K. Lo, Q. Lu, L. Zhu, H. Y. Paik, X. Xu, and C. Wang, Architectural patterns for the design of federated learning systems, *J. Syst. Software*, vol. 191, p. 111357, 2022.
[37] M. Mohri, G. Sivek, and A. T. Suresh, Agnostic federated learning, in *Proc. 36th Int. Conf. Machine Learning*, Long Beach, CA, USA, 2019, pp. 4615–4625.
[38] W. Du, D. Xu, X. Wu, and H. Tong, Fairness-aware agnostic federated learning, in *Proc. 2021 SIAM Int. Conf. Data Mining*, Washingtou, WA, USA, 2021, pp. 181–189.
[39] T. Li and S. Hu, A. Beirami, and V. Smith, Ditto: Fair and robust federated learning through personalization, in *Proc. International Conference on Machine Learning*, Virtual Event , 2021, pp. 6357–6368.
[40] Y. Fraboni, R. Vidal, and M. Lorenzi, Free-rider attacks on model aggregation in federated learning, in *Proc. 24th Int. Conf. Artificial Intelligence and Statistics*, Virtual Event, 2021, pp. 1846–1854.
[41] M. Tang and V. W. S. Wong, An incentive mechanism for cross-silo federated learning: A public goods perspective, in *Proc. IEEE INFOCOM 2021-IEEE Conf. Computer Communications*, Vancouver, Canada, 2021, pp. 1–10.
[42] Y. Qi, M. S. Hossain, J. Nie, and X. Li, Privacy-preserving blockchain-based federated learning for traffic flow prediction, *Fut. Generat. Comput. Syst.*, vol. 117, pp. 328–337, 2021.
[43] G. Paragliola, Evaluation of the trade-off between performance and communication costs in federated learning scenario, *Fut. Generat. Comput. Syst.*, vol. 136, pp. 282–293, 2022.
[44] A. Ghorbani and J. Zou, Data shapley: Equitable valuation of data for machine learning, in *Proc. 36th Int. Conf. Machine Learning*. Long Beach, CA, USA, 2019, pp. 2242–2251.
[45] R. Jia, D. Dao, B. Wang, F. A. Hubis, N. Hynes, N. M. Gürel, B. Li, C. Zhang, D. Song, and C. J. Spanos, Towards efficient data valuation based on the shapley value, in *Proc. 22nd Int. Conf. Artificial Intelligence and Statistics*, Naha, Japan, 2019, pp. 1167–1176.
[46] T. Song, Y. Tong, and S. Wei, Profit allocation for federated learning, in *Proc. 2019 IEEE Int. Conf. Big Data*, Los Angeles, CA, USA, 2019, pp. 2577–2586.
[47] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, Federated learning for healthcare informatics, *J. Healthc. Inform. Res.*, vol. 5, no. 1, pp. 1–19, 2021.
[48] X. Wei, Q. Li, Y. Liu, H. Yu, T. Chen, and Q. Yang, Multi-agent visualization for explaining federated learning, in *Proc. Twenty-Eighth Int. Joint Conf. Artificial Intelligence*, Macao, China, 2019, pp. 6572–6574.
[49] 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 Intern. Things J.*, vol. 6, no. 6, pp. 10700–10714, 2019.
[50] G. Wang, C. X. Dang, and Z. Zhou, Measure contribution of participants in federated learning, in *Proc. 2019 IEEE Int. Conf. Big Data*, Los Angeles, CA, USA, 2019, pp. 2597–2604.
[51] M. Kearns and D. Ron, Algorithmic stability and sanity-check bounds for leave-one-out cross-validation, in *Proc. Tenth Ann. Conf. Computational Learning Theory*, Nashville, TN, USA, 1997, pp. 152–162.
[52] Y. Kwon, M. A. Rivas, and J. Zou, Efficient computation and analysis of distributional Shapley values, in *Proc. 24th Int. Conf. Artificial Intelligence and Statistics*, Virtual Event, 2021, pp. 793–801.
[53] H. W. Kuhn and A. W. Tucker, *Contributions to the Theory of Games* (*AM-28*). Princeton, NJ, USA: Princeton University Press, 1953.
[54] T. Wang, J. Rausch, C. Zhang, R. Jia, and D. Song, A principled approach to data valuation for federated learning, in *Federated Learning*: *Privacy and Incentive*, Q. Yang, L. Fan, and H. Yu, eds. Cham, Switzerland: Springer, 2020, pp. 153–167.
[55] A. Ghorbani, M. P. Kim, and J. Zou, A distributional framework for data valuation, in *Proc. 37th Int. Conf. Machine Learning*, Virtual Event, 2020, p. 331.
[56] H. Yu, Z. Liu, Y. Liu, T. Chen, M. Cong, X. Weng, D. Niyato, and Q. Yang, A fairness-aware incentive scheme for federated learning, in *Proc. AAAI/ACM Conf. AI, Ethics, and Society*, New York, NY, USA, 2020, pp. 393–399.
[57] L. Lyu, X. Xu, Q. Wang, and H. Yu, Collaborative fairness in federated learning, in *Federated Learning*: *Privacy and Incentive*, Q. Yang, L. Fan, and H. Yu, eds. Cham, Switzerland: Springer, 2020, pp. 189–204.
[58] D. C. Nguyen, M. Ding, Q. V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, Federated learning meets blockchain in edge computing: Opportunities and challenges, *IEEE Intern. Things J.*, vol. 8, no. 16, pp. 12806–12825, 2021.
[59] A. C. Yao, Protocols for secure computations, in *Proc. 23rd Ann. Symp. Foundations of Computer Science*, Chicago, IL, USA, 1982, pp. 160–164.
[60] D. Rathee, M. Rathee, N. Kumar, N. Chandran, D. Gupta, A. Rastogi, and R. Sharma, Cryptflow2: Practical 2-party secure inference, in *Proc. 2020 ACM SIGSAC Conf. Computer and Communications Security*, Virtual Event, 2020, pp. 325–342.
[61] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain, *IEEE Intern. Things J.*, vol. 8, no. 14, pp. 11743–11757, 2021.

[62] K. Toyoda and A. N. Zhang, Mechanism design for an incentive-aware blockchain-enabled federated learning platform, in *Proc. 2019 IEEE Int. Conf. Big Data*, Los Angeles, CA, USA, 2019, pp. 395–403.
[63] P. Ramanan and K. Nakayama, BAFFLE: Blockchain based aggregator free federated learning, in *Proc. 2020 IEEE Int. Conf. Blockchain*, Rhodes, Greece, 2020, pp. 72–81.
[64] H. Kim, J. Park, M. Bennis, and S. L. Kim, Blockchained on-device federated learning, *IEEE Commun. Lett.*, vol. 24, no. 6, pp. 1279–1283, 2020.
[65] X. Bao, C. Su, Y. Xiong, W. Huang, and Y. Hu, FLChain: A blockchain for auditable federated learning with trust and incentive, in *Proc. 2019 5th Int. Conf. Big Data Computing and Communications*, Qingdao, China, 2019, pp. 151–159.
[66] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu, and L. Zhu, Blockchain-based federated learning for device failure detection in industrial IoT, *IEEE Intern. Things J.*, vol. 8, no. 7, pp. 5926–5937, 2021.
[67] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, Reliable federated learning for mobile networks, *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 72–80, 2020.
[68] K. He, X. Zhang, S. Ren, and J. Sun, Deep residual learning for image recognition, in *Proc. 2016 IEEE Conf. Computer Vision and Pattern Recognition*, Las Vegas, NV, USA, 2016, pp. 770–778.
[69] W. Huang, T. Li, D. Wang, S. Du, J. Zhang, and T. Huang, Fairness and accuracy in horizontal federated learning, *Inf. Sci.*, vol. 589, pp. 170–185, 2022.
[70] Z. Wang, X. Fan, J. Qi, C. Wen, C. Wang, and R. Yu, Federated learning with fair averaging, in *Proc. Thirtieth Int. Joint Conf. Artificial Intelligence*, Montreal, Canada, 2021, pp. 1615–1623.

Minghao Yao received the MEng degree from Northeastern University, China in 2021. He is currently pursuing the PhD degree in computer science and technology at School of Computer Science and Technology, Xi'an Jiaotong University, China. His research interests include federated learning and blockchain.

Saiyu Qi received the BEng degree in computer science and technology from Xi'an Jiaotong University, China in 2008, and the PhD degree in computer science and engineering from Hong Kong University of Science and Technology, China in 2014. He is currently an associate professor at School of Computer Science and Technology, Xi'an Jiaotong University, China. His research interests include applied cryptography, cloud security, distributed systems, and pervasive computing.

Zhen Tian received the MEng degree from Northeastern University, China in 2021. He is currently pursuing the PhD degree in computer science and technology at School of Computer Science and Technology, Xi'an Jiaotong University, China. His research interests include federated learning and blockchain.

Qian Li received the PhD degree in computer science and technology from Xi'an Jiaotong University, China in 2021, where he is currently an assistant professor at School of Cyber Science and Engineering. His research interests include deep adversarial learning, artificial intelligence security, and optimization of theory.

Yong Han received the MEng degree in computer science and technology from Jiangxi Normal University, China in 2022. He is currently a master student at School of Computer Science and Technology, Xi'an Jiaotong University, China. His research interests include blockchain technology, distributed systems, and federated learning.

Haihong Li received the BEng degree in agricultural mechanization and automation from Northwest A&F University, China in 2022. Currently, he is a master student in computer technology at School of Computer Science and Technology, Xi'an Jiaotong University, China. His research interests include federated learning and blockchain systems.

Yong Qi received the PhD degree from Xi'an Jiaotong University, China. He is currently a full professor at Xi'an Jiaotong University, China. His research interests include operating system, distrusted systems, and cloud computing.