Blockchain-enabled Federated Learning: A Survey

YOUYANG QU, Data61, Commonwealth Scientific and Industrial Research Organisation, Australia
MD PALASH UDDIN, School of Information Technology, Deakin University, Australia
CHENQUAN GAN, School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, China
YONG XIANG, School of Information Technology, Deakin University, Australia
LONGXIANG GAO, Qilu University of Technology (Shandong Academy of Sciences), and Shandong Computer Science Center (National Supercomputer Center in Jinan), China
JOHN YEARWOOD, School of Information Technology, Deakin University, Australia

Federated learning (FL) has experienced a boom in recent years, which is jointly promoted by the prosperity of machine learning and Artificial Intelligence along with emerging privacy issues. In the FL paradigm, a central server and local end devices maintain the same model by exchanging model updates instead of raw data, with which the privacy of data stored on end devices is not directly revealed. In this way, the privacy violation caused by the growing collection of sensitive data can be mitigated. However, the performance of FL with a central server is reaching a bottleneck, while new threats are emerging simultaneously. There are various reasons, among which the most significant ones are centralized processing, data falsification, and lack of incentives. To accelerate the proliferation of FL, blockchain-enabled FL has attracted substantial attention from both academia and industry. A considerable number of novel solutions are devised to meet the emerging demands of diverse scenarios. Blockchain-enabled FL provides both theories and techniques to improve the performance of FL from various perspectives. In this survey, we will comprehensively summarize and evaluate existing variants of blockchain-enabled FL, identify the emerging challenges, and propose potentially promising research directions in this under-explored domain.

CCS Concepts: • **Security and privacy → Privacy-preserving protocols**; **Social engineering attacks**; **Social aspects of security and privacy;**

Additional Key Words and Phrases: Federated learning, blockchain, attacks, countermeasures

ACM Reference format:
Youyang Qu, Md Palash Uddin, Chenquan Gan, Yong Xiang, Longxiang Gao, and John Yearwood. 2022. Blockchain-enabled Federated Learning: A Survey. *ACM Comput. Surv.* 55, 4, Article 70 (November 2022), 35 pages.
https://doi.org/10.1145/3524104

This work was supported in part by the Australian Research Council under grant DP220100983.
Authors' addresses: Y. Qu, Data61, Commonwealth Scientific and Industrial Research Organisation, Australia; email: youyang.qu@data61.csiro.au; M. P. Uddin, Y. Xiang (corresponding author), and J. Yearwood, School of Information Technology, Deakin University, Australia; emails: mpuddin@deakin.edu.au, yong.xiang@deakin.edu.au, john.yearwood@deakin.edu.au; C. Gan, School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, China; email: gancq@cqupt.edu.cn; L. Gao (corresponding author), Qilu University of Technology (Shandong Academy of Sciences), and Shandong Computer Science Center (National Supercomputer Center in Jinan), China; email: longxiang.gao@deaklin.edu.au.

0360-0300/2022/11-ART70 $15.00
https://doi.org/10.1145/3524104

1 INTRODUCTION

In recent years, with the tremendous improvement in computing power, algorithms, and data volume, the development of **Machine Learning (ML)** approaches for **Artificial Intelligence (AI)** has set off wave after wave, ranging from face recognition and living body detection to autonomous driving and precision marketing, which has greatly enriched and facilitated daily human life [1–4]. However, in reality, ML is not a panacea and requires a large amount of high-quality data to support it [5–7]. Only a few giant companies in the world have strength in this respect, while the vast majority of business enterprises are faced with the dilemma of low data volume and poor data quality, leading to difficulty in fully realizing and developing high-quality ML technologies.

With the advent of the big data era, data is wealth. Therefore, data privacy protection and security have become the most focused-on issues nowadays [8]. Obviously, attaching importance to data privacy protection and security has become a worldwide trend, and the promulgation of a series of laws and regulations has made it more difficult to obtain data [9, 10]. These rising data privacy preservation issues have become a crucial bottleneck in real-life application development through ML algorithms. From the angle of the industries, due to industry competition, privacy security issues, complex administrative procedures, and other associated problems, data often exist in the form of *data isolated islands*. Even the realization of centralized data integration between different departments of the same company faces many obstacles in achieving data inter-connectivity. In fact, it is almost impossible to integrate data scattered in various places and institutions, and the costs involved are enormous [11]. As a consequence, this data isolation scenario also brings unprecedented challenges to the development of ML algorithms.

To mitigate the aforementioned difficulties related to data privacy preservation in the ML setup, several solutions have been presented using the contexts of **Differential Privacy (DP)** [12–14], **Homomorphic Cryptography (HC)** [15–17], and **Secure Multi-Party Computation (SMPC)** [18–20]. The amount of additive random noise in DP mechanisms needs to be fine-tuned as the addition of more noise can improve the privacy of data but decrease the ML accuracy significantly. Similarly, computing encrypted learning data may be limited to the use of only a linear model [15] or a very small amount of entities involved [16]. Although SMPC can be used for large-scale distributed ML, it cannot provide a guarantee of information leakage from it. Therefore, there is still a need for developing a robust privacy-preserving ML strategy for protecting data privacy during model training [7, 8]. However, in view of the above-mentioned second problem that is difficult to achieve and develop, fails to allow rough exchange, and is unwilling to contribute value, the original data processing mode in the field of ML—that is, one party collects data; then transfers data to the other party for processing, cleaning, and modeling; and finally sells the model to a third party—is no longer competent [6, 21]. Consequently, how to design an ML framework under the premise of meeting the requirements of data privacy, security, and supervision so that ML systems can use their own data more efficiently and accurately is an important topic in the current development of AI [9]. In this context, **Federated Learning (FL)** came into being.

FL is also known as federated ML, joint learning, or alliance learning. It is an ML framework that can effectively help multiple organizations to perform data usage and ML model training while meeting the requirements of user privacy protection, data security, and government regulations. This concept was first proposed by Google in 2016 to solve the problem of locally updating models of Android mobile phone end users [22–24]. Its design goal is to ensure information security during big data exchange; protect terminal data and personal data privacy; and, under the premise of legal compliance, develop efficient ML between multiple participants or multiple computing nodes. This scenario is also called horizontal FL. For different types of data samples, in addition to horizontal FL, there are two other different ways, namely vertical FL and federated transfer

learning. Thus, the emergence of FL provides new ideas for AI to break the data barrier and for further development. Existing research lays the most focus on developing core FL optimizations for reducing communication overhead [22, 25–36] and heterogeneity issues [28, 37–45]. However, beyond these, FL is still confronted with three crucial drawbacks, which are centralized processing of locally trained ML models, being vulnerable to data falsification, and lack of incentive mechanism for the participating nodes for real-life deployment.

There are a few pioneering works discussing the decentralized solution using a gossip protocol [46–48]. The gossip protocol is a key component of almost all blockchain consensus algorithms including PoW, PoS, and various others [49]. Although a gossip protocol can be used to achieve decentralized federated learning, it lacks several key features, such as decentralized storage on the public ledger and cross-validation, which are basic functionalities of blockchain. Pure consensus algorithms like the gossip protocol do not enable decentralized storage (public ledger) and cross-validation. Consequently, although federated learning can be performed in a decentralized way, the model parameters stored on each local device are neither synchronized nor verified. Therefore, single-point failure issues toward storage still remain.

To overcome these shortcomings, blockchain-enabled FL is proposed and extended to meet various real-world demands. Regarding blockchain, it is a public ledger that each node in a blockchain network (or a selected committee) has an equal role and makes joint efforts to maintain the community by reaching a consensus and recording the public ledger locally. It enables trust in untrustworthy scenarios [50–52]. The advantageous features of blockchain can mitigate the negative impact of the three identified challenges of FL [7, 53]. Decentralization and high scalability features of blockchain allow fully or partially decentralized FL, which avoids possible man-in-the-middle attacks, single-point failure, and so forth [54, 54]. The built-in incentive mechanism and high availability guarantee the high participant motivation of end devices, especially the high-performance ones [55]. Moreover, authenticity, Byzantine resilience, persistence, and anonymity of blockchain jointly contribute to the promotion of FL's security and privacy protection level [56, 57].

Several surveys have been conducted to look into the integration of blockchain and federated learning from various perspectives. In [58], Nguyen et al. discussed blockchain-enabled FL considering the communication cost and resource allocation in mobile edge computing scenarios. In [59], Ali et al. discussed this topic within the scope of the Internet of Things, where blockchain and federated learning are separately discussed in detail, while the integration of them is presented with structures and outlooks. In addition to these two surveys, there are a few other FL-oriented surveys investigating blockchain-enabled FL on a section level [60–65]. In [60], Aledhari et al. showed a basic structure of blockchain-enabled FL as one of the FL paradigms and analyzed the potential of optimization toward blockchain-enabled FL in resource-constrained IoT scenarios. Zeng et al. and Zhan et al. reviewed the application of blockchain for incentive mechanisms of FL, respectively [62, 63]. Khan et al. introduced the structures of blockchain-enabled FL for edge networks and IoT in [64, 65], respectively. To sum up, the existing surveys did not provide a comprehensive review of blockchain-enabled federated learning from a systematic view considering the decentralized structures built upon consensus algorithms, incentive mechanisms, privacy and security protection, and the gamut of application scenarios. In this survey, we will elaborate on how to use blockchain technology to promote the consummation of FL from the perspectives of decentralization, incentivization, and resistance to several attacks.

The remainder of this article is organized as follows. Section 2 elaborates on the working principles of FL and blockchain. In Section 3 and Section 4, we describe the state-of-the-art methods proposed in the context of blockchain-enabled FL for generating a high-quality ML model making an effective tradeoff among the identified FL challenges. We then present open issues followed by

potential research directions from the perspective of blockchain-enabled FL in Section 5. At last, Section 6 recapitulates the ideas and concludes the article.

2 PRELIMINARIES AND PROBLEM IDENTIFICATION

In this section, we present an overview of FL and blockchain. We articulate the research status of FL and identify three primary challenges of existing FL systems. Then, we show the working flow and the corresponding advantageous features of the blockchain and how it potentially mitigates the negative impacts of the three identified challenges.

2.1 Overview of FL

Nowadays, 7 million connected **Internet of Things (IoT)** devices and 3 million smartphones are being operated along with a growing number of other computing and embedded or end-edge devices [66]. These devices are integrated with advanced modern sensors and an increasing number of communication and computing facilities. These enormous devices connected in distributed networks are producing an unprecedented amount of privately sensitive data that are remarkably suitable for different ML tasks such as analysis of sentiments and images, analysis of burglary in smart homes, critical clinical functions like diabetics analysis and heart disease prediction, semantic location, activities recognition of mobile phone users, and so forth [67–69]. Beyond, these powerful devices can significantly be employed for different crowd-sensing activities, e.g., monitoring of air quality [70], and medical purposes [71]. However, as the data generated by these distributed devices are privately sensitive, they are unsuitable to bring into a common data center for ML applications. Consequently, FL is presented to accomplish such ML tasks that enable the end-edge devices to train a common **Deep Neural Network (DNN)** [72] collaboratively with their own private data [25].

In the classical FL strategy, a small fraction m of total K participating devices are selected for training the server-sent initial or aggregated model w^t in each communication round, $t = 0, 1, \ldots,$ Then, each trained model w_k^{t+1} of k^{th} device is uploaded to the FL server for producing shared global model w^{t+1} through aggregation, which is subsequently sent back to the other m selected devices for retraining. This process is repeated until reaching the convergence of training as illustrated in Figure 1. The last desired global model w^{t+1} produced by the FL server may then be transferred to individual devices for application purposes. In this manner, individual device's data privacy is preserved as the devices do not need to share their private data with each other except the trained models only. As a successful privacy-preserving and large-scale distributed ML paradigm, renowned service providers have already started to deploy FL solutions [11, 73]. In addition, FL setups are implementable for various privacy-sensitive applications through learning data stored at edge devices [42, 74–78]. To this end, we essentially discuss the featured advantages of classical FL that make it a more exclusive privacy-preserving distributed ML paradigm.

2.1.1 Privacy Preservation. Privacy preservation is the most advantageous feature of the FL paradigm, whose objective is to protect direct access of devices' own data through exchanging only model updates calculated on an individual's private data samples. In this way, the data privacy of individual devices is protected as the data are not transferred directly among devices except the model, which is also substituted after every aggregation phase.

The works presented in a conventional ML context for privacy preservation using the DP mechanism [12–14, 79–81], HC [15–17], and SMPC [18–20] are further adopted in the FL setup; [82–86] demonstrate additional privacy supports using DP, while [87, 88] present the mechanism for privacy preservation based on SMPC. Although SMPC approaches can attain original test performance along with high privacy guarantee, these methods require additional communication cost

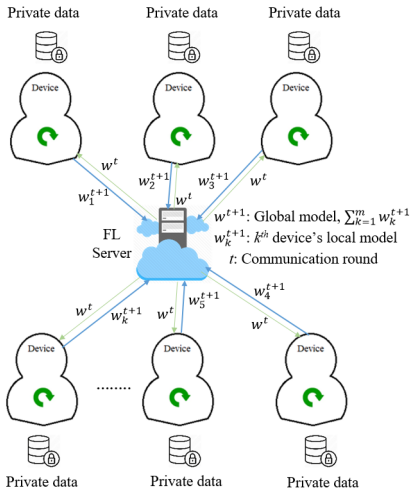

Fig. 1. Overview of the FL training strategy for producing aggregated global ML model using devices' private data.

in the system. In addition, as the hyperparameters associated with [84, 85] may have a damaging impact on test results and communication, [86] presents a robust gradient clipping strategy to alleviate the issue of hyperparameter adjustment, [83] offers better model generalization considering local privacy, [40] applies DP in a meta-learning context with an extension to a convex objective, [89] presents a privacy mechanism through binding the server to provide proof of aggregation results to the end-devices, and finally, [90] investigates a differentially private FL in an asynchronous manner for urban applications. Thus, these significant works essentially clarify the superior privacy protection scheme in the emerged FL paradigm.

2.1.2 Communication Efficiency. In the FL setting, communication among devices and the central server is the crucial bottleneck that, together with the privacy preservation mechanism, entails devices' own data to be kept private. As opposed to data center centralized-distributed ML [91–93], the number of collaborating devices in FL can be over millions and communication can thus be significantly slower than local computation because of several factors [94, 95]. Besides, the upload speed is still not inclinable to the download speed in a distributed network. As a consequence, FL solutions are designed to generate the global shared model in such a way that the collaborating devices require as little communication as possible with the server while ensuring maximum test performance. Although the conventional distributed ML algorithms are infeasible to be directly deployed for FL training, research is done by exploiting different views of classical ML and distributed ML algorithms to best settle for communication-efficient FL optimization, which aims to recurrently transfer as small model updates as possible through reducing the global communication rounds. In addition, sometimes, the compressive representation of weights and hyperparameters of the models is considered for faster transfer to substantially improve communication efficiency.

Transfer of Less Model Update: The conventional mini-batch **Stochastic Gradient Descent (SGD)** methods [96–100] presented for classical distributed ML optimizations are shown to have limited communication efficiency by distributed data processing paradigms [101, 102]. Then, based on primal-dual local-updating methods, numerous communication-efficient works are presented for convex distributed optimizations [101, 103–106], while [93, 107] tackle non-convex distributed

optimization objectives. In the FL setup, the baseline optimization algorithms called **Federated Averaging (FedAvg)** [25] and **Federated Stochastic Variance Reduced Gradient (FedSVRG)** [22] obtain communication efficiency through the use of classical SGD parallelism and full gradient calculation by **Stochastic Variance Reduced Gradient (SVRG)** [108], respectively. In addition, a genetic algorithm-based evolving DNN has been presented very recently that aims to optimize the structure of DNN models through the adaptation of a multi-objective evolutionary algorithm [26]. However, [27] modifies FedAvg substantially to present FedProx, which reduces communication rounds tackling systems and data heterogeneity, and [36] suggests to use momentum gradient descent instead of conventional SGD for reducing communications, while [28] presents a systems-aware optimization approach called MOCHA, which supersedes the performance of FedAvg in terms of communication efficiency, stragglers, and fault tolerance. However, as the aforementioned FL local-update mechanisms consider the synchronous transmission of model updates, [29, 30] present some sort of asynchronous update transmission for making a tradeoff between communication efficiency and model performance.

Transfer of Compressed Model: Similar to classical model compression strategies [109–111] through sub-sampling, quantization, or sparsification used in data center distributed ML, the model compression for the FL setup makes FL more stable to be communication efficient. In FL optimization, [31] designs to make the updated models sparse and low rank, then performs compression using sub-sampling, quantization, and random rotations, while [32] performs lossy model compression with a dropout strategy and [112] adopts a Golomb lossless coding strategy for model compression. However, [34] identifies redundant gradient for compression and [35] proposes extrapolation model compression and difference model compression for reducing the communication cost. In this way, the FL paradigm possesses communication efficiency through injecting more computations in the participating edge devices.

2.1.3 Robust to Statistical and System Heterogeneity. The local devices collaborating in FL training usually produce and collect data in a **non-Independent and Identically Distributed (non-IID)** manner, typically considered as an instance of statistical heterogeneity. The non-IID data distribution manner is tackled in FL optimization more suitably than other classical distributed ML through the use of multi-task learning and meta-learning strategies [28, 40], where these two contexts provide device-specific or personalized model training. Specifically, flourishing works such as [28, 37–40, 42] have been deployed for modeling a non-homogeneous data setup using meta-learning [113] and multi-task learning [114, 115] of the conventional ML literature. In addition, as these methods are restricted to only convex objectives with less capability to scale large networks, several methods are also presented for dealing with non-convex optimizations [38], handling large-size networks [40], addressing cyclic patterns among devices [39], and personalizing the device model using transfer learning [42]. However, [43–45] design to cope with fairness, modifying the local device optimization strategy based on the variation of local losses.

Systems heterogeneity primarily occurs in FL optimization because communication, computation, and storage abilities differ from device to device due to the mutability of network connectivity (WiFi, 5G, etc.) and hardware (memory, CPU, battery, etc.). Moreover, it is obvious that a device can be unreliable as well as can be dropped out due to power constraints or poor connectivity. The systems heterogeneity desperately increases challenges like fault tolerance and straggler mitigation. However, the FL designs alleviate these heterogeneity issues through (1) undergoing the heterogeneity of hardware architecture [29, 116], inheriting conventional ML heterogeneity mitigation approaches [117–119]; (2) tackling dropped-out devices in training [27, 28]; and (3) figuring a small number of participation in each training round [25, 27, 28, 31, 36, 73, 120–123].

2.2 Primary Challenges of FL

Based on the discussion and observation of the presented classical strategies for benefiting the emerged FL paradigm, it can be realized that most methods primarily focus on reducing communication overhead for ensuring a convergence guarantee and additional privacy preservation, and tackling statistical non-homogeneity [28, 37–40, 42]. In this type of algorithmic development, either the local model update strategy is redesigned or sometimes the aggregation strategy or both are redesigned substantially [124–127]. However, more practical benefits of the FL setup are desired for real-life deployment. To achieve those, we identify three primary challenges in existing FL systems as discussed below:

- **Centralized processing:** As classical FL involves a single central server for handling all required operations, it leads to possible single-point failure, man-in-the-middle attack, and so forth. In addition, the volume of involved edge devices is massive so that the network overload becomes increasingly serious due to limited bandwidth and scalability [53, 128–130].
- **Lack of incentive mechanism:** An emerging trend is that edge devices with high quality of data and performance are not sufficiently incentivized to participate and contribute. Obviously, this lacking will seriously cause potential device dropout from collaboration [131–137].
- **Low robustness:** Leading attacks such as poisoning attacks and Byzantine attacks will mislead the training process and significantly impact the accuracy of the system, disable the convergence of the maintained model, or even lead to denial of services [138–142].

2.3 Briefing of Blockchain

In this subsection, we introduce the blockchain technology, its advantageous features, and how these features can potentially solve the identified issues of FL (shown in Section 2.2) in a systematic but concise manner.

2.3.1 Preliminaries of Blockchain. In 2008, Satoshi Nakamoto released Bitcoin 1.0 [143] to the public, which facilitates the booming of its underlying technology, in particular, blockchain [144]. After this, blockchain attracted extensive interest and grew to what it is today. Nowadays, blockchain has developed into a wide range of variants that meet diverse demands in real-world scenarios.

In Figure 2, we show a generalized structure of the blockchain. It can be observed that the blocks append one after another in a virtual way. This is achieved by storing the hash value of the previous block header. In terms of a block, there are two key components: block header and block body, which are also shown in Figure 2. Usually, a block body simply contains the data to be stored in the form of transactions. A block header contains much more information, usually including the hash value of the previous block header, root of the hash tree, and so forth. The authentication of transactions is validated by an asymmetric cryptography mechanism [145]. Sometimes, in an untrustworthy environment, a digital signature might be used based on the asymmetric cryptography [146]. The detailed information of a general block header is shown as follows:

- **Version of block:** contains a cluster of block validation protocols to be followed
- **Hash of the previous block header:** appends to the last block with a 256-bit hash value
- **Merkle tree root:** represents all transactions with a 256-bit hash value
- **Timestamp:** is measured in seconds since the initial time
- **nBits:** is the current hashing target
- **Consensus:** contains the protocols and constraints to reach the consensus

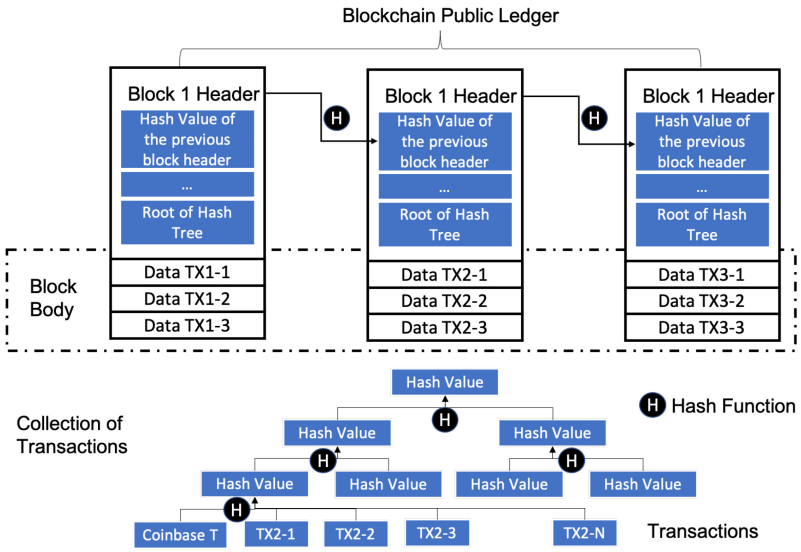

Fig. 2. A generalized structure of blockchain systems.

From the perspective of permission, blockchain is categorized into public blockchain [52, 147, 148], private blockchain [149–151], and consortium blockchain [152–154]. Regardless of the categorization, the basic workflow is the same in essence. A blockchain starts from a genesis block where some initial settings are stored, for example, the total number of tokens and the incentive mechanism. At least two types of users are required, which are miners and normal users. Miners generate their Proof of Contribution to obtain the opportunity to generate a candidate block, which is incentivized by rewards such as tokens. The candidate block is broadcast to all miners and then verified using cross-validation. If all miners or a selected committee can reach a consensus, the candidate block is appended to the end of the blockchain. To achieve decentralization, all nodes in the blockchain networks have a copy of the public ledger, which records all verified data.

2.3.2 Advantageous Features of Blockchain. In blockchain-enabled federated learning, the dedicated advantageous features are authentication and traceability, high availability, high scalability, decentralization, Byzantine resilience, persistence, and anonymity [54, 56, 140, 144]. These highlighting features can significantly improve the current FL paradigms in terms of privacy protection, accuracy, attack resistance, and so forth. A detailed explanation of each feature is as follows:

- **Authentication and Traceability:** Due to the excellent verification mechanisms, blockchain systems can ensure the authentication of the data. In addition, since the data is stored in the public ledger, it is recorded and traceable.
- **High Availability:** This allows the edge devices to join and leave the system and perform learning tasks anytime.
- **High Scalability:** The new paradigms enable high concurrency, high communication efficiency, and low storage complexity.
- **Decentralization:** The involvement of a centralized authority is minimized or even removed based on the specific design.
- **Byzantine Resilience:** Another advantage of blockchain is to be false-tolerant in terms of Byzantine issues, which is guaranteed by the high-class consensus mechanisms.

- **Persistency:** All transactions are confirmed and stored in each local public ledger, which makes it almost impossible to be falsified. Besides, the candidate block and corresponding transactions are verified by other nodes. Therefore, it is easy to detect any falsification.
- **Anonymity:** In a blockchain system, users interact with each other using a pseudo-name (such as address). Users are allowed to use multiple pseudo-names when necessary to avoid privacy leakage. No trusted central authority exists to maintain the privacy information of users and thereby the privacy could be preserved. However, privacy preservation is not perfect due to some built-in constraints of the blockchain systems.

The advantages of blockchain include but are not limited to the above ones. To better clarify, we skip the others to avoid the distraction of readers.

2.4 Further Discussion on the Integration of Blockchain and Federated Learning

In this part, we mainly focus on how blockchain benefits FL. In addition, we further discuss how FL potentially benefits blockchain for the readers' reference.

2.4.1 Discussion on How Blockchain Benefits FL. The advantageous features of blockchain discussed in Section 2.3.2 make joint efforts to address the three identified drawbacks of existing FL paradigms.

The first drawback of existing FL systems is centralized processing [55, 155, 156]. It leads to possible single-point failure, man-in-the-middle attack, and so forth [7, 135, 140, 157]. In addition, the volume of involved edge devices is so massive that the network overload becomes increasingly serious due to limited bandwidth and scalability. One of the greatest advantages of blockchain is decentralization (fully or partially) depending on if it is a public, private, or consortium blockchain [131]. The decentralization of FL can avoid potential single-point failure, man-in-the-middle attack, and so forth, by enabling a device to be the aggregator (central server) in a specific round [53]. The temporary aggregator is selected by a specific consensus algorithm such as PoW or PoS [49]. The pre-defined rules make sure that the selected device has enough computation and storage resources as well as high-quality data. Therefore, PoW is a better choice compared with other consensus algorithms in this particular scenario. In addition, blockchain has the potential to resist Byzantine issues, which is a primary issue in existing FL systems [48, 49]. The advanced consensus algorithms and high scalability make sure eligible updates of the end devices are recorded and used to generate the global updates [129]. In each round, only a part of the end devices are chosen based on their performance [158]. The rest of the end devices can compete for the next round by upgrading their equipment or improving the data quality. Either way contributes to the fast convergence of the current FL system with the impact of Byzantine issues.

The second drawback is the lack of an incentive mechanism. An emerging trend is that edge devices with high performance are not sufficiently incentivized to participate and contribute in an FL system [124, 159–161]. The reason is intuitive that high-performance devices may only gain marginal benefits by working with low-performance devices. But this situation could be significantly solved by the incentive mechanism provided by the blockchain systems. As an underlying structure, blockchain is able to provide rewards to users or miners in it [49]. The rewards could be token, which is the most popular form; data that is an asset in FL scenarios; or even more [125]. High availability also motivates the devices to participate. Since it is not compulsory for the end devices to be online on the time, the blockchain provides sufficient flexibility to them such that the high-performance devices still have priority to be chosen after returning from other tasks [134, 159, 162].

The third drawback is low robustness. Leading attacks such as poisoning attacks and Byzantine attacks mislead the training process and significantly impact the accuracy of the output, disable

the convergence of the maintained model, or even lead to denial of services [129, 130, 141, 142]. Security is an advanced built-in feature of blockchain, especially its high resistance to several leading attacks, such as background-knowledge attacks, collusion attacks, DDoS attacks, poisoning attacks, Byzantine attacks, and inference attacks. This is guaranteed by the authentication, traceability, persistence, anonymity, and high scalability of the blockchain [49]. Since the data cannot be falsified, which is ensured by authentication and traceability, poisoning attacks and inference are difficult to launch [7, 163]. High scalability and verification mechanisms help eliminate DDoS attacks and Byzantine attacks. Moreover, anonymity can defeat background knowledge attacks and collusion attacks to some extent.

2.4.2 Discussion on How FL Benefits Blockchain. We discuss how FL benefits blockchain from aspects of privacy-preserving cross-chain data exchange and a novel energy-saving consensus algorithm.

In addition to cryptocurrencies, most other real-world blockchain applications are based on consortium blockchain and private blockchain [49]. Therefore, cross-chain technology emerges to enable the data exchange of multiple blockchains. However, privacy issues are the main concern in this scenario. Federated learning and its variant, federated transfer learning, enables the privacy-preserving cross-chain data exchange of different blockchains by maintaining the same machine learning models [164, 165]. This is applicable to most cases where optimization or prediction is expected.

Federated learning also provides a potential direction for developing an energy-saving consensus algorithm. In most consensus algorithms, especially PoW-based ones, the miners contribute a huge amount of computation resources to compete for the blockchain generation opportunity, which leads to a huge waste of computation power [128, 166, 167]. However, if the consensus process can be integrated with the federated learning process, then no extra computation resources will be needed to perform a separate consensus algorithm. In this way, the computation power can be used for both federated learning and consensus at the same time, resulting in enormous energy savings [128].

2.4.3 Discussion on Overheads Brought by Blockchain in FL. In the above subsections, we have shown how blockchain and FL can mutually benefit each other. However, it is non-negligible that the integration of blockchain into FL may potentially result in extra communication and computation overheads.

In terms of computation overhead, the value varies significantly based on the deployed consensus algorithm. If it is a PoW-based consensus algorithm, a vast amount of computation overhead is required for the mining process, which is designed for generating a winning miner [168]. For PoS-based consensus algorithms, the computation overhead is low and has little impact on the system [154]. Another popular series of consensus algorithms, namely, committee-based algorithms, target deriving a tradeoff between PoW and PoS and is able to flexibly adjust to find an optimized balance between computation overhead and security. In addition, no matter what kind of consensus algorithm is deployed, the cross-validation process consumes a certain amount of computation overhead since the cross-validation in this context requires testing on the global model parameters by training the test datasets [49].

From the communication perspective, public blockchain may require all miners to broadcast the local model parameters to the whole network. If the number of miners is great, the communication overhead increases exponentially [128]. Besides, after the candidate block is generated, the propagation of the candidate block requires further communication overhead for all miners to send a verified acknowledgment of the authenticated data for consensus purposes. No matter what kind

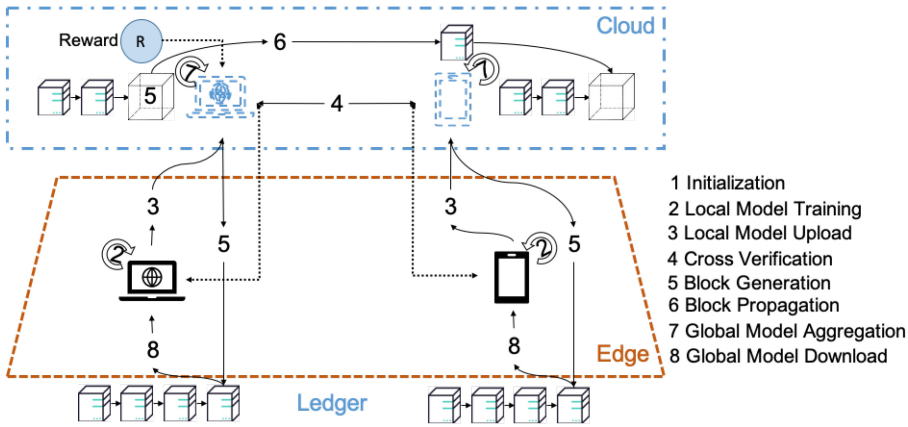

Fig. 3. A generalized blockchain-based FL paradigm.

of consensus algorithm is deployed, the consensus process is based on a massive amount of mutual communication in Peer-to-Peer networks [169, 170].

To mitigate the overheads brought by blockchain, new consensus algorithms are proposed. For example, Qu et al. proposed a **Proof of Federated Learning (PoFL)** in [128]. PoFL uses the computation overhead of local training in FL as the proof to reach the consensus, which reduces the mining power wastage caused by PoW. In this way, PoFL can significantly save the computation overhead. Another example is that Li et al. devised a novel committee-based consensus algorithm to reduce the communication overheads [129].

3 EXISTING RESEARCH STATUS OF BLOCKCHAIN-ENABLED FL

In this section, we present the generalized structure and workflow of blockchain-enabled FL as well as technical details of leading research.

3.1 A Generalized Architecture of Blockchain-enabled FL

The integration of blockchain and FL is natural. Both of them are distributed and privacy/security oriented [171]. Some issues of FL limit its further application and development, while blockchain can mitigate these issues with its self-existent advantages [55, 172]. Thus, a novel paradigm, namely, blockchain-enabled FL, is emerging and experiencing a fast boom. Directing against the three identified weaknesses, we demonstrate how blockchain can solve them with new architectures, new policies, or even more.

A generalized blockchain-based FL instance is shown in Figure 3. Different from the traditional FL systems, this structure allows fully decentralized FL such that each device can lead the aggregation process in a specific round of learning. In addition, all the local updates are verified before being processed. In this way, the performance of FL can be further improved.

In this context, we use *participants* to denote the entities taking part in the training process in classic FL and *miners* to denote all the participants of the blockchain-enabled federated learning system. In some reviewer papers, mechanisms are deployed to select a group of local models. The miners associated with the selected local models are defined as the *training miners*, who are involved in both the FL training and consensus processes. Besides, we name the miner who generates the candidate block as the *aggregation miner*. The detailed procedures are as follows:

Initialization: The parameters are randomly selected from a pre-defined objective function and the global gradient, which follows a uniform distribution.

Local model update: The end devices train the local model with respect to the required number of iterations.

Local model upload: Miners and end devices are bonded. The end device uploads the local model parameters to the miner. In addition, the corresponding local computation time is uploaded for verification purposes.

Cross-verification: The miners verify the associated end devices' model parameters and computing time in sequence. Whether the computing time is proportional to the size of data decides the reliability of the model parameters. The verified data is stored in the potential block of the miner until all model parameters are verified and stored in a block.

Block generation: A consensus algorithm runs in each round. It stops when a winning miner obtains the block generation opportunity and generates a candidate block while forcing the other miners to stop competing for the block generation opportunity.

Block propagation: The winning miner broadcasts the candidate block to all parties as a new block. All miners in the system append the new block on their local ledgers if verified. To prevent forking, a specially designed signal *ACK* is used and transmitted if a miner does not identify any forking. Every miner takes action after receiving *ACK* from all other miners. If not, the process will be suspended and the iteration restarted from the beginning.

Global model update: The selected miner aggregates all local model parameters by using **distributed approximate Newton (DANE)**, after which the new global parameters will be written into a block.

Global model download: All end devices are allowed to download the global parameters from the new block and decide to continue in the next round or not.

3.2 Existing Leading Research on Blockchain-enabled FL

For the readers' convenience, we show the existing leading research of blockchain-enabled FL with a description of technical details in Table 1. We provide the key technical details, experimental data distribution, machine learning model for FL, and datasets, respectively. Table 1 is able to demonstrate the big picture of current research status in terms of blockchain-enabled FL.

In the existing literature, researchers either focus on the dedicated blockchain-enabled FL for various application scenarios including on-device or **Internet of Vehicles (IoV)** or improve the performance from the perspectives of efficiency, reliability, or security and privacy.

Blockchain-enabled FL is experiencing fast popularization, especially for on-device scenarios. In [124–127, 158], the authors proposed several paradigms to achieve on-device blockchain-enabled FL. All the research considers horizontal federated learning where the data is **identical and independently distributed (IID)**. Besides, Qu et al. also consider the non-IID data problem in [126]. Excect for the search in [125], all models deploy **Convolutional Neural Network (CNN)** on various datasets including MovieLens, MNIST, and CIFAR10.

IoV is a special case of on-device scenarios that has become increasingly prevalent in recent several years. The vehicles in IoV hold extensive sensitive information of the drivers. Besides, most new vehicles, including electric vehicles and drones, are now equipped with high-performance CUP and storage, which provides a foundation for blockchain-enabled FL. In [130, 173, 174], the authors propose a consensus algorithm entitled Proof-of-Knowledge, analyze IoV dynamics, and devise a novel double-chain structure, respectively. Currently, only horizontal FL with IID data distribution is considered. Two types of ML models, CNN and **Multi-layer Perceptron (MLP),** are deployed on real-world datasets including MNIST, CIFAR10, and Uber pickups.

Since blockchain and FL are both resource-consuming techniques, numerous studies have been conducted to improve the efficiency of blockchain-enabled FL [175, 176]. In [161], Fan et al. propose to use payment channel techniques, while asynchronous global aggregation methods are proposed

Table 1. Blockchain-enabled Federated Learning

Group	Ref.[1]	Detail	Data Dist.[2]	Model	Dataset
On-device blockchain-enabed FL	[124]	CREAT: FL model parameter compression method with blockchain-based cross validation	H, I	CNN	MovieLens
	[125]	BlockFL: the pioneering work with basic structure definition and latency analysis	H, I	N/A	N/A
	[126]	D2C: Deployment for cognitive computing with Markov-decision-process-based poisoning attack resistance	H, I, N	CNN	MNIST, CIFAR10
	[127]	Blockchain-enabled FL for crowdsensing with differential privacy protection	H, I	CNN	MNIST
	[158]	Deep reinforcement learning optimization method to minimize time and computing power consumption	H, I	CNN	MNIST
Efficient blockchain-enabled FL	[161]	A hybrid blockchain-enabled FL that improves efficiency using payment channel technique	H, I	N/A	MNIST
	[162]	BAFL: Asynchronous blockchain-enabled FL that improves efficiency by asynchronous global aggregation and optimal block generation rate	H, I	CNN	MNIST
	[159]	DTWN: Using digital twin to deploy permissioned blockchain-enabled FL	H, I	CNN	CIFAR10
	[177]	BAFFLE: Allowing the local devices to locally update the global model parameters for personalized local FL	H, I	DNN	NYC Taxi
	[155]	Another pioneering research in Industrial Internet of Things (IIoT) that integrates differential privacy	H, I	N/A	Reuters
	[53]	Weight-based selection of local models with incentive mechanism	H, N	MLP	MNIST
	[128]	A novel and efficient consensus algorithm named Proof-of-Federated-Learning (PoFL)	H, I	N/A	CIFAR10
	[129]	BFLC: An efficient committee-based consensus mechanism with a tailor-designed storage pattern	H, I	N/A	FEMNIST

(Continued)

Table 1. Continued

Group	Ref.[1]	Detail	Data Dist.[2]	Model	Dataset
Reliable blockchain-enabled FL	[134]	VFChain: Reliable rotation of committee members with verifiable and audibility	H, I	CNN	MNIST
	[136, 137]	Improved reliability with an incentive mechanism based on reputation and contract theory	H, I	N/A	MNIST
	[135]	Poster: Reliable and accountable FL considering the immutability and decentralization of blockchain	H, I	N/A	Breast Cancer Dataset
	[131, 132]	FLchain and EFLchain: Ensemble learning where baseline global models are trained on the blockchain via federated learning (FLchain)	H, I, N	N/A	N/A
	[178]	Addressing data heterogeneity issue in IIoT device failure detection using a global aggregation algorithm named centroid distance weighted federated averaging	H, I	LR, NN	Air-conditioning
	[163]	Dymamic selection of participants to possess expected properties with a high probability in an iterative manner against unintended property leakage	H, I	CNN	LFW, MNIST, CelebA, CASIA
	[133]	Consortium blockchain-enabled FL for healthcare alliance with fine-grained access control	H, I, N	N/A	N/A
	[179]	An anomaly detection model using blockchain-enabled FL by auditing local models using advanced features of blockchain	H, I	CNN	CICIDS 2017
Blockchain-enabled FL for IoV	[173]	A novel consensus algorithm called Proof-of-Knowledge built upon a multi-leader and multi-player non-cooperative game	H, I	CNN, MLP	MNIST, CIFAR10
	[174]	Theoretical analysis on IoV dynamics considering wireless channels and cellular networks	H, I	N/A	N/A
	[130]	PermiDAG: Double-chain structure including a permissioned main blockchain and a local Directed Acyclic Graph (DAG) with asynchronous global aggregation	H, I	CNN	Uber pickups, MNIST

(Continued)

Table 1. Continued

Group	Ref.[1]	Detail	Data Dist.[2]	Model	Dataset
Private and Secure blockchain-enabled FL	[138]	Biscotti: Integrating several advanced technologies to resist leading attacks including Sybil attacks, information leakage attacks, and poisoning attacks	H, I	N/A	MNIST, Credit Card
	[139]	Differential privacy is used to preserve the privacy of local model gradients	H, V, I, N,	N/A	N/A
	[140]	PIRATE: Proposing a sharding-based blockchain protocol with an anomaly detection algorithm to defeat data falsification	H, I	SGD	N/A
	[141]	DeepChain: Collaborative machine learning with privacy protection and audibility of local model parameters	H, I	CNN	MNIST
	[142]	A novel normalization technique that can achieve a higher model accuracy than the traditional batch normalization	H, I	CNN	MNIST

[1]Reference paper that belongs to the specific group.
[2]Data distribution across nodes: H: horizontal, V: Vertical, I: IID, N: non-IID.

to accelerate the convergence speed in [162, 177]. In [159], Lu et al. put forward the digital twin-based method, which can reduce the latency. In [53, 128, 129], the authors conduct a local model selection procedure based on specific consensus algorithms. Almost all research considers the basic settings, namely, horizontal FL with IID data, except the research in [53], which can handle the non-IID problem. CNN, DNN, and MLP models are deployed on MNIST, FEMNIST, CIFAR10, NYC Taxi, and Reuters.

In addition to efficiency, researchers also aim at the enhancement of reliability. Reliability is improved using various technologies, including modification of consensus algorithms [134, 135], novel incentive mechanisms [136, 137], global aggregation using ensemble learning [131, 132], anomaly detection [178, 179], local model selection [163], and fine-grained access control [133]. Authors additionally consider the non-IID problem in [131–133] compared with other publications that only discuss horizontal FL with IID data. CNN, **Neural Networks (NNs)**, and **Logistic Regression (LR)** are deployed on real-world datasets including MNIST, Breast Cancer Dataset, LWF, CelebA, CASIA, and CICIDS 2017.

Although almost all of the relevant research discusses security or privacy, several models are specially established to address these issues in [138–142, 180]. We will comprehensively discuss the security and privacy of all existing research in Section 4.3. Nagar conduct early research to integrate differential privacy into blockchain-enabled FL [139]. In [138], Shayan et al. integrate several advanced technologies, including differential privacy and cryptography methods, to achieve high-level protection against Sybil attacks, poisoning attacks, and information leakage attacks. In [140, 141], blockchain systems are utilized or re-structured to provide additional protection by cross-validation and sharding, respectively. At last, Zhao et al. proposed a novel normalization

technique of the ML training process to achieve the expected protection [142]. The search in [139] considers both horizontal and vertical FL with IID and non-IID data, while the others only focus on horizontal FL with IID data. SGD and CNN are deployed on real-world datasets including MNIST and Credit Card.

4 ANALYSIS ON THE PERFORMANCE OF BLOCKCHAIN-ENABLED FL

In this section, we show how blockchain can mitigate the identified disadvantages of FL from three angles including decentralization, incentive mechanisms, and security and privacy resistance. The above-articulated research in this domain is analyzed in the following subsections.

4.1 Consensus-based Decentralization

This subsection focuses on the decentralization of FL and how the block generator selection impacts it from the perspective of the consensus algorithm. There are fully decentralized FL, partially decentralized FL, and a hybrid FL that is flexible to switch around. In this article, we consider all currently deployed consensus algorithms in blockchain-enabled FL, including PoW, PoS, PoFL, **Proof-of-Authority (PoA)**, **Practical Byzantine Fault Tolerance (PBFT)**, Committee-based ones, and **Proof-of-Quality (PoQ)**.

4.1.1 Decentralization. Blockchain-enabled FL has the potential to achieve fully decentralized FL, partially decentralized FL, or a hybrid one, considering the deployed consensus algorithm shown in Table 2. Fully decentralized FL allows each of the end devices the probability to lead a specific round of training processes and play the role of aggregator (central server). The probability is proportional to the resources it processes, including computing and storage power, quality of local data, network stability, and so forth. Partially decentralized FL allows a selected miner or a selected committee to achieve the consensus and decide the candidate block. Besides, some of the blockchain-enabled FL systems choose a flexible consensus algorithm (e.g., a committee-based one) such that it could be either fully decentralized or partially decentralized, which is also named hybrid in this context.

Fully decentralized FL is realized mostly due to the adoption of PoW, which is deployed in [125, 126, 139, 161, 162, 174, 178]. Therefore, nearly all blockchain-enabled FL can enable the fully distributed FL, which eliminates the risks of single-point failure, man-in-the-middle attack, and so forth. However, the performance of fully decentralized FL is constrained by the consensus algorithm and the selection mechanism, in which the aggregator and the end devices are chosen.

The partially decentralized FL can be achieved by several consensus algorithms, including committee-based ones [127, 129, 134, 136, 140, 163, 181, 182], PoFL [128, 138, 173], PoA [177], and PoQ [155]. The committee-based consensus algorithms select a group of committee members for fast convergence, while PoFL, PoA, and PoQ are variants of committee-based consensus algorithms that choose a committee member using a special rule that mainly considers local model accuracy.

The hybrid decentralized FL is determined by the consensus algorithm used by a certain system. In [124, 130, 139, 142, 158, 159, 162], the systems deployed PoS or **delegated Proof-of-Stake (DPoS)**, which is a flexible consensus algorithm that can achieve either the fully decentralized FL or the partially decentralized FL. PBFT is another popular consensus algorithm that achieves hybrid decentralized FL, which is adopted in [136, 142, 162, 174].

4.1.2 Consensus Algorithm and Membership Selection. To better enhance privacy protection while upgrading the learning performance, it is necessary to identify the trustful nodes with high-quality data. Blockchain can offer high-level membership selection methods to achieve final

Table 2. Consensus-based Decentralization of FL

	PoW	(D)PoS	PoFL	PoA	(P)BFT	Committee	PoQ	N/A
Kim et al. [55]	√	×	×	×	×	×	×	×
Preuveneers et al. [179]	×	×	×	×	×	√	×	×
Lu et al. [155]	×	×	×	×	×	×	√	×
Zhou et al. [140]	×	×	×	×	×	√	×	×
Kim and Hong [53]	×	×	×	×	×	×	×	√
Majeed and Hong [131]	×	×	×	×	×	×	×	√
Majeed and Hong [132]	×	×	×	×	×	×	×	√
Awan et al. [135]	×	×	×	×	×	×	×	√
Zhao et al. [127]	×	×	×	×	×	√	×	×
Qu et al. [128]	×	×	√	×	×	×	×	×
Kang et al. [137]	×	×	×	×	√	×	×	×
Passerat-Palmbach et al. [133]	×	×	×	×	×	×	×	√
Nagar et al. [139]	√	√	×	×	×	×	×	×
Ramanan et al. [177]	×	×	×	√	×	×	×	×
Weng et al. [141]	×	×	×	×	×	√	×	×
Qu et al. [126]	√	×	×	×	×	×	×	×
Chai et al. [173]	×	×	√	×	×	×	×	×
Pokhrel and Choi [174]	√	×	×	×	√	×	×	×
Lu et al. [130]	×	√	×	×	×	×	×	×
Lu et al. [158]	×	√	×	×	×	×	×	×
Li et al. [129]	×	×	×	×	×	√	×	×
Zhang et al. [178]	√	×	×	×	×	×	×	×
Zhao et al. [142]	×	√	×	×	√	×	×	×
Lu et al. [159]	×	√	×	×	×	×	×	×
Shayan et al. [183]	×	×	√	×	×	×	×	×
Cui et al. [124]	×	√	×	×	×	×	×	×
Peng et al. [134]	×	×	×	×	×	√	×	×
Kang et al. [160]	×	×	×	×	×	√	×	×
Fan et al. [161]	√	×	×	×	×	×	×	×
Shen et al. [163]	×	×	×	×	×	√	×	×
Feng et al. [162]	√	√	×	×	√	×	×	×

√ denotes (possible) deployment; × denotes not supported; N/A denotes not applicable or not specified.

consensus. Currently, there are a lot of representative membership selection methods, among which the most popular ones are PoW [55, 57] and PoS [179, 184]. In addition, the verification mechanism of blockchain can also help to manage the trustful nodes that significantly contribute to the learning process. The classification of current consensus algorithms and member selection methods corresponding to the decentralization status is shown in Table 2.

The consensus algorithm and member selection are two essential components of blockchain-enabled FL and are intercorrelated to each other. In this subsection, we discuss them as a whole in the following parts. As shown in Table 2, PoW is still the mainstream method adopted in this domain, where the applied rate is nearly 80%, which is consistent with a broader environment. In particular, PoW is regarded as the most feasible method in blockchain systems [57]. In all existing works, PoW is not fully discussed in detail. Usually, they choose the classic PoW algorithm used by

Bitcoin. However, the direct deployment of PoW in blockchain-based FL systems is not practical since efficiency is one of the primary indexes here [128]. In addition, since FL requires massive computation resources, it is impossible to provide extra computation power to reach a consensus with PoW. To address this issue, in [128], Qu et al. proposed a dedicated consensus algorithm built up with PoW, which is **Proof of FL (PoFL)**. PoFL tries to replace the nonce finding problem with a learning task, with which no extra computing power is required for the consensus process. However, how to maintain a stable consensus procedure using FL is barely analyzed. In addition, there are three methods adopting PoS to reach consensus [135, 177, 179]. Similarly, these three works directly use the classic PoS algorithm, which requires further modification for this scenario. Although the efficiency could be improved, there is a chance of secret mining attacks. This brings additional turbulence to the FL tasks. Nowadays, advanced systems are using the combination of PoW and PoS to maintain efficiency while guaranteeing security features, which is not mentioned in current works in this domain.

4.2 Incentive Mechanism

In most existing works, the incentive mechanism is mentioned as a key promotion when blockchain is leveraged as the underlying structure of FL. Then the incentive mechanism includes financial rewards like tokens, data rewards like preciser updates, or not specified.

The incentive mechanism solves the problem of fairness. In an FL system, there are various devices with different computational resources and data resources. Therefore, it is necessary that participants with better resources should have extra benefits compared to participants with little contribution. Otherwise, the capable participants lose their incentives to further contribute. In a traditional FL system, it is impossible to establish such an incentive mechanism due to its nature. That's why blockchain is essential in this case by introducing the incentive mechanism into the FL system. With this, the capable participants are active to share their local updates based on their superior computational and data resources.

As shown in Table 3, incentive mechanisms attract wide concern from researchers in FL cases, while blockchain is famous for its incentive mechanisms, such as Bitcoin. Therefore, tokens, as the most intuitive form of incentive, could be provided to participants of FL in this scenario, which is discussed in [53, 55, 127]. In all three of these models, tokens are provided to the participants. The tokens could be traded inside the system, or even gain financial value in the market, like Ethereum. In addition to the tokens, in [55], Kim et al. pointed out a direction in which we can use a data reward in a blockchain-enabled FL system. The rationale behind this is that data is the most important asset in FL systems; therefore, it is practical to reward the participants with data or model updates. However, a detailed incentive mechanism is not provided in this work. Beyond these two forms, there are several other works mentioning the incentive mechanism but that did not provide a specific one. Among these works, Nagar et al. carried out a novel methodology in which the rewards could be proportional to the contribution of the participants, compared to the fixed rewards in traditional scenarios [139]. As the incentive mechanism is an optional function of blockchain, there are two models not providing it to the participants [155, 179]. But the lack of an incentive mechanism partially invalidates the advantages of blockchain, which is a minor disadvantage of these two models.

4.3 Attack Resistance

As a new learning paradigm building upon current models, FL suffers from both traditional attacks and targeted unique attacks in various forms. These attacks may impact the accuracy of the output, disable the convergence of the maintained model, or even lead to denial of services, which is unacceptable to both service providers and service users.

Table 3. Incentive Mechanism

	Financial Rewards	Data Rewards	Not Specified	No Reward
Kim et al. [55]	√	√	×	×
Preuveneers et al. [179]	×	×	×	√
Lu et al. [155]	×	×	×	√
Zhou et al. [140]	×	×	√	×
Kim and Hong [53]	√	×	×	×
Majeed and Hong [131]	×	×	√	×
Majeed and Hong [132]	×	×	√	×
Awan et al. [135]	×	×	√	×
Zhao et al. [127]	√	×	×	×
Qu et al. [128]	×	×	√	×
Kang et al. [137]	×	×	√	×
Passerat-Palmbach et al. [133]	×	×	√	×
Nagar et al. [139]	×	×	√	×
Ramanan et al. [177]	×	×	√	×
Weng et al. [141]	√	√	×	×
Qu et al. [126]	×	×	×	√
Chai et al. [173]	×	×	×	√
Pokhrel and Choi [174]	×	×	√	×
Lu et al. [130]	√	×	×	×
Lu et al. [158]	×	×	√	×
Li et al. [129]	×	×	√	×
Zhang et al. [178]	×	×	√	×
Zhao et al. [142]	√	×	×	×
Lu et al. [159]	×	×	√	×
Shayan et al. [183]	×	×	√	×
Cui et al. [124]	×	×	√	×
Peng et al. [134]	×	×	√	×
Kang et al. [160]	×	×	√	×
Fan et al. [161]	×	×	√	×
Shen et al. [163]	√	×	×	×
Feng et al. [162]	×	×	√	×

√ denotes fully supported; × denotes not supported.

The leading attacks include background knowledge attacks [6], collusion attacks [185], **distributed denial of service attacks (DDoS)** [179], poisoning attacks [155], Byzantine attacks [140], and inference attacks [5].

The background knowledge attack is a far-reaching privacy-oriented attack that many other attacks stem from. In this scenario, each device has its own local data as its background knowledge data. Since it regularly receives the global model updates from a central authority, there is a possibility the device could launch background knowledge attacks based on the differences. This leads to privacy leakage to a certain extent.

The collusion attack is a specific type of background knowledge attack, where multiple parties contribute their background knowledge for aggregation so that more sensitive information might

be revealed. In an FL system, it is easy to launch such an attack since there are many devices that are free to join and leave.

The DDoS attack is also a classic attack but has some new features in this scenario. In a large-scale FL system, there might be thousands of edge devices participating in the learning task. This may cause over-occupation of the communication channels or overload of the computational resources. Subsequently, there might be high-latency or even physical failure of communication and computing infrastructure, hence resulting in a denial of service.

The poisoning attack is an increasingly popular leading attack in the data manipulation domain. The main target of these attacks is to mislead the learning output. In classic FL cases, there is no filter mechanism to select the devices or permission management on which devices could contribute. This gives adversaries the opportunity to upload specially designed falsified data, which may lead to either non-convergence or deviated outputs.

Byzantine attacks exist in the FL systems that allow flexible learning time. This is usually required in large-scale systems, in which diverse edge devices have various computation and communication powers. This leads to Byzantine issues since it is difficult to manage the edge devices and prevent the adversaries' malicious behaviors.

The inference attacks target categories of privacy by mounting tracing attacks and reconstruction attacks. These two forms of attacks negatively impact the performance of FL paradigms. By launching a reconstruction attack, the target of adversaries is to deduce the information within the records. With a tracing attack, the target switches to identify the existence of an individual in a specific dataset.

To defeat the attacks in different scenarios, some research has been conducted in the recent 2 years. The performance of current research against the leading attacks is shown in Table 4, which is followed by detailed discussions.

4.3.1 Performance against Background Knowledge Attack. From Table 4, we observe that most current models are incapable of defending background knowledge attacks. Although FL is designed to protect the privacy of local data stored on local devices, it has some built-in flaws. In the existing research of FL, non-IID data is a mainstream assumption, which guarantees the performance of FL. However, non-IID data means the universal form of the data is the background knowledge to all devices, and thereby, privacy leakage cannot be avoided if there are malicious inside adversaries. To address this, several add-on algorithms are put into current models to fully defend the attacks [127, 128, 155]. In [128], homomorphic cryptography is used to guarantee privacy when the data is shared among multiple parties. Although the efficiency is low and it requires extra design, the performance regarding privacy protection is satisfying. In [127, 155], differential privacy is used to preserve privacy. Differential privacy has superior performance to defend background knowledge attacks and collusion attacks [186, 187]. Therefore, these two models acquire privacy-preserving features by integrating differential privacy into blockchain-enabled FL. Besides, the models proposed in [53, 137, 139] have the potential to protect data against background knowledge attacks. This is because all three models have a membership selection phase using blockchain, which guarantees the number of edge devices participating in the learning process to some extent. But the privacy protection is not fully guaranteed because none of the three models gives a clear picture of the membership selection mechanism.

4.3.2 Performance against Collusion Attack. Moving on to the collusion attack, it is a specific form of background knowledge attack when multiple parties are involved. From our analysis, it could be observed that collusion attacks can be properly defended in about half of the blockchain-enabled FL systems. The collusion attacks are fully valid in [55, 131, 133, 140, 177] while partially valid in [132]. Similar to the background knowledge attack scenarios, the collusion-attack-resistant

Table 4. Performance against Attacks

	Background Knowledge Attack	Collusion Attack	DDoS Attack	Poisoning Attack	Byzantine Attack	Inference Attack
Kim et al. [55]	×	×	×	√	N/A	N/A
Preuveneers et al. [179]	×	√	√	√	√	×
Lu et al. [155]	√	√	×	√	N/A	N/A
Zhou et al. [140]	×	×	√	√	√	N/A
Kim and Hong [53]	N/A	√	×	√	×	N/A
Majeed and Hong [131]	×	×	×	√	N/A	×
Awan et al. [135]	×	√	N/A	√	N/A	√
Zhao et al. [127]	√	√	×	√	N/A	N/A
Majeed and Hong [132]	×	N/A	√	√	√	√
Qu et al. [128]	√	√	×	√	N/A	√
Kang et al. [137]	N/A	√	×	√	N/A	×
Passerat-Palmbach et al. [133]	×	×	×	√	N/A	N/A
Nagar et al. [139]	N/A	√	N/A	√	×	N/A
Ramanan et al. [177]	×	×	×	√	N/A	N/A
Weng et al. [141]	×	×	×	√	N/A	N/A
Qu et al. [126]	×	√	√	√	√	×
Chai et al. [173]	√	√	×	√	N/A	N/A
Pokhrel and Choi [174]	×	×	√	√	√	N/A
Lu et al. [130]	N/A	√	×	√	×	N/A
Lu et al. [158]	×	×	×	√	N/A	×
Li et al. [129]	×	√	N/A	√	N/A	√
Zhang et al. [178]	√	√	×	√	N/A	N/A
Zhao et al. [142]	×	N/A	√	√	√	√
Lu et al. [159]	√	√	×	√	N/A	√
Shayan et al. [183]	N/A	√	×	√	N/A	×
Cui et al. [124]	×	×	×	√	N/A	N/A
Peng et al. [134]	N/A	√	N/A	√	×	N/A
Kang et al. [160]	×	×	×	√	N/A	N/A
Fan et al. [161]	×	√	N/A	√	N/A	√
Shen et al. [163]	√	√	×	√	N/A	N/A
Feng et al. [162]	×	N/A	√	√	√	√

√ denotes fully resistant; × denotes not resistant; N/A denotes not applicable.

models benefit from cryptography, differential privacy, and member management. By contrast, the models fail to provide resistance to collusion attacks and suffer from various imperfect settings. First, in [140], the model suffers from Byzantine attacks, which are a variant of collusion attacks. Then, in the cases of [55, 133], the blockchain and FL are plugged together without any advanced privacy-aware and secure mechanisms, which makes them vulnerable to most attacks. This also indicates that it is not sufficient enough to simply replace the central authority of FL with a public ledger. Built upon the baseline models, the authors further improved the paradigms in [131, 177], in particular, by establishing the "global model state trie" and fully decentralizing the system using blockchain, respectively. However, lack of protection and member management mechanisms

result in poor performance against preventing collusion inside the learning systems, although performance against other types of attacks upgrades somehow. The only partially resistant model [132] is based on previous work [131]. In the baseline work [131], the replacement of central authority with blockchain provides some advanced features such as authentication of data. However, the involved edge devices can choose collusion without any constraints. To tackle this issue, the authors devised an ensemble learning model built upon the FL model. Ensemble learning allows contriving a strong model by combining several weaker models. With different underlying machine learning algorithms, diversity in hyper-parameters and enhanced accuracy can be obtained even using the same datasets. Since the model of each edge device is different, the background knowledge is different in format and it requires further computation and reasoning resources to launch collusion attacks. In most cases, the adversaries are less incentivized to collude with each other, which improves the resistance to a specific level.

4.3.3 Performance against DDoS Attack. From the aspect of the DDoS attack, current blockchain-based FL systems still need to be reinforced, especially in large-scale cases. From Table 4, there are only three models that can fully resist DDoS attacks [132, 140, 179], while two of them have the potential to resist [135, 139]. Traditional DDoS attacks are usually found in distributed systems where a large number of devices (bots) may be gathered to send requests to a central server to make it disabled when the server is overloaded. The blockchain-enabled FL systems face the same issue. As a distributed system, an adversary is able to hack or rent thousands of bots to launch such attacks by sending the model updates for aggregation simultaneously, which the system may not be able to undertake due to limited computation and communication resources. In most existing models, they enable high availability and allow the edge devices to join or leave with freedom, in which DDoS attacks are rooted. Therefore, the models failing to protect against DDoS attacks are those that are unable to manage members properly, such as [131]. In terms of the attack-proof models, several advanced methods are deployed. In [179], chained anomaly detection is the key contribution to monitor the behaviors of the participants. This model requires that the model updates are accountable and auditable so that any malicious devices can be detected and blacklisted. In future work, the authors plan to deal with the unreliable network connectivity and intermittently connected nodes to perfect the detection mechanism. Differently, the authors use a Byzantine-resistant feature to deal with DDoS attacks in [140]. This is a sharding-based blockchain system, in which the members are following the procedures of random committee selection, intra-committee consensus, and global consensus. This sharding-based method only aggregates the model updates of the committee members, and the other members can only function in the global consensus phase. In this way, communication traffic jams and computation overload are avoided. Another exceptional model is still the ensemble learning in [132]. The reason this model is attack proof is that it only has several high-quantity nodes. Dissimilar to the other blockchain-based FL models, it trains different machine learning models rather than the same one. Since effective machine learning models are few in number, only a few edge devices with high-quality data can be selected, and then tasks are performed on them. This disables the quantitative superiority of the adversaries and thereby defeats DDoS attacks. Two partially resistant models have their unique features as well. In [139], the model is built upon a consortium blockchain with a membership selection mechanism. The governess of a consortium blockchain is superior compared with the public blockchain, while membership selection could contribute from another angle. The performance of this model depends on the specific membership selection method and how the governess is defined. In [135], the authors leveraged homomorphic cryptography for data sharing. The advantage of this model is that malicious users may not be able to encrypt and decrypt the data with the right keys, while the disadvantage is that homomorphic cryptography brings in

extra communication and computation cost, which is a bottleneck regarding the defense of DDoS attacks.

4.3.4 Performance against Poisoning Attack. The poisoning attack is a type of leading attack in the machine learning domain. FL is an advanced learning paradigm that can accommodate all existing machine learning algorithms, such as reinforcement learning and deep learning. Therefore, FL suffers from poisoning attacks as well. Furthermore, since the local updates are from multiple edge devices, it is even more difficult to verify the authenticity of the uploaded data. The good news is that all existing models claim the resistance of poisoning attacks as one of the key contributions, like [155]. The resistance of poisoning attacks originates from the progressive features provided by the blockchain. Let's take the fully decentralized model in [155] as an example. In blockchain-enabled FL systems, all the learning participants can be regarded as the users in the blockchain, in which some of them are miners while the rest are just normal users. In each round, one of the participants can be the winner selected by Proof of Work or Proof of Stake [188]. The winner then collects the most recent transaction data (model updates in this case) and saves them in a block to append on a blockchain. Before storing the model updates, all the data should be verified by all members or a selected committee. The verified model updates are saved and used for further processing, while the falsified data is detected and discarded. In some of the blockchain systems, there is a trust management mechanism to give rewards or penalties to trustful or malicious users, respectively, such as [189]. This provides extra incentive to the miners who perform trustful operations in the system. Since falsified data can be identified, the poisoning attack can be defeated. Another thing worth mentioning is that poisoning attacks are evolving ceaselessly, which poses new threats to blockchain-enabled FL systems. For instance, in [190], a novel form of poisoning attack is proposed, in which the global model is poisoned and replaced so that the final outputs are inaccurate and misleading. As far as we know, current models barely took the improved poisoning attacks into consideration.

4.3.5 Performance against Byzantine Attack. The Byzantine attack is a type of primary attack in distributed systems. In blockchain-enabled systems, if most edge devices have similar computation and communication resources, then the system can set a fixed learning time for each round so that the Byzantine attacks can be eliminated. However, the widespread nature of FL determines that the application is increasingly wider in range. In different scenarios, there are various edge devices with diverse computation and communication resources, which results in different processing times. In this scenario, fixed learning time is not applicable and a Byzantine-resilient learning model is required. In existing research, most models fail to consider this dynamic scenario and thereby barely discuss Byzantine attacks in blockchain-enabled FL systems. There is only one model that cannot resist Byzantine attacks [139], while four of them can fully resist them [132, 140, 179]. The rest of the models can only partially defend the attacks to some extent. The authors are the first to propose the Byzantine attack issues in [140]. To solve this issue, the authors developed a sharding-based blockchain protocol so that model updates and gradient aggregations can be well protected. In [179], the model has the ability to detect anomalous behavior of edge devices as mentioned above, so it is Byzantine resilient by removing the malicious devices. The ensemble learning in [132] also has good performance against Byzantine attacks. The rationale is still the limited number of participants, which is easy to manage and coordinate. Similarly, in [53], the authors perform membership selection based on two indexes, which are local learning accuracy and participation frequency. By selecting legitimate members, this model can reduce the side impact of the Byzantine problem. In contrast, the model proposed in [139] performs poorly due to the adoption of a consortium blockchain. The consortium blockchain has several authorities and

operates in a relatively private scenario. It is hard to reach a proper consensus if the authorities do not work with each other in a trustful and cooperative way.

4.3.6 Performance against Inference Attack. Inference attacks are popular in FL scenarios. As mentioned above, inference attacks include two forms, which are tracking and reconstruction. As shown in Table 4, three out of all the models can fully resist inference attacks [128, 132, 135], while three of them cannot resist them [131, 137, 179]. The other models have the potential to resist inference attacks to a certain degree. In both [128, 135], homomorphic cryptography is leveraged to enable privacy-preserving data sharing. In this way, the data can be processed in cipher-text rather than plain-text, which prevents the adversaries from learning anything more based on pre-existing background knowledge. Differently, in [132], the heterogeneity of each learning model determines that the inference attacks cannot be performed. Each device has a unique machine learning task, while no one knows what machine learning tasks are running on other devices. Among the three non-resistant models, the one in [179] is the only model that can detect the anomaly. However, improving the detection accuracy requires gathering sensitive data for analysis and learning. The gathering of the data reveals some sensitive information or even leaks of more implicit information. The other two models cannot resist inference attacks because they only focus on the combination of FL and blockchain without considering other complex and privacy-preserving issues in this scenario.

5 OPEN ISSUES AND POTENTIAL SOLUTIONS

In this section, we present open issues in the blockchain-based FL as well as the corresponding potential solutions. Based on the above analysis, we systematically show how blockchain can moderate the negative impact of the three identified challenges. However, existing research fails to fully address the issues in all scenarios. Through the following discussion, we aim at shedding light on future research directions of this under-explored domain for upcoming readers and researchers.

5.1 Improving Performance of Decentralized FL

From the perspectives of advanced consensus algorithms and optimal tradeoff, we discuss how to improve the performance of decentralized FL to fill the gap between existing research and real-world application.

5.1.1 Green and Energy-effective Consensus Algorithms. Blockchain-enabled FL systems need PoW to guarantee security and other performance since PoW can fully ensure the decentralized feature and subsequently guarantee the performance of FL. But the traditional PoW requires a massive volume of computation power to compete for the block generation power, which results in the degradation of learning performance. An instance is that the power consumption of Bitcoin mining is slightly higher than the total consumption of Switzerland. Therefore, it is essential to modify the current PoW consensus algorithm into an energy-efficient one so that more computation power remains for the learning process.

One potential solution is to replace the nonce-finding problem with an FL task. By setting a learning accuracy threshold, the system can reach a PoW consensus. By this means, all the computation power is used in the training and learning tasks and the devices failing in the competition also contribute to the convergence. This method can help build a personalized incentive mechanism discussed in the following subsections. With careful design, blockchain and FL are mutually beneficial to each other. If the PoW procedure is achieved by FL tasks, no extra computation power is wasted. In this way, the energy could be saved, while the learning performance could be lifted simultaneously.

5.1.2 Trade-off between Learning Performance vs. Others. Although learning performance is the primary priority in the FL systems, other indexes, such as convergence efficiency, privacy protection level, energy consumption, and block generation rate, should also be considered. Therefore, it is vital to work out the optimal tradeoff between learning performance and other indexes.

Usually, an optimized tradeoff can be derived from a pair of contrary indexes. In terms of learning accuracy vs. convergence efficiency, one potential solution is to develop blockchain-based asynchronous and semi-asynchronous FL systems. The optimized blockchain-based asynchronous and semi-asynchronous FL are believed to reach a comparable learning accuracy with significant efficiency improvement.

The tradeoff between learning accuracy and privacy protection is considered but not well addressed in existing research. The direct implementation of differential privacy or homophobic encryption is not applicable. Differential privacy harms the data utility of local model parameters, while homophobic encryption is highly resource consuming. This might be tackled by novel differential privacy mechanisms that target data utility improvement. For example, generative adversarial nets can be used to add controllable random noise to achieve differential privacy, while game theory can better optimize the injected noise volume based on real-world demands.

The balance between learning accuracy and energy consumption also attracts a lot of attention. The energy wastage is mainly caused by the consensus process of blockchain. Therefore, it is reasonable to develop novel consensus algorithms to mitigate these issues. For example, there is the potential to use the local training computation power of FL to work as a proof of contribution such that the consensus algorithm no longer needs the resource-consuming mining process. Besides, the local model contribution of each round could be used as the proof as well. In this context, more variants of Pow and PoS can be developed to achieve efficient and secure consensus. In this way, a considerable amount of computation power can be saved.

From the aspect of the block generation rate, it is a more complex index that may need to consider convergence efficiency, privacy protection, energy usage, and so forth. Therefore, the tradeoff here should be a multi-objective optimization problem. In a particular scenario, the **nondominated sorting genetic algorithm 2 (NSGA-2)** has the potential to derive the tradeoff since it is a multi-objection optimization algorithm. After carefully designing the objective function of the model, NSGA-2 is able to achieve optimization in finite time. By modifying NSGA-2 and fitting it into blockchain-enabled FL systems, we can generate a flexible and generalized optimization model and extend it into any specific scenarios by adjusting the parameters in the pre-defined objective function. However, with a multi-objection problem it can be hard to configure the parameters and the optimization toward each index is usually limited.

5.2 Promoting the Sense of Participation

To further motivate all end devices to participate in the learning process, especially the high-performance end devices, we propose to implement a personalized incentive mechanism and optimize the member selection mechanism based on game theory.

5.2.1 Personalized Incentive Mechanism. In traditional blockchain systems, the incentive mechanism is a distributing token and the number of rewards is usually fixed for the winner or a group of winners. This is not applicable to blockchain-enabled FL. The participants have different computation power and the contribution is dependent on the quality of data as well. As mentioned in Section 5.1.1, all participants make contributions to the learning convergence, and subsequently, all contributors should be rewarded, unlike the traditional blockchain systems.

Thus, we propose a novel personalized incentive mechanism. Based on the green and energy-effective consensus algorithm we mentioned in Section 5.1.1, all participants work together to

reach the consensus and everyone is part of the winning group. In this case, if we use the token as an example, then the token is distributed to everyone proportional to the contribution. Besides, the incentive could be two-fold. For devices that are not selected as participants of the learning process, they can pay tokens to the winners to gain access to the new global model. Moreover, the incentive mechanism should be diverse in form, such as a data reward or even a computation power reward corresponding to the specific scenarios.

5.2.2 Optimal Member Selection Based on Game Theory. In a large-scale FL system, all devices want to participate in the learning process and improve their local model with the help of a federation. However, the quality of data and the power of devices are of great difference. Since the aggregation of local updates costs a lot of computation power, it is necessary to choose devices with high-quality data and high computation power. In a traditional blockchain, this could be achieved by PoW or PoS, which is not perfectly feasible in this particular scenario.

To address this issue, it is possible to use a dynamic game process based on the Markov decision process. It is hard to select the optimal devices at their first place, so it may take several iterations to optimize the selected devices. We can model the contribution of devices and the improvement of the global model as two actions. Then, built upon the actions and system states, we use a QoS-based payoff function to finalize the objective function. Reinforcement learning methods, such as Q-learning and SARSA, can be used to derive the Nash Equilibrium of the game, which is the optimal batch of devices.

5.3 Advancing the Security and Privacy Level

Security and privacy are the key factors through which FL can successfully reach a convergence and have a proper output. To deal with emerging security and privacy issues, we suggest conducting attack-proof performance upgradation, redactable FL with blockchain, and privacy-preserving FL model update sharing.

5.3.1 Attack-proof Performance Upgradation. In nearly all the existing works, the authors claimed that poisoning attacks can be eliminated due to the verification mechanism of blockchain. However, in a non-transaction scenario, the authentication of data is hard to verify because the data lacks causality. In FL, the poisoning attacks generate falsified local model updates, which can be verified iff the expected updates are pre-known. In addition, novel poisoning attacks are emerging with new features as mentioned in Section 4.3, which pose additional challenges to guarantee the authenticity of the data. Moreover, there are various other attacks that jointly bring negative impacts to current blockchain-enabled FL systems.

To address this, we plan to design new protocols based on the current blockchain system and establish a trust management system. Rather than establishing a committee randomly, we propose an iterated committee based on a trust value. At first, the system trains the data with random committees and identifies the convergence tendency. Then any committee members who upload the local updates and contribute to the convergence will gain a higher trust value and vice versa. In this way, the system can gradually eliminate the negative impact of poisoning attacks. The iterated mechanism can be optimized with advanced tools such as convex optimization. In terms of other attacks, new mechanisms are also required in different scenarios. In the following subsections, we propose several other open issues and try to address the attack issues combined with them by implementing other theories, such as differential privacy and game theory.

5.3.2 Redactable FL with Blockchain. Although existing models have the potential to prevent poisoning attacks, they cannot fully prevent malicious data manipulation. Thus, it is reasonable to ask for a redactable mechanism to revise the generated blocks. In addition, some of the sensitive

model updates may require further privacy protection after it is aggregated in a specific iteration of learning. This requires redactable operations as well.

Motivated by this, we plan to use a modified Chameleon-hash function, which is also known as trapdoor-hash functions. They are hash functions that feature a trapdoor that allows one to find arbitrary collisions in the domain of the functions. With a modified version, we replace the normal hash function such as SHA256. This enables a roll-back when a misleading global update is identified in the next round when a redactable consensus is achieved. This guarantees a remedial measure that current systems haven't considered.

5.3.3 Privacy-preserving Model Update Sharing. The privacy of model updates has long been an issue for FL. Although the usage of blockchain can guarantee the authenticity of the data, it raises other concerns. All participants are able to see the model updates of others for verification. If there are malicious users launching stealthy attacks secretly, the publicly accessed data turns into the disadvantage of this system. Therefore, a privacy-preserving update-sharing model is urgently demanded.

To solve this issue, differential privacy could be used. If the model updates are processed with differentially private mechanisms, the privacy of data could be preserved but some noise is injected into the model updates. With a large number of devices participating in the learning process, this side effect can be eliminated since the noise usually complies with the Laplace mechanism, in which the mean value is zero.

6 SUMMARY AND CONCLUSION

Blockchain-enabled FL has been and will keep generating widespread attention in this big data era. However, the existing paradigms become increasingly impractical and difficult to follow from both perspectives of introductory and in-depth exploration of state-of-the-art models. To tackle this issue, we focus on three crucial issues of blockchain-enabled FL, which are decentralization, incentive mechanism, and membership selection. We systematically introduce the evaluation matrix and analysis criteria. In addition, we categorize the leading attacks and evaluate the performance of all existing countermeasures in a systematic manner. The amount of novel schemes for blockchain-enabled FL grows by the month. Despite this, we believe this survey is sufficiently comprehensive that new schemes can be appended and categorized correspondingly. Improvements to this may include the quantitative measurement and analysis of the schemes. This survey provides clear insights into the picture of blockchain-enabled FL from a brand-new perspective. We anticipate this work to be helpful to the community, providing potentially promising directions and simplifying future designs, including but not limited to motivating coherent compositions uncovered by the proposed categorization and analysis.

REFERENCES

[1] Michael I. Jordan and Tom M. Mitchell. 2015. Machine learning: Trends, perspectives, and prospects. *Science* 349, 6245 (2015), 255–260.

[2] Kate Crawford and Ryan Calo. 2016. There is a blind spot in AI research. *Nature* 538, 7625 (2016), 311–313.

[3] Yoshua Bengio et al. 2009. Learning deep architectures for AI. *Foundations and Trends® in Machine Learning* 2, 1 (2009), 1–127.

[4] Yuji Roh, Geon Heo, and Steven Euijong Whang. 2019. A survey on data collection for machine learning: A big data-AI integration perspective. *IEEE Transactions on Knowledge and Data Engineering* 33 (2019), 1328–1347.

[5] Milad Nasr, Reza Shokri, and Amir Houmansadr. 2019. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In *2019 IEEE Symposium on Security and Privacy (SP'19)*. IEEE, 739–753.

[6] Zhibo Wang, Mengkai Song, Zhifei Zhang, Yang Song, Qian Wang, and Hairong Qi. 2019. Beyond inferring class representatives: User-level privacy leakage from federated learning. In *IEEE Conference on Computer Communications (IEEE INFOCOM'19)*. IEEE, 2512–2520.

[7] Youyang Qu, Longxiang Gao, Tom H. Luan, Yong Xiang, Shui Yu, Bai Li, and Gavin Zheng. 2020. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal* 7 (2020), 5171–5183.

[8] Anand D. Sarwate and Kamalika Chaudhuri. 2013. Signal processing and machine learning with differential privacy: Algorithms and challenges for continuous data. *IEEE Signal Processing Magazine* 30, 5 (Sept. 2013), 86–94. DOI: http://dx.doi.org/10.1109/MSP.2013.2259911

[9] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology* 10, 2 (2019), 12:1–12:19. http://arxiv.org/abs/1902.04885 arXiv: 1902.04885.

[10] EU. 2006. Regulation (EU) 2016/679 of the european parliament and of the council. https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/.

[11] WeBank AI Group. 2018. Federated learning white paper V1.0. *Technical Report* (2018).

[12] Kamalika Chaudhuri, Claire Monteleoni, and Anand D. Sarwate. 2011. Differentially private empirical risk minimization. *Journal of Machine Learning Research* 12 (2011), 1069–1109.

[13] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep learning with differential privacy. In *ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. 308–318. DOI: http://dx.doi.org/10.1145/2976749.2978318

[14] Roger Iyengar, Joseph P. Near, and Dawn Song. 2019. Towards practical differentially private convex optimization. In *ACM Conference on Computer and Communications Security (CCS'19)*. 299–316.

[15] V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft. 2013. Privacy-preserving ridge regression on hundreds of millions of records. In *2013 IEEE Symposium on Security and Privacy*. 334–348.

[16] Jiawei Yuan and Shucheng Yu. 2014. Privacy preserving back-propagation neural network learning made practical with cloud computing. *IEEE Transactions on Parallel and Distributed Systems* 25, 1 (2014), 212–221.

[17] Raphael Bost, Raluca Ada Popa, Stephen Tu, and Shafi Goldwasser. 2015. Machine learning classification over encrypted data. In *Proceedings 2015 Network and Distributed System Security Symposium*.

[18] Payman Mohassel and Peter Rindal. 2018. ABY^3: A mixed protocol framework for machine learning. In *ACM SIGSAC Conference on Computer and Communications Security*. 35–52.

[19] Valerie Chen, Valerio Pastro, and Mariana Raykova. 2018. Secure computation for machine learning with SPDZ. In *International Conference on Neural Information Processing Systems (NIPS'18)*.

[20] Bita Darvish Rouhani and M. Sadegh Riazi. 2018. DeepSecure: Scalable provably-secure deep learning. In *55th ACM/ESDA/IEEE Design Automation Conference (DAC'18)*. 1–6.

[21] Geetha Jagannathan and Rebecca N. Wright. 2005. Privacy-preserving distributed k-means clustering over arbitrarily partitioned data. In *Proceeding of the 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining (KDD'05)*. ACM Press, 593–599. DOI: http://dx.doi.org/10.1145/1081870.1081942

[22] Jakub Konecny, H. Brendan McMahan, and Peter Richtarik. 2016. Federated optimization: Distributed machine learning for on-device intelligence. *Computing Research Repository (CoRR)* (2016), 38.

[23] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtarik, Ananda Theertha Suresh, and Dave Bacon. 2016. Federated learning: Strategies for improving communication efficiency. In *NIPS Workshop on Private Multi-Party Machine Learning*.

[24] H. Brendan McMahan, Eider Moore, Daniel Ramage, and Blaise Agüera y Arcas. 2016. Federated learning of deep networks using model averaging. *ArXiv* abs/1602.05629 (2016).

[25] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise AgÃijera y Arcas. 2017. Communication-efficient learning of deep networks from decentralized data. In *20th International Conference on Artificial Intelligence and Statistics (AISTATS'17)*. 1273–1282.

[26] Hangyu Zhu and Yaochu Jin. 2019. Multi-objective evolutionary federated learning. *IEEE Transactions on Neural Networks and Learning Systems* (2019), 1–13. DOI: http://dx.doi.org/10.1109/TNNLS.2019.2919699

[27] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. 2019. Federated optimization in heterogeneous networks. *arXiv:1812.06127* (2019).

[28] Virginia Smith, Chao-Kai Chiang, Maziar Sanjabi, and Ameet S. Talwalkar. 2017. Federated multi-task learning. In *International Conference on Neural Information Processing Systems (NIPS'17)*.

[29] Yang Chen, Xiaoyan Sun, and Yaochu Jin. 2019. Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation. *IEEE Transactions on Neural Networks and Learning Systems* (2019), 1–10.

[30] Guangxu Zhu, Yong Wang, and Kaibin Huang. 2020. Broadband analog aggregation for low-latency federated edge learning. *IEEE Transactions on Wireless Communications* 19, 1 (2020), 491–506.

[31] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. 2016. Federated learning: Strategies for improving communication efficiency. In *International Conference on Neural Information Processing Systems (NIPS'16)*.

[32] Sebastian Caldas, Jakub Konečny, H. Brendan McMahan, and Ameet Talwalkar. 2019. Expanding the reach of federated learning by reducing client resource requirements. *arXiv:1812.07210* (2019).
[33] Felix Sattler, Simon Wiedemann, Klaus-Robert Müller, and Wojciech Samek. 2019. Robust and communication-efficient federated learning from non-IID data. *arXiv:1903.02891 [cs, stat]* (March 2019). http://arxiv.org/abs/1903.02891 arXiv: 1903.02891.
[34] Yujun Lin, Song Han, Huizi Mao, Yu Wang, and William J. Dally. 2018. Deep gradient compression: Reducing the communication bandwidth for distributed training. In *International Conference on Learning Representations*.
[35] Hanlin Tang, Shaoduo Gan, Ce Zhang, Tong Zhang, and Ji Liu. 2018. Communication compression for decentralized training. In *International Conference on Neural Information Processing Systems (NIPS'18)*.
[36] Wei Liu, Li Chen, Yunfei Chen, and Wenyi Zhang. 2020. Accelerating federated learning via momentum gradient descent. *IEEE Transactions on Parallel and Distributed Systems* 31, 8 (2020), 1754–1766.
[37] Fei Chen, Zhenhua Dong, Zhenguo Li, and Xiuqiang He. 2018. Federated meta-learning for recommendation. *arXiv:1802.07876* (2018).
[38] Luca Corinzia and Joachim M. Buhmann. 2019. Variational federated multi-task learning. *arXiv:1906.06268* (2019).
[39] Hubert Eichner, Tomer Koren, H. Brendan McMahan, Nathan Srebro, and Kunal Talwar. 2019. Semi-cyclic stochastic gradient descent. In *36th International Conference on Machine Learning*.
[40] Mikhail Khodak, Maria-Florina F. Balcan, and Ameet S. Talwalkar. 2019. Adaptive gradient-based meta-learning methods. In *International Conference on Neural Information Processing Systems (NIPS'19)*. 5917–5928.
[41] Eunjeong Jeong, Seungeun Oh, Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. 2018. Communication-efficient on-device machine learning: Federated distillation and augmentation under non-IID private data. In *International Conference on Neural Information Processing Systems (NIPS'18)*.
[42] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, and Dusit Niyato. 2019. Mobile edge computing, blockchain and reputation-based crowdsourcing IoT federated learning: A secure, decentralized and privacy-preserving system. *CoRR* (2019).
[43] Li Huang, Yifeng Yin, Zeng Fu, Shifa Zhang, Hao Deng, and Dianbo Liu. 2019. LoAdaBoost:Loss-based adaboost federated machine learning on medical data. *arXiv:1811.12629* (2019).
[44] Mehryar Mohri, Gary Sivek, and Ananda Theertha Suresh. 2019. Agnostic federated learning. In *36th International Conference on Machine Learning*.
[45] Tian Li, Maziar Sanjabi, and Virginia Smith. 2020. Fair resource allocation in federated learning. In *International Conference on Learning Representations*.
[46] István Hegedűs, Gábor Danner, and Márk Jelasity. 2021. Decentralized learning works: An empirical comparison of gossip learning and federated learning. *Journal of Parallel and Distributed Computing* 148 (2021), 109–124.
[47] István Hegedűs, Gábor Danner, and Márk Jelasity. 2019. Decentralized recommendation based on matrix factorization: A comparison of gossip and federated learning. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*. Springer, 317–332.
[48] Stefano Savazzi, Monica Nicoli, and Vittorio Rampa. 2020. Federated learning with cooperating devices: A consensus approach for massive IoT networks. *IEEE Internet of Things Journal* 7, 5 (2020), 4641–4654.
[49] Laphou Lao, Zecheng Li, Songlin Hou, Bin Xiao, Songtao Guo, and Yuanyuan Yang. 2020. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Computing Surveys (CSUR)* 53, 1 (2020), 1–32.
[50] Thang N. Dinh and My T. Thai. 2018. AI and blockchain: A disruptive integration. *Computer* 51, 9 (Sept. 2018), 48–53. DOI: http://dx.doi.org/10.1109/MC.2018.3620971
[51] Khaled Salah, M. Habib Ur Rehman, Nishara Nizamuddin, and Ala Al-Fuqaha. 2019. Blockchain for AI: Review and open research challenges. *IEEE Access* 7 (2019), 10127–10149. DOI: http://dx.doi.org/10.1109/ACCESS.2018.2890507
[52] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation* 2, 6–10 (2016), 71.
[53] You Jun Kim and Choong Seon Hong. 2019. Blockchain-based node-aware dynamic weighting methods for improving federated learning performance. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS'19)*. IEEE, 1–4.
[54] Guy Zyskind, Oz Nathan, et al. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*. IEEE, 180–184.
[55] Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. 2019. Blockchained on-device federated learning. *IEEE Communications Letters* (2019), 1279–1283.
[56] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang. 2018. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering* 30, 7 (2018), 1366–1385.

[57] Arthur Gervais, Ghassan O . Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 3–16.

[58] Dinh C. Nguyen, Ming Ding, Quoc-Viet Pham, Pubudu N. Pathirana, Long Bao Le, Aruna Seneviratne, Jun Li, Dusit Niyato, and H. Vincent Poor. 2021. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal* 8 (2021), 12806–12825.

[59] Mansoor Ali, Hadis Karimipour, and Muhammad Tariq. 2021. Integration of blockchain and federated learning for internet of things: Recent advances and future challenges. *Computers & Security* (2021), 102355.

[60] Mohammed Aledhari, Rehma Razzak, Reza M. Parizi, and Fahad Saeed. 2020. Federated learning: A survey on enabling technologies, protocols, and applications. *IEEE Access* 8 (2020), 140699–140725.

[61] Ahmed Imteaj, Urmish Thakker, Shiqiang Wang, Jian Li, and M. Hadi Amini. 2021. A survey on federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal* 9 (2021), 1–24.

[62] Rongfei Zeng, Chao Zeng, Xingwei Wang, Bo Li, and Xiaowen Chu. 2021. A comprehensive survey of incentive mechanism for federated learning. *arXiv preprint arXiv:2106.15406* (2021).

[63] Yufeng Zhan, Jie Zhang, Zicong Hong, Leijie Wu, Peng Li, and Song Guo. 2021. A survey of incentive mechanism design for federated learning. *IEEE Transactions on Emerging Topics in Computing* 10 (2021), 1035–1044.

[64] Latif U. Khan, Walid Saad, Zhu Han, Ekram Hossain, and Choong Seon Hong. 2021. Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials* 23 (2021), 1759–1799.

[65] Latif U. Khan, Shashi Raj Pandey, Nguyen H. Tran, Walid Saad, Zhu Han, Minh N. H. Nguyen, and Choong Seon Hong. 2020. Federated learning for edge networks: Resource optimization and incentive mechanism. *IEEE Communications Magazine* 58, 10 (2020), 88–93.

[66] Knud Lasse Lueth. 2018. State of the IoT 2018: Number of IoT devices now at 7B âĂŞ market accelerating. *IOT Analytics* (2018).

[67] Adrian Nilsson, Simon Smith, Gregor Ulm, Emil Gustavsson, and Mats Jirstrand. 2018. A performance evaluation of federated learning algorithms. In *2nd Workshop on Distributed Infrastructures for Deep Learning*. 1–8.

[68] Jihong Park, Sumudu Samarakoon, Mehdi Bennis, and Merouane Debbah. 2019. Wireless network intelligence at the edge. *Proceedings of the IEEE* 107, 11 (Nov. 2019), 2204–2239. DOI: http://dx.doi.org/10.1109/JPROC.2019.2941458

[69] Olivia Choudhury, Aris Gkoulalas-Divanis, Theodoros Salonidis, Issa Sylla, Yoonyoung Park, Grace Hsu, and Amar Das. 2019. Differential privacy-enabled federated learning for sensitive health data. *arXiv:1910.02578* (2019).

[70] Raghu Ganti, Fan Ye, and Hui Lei. 2011. Mobile crowdsensing: Current state and future challenges. *IEEE Communications Magazine* 49, 11 (Nov. 2011), 32–39.

[71] Rudiger Pryss, Manfred Reichert, Jochen Herrmann, Berthold Langguth, and Winfried Schlee. 2015. Mobile crowd sensing in clinical and psychological trials – A case study. In *IEEE 28th International Symposium on Computer-based Medical Systems*. 23–24.

[72] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. 2015. Deep learning. *Nature* 521, 7553 (May 2015), 436–444.

[73] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub KoneÄĮnÃ¡, Stefano Mazzocchi, H. Brendan McMahan, Timon Van Overveldt, David Petrou, Daniel Ramage, and Jason Roselander. 2019. Towards federated learning at scale: System design. In *2nd SysML Conference*. 374–388.

[74] Muhammad Ammad-ud din, Elena Ivannikova, Suleiman A. Khan, Were Oyomno, Qiang Fu, Kuan Eeik Tan, and Adrian Flanagan. 2019. Federated collaborative filtering for privacy-preserving personalized recommendation system. *arXiv:1901.09888* (2019).

[75] Andrew Hard, Kanishka Rao, Rajiv Mathews, Swaroop Ramaswamy, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. 2019. Federated learning for mobile keyboard prediction. *arXiv:1811.03604* (2019).

[76] Li Huang, Andrew L. Shea, Huining Qian, Aditya Masurkar, Hao Deng, and Dianbo Liu. 2019. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. *Journal of Biomedical Informatics* 99, 103291 (Nov. 2019).

[77] Swaroop Ramaswamy, Rajiv Mathews, Kanishka Rao, and Françoise Beaufays. 2019. Federated learning for emoji prediction in a mobile keyboard. *arXiv:1906.04329* (2019).

[78] Santiago Silva, Boris A. Gutman, Eduardo Romero, Paul M. Thompson, Andre Altmann, and Marco Lorenzi. 2019. Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data. In *16th International Symposium on Biomedical Imaging (ISBI'19)*. 270–274.

[79] John C. Duchi, Michael I. Jordan, and Martin J. Wainwright. 2012. Privacy aware learning. In *International Conference on Neural Information Processing Systems (NIPS'12)*. 1–57.

[80] Cynthia Dwork and Aaron Roth. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science* 9, 3–4 (2014), 211–407.
[81] Nicholas Carlini, Chang Liu, ÃŽlfar Erlingsson, Jernej Kos, and Dawn Song. 2019. The secret sharer: Evaluating and testing unintended memorization in neural networks. *arXiv:1802.08232* (2019).
[82] Naman Agarwal, Ananda Theertha Suresh, Felix Yu, Sanjiv Kumar, and H. Brendan Mcmahan. 2018. cpSGD: Communication-efficient and differentially-private distributed SGD. In *International Conference on Neural Information Processing Systems (NIPS'18)*.
[83] Abhishek Bhowmick, John Duchi, Julien Freudiger, Gaurav Kapoor, and Ryan Rogers. 2019. Protection against reconstruction and its applications in private federated learning. *arXiv:1812.00984* (2019).
[84] Robin C. Geyer, Tassilo Klein, and Moin Nabi. 2018. Differentially private federated learning: A client level perspective. *arXiv:1712.07557* (2018).
[85] H. Brendan McMahan, Daniel Ramage, Kunal Talwar, and Li Zhang. 2018. Learning differentially private recurrent language models. In *International Conference on Learning Representations*.
[86] Om Thakkar, Galen Andrew, and H. Brendan McMahan. 2019. Differentially private learning with adaptive clipping. *arXiv:1905.03871* (2019).
[87] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. 2017. Practical secure aggregation for privacy-preserving machine learning. In *Conference on Computer and Communications Security*. 1175–1191.
[88] Badih Ghazi, Rasmus Pagh, and Ameya Velingker. 2019. Scalable and differentially private distributed aggregation in the shuffled model. *arXiv:1906.08320* (2019).
[89] Guowen Xu, Hongwei Li, Sen Liu, Kan Yang, and Xiaodong Lin. 2019. VerifyNet: Secure and verifiable federated learning. *IEEE Transactions on Information Forensics and Security* 15 (2019), 911–926.
[90] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. 2020. Differentially private asynchronous federated learning for mobile edge computing in urban informatics. *IEEE Transactions on Industrial Informatics* 16, 3 (2020), 2134–2143.
[91] Jeffrey Dean, Greg S. Corrado, Rajat Monga, Kai Chen, Matthieu Devin, Quoc V. Le, Mark Z. Mao, Marc'Aurelio Ranzato, Andrew Senior, Paul Tucker, Ke Yang, and Andrew Y. Ng. 2012. Large scale distributed deep networks. In *International Conference on Neural Information Processing Systems (NIPS'12)*.
[92] Daniel Povey, Xiaohui Zhang, and Sanjeev Khudanpur. 2014. Parallel training of deep neural networks with natural gradient and parameter averaging. In *International Conference on Artificial Intelligence and Statistics (AISTATS'14)*.
[93] Sixin Zhang, Anna Choromanska, and Yann LeCun. 2015. Deep learning with elastic averaging SGD. In *International Conference on Neural Information Processing Systems (NIPS'15)*.
[94] Junxian Huang, Feng Qian, Yihua Guo, Yuanyuan Zhou, Qiang Xu, Z. Morley Mao, Subhabrata Sen, and Oliver Spatscheck. 2013. An in-depth study of LTE: Effect of network protocol and application behavior on performance. *ACM SIGCOMM Computer Communication Review* 43, 4 (2013), 363–374.
[95] C. H. van Berkel. 2009. Multi-core for mobile phones. In *Conference on Design, Automation and Test in Europe*.
[96] Ofer Dekel, Ran Gilad-Bachrach, Ohad Shamir, and Lin Xiao. 2012. Optimal distributed online prediction using mini-batches. *Journal of Machine Learning Research* 13 (2012), 165–202.
[97] Zheng Qu, Peter Richtarik, and Tong Zhang. 2015. Quartz: Randomized dual coordinate ascent with arbitrary sampling. In *International Conference on Neural Information Processing Systems (NIPS'15)*.
[98] Peter Richtárik and Martin Takáč. 2016. Distributed coordinate descent method for learning with big data. *Journal of Machine Learning Research* 17 (2016), 1–12.
[99] Shai Shalev-Shwartz and Tong Zhang. 2013. Accelerated mini-batch stochastic dual coordinate ascent. In *International Conference on Neural Information Processing Systems (NIPS'13)*.
[100] Ohad Shamir and Nathan Srebro. 2014. Distributed stochastic optimization and learning. In *52nd Annual Allerton Conference on Communication, Control, and Computing*. 850–857.
[101] Virginia Smith, Simone Forte, Chenxin Ma, Martin Takáč, Michael I. Jordan, and Martin Jaggi. 2018. CoCoA: A general framework for communication-efficient distributed optimization. *Journal of Machine Learning Research* 18 (2018), 1–49.
[102] Sebastian U. Stich. 2019. Local SGD converges fast and communicates little. In *International Conference on Learning Representations*.
[103] Martin Jaggi, Virginia Smith, Martin Takac, Jonathan Terhorst, Sanjay Krishnan, Thomas Hofmann, and Michael I. Jordan. 2014. Communication-efficient distributed dual coordinate ascent. In *International Conference on Neural Information Processing Systems (NIPS'14)*.
[104] Ching-pei Lee and Dan Roth. 2015. Distributed box-constrained quadratic optimization for dual linear SVM. In *32nd International Conference on Machine Learning*. 987–996.

[105] Chenxin Ma, Virginia Smith, Martin Jaggi, Michael I. Jordan, Peter Richtárik, and Martin Takáč. 2015. Adding vs. averaging in distributed primal-dual optimization. In *International Conference on Machine Learning*. 1973–1982.
[106] Tianbao Yang. 2013. Trading computation for communication: Distributed stochastic dual coordinate ascent. In *International Conference on Neural Information Processing Systems (NIPS'13)*.
[107] Benjamin Recht, Christopher Re, Stephen Wright, and Feng Niu. 2011. Hogwild: A lock-free approach to parallelizing stochastic gradient descent. In *International Conference on Neural Information Processing Systems (NIPS'11)*.
[108] Rie Johnson and Tong Zhang. 2013. Accelerating stochastic gradient descent using predictive variance reduction. In *International Conference on Neural Information Processing Systems (NIPS'13)*.
[109] Hongyi Wang, Scott Sievert, Zachary Charles, Shengchao Liu, Stephen Wright, and Dimitris Papailiopoulos. 2018. ATOMO: Communication-efficient learning via atomic sparsification. In *International Conference on Neural Information Processing Systems (NIPS'18)*.
[110] Hantian Zhang, Jerry Li, Kaan Kara, Dan Alistarh, Ji Liu, and Ce Zhang. 2017. ZipML: Training linear models with end-to-end low precision, and a little bit of deep learning. In *34th International Conference on Machine Learning*. 4035–4043.
[111] Frank Seide, Hao Fu, Jasha Droppo, Gang Li, and Dong Yu. 2015. 1-Bit stochastic gradient descent and its application to data-parallel distributed training of speech DNNs. In *15th Annual Conference of the International Speech Communication Association*.
[112] Felix Sattler, Simon Wiedemann, Klaus-Robert Muller, and Wojciech Samek. 2019. Robust and communication-efficient federated learning from non-i.i.d. data. *IEEE Transactions on Neural Networks and Learning Systems* (2019), 1–14.
[113] Sebastian Thrun and Lorien Pratt. 2012. *Learning to Learn*. Springer Science & Business Media.
[114] Rich Caruana. 1997. Multitask learning. *Machine Learning* 28, 1 (1997), 41–75.
[115] Theodoros Evgeniou and Massimiliano Pontil. 2004. Regularized multi–task learning. In *International Conference on Knowledge Discovery and Data Mining*. 109–117.
[116] Jinho Choi and Shiva Raj Pokhrel. 2019. Federated learning with multichannel ALOHA. *IEEE Wireless Communications Letters* (2019), 499–502.
[117] Wei Dai, Abhimanu Kumar, Jinliang Wei, Qirong Ho, Garth Gibson, and Eric P. Xing. 2015. High-performance distributed ML at scale through parameter server consistency models. In *29 AAAI Conference on Artificial Intelligence*.
[118] Qirong Ho, James Cipar, Henggang Cui, Seunghak Lee, Jin Kyu Kim, Phillip B. Gibbons, Garth A. Gibson, Greg Ganger, and Eric P. Xing. 2013. More effective distributed ML via a stale synchronous parallel parameter server. In *International Conference on Neural Information Processing Systems (NIPS'13)*.
[119] Martin Zinkevich, Markus Weimer, Lihong Li, and Alex J. Smola. 2010. Parallelized stochastic gradient descent. In *International Conference on Neural Information Processing Systems (NIPS'10)*.
[120] Krishna Pillutla, Sham M. Kakade, and Zaid Harchaoui. 2019. Robust aggregation for federated learning. *Technical Report* (2019).
[121] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. 2016. Practical secure aggregation for federated learning on user-held data. In *International Conference on Neural Information Processing Systems (NIPS'16)*.
[122] Takayuki Nishio and Ryo Yonetani. 2019. Client selection for federated learning with heterogeneous resources in mobile edge. In *International Conference on Communications (ICC'19)*. 1–6.
[123] Jiawen Kang, Zehui Xiong, Dusit Niyato, Han Yu, Ying-Chang Liang, and Dong In Kim. 2019. Incentive design for efficient federated learning in mobile networks: A contract theory approach. In *IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS'19)*. 1–5.
[124] Laizhong Cui, Xiaoxin Su, Zhongxing Ming, Ziteng Chen, Shu Yang, Yipeng Zhou, and Wei Xiao. 2020. CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing. *IEEE Internet of Things Journal* (2020).
[125] Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. 2019. Blockchained on-device federated learning. *IEEE Communications Letters* (2019), 1–1. DOI: http://dx.doi.org/10.1109/LCOMM.2019.2921755
[126] Youyang Qu, Shiva Raj Pokhrel, Sahil Garg, Longxiang Gao, and Yong Xiang. 2020. A blockchained federated learning framework for cognitive computing in industry 4.0 networks. *IEEE Transactions on Industrial Informatics* 17 (2020), 2964–2973.
[127] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, and Dusit Niyato. 2019. Mobile edge computing, blockchain and reputation-based crowdsourcing IoT federated learning: A secure, decentralized and privacy-preserving system. *arXiv preprint arXiv:1906.10893* (2019).
[128] Xidi Qu, Shengling Wang, Qin Hu, and Xiuzhen Cheng. 2021. Proof of federated learning: A novel energy-recycling consensus algorithm. *IEEE Transactions on Parallel and Distributed Systems* 32, 8 (2021), 2074–2085.

[129] Yuzheng Li, Chuan Chen, Nan Liu, Huawei Huang, Zibin Zheng, and Qiang Yan. 2020. A blockchain-based decentralized federated learning framework with committee consensus. *IEEE Network* 35 (2020), 234–241.
[130] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. 2020. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology* 69, 4 (2020), 4298–4311.
[131] Umer Majeed and Choong Seon Hong. 2019. FLchain: Federated learning via MEC-enabled blockchain network. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS'19)*. IEEE, 1–4.
[132] Umer Majeed and Choong Seon Hong. n.d. EFLChain: Ensemble learning via federated learning over blockchain network: A framework. ([n. d.]), 845–847.
[133] Jonathan Passerat-Palmbach, Tyler Farnan, Robert Miller, Marielle S. Gross, Heather Leigh Flannery, and Bill Gleim. 2019. A blockchain-orchestrated federated learning architecture for healthcare consortia. *arXiv preprint arXiv:1910.12603* (2019).
[134] Zhe Peng, Jianliang Xu, Xiaowen Chu, Shang Gao, Yuan Yao, Rong Gu, and Yuzhe Tang. 2021. VFChain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Transactions on Network Science and Engineering* 9 (2021), 173–186.
[135] Sana Awan, Fengjun Li, Bo Luo, and Mei Liu. 2019. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2561–2563.
[136] Jiawen Kang, Zehui Xiong, Dusit Niyato, Han Yu, Ying-Chang Liang, and Dong In Kim. 2019. Incentive design for efficient federated learning in mobile networks: A contract theory approach. In *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS'19)*. IEEE, 1–5. DOI: http://dx.doi.org/10.1109/VTS-APWCS.2019.8851649
[137] Jiawen Kang, Zehui Xiong, Dusit Niyato, Yuze Zou, Yang Zhang, and Mohsen Guizani. 2019. Reliable federated learning for mobile networks. *arXiv preprint arXiv:1910.06837* (2019).
[138] Muhammad Shayan, Clement Fung, Chris J. M. Yoon, and Ivan Beschastnikh. 2019. Biscotti: A ledger for private and secure peer-to-peer machine learning. *arXiv:1811.09904 [cs, stat]* (Feb. 2019). http://arxiv.org/abs/1811.09904 arXiv: 1811.09904.
[139] Anudit Nagar. 2019. Privacy-preserving blockchain based federated learning with differential data sharing. *arXiv preprint arXiv:1912.04859* (2019).
[140] Sicong Zhou, Huawei Huang, Wuhui Chen, Zibin Zheng, and Song Guo. 2019. PIRATE: A blockchain-based secure framework of distributed machine learning in 5G networks. *arXiv preprint arXiv:1912.07860* (2019).
[141] Jiasi Weng, Jian Weng, Jilian Zhang, Ming Li, Yue Zhang, and Weiqi Luo. 2019. Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing* 18 (2019), 2438–2455.
[142] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. 2020. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet of Things Journal* 8 (2020), 1817–1829.
[143] Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-peer Electronic Cash System*. Technical Report. Manubot.
[144] Christopher Natoli, Jiangshan Yu, Vincent Gramoli, and Paulo Esteves-Verissimo. 2019. Deconstructing blockchains: A comprehensive survey on consensus, membership and structure. *IEEE Communications Surveys & Tutorials* (2019).
[145] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, and Helge Janicke. 2018. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal* 6, 2 (2018), 2188–2204.
[146] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services* 14, 4 (2018), 352–375.
[147] Yutao Jiao, Ping Wang, Dusit Niyato, and Kongrath Suankaewmanee. 2019. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. *IEEE Transactions on Parallel and Distributed Systems* 30, 9 (2019), 1975–1989.
[148] Lei Xu, Nolan Shah, Lin Chen, Nour Diallo, Zhimin Gao, Yang Lu, and Weidong Shi. 2017. Enabling the sharing economy: Privacy respecting contract based on public blockchain. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. 15–21.
[149] Mengmeng Yang, Tianqing Zhu, Kaitai Liang, Wanlei Zhou, and Robert H. Deng. 2019. A blockchain-based location privacy-preserving crowdsensing system. *Future Generation Computer Systems* 94 (2019), 408–418.
[150] Sara Rouhani and Ralph Deters. 2017. Performance analysis of ethereum transactions in private blockchain. In *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS'17)*. IEEE, 70–74.
[151] Tien Tuan Anh Dinh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan. 2017. Blockbench: A framework for analyzing private blockchains. In *Proceedings of the 2017 ACM International Conference on Management of Data*. 1085–1100.

[152] Keke Gai, Yulu Wu, Liehuang Zhu, Meikang Qiu, and Meng Shen. 2019. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Transactions on Industrial Informatics* 15, 6 (2019), 3548–3558.
[153] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. 2017. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics* 14, 8 (2017), 3690–3700.
[154] Jiawen Kang, Zehui Xiong, Dusit Niyato, Ping Wang, Dongdong Ye, and Dong In Kim. 2018. Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks. *IEEE Wireless Communications Letters* 8, 1 (2018), 157–160.
[155] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. 2019. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics* 16 (2019), 4177–4186.
[156] Lei Cui, Youyang Qu, Gang Xie, Deze Zeng, Ruidong Li, Shigen Shen, and Shui Yu. 2021. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Transactions on Industrial Informatics* 18 (2021), 3492–3500.
[157] Yinghui Liu, Youyang Qu, Chenhao Xu, Zhicheng Hao, and Bruce Gu. 2021. Blockchain-enabled asynchronous federated learning in edge computing. *Sensors* 21, 10 (2021), 3335.
[158] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. 2021. Blockchain and federated learning for 5G beyond. *IEEE Network* 35 (2021), 219–225.
[159] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. 2020. Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks. *IEEE Transactions on Industrial Informatics* 17 (2020), 5098–5107.
[160] Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. 2019. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal* 6, 6 (2019), 10700–10714.
[161] Sizheng Fan, Hongbo Zhang, Yuchen Zeng, and Wei Cai. 2020. Hybrid blockchain-based resource trading system for federated learning in edge computing. *IEEE Internet of Things Journal* 8 (2020), 2252–2264.
[162] Lei Feng, Yiqi Zhao, Shaoyong Guo, Xuesong Qiu, Wenjing Li, and Peng Yu. 2021. Blockchain-based asynchronous federated learning for internet of things. *IEEE Transactions on Computers* 71 (2021), 1092–1103.
[163] Meng Shen, Huan Wang, Bin Zhang, Liehuang Zhu, Ke Xu, Qi Li, and Xiaojiang Du. 2020. Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing. *IEEE Internet of Things Journal* 8 (2020), 2265–2275.
[164] Wang Xiaoding, Sahil Garg, Hui Lin, Md Jalilpiran, Jia Hu, and M. Shamim Hossain. 2021. Enabling secure authentication in industrial IoT with transfer learning empowered blockchain. *IEEE Transactions on Industrial Informatics* 17 (2021), 7725–7733.
[165] Xiantao Jiang, F. Richard Yu, Tian Song, Zhaowei Ma, Yanxing Song, and Daqi Zhu. 2020. Blockchain-enabled cross-domain object detection for autonomous driving: A model sharing approach. *IEEE Internet of Things Journal* 7, 5 (2020), 3681–3692.
[166] Evangelos Pournaras. 2019. Proof of witness presence: Blockchain consensus for augmented democracy in smart cities. *arXiv:1907.00498 [cs]* (Oct. 2019). http://arxiv.org/abs/1907.00498 arXiv: 1907.00498.
[167] Ali Shoker. 2018. Brief announcement: Sustainable blockchains through proof of exercise. In *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing (PODC'18)*. ACM Press, 269–271. DOI: http://dx.doi.org/10.1145/3212734.3212781
[168] Sunny King. n.d. Primecoin: Cryptocurrency with prime number proof-of-work. 6.
[169] Dana Yang, Seohee Yoo, Inshil Doh, and Kijoon Chae. 2021. Selective blockchain system for secure and efficient D2D communication. *Journal of Network and Computer Applications* 173 (2021), 102817.
[170] Rateb Jabbar, Noora Fetais, Mohamed Kharbeche, Moez Krichen, Kamel Barkaoui, and Mohammed Shinoy. 2021. Blockchain for the internet of vehicles: How to use blockchain to secure vehicle-to-everything (V2X) communication and payment? *IEEE Sensors Journal* 21 (2021), 15807–15823.
[171] D. N. Dillenberger, P. Novotny, Q. Zhang, P. Jayachandran, H. Gupta, S. Hans, D. Verma, S. Chakraborty, J. J. Thomas, M. M. Walli, et al. 2019. Blockchain analytics and artificial intelligence. *IBM Journal of Research and Development* 63, 2/3 (2019), 5–1.
[172] U. Majeed and C. S. Hong. 2019. FLchain: Federated learning via MEC-enabled blockchain network. In *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, IEEE, 1–4.
[173] Haoye Chai, Supeng Leng, Yijin Chen, and Ke Zhang. 2020. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems* 22 (2020), 3975–3986.
[174] Shiva Raj Pokhrel and Jinho Choi. 2020. Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Transactions on Communications* 68, 8 (2020), 4734–4746.

[175] Chenhao Xu, Youyang Qu, Yong Xiang, and Longxiang Gao. 2021. Asynchronous federated learning on heterogeneous devices: A survey. *arXiv preprint arXiv:2109.04269* (2021).
[176] Chenhao Xu, Youyang Qu, Peter W. Eklund, Yong Xiang, and Longxiang Gao. 2021. BAFL: An efficient blockchain-based asynchronous federated learning framework. In *2021 IEEE Symposium on Computers and Communications (ISCC'21)*. IEEE, 1–6.
[177] Paritosh Ramanan, Kiyoshi Nakayama, and Ratnesh Sharma. 2019. BAFFLE: Blockchain based aggregator free federated learning. *arXiv preprint arXiv:1909.07452* (2019).
[178] Weishan Zhang, Qinghua Lu, Qiuyu Yu, Zhaotong Li, Yue Liu, Sin Kit Lo, Shiping Chen, Xiwei Xu, and Liming Zhu. 2020. Blockchain-based federated learning for device failure detection in industrial IoT. *IEEE Internet of Things Journal* 8 (2020), 5926–5937.
[179] Davy Preuveneers, Vera Rimmer, Ilias Tsingenopoulos, Jan Spooren, Wouter Joosen, and Elisabeth Ilie-Zudor. 2018. Chained anomaly detection models for federated learning: An intrusion detection case study. *Applied Sciences* 8, 12 (2018), 2663.
[180] Yichen Wan, Youyang Qu, Longxiang Gao, and Yong Xiang. 2021. Privacy-preserving blockchain-enabled federated learning for B5G-driven edge computing. *Computer Networks* (2021), 108671.
[181] Davy Preuveneers, Vera Rimmer, Ilias Tsingenopoulos, Jan Spooren, Wouter Joosen, and Elisabeth Ilie-Zudor. 2018. Chained anomaly detection models for federated learning: An intrusion detection case study. *Applied Sciences* 8, 12 (Dec. 2018), 2663. DOI: http://dx.doi.org/10.3390/app8122663
[182] Jiasi Weng, Jian Weng, Jilian Zhang, Ming Li, Yue Zhang, and Weiqi Luo. 2019. DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing* 18 (2019), 2438–2455. DOI: http://dx.doi.org/10.1109/TDSC.2019.2952332
[183] Muhammad Shayan, Clement Fung, Chris J. M. Yoon, and Ivan Beschastnikh. 2020. Biscotti: A blockchain system for private and secure federated learning. *IEEE Transactions on Parallel and Distributed Systems* 32 (2020), 1513–1525.
[184] Paul Cos, Arnold J. Vlietinck, Dirk Vanden Berghe, and Louis Maes. 2006. Anti-infective potential of natural products: How to develop a stronger in vitro "proof-of-concept." *Journal of Ethnopharmacology* 106, 3 (2006), 290–302.
[185] Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. 2019. Exploiting unintended feature leakage in collaborative learning. In *2019 IEEE Symposium on Security and Privacy (SP'19)*. IEEE, 691–706.
[186] Cynthia Dwork. 2008. Differential privacy: A survey of results. In *International Conference on Theory and Applications of Models of Computation*. Springer, 1–19.
[187] Youyang Qu, Shui Yu, Wanlei Zhou, Sancheng Peng, Guojun Wang, and Ke Xiao. 2018. Privacy of things: Emerging challenges and opportunities in wireless internet of things. *IEEE Wireless Communications* 25, 6 (2018), 91–97.
[188] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. 2017. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*. Springer, 357–388.
[189] Matthew Ritter. 2015. *Repcoin: The Only Reputation Market*. Ph.D. Dissertation. Dartmouth College.
[190] Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. 2018. How to backdoor federated learning. *arXiv preprint arXiv:1807.00459* (2018).

Received 7 May 2020; revised 22 November 2021; accepted 28 February 2022