future internet

Review

A Survey on Blockchain-Based Federated Learning

Lang Wu, Weijian Ruan *, Jinhui Hu and Yaobin He

China Electronics Technology Group Corporation (CETC), Key Laboratory of Smart City Model Simulation and Intelligent Technology, The Smart City Research Institute of CETC and National Center for Applied Mathematics Shenzhen (NCAMS), Shenzhen 518038, China; wulang@cetc.com.cn (L.W.); hujinhui@cetc.com.cn (J.H.); heyaobin@cetc.com.cn (Y.H.)

* Correspondence: ruanweijian@cetc.com.cn

Abstract: Federated learning (FL) and blockchains exhibit significant commonality, complementarity, and alignment in various aspects, such as application domains, architectural features, and privacy protection mechanisms. In recent years, there have been notable advancements in combining these two technologies, particularly in data privacy protection, data sharing incentives, and computational performance. Although there are some surveys on blockchain-based federated learning (BFL), these surveys predominantly focus on the BFL framework and its classifications, yet lack in-depth analyses of the pivotal issues addressed by BFL. This work aims to assist researchers in understanding the latest research achievements and development directions in the integration of FL with blockchains. Firstly, we introduced the relevant research in FL and blockchain technology and highlighted the existing shortcomings of FL. Next, we conducted a comparative analysis of existing BFL frameworks, delving into the significant problems in the realm of FL that the combination of blockchain and FL addresses. Finally, we summarized the application prospects of BFL technology in various domains such as the Internet of Things, Industrial Internet of Things, Internet of Vehicles, and healthcare services, as well as the challenges that need to be addressed and future research directions.

Keywords: blockchain; federated learning; security and privacy; Internet of Things

check for updates

Citation: Wu, L.; Ruan, W.; Hu, J.; He, Y. A Survey on Blockchain-Based Federated Learning. *Future Internet* **2023**, *15*, 400. https://doi.org/10.3390/fi15120400

Academic Editor: Giovanni Pau

Received: 8 November 2023
Revised: 30 November 2023
Accepted: 1 December 2023
Published: 12 December 2023

1. Introduction

Currently, artificial intelligence (AI) technology is advancing rapidly, transitioning from its invention phase a few years ago to the phase of practical application. AI technology is being applied in an increasing number of scenarios. However, as algorithms and computing power have significantly improved, there is a growing demand for larger datasets and increased emphasis on data privacy protection. How to meet the data requirements of AI models in this context has become an urgent challenge in the development of AI technology today.

Presently, machine learning (ML) algorithms increasingly rely on vast amounts of data. However, the reality is that, due to privacy constraints, data are scattered across different organizations. Therefore, the current development of AI faces two challenges: the data silo problem and issues related to data security and privacy. Firstly, the data silo problem greatly limits the availability of big data. Despite the internet generating billions of data daily, there is a lack of useful, high-dimensional, high-quality data. Secondly, countries worldwide are strengthening their data security protection and privacy. Strict regulations on user data privacy and security management are becoming a global trend. Without providing users with reliable privacy protection methods, the issue of data insufficiency will severely restrict the development of AI.

Due to these factors, the emerging ML technique, federated learning (FL) [1,2], has become a popular research topic in the field of ML. The main idea of FL is to enable a large number of user devices that store data locally (referred to as clients) to collaboratively train a single ML model without the need to share their raw data. For example, data from different hospitals are often isolated, creating data silos. Because each data silo has limitations in terms of data size and approximation to the actual distribution, a single hospital may struggle to train and attain high-quality models with high prediction accuracy for specific tasks. Ideally, if multiple hospitals could collaborate and combine their data to train ML models collectively, more accurate training results could be achieved. However, due to various policies and regulations, data cannot be easily shared between hospitals. Similarly, the data silo phenomenon is prevalent in many other fields, including finance, government, and supply chains. Additionally, policies like the general data protection regulation (GDPR) [3] set rules for data sharing between different organizations. As a result, developing an FL method that can deliver excellent prediction accuracy while adhering to policies and regulations to protect privacy is a highly challenging endeavor.

In addition, FL also has its unique set of challenges. Primarily, the paradigm often necessitates the involvement of a considerable number of users with diverse cultural backgrounds and intricate behavioral patterns, complicating mutual trust and augmenting the risk of inadvertent privacy breaches for honest participants [4–8]. FL protects users' sensitive data by keeping the source data local and only exchanging model updates, such as gradient information. However, research indicates that gradient information can leak users' private data [9–15]. Attackers can indirectly infer label information and dataset membership information through the gradient information uploaded by clients. Carlini et al. [13] extracted sensitive user data, such as specific bank card numbers, from a recursive neural network trained on users' language data. Fredrikson et al. [10] investigated how to steal data privacy from model information and conducted inversion attacks on linear regression models through dosage prediction experiments, obtaining sensitive patient information. Hitaj et al. [12] launched attacks on model aggregation using generative adversarial networks (GANs). The experimental results show that malicious clients can steal users' data privacy by generating similar local model updates. Gei et al. [15] demonstrated the feasibility of reconstructing input data from gradient information, independent of the deep network architecture, and recovered a batch of input images using cosine similarity and adversarial attack methods. Secondly, the attainment of a global model in FL involves multiple iterative rounds of model updates from users, engendering significant communication overhead and incurring additional storage costs during network transmission [16,17]. Moreover, the distinction between federated learning and distributed computing lies in the fact that the dataset in FL comes from various end-user terminals, and the features of data generated by these users are often non-independent and non-identically distributed (non-IID). Traditional distributed framework algorithms perform well only when dealing with independent and identically distributed (IID) data, while they encounter challenges such as difficulty in convergence and excessive communication rounds when handling non-IID data [18]. Thirdly, the integrity of the global model may be compromised due to malevolent participants or a central server susceptible to cyber-attacks [19]. Lastly, the local devices involved could themselves be malicious or vulnerable to exploitation, potentially resulting in the unauthorized disclosure or manipulation of transmitted information [20].

In recent years, blockchain technology, originating from Bitcoin, has undergone rapid advancement [21]. Built upon a decentralized peer-to-peer network architecture, blockchains ensure that transactional data are stored across all network nodes, while its immutability and consistency are guaranteed by consensus algorithms. Innovatively establishing decentralized trust, blockchain technology allows individuals to opt for believing in the reliability of cryptographic algorithms and the honesty of the majority of nodes within the peer-to-peer network, rather than being compelled to place trust in a single entity [22]. This mechanism of decentralized trust offers a new avenue for augmenting the capabilities of FL. For instance, FL can not only leverage the consistency provided by blockchain's consensus mechanisms to establish trustworthy interactions within an untrusted environment but can also utilize the economic property derived from blockchain's incentive schemes to effectively promote information sharing within the federated ecosystem. Through the accumulated technical advancements in FL and blockchains over the years, as well as their exploration and applications in various relevant fields, blockchain-based federated learning (BFL) has gained the capability and prospects for applications in highly privacy-sensitive industries. Due to the advantages of blockchain in areas such as identity verification, decentralization, traceability, and immutability, many research efforts have used blockchains as underlying structures for FL. They achieve distributed model aggregation tasks by designing protocols on top of the blockchain. While blockchain is an effective way to replace the central server in FL and enhances security in the storage and update processes of FL models, it also introduces new challenges in FL application scenarios, such as training efficiency, resource allocation, and communication delays.

At present, limited literature exists that explores the integration of blockchain and FL. Toyoda et al. [23] introduced the categories and platforms of blockchain technologies employed in existing BFL research work, and made comparisons between various BFL frameworks. Hou et al. [24] compared and summarized some prevailing BFL frameworks, underlying BFL infrastructures, and applications of BFL. Wahab et al. [25] engaged in a comprehensive survey targeting FL, wherein the comparative analysis spanned aspects such as architectural paradigms, communication efficiency, incentive mechanisms, privacy preservation, and secure aggregation schemes, and also incorporated an investigation of certain BFL architectures. Nguyen et al. [26] explored the integration of blockchain and FL, taking into account communication costs and resource allocation in mobile edge computing scenarios. Issa et al. [27] delved into this topic within the context of the Internet of Things. They provided detailed discussions on both blockchains and FL separately, and presented structures and perspectives on their integration. Li et al. [28] examined the architecture of BFL, covering aspects such as types, design, model enhancement, and incentive mechanisms.

It is evident that these surveys predominantly focus on the BFL framework and its prospective applications in the field of AI, yet lack an in-depth analysis of the pivotal issues addressed by BFL, as well as a comprehensive discussion on its applicability in more expansive scenarios. Therefore, this work originates from the framework of BFL, providing an incisive discourse on key challenges in FL that are ameliorated through the integration of blockchains. It further elaborates on the prospective applications of BFL in multiple domains, including the Internet of Things (IoT), Industrial Internet of Things (IIoT), Internet of Vehicles (IoV), and healthcare services. The paper undertakes a holistic and rigorous analysis and comparative evaluation across three critical dimensions—fundamental architecture, core technologies, and future applications—to ultimately summarize the innovative directions and applicative frontiers where blockchains and FL converge.

The main contributions of this work are as follows:

- We offer an overview encompassing the definition, architectural design, and challenges of both blockchains and FL. We also delve into the motivations driving the application of blockchains in the context of FL.
- We categorize BFL frameworks into three distinct classes based on how blockchains participated in the FL process within individual nodes.
- We elaborate on how to use blockchain technology to mitigate the challenges of FL from the perspectives of decentralization, incentive mechanisms, attack resistance, privacy protection, and efficiency enhancement.
- We compile a comprehensive list of current viable applications for BFL and engage in discussions regarding the promising future directions and unresolved issues in the field of BFL.

The rest of this article is organized as follows. In Section 2, we introduce the basics of FL and blockchains, and we present the frameworks and functions of BFL in Section 3. In Section 4, we investigate the applications of BFL in different domains. Discussions of the current challenges and future research directions of BFL are presented in Section 5, and we conclude the paper in Section 6.

2. Preliminary

2.1. Overview of Federated Learning

Conventional ML algorithms necessitate the centralization of raw data on high-computational-capacity cloud servers for model training, thereby engendering uncontrollable data flow and vulnerability to sensitive data leakage. Mcmahan et al. [17] introduced the concept of FL in 2017, allowing for the preservation of user privacy during the ML process without the aggregation of source data into a shared training dataset. Essentially, FL is a form of distributed machine learning technology, the workflow of which is depicted in Figure 1.

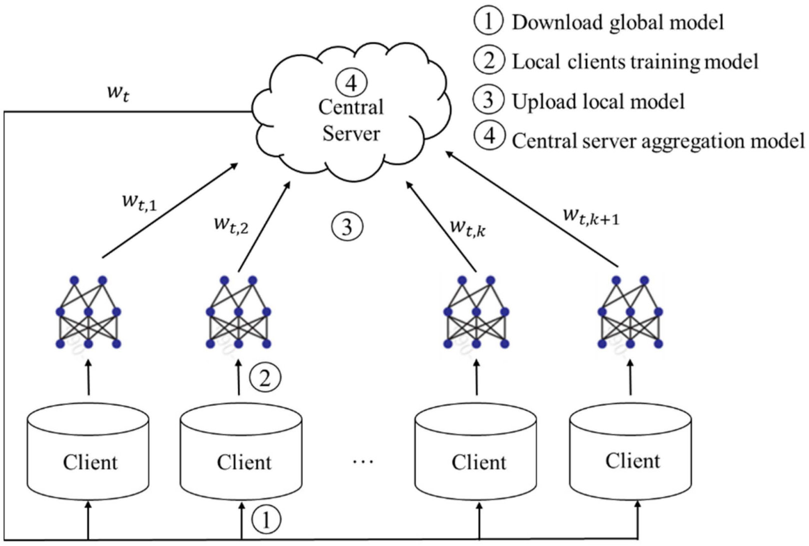

Figure 1. The workflow of *FL*.

Client devices, such as mobile phones, computers, and IoT devices, work together to train ML models under the supervision of a central server. In this configuration, the client devices are in charge of training local data to build local models. The central server performs weighted aggregation of these local models to produce a global model. Through iterative cycles of this process, a model w is ultimately obtained that closely approximates the outcomes of centralized ML algorithms, thereby effectively mitigating numerous privacy risks associated with the aggregation of source data in traditional ML paradigms.

The iterative process of FL is outlined below:

1. Client devices retrieve the global parameter w_{t-1} from the server;
2. Each client k trains its local data to derive its local model $w_{t,k}$ (signifying the local model update for the k^{th} client in the t^{th} communication round);
3. All participating clients transmit their local model updates to the central server;
4. Upon receiving updates from diverse clients, the central server executes weighted aggregation operations to formulate the global model w_t (indicating the global model update in the t^{th} communication round).

Foremost, FL technology exhibits the following distinctive attributes: (1) The raw data engaged in FL are retained locally on client devices, with only model updates being exchanged with the central server. (2) The jointly trained model is shared collectively among all participating entities. (3) The ultimate model accuracy of FL approximates that of centralized machine learning methodologies. (4) The quality of the training data contributed by participants in FL is directly correlated with the precision of the resultant global model.

2.2. Threats and Challenges of FL

Since the concept of FL was proposed, it has quickly attracted widespread attention and research in the academic community. However, there are still many threats and challenges that urgently need to be addressed in this research direction. The most core issues include single point of failure [29–31], lack of incentive mechanisms [20,32], poisoning attacks [33–37], defects in privacy policies [9–12,14] and low communication efficiency [16,17,38]. These issues have greatly limited the further development and application of FL.

Single Point of Failure: The central server in FL is susceptible to malicious updates, causing defects in the global model update. This affects all local model updates and reduces their accuracy. Additionally, FL requires local devices to upload local model updates to the central server. When too many devices are transmitting models simultaneously, it can lead to network overload.

Lack of Incentive Mechanism: FL generally assumes that each local device willingly contributes data resources to the global model. However, this does not align with reality. The lack of an incentive mechanism affects participants' motivation to contribute, and some participants may even obtain rewards without contributing data, leading to unfair economic compensation.

Poisoning Attacks: Malicious users may deliberately upload carefully calculated malicious local training models to affect global model training, intentionally sabotaging predictive outcomes of machine learning. This is mainly because FL lacks the ability to monitor and diagnose malicious users or malicious model updates.

Defects in Privacy Policies: Despite training data resources being stored on local devices, the FL framework may still lead to a leakage of training data privacy. In a real network environment, it is challenging to assess the motivations of participating clients in the training process, and ensuring the trustworthiness of the central server is equally difficult. Relying solely on model updates to protect user privacy appears to be insufficient.

Low Communication Efficiency: Since FL requires communication between clients and servers to transmit local learning models and perform multiple rounds of model training iterations for local or global model updates, the communication efficiency between the client and server, as well as the model training efficiency, can also affect FL performance.

2.3. Overview of Blockchains

Blockchains, initially introduced as part of a payment system known as Bitcoin by Nakamoto in 2008 [21], has become one of the most widely adopted disruptive technologies in various financial and industrial applications. It is essentially a distributed and immutable ledger consisting of blocks that are shared among untrusted participants within a peer-to-peer (P2P) network, eliminating the need for a trusted central authority [39]. To ensure the validity of all transactions before they are recorded, consensus algorithms are employed. As illustrated in Figure 2 each block in the chain contains a hash of the preceding block, ensuring the immutability of the blocks [40]. To maintain data integrity, all network participants maintain identical copies of the ledger. When a new transaction is generated, it is disseminated to specific nodes within the network, often referred to as miners. These miners validate the incoming transaction by verifying its associated signature. Upon validation, they proceed to create a new block and distribute it across the network, reaching a consensus through a distributed process. Once the miners reach a consensus and validate the new block, it is appended to the distributed ledger. From a structural perspective, a block consists of two parts: the block header and the block body. Key information in the block header includes the current version number, the hash value of the previous block, a timestamp, a random number (Nonce), and the hash value of the Merkle Root [41].

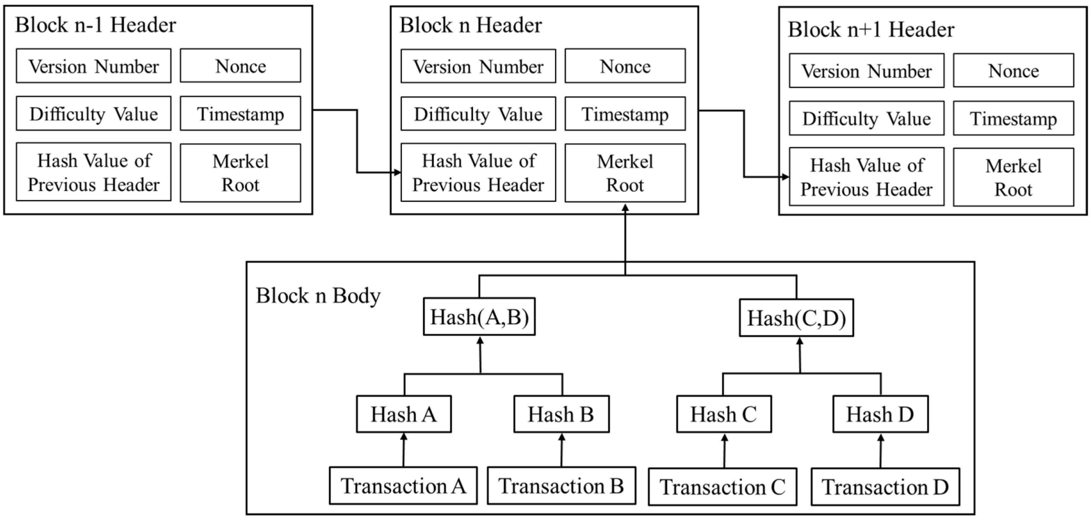

Figure 2. Structure of a blockchain.

Blockchains can be categorized into four main types: public blockchains [42–44], consortium blockchains [45–47], and private blockchains [48–51]. A public blockchain is a system where anyone in the network can access the blockchain at any time. It is usually considered fully decentralized and highly anonymous, and the data are immutable. Consortium blockchains are managed collectively by a number of enterprises or institutions. Data are recorded and maintained by verified participants, and these nodes have the permission to read the data. A private blockchain is a blockchain controlled by a particular organization or user. The rules for controlling the number of participating nodes are strict, resulting in very fast transaction speeds and a higher level of privacy. It is less susceptible to attacks, and while it offers higher security compared to public blockchains, its degree of decentralization is significantly reduced.

2.4. Architecture of Blockchains

Blockchain technology has undergone more than a decade of development. Although there is currently no standardized development form, we can still categorize blockchains into six layers based on the commonalities of the working modes of existing blockchain platforms: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [22], as shown in Figure 3.

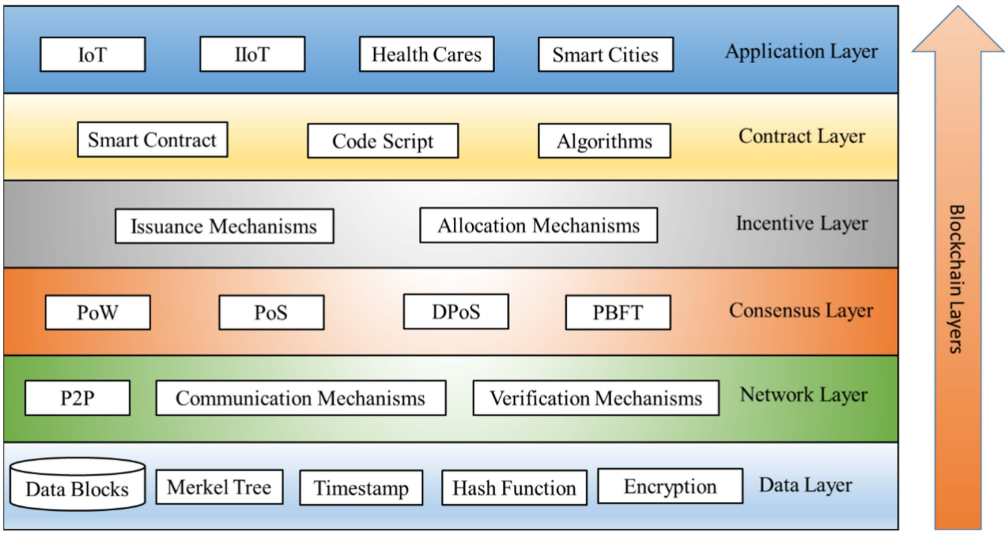

Figure 3. Systematic blockchain architecture.

A. *Data layer*

The data layer is the bottom-most layer of the blockchain platform. This layer primarily uses data structures such as Merkle trees to organize and manage data within the blockchain, and employs hash functions and asymmetric encryption technologies to ensure the integrity and security of the blockchain data. Each block contains the root hash of the Merkle tree and information like the preceding block's hash, timestamp, nonce, block version number, and current difficulty value. The Merkle tree [39] is a data structure constructed using hash pointers to organize data. In a blockchain, transaction data within the block body are built into a binary Merkle tree. The leaves are the hash values of the transaction data, while the non-leaf nodes contain the sum of the hash values of its two child nodes, as is shown in Figure 2. The purpose of organizing transactions with a Merkle tree is to quickly verify whether any transaction has been tampered with. The use of the Merkle tree in blockchain allows nodes to quickly summarize and verify the integrity and existence of transaction data within a block [52].

B. *Network layer*

The network layer primarily furnishes mechanisms for information exchange among each node within the blockchain network, including the P2P network mechanism, the information communication mechanism, and the data verification mechanism. With a P2P network, the messages are directly propagated between nodes. Each node has the same functionality and status, and there is no centralized device. Each node is responsible for routing, block data validation, block data propagation, transaction information packaging, and discovering new nodes [39]. Under the P2P networking method, the system can still operate normally even if any node breaks down.

C. *Consensus layer*

In a distributed blockchain system, the mechanism by which mutually distrustful nodes reach a consensus on certain data or proposals within a specified time is called the consensus mechanism. Blockchains have proposed the evaluation standard of the "impossible triangle" for the consensus mechanism [53], that is, the three characteristics of decentralization, scalability, and security cannot be satisfied simultaneously. Various types of blockchains have different degrees of decentralization and numbers of nodes participating in the consensus, so the consensus mechanisms they use are also distinct. Public chains have a huge number of nodes participating in the consensus and a higher degree of decentralization. They generally use consensus mechanisms such as proof of work (PoW) [54], proof of stake (PoS) [55], and delegated proof of work (DPoS) [56]. Private chains have fewer nodes and a lower degree of decentralization. They generally use consensus mechanisms such as Paxos [57] and Raft [58]. Compared with public chains, consortium chains have fewer nodes and the feature of "partial decentralization". They generally use the practical Byzantine fault tolerance (PBFT) [59] mechanism.

D. *Incentive layer*

Nodes within a blockchain network do not inherently contribute their computational power to create new blocks unless there are incentives in place. These incentives are governed by an incentive layer where miners are rewarded, which follows predefined protocols. Generally, these rewards are granted upon the successful creation of a new block, or they can be earned by charging fees for processing transactions. By providing these economic incentives, miners are motivated to engage in mining activities with integrity.

E. *Contract layer*

The contract layer encompasses various forms of code, scripts, and smart contracts responsible for governing the operations of the blockchain. Smart contracts are encoded into the blockchain using computer languages and are equipped with trigger conditions for specific events. When these events occur, smart contracts are executed automatically in accordance with predefined rules. Smart contracts have the capability to autonomously address matters within the blockchain network, eliminating the need for third-party intervention and enhancing the blockchain's autonomy and transparency.

F. Application layer

At present, blockchain technology is gradually entering the Blockchain 3.0 phase, and various applications based on blockchain technology are developing steadily. The digital currency application, which was the original use of blockchains, still attracts much attention, and many people remain enthusiastic about investing in digital currencies. Blockchains have been applied extensively in areas including finance [60,61], supply chain management [62,63], IoT [64,65], etc.

It is important to emphasize that not all the layers mentioned above need to be integrated into every blockchain. The lower three layers can be considered as foundational layers that are crucial, while the upper three layers may not be necessary for all blockchain implementations.

3. Blockchain-Based Federated Learning

In the traditional FL architecture, a central server is responsible for collecting, aggregating, and broadcasting the new global model, which may lead to the following problems: (a) The stability of the central server might be affected by cloud service providers; (b) the central server might show favoritism towards certain clients; and (c) a malicious central server might poison the model or collect private information from clients. To address these issues, the most direct solution is to remove the central server and let the client nodes handle the corresponding tasks [66–68]. This requirement aligns well with the inherent characteristics of blockchain technology. Recent studies have used the blockchain's distributed storage architecture as the foundational framework for FL [69–79]. By designing protocols on the upper layer of the blockchain, they implement the task of model aggregation running for clients. At the same time, the rational incentive mechanism in the blockchain provides a technical solution to enhance the enthusiasm of all participants to actively participate in FL model training.

3.1. Frameworks of BFL

This section summarizes and compares the blockchain-based federated learning (BFL) frameworks proposed in the literature collected for this article, and analyzes their different design approaches. Figure 4 shows the schematic diagram of the BFL framework classification summarized in this article.

First, a traditional FL framework usually consists of a central server and multiple users (or devices/clients). Early typical BFL frameworks generally used decentralized blockchains to replace the central server in traditional FL frameworks. The main purpose was to address the problems of single-point trust and failures caused by the central server [80–83]. An example of this type of framework is shown in Figure 5. Users submit their local models to the miners maintaining the blockchain. The miners carry out cross-validation, model aggregation, and other steps, and produce a consistent global model based on the consensus mechanism. They then use blocks to store and propagate this global model. Users can download the consistent global model from the block to their local devices for the next round of training. In addition to using blockchains to replace the central server, this kind of typical framework usually has two features. Before model aggregation, by introducing mechanisms such as cross-validation, it ensures that the local models participating in the global model update conform to the direction of the global model update, preventing users from using malicious models to jeopardize the security of the global model. Furthermore, by introducing a reward mechanism, users can be incentivized to contribute high-quality data and actively participate in training, effectively alleviating the fairness problem of FL. This prevents users with different contributions from receiving similar rewards, in case of users slacking off.

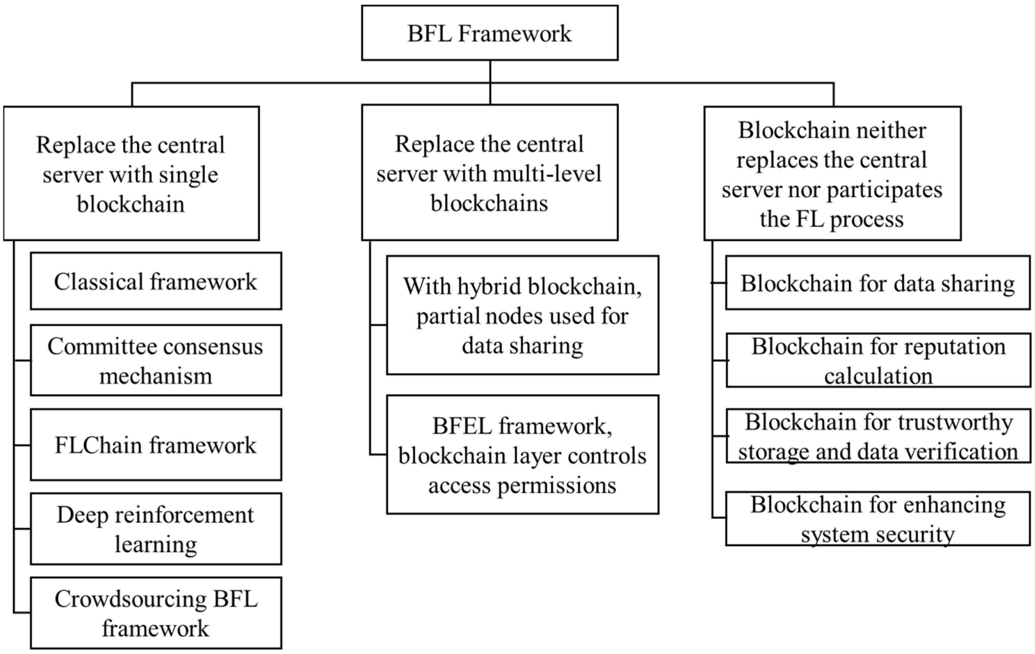
BFL Framework
Replace the central server with single blockchain
Classical framework
Committee consensus mechanism
FLChain framework
Deep reinforcement learning
Crowdsourcing BFL framework
Replace the central server with multi-level blockchains
With hybrid blockchain, partial nodes used for data sharing
BFEL framework, blockchain layer controls access permissions
Blockchain neither replaces the central server nor participates the FL process
Blockchain for data sharing
Blockchain for reputation calculation
Blockchain for trustworthy storage and data verification
Blockchain for enhancing system security

Figure 4. Types of BFL frameworks.

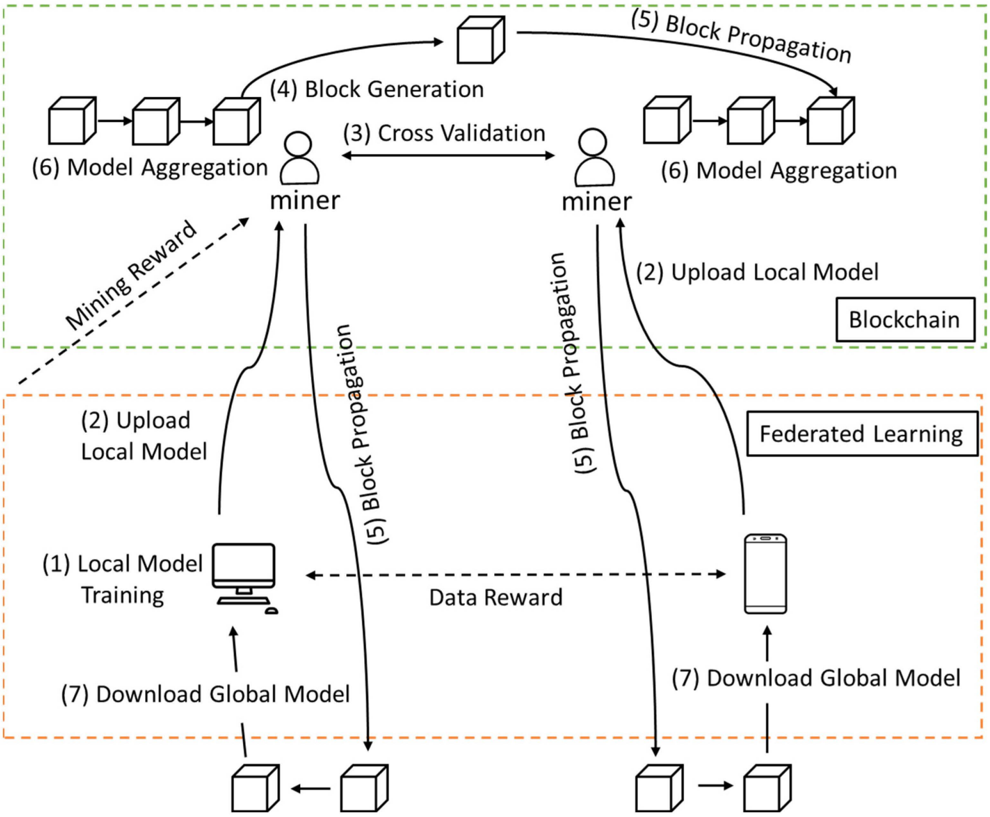

Figure 5. A generalized BFL paradigm.

On the basis of this typical framework, some BFL frameworks have led to further innovation in areas such as consensus mechanisms and reward mechanisms. The BFL framework with a committee consensus framework proposed in [30] does not adopt the commonly used PoW consensus mechanism, but instead proposes the committee consensus mechanism (CCM). A feature of this mechanism is the use of a committee composed of some honest nodes to carry out local gradient verification of the model and block generation. Because only a subset of nodes participate in local model verification and global model updates, the overall efficiency of FL is significantly improved. This mechanism requires nodes outside the committee to send their local models to committee nodes for verification and scoring, and only allows qualified models to participate in global model updates. By this mechanism, to enhance security, members of the committee are periodically replaced based on node historical performance scores and smart contracts. Hieu et al. [84] introduced deep reinforcement learning to find the optimal system parameters that can minimize system delay, energy consumption, and total rewards, including recommended data volume and energy consumption when users train local models, as well as block generation rate. The FL, via the MEC-enabled blockchain network (FLChain) framework proposed in [85], includes both mobile devices and edge devices. Mobile devices primarily update local models using data samples on the devices, while edge devices provide more abundant network resources for resource-limited mobile devices and also act as nodes in the FLChain network to maintain the blockchain. FLChain utilizes the channel technology in the consortium blockchain Hyperledger Fabric, leveraging the isolation feature of the channels to enhance the security of global model training and provide a certain degree of data privacy preserving. Li et al. [86] proposed a crowdsourcing BFL framework called the crowd computing secure framework based on blockchain technology and FL (CrowdSFL). Its main purpose is to reduce user costs during crowdsourcing and to ensure its security. In CrowdSFL, the entire crowdsourcing system is built on the blockchain, and every participant has an independent blockchain account. CrowdSFL introduces a data interaction mode controlled by smart contracts, ensuring that the data are uploaded in the correct format and stored in blocks.

The aforementioned BFL frameworks all use a single type of blockchain to replace the central server used in traditional FL. In recent years, a few studies have proposed BFL frameworks that replace central servers with more complex multi-level blockchains. Lu et al. [87] proposed a BFL framework based on a hybrid blockchain called the permissioned blockchain and the local Directed Acyclic Graph (PermiDAG). In this framework, the hybrid blockchain uses a permissioned blockchain running on the road side unit (RSU) as the main chain, while allowing vehicle nodes to form multiple local directed acyclic graphs (DAG). The permissioned blockchain serving as the main chain is responsible for recording information related to data sharing and parameters related to global model aggregation. Multiple local DAGs formed by vehicle nodes are used to enhance the efficiency of data sharing, as well as to store data-sharing events and trained model parameters as transactions in blocks. At the same time, based on the local DAG, neighboring vehicle nodes communicate with each other, obtaining local models of nearby vehicles, and use these models to enhance their own local models, realizing the asynchronous learning process. Additionally, the blockchain-empowered federated edge learning (BFEL) framework proposed in [88] also adopts a multi-level blockchain structure. This framework consists of an application layer and a blockchain layer, with the application layer mainly responsible for executing the FL process. The blockchain layer in this framework includes a main chain based on a public blockchain and multiple sub-chains based on consortium blockchains. By leveraging multiple sub-chains to set access permissions, this framework can enhance the data-privacy-preserving capabilities and achieve performance isolation.

However, in some BFL frameworks, the blockchain neither directly replaces the central server nor directly participates in the traditional FL process. For example, in the BFL framework proposed in [89], the blockchain is only used to implement data sharing functions. The blockchain in this framework contains three different types of transactions: (1) retrieval transactions, allowing nodes to notify other nodes of the requested model information; (2) model transactions, allowing nodes to pass model training data to other nodes; and (3) data sharing transactions, allowing nodes to return the shared data to the requester. Specifically, a data requester sends a data sharing request to the blockchain. The blockchain conducts a retrieval transaction to check whether the cache already contains the corresponding data: if it exists, the blockchain returns the query result and the requested data model directly to the requester and generates a data sharing transaction; if not, the blockchain performs a multi-party information retrieval process, forms a model training committee, uses model transactions for model training, generates the model required by the requester, and caches the model for future needs while returning it to the requester. In the fine-grained FL framework proposed in [90], the execution of FL mainly takes place in cloud nodes and fog nodes. The blockchain in this framework does not directly participate in FL and is mainly responsible for calculating and storing the reputations of various nodes participating in FL. Moreover, in the BFL framework for equipment fault detection in the industrial IoT proposed in [91], the blockchain is mainly used for trustworthy storage and verification of client data. In this framework, clients regularly create Merkle trees to organize data collected from sensors and store the Merkle root in the blockchain. In the event of future disputes, the Merkle root stored in the blockchain can be used as evidence to help resolve the disputes. The BFL framework based on a consortium blockchain proposed in [92] aims to enhance edge computing capabilities in the digital twin wireless network model. This framework consists of various types of terminal users, such as IoT devices, mobile devices, base stations, and macro base stations. Base stations are responsible for executing the local training of FL, while macro base stations act as the central servers for FL. Since FL cannot solve the trust issue between twin terminal users, this framework introduces a consortium blockchain to enhance system security, uses the blockchain to record data via the digital twin process, and manages users by controlling access permissions.

3.2. Functions of BFL

In this section, we investigate the specific functions of BCFL with the perspective of how blockchains mitigate the challenges faced by FL, which was introduced in Section 2.2 Specifically, we demonstrate this from five angles, including decentralization, incentive mechanisms, attack resistance, privacy protection, and efficiency enhancement.

3.2.1. Decentralization

In FL, due to the central aggregation function of the server, once its device is subjected to a single-point attack by adversaries, it poses a significant security risk to the entire learning framework [93–96]. To enhance the security, trustworthiness, and reliability of the framework, Majeed et al. [85] proposed a BFL architecture to improve the security of FL. Basically, for each global model, the framework creates a new channel to store a specific channel ledger, and concurrently creates a "global model state tree" to track weight updates of the global model. Sharma et al. [97] utilized offline and online blockchains to store temporary training data from a large number of nodes in real-time, a technique based on a distributed multi-layer computing framework. The multi-layer and multi-chain structure effectively reduces the impact of network failures and malicious attacks on FL. Arachchige et al. [98] developed a framework called PriModChain by integrating differential privacy, FL, the Ethereum blockchain, and smart contracts. It offers privacy, security, and reliability for FL applications in the industrial IoT. However, the operating efficiency of the framework restricts its further development. Lu et al. [87] introduced a novel hybrid blockchain architecture composed of a permissioned blockchain and a local DAG. It aims to enable effective data sharing in vehicular networks, thereby enhancing the reliability of the learning model. Pokhrel et al. [81] introduced a multi-level trust framework using a private blockchain to ensure end-to-end trustworthiness, from observation to learning and verification of local model updates.

3.2.2. Incentive Mechanism

In order to solve the problem of a lack of incentive mechanism, BFL usually uses blockchain technology to construct incentive mechanisms to achieve the expected behaviors, or penalty mechanisms towards abnormal behaviors, to stimulate the enthusiasm of local users to contribute to the global model update [99,100]. Kim et al. [101] proposed the BlockFL framework, in which each device uploads its local model updates to related miners in the blockchain network. Miners are responsible for exchanging and verifying model updates, recording them in the blockchain, and providing corresponding rewards. Kang et al. [102] introduced the concept of reputation as a measure of client trustworthiness, and used a multi-weighted subjective logic model to design a reputation-based trustworthy client selection scheme. At the same time, they used the immutability of blockchains to implement distributed reputation management and used contract theory to provide corresponding rewards by analyzing the computational power investment and model quality of the clients participating in model building. Weng et al. [103] proposed the DeepChain scheme, distinguishing clients' performances in terms of activity and compatibility during the training process and urging clients to send correct and high-quality model updates. They also used blockchain technology to ensure model security and the audibility of the training process, achieving the objectives of confidentiality, audibility, and fairness. Kim et al. [104] used blockchain technology to record all model updates comprehensively, and provided generous rewards to incentivize users to participate in FL. They proposed a weight-based client subset selection scheme, selecting clients for training based on the accuracy of each client's local model and the frequency of their participation in training, achieving high stability and faster convergence speed. Zhan et al. [105] designed an incentive mechanism based on deep reinforcement learning (DRL), applying traditional resource allocation strategies to the specialized distributed scenario of FL, in order to achieve optimal training strategies and pricing strategies for edge nodes.

3.2.3. Attack Resistance

To address the problem of poisoning attacks, BFL typically employs consensus mechanisms deployed in the blockchain to verify model updates, thus effectively preventing poisoning attacks [106–108]. Qu et al. [82] proposed replacing the central server with a blockchain system to utilize the blockchain's immutable nature to eliminate poisoning attacks. Kang et al. [88] introduced a proof-of-validation (PoV) consensus mechanism used to collaboratively verify the update quality of local models among predefined miners. In this scheme, only validated model updates can be stored in a block, thereby preventing poisoning attacks. To reduce malicious poisoning model updates, Zhao et al. [109] proposed a reputation-based crowdsourcing incentive mechanism. Under this mechanism, if a user is detected to be making malicious updates, their update model will be rejected. They will not only miss out on rewards for that update round, but will also have their reputation reduced, affecting future profits and leading to penalties. Zhang et al. [110] introduced a scoring mechanism to determine whether a device is malicious and might launch poisoning attacks, thereby selecting trainers to participate in the model update to resist such attacks. Shayan et al. [111] proposed a multi-Krum consensus mechanism, which rejects model updates that go against the direction of most model updates. In each update round, a validation peer committee is elected by majority vote. This committee uses multi-Krum to reject malicious model updates, thus preventing poisoning attacks. Chen et al. [112] introduced a decentralized validation mechanism to verify local model updates. This mechanism votes on the validity of each model, then uses the voting results to eliminate potential malicious devices.

3.2.4. Privacy Protection

To forestall privacy breaches, certain BFL schemes incorporate additional privacy protocols [79,113–115]. For instance, Martinez et al. [116] implemented homomorphic encryption to safeguard the privacy of the training model. Shayan et al. [111] developed Biscotti, a decentralized P2P scheme based on blockchain, employing a verifiable secret sharing scheme for secure model aggregation to fortify individual privacy. Blockchain and FL technologies were combined by Ren et al. [117] to devise an intrusion detection algorithm suitable for lightweight network devices, with the aim of safeguarding the data privacy of network users during data sharing. Feng et al. [78] harnessed the decentralization and tamper-proof attributes of blockchains, storing data records and critical information on the blockchain while the complete data were encrypted and stored in a distributed database, ensuring secure storage to prevent the leakage of users' private data. Weng et al. [103] employed the Paillier algorithm to encrypt users' model parameters, subsequently uploading them to the blockchain. After the completion of the model updates, collaborative decryption was executed by a consortium of users. In the context of data security and sharing requisites in the IIoT and Smart Transportation, Lu et al. [89] and Qi et al. [118] deployed local differential privacy techniques. They introduced noise to the raw data prior to feature extraction and sharing to thwart privacy attacks. The Adaptive Differential Privacy FedAvg (ADPFe-dAvg) algorithm was presented by Zhang et al. [119] to protect the client's historical data during the entire training phase and prevent member inference attacks in visual object identification modeling. ADPFedAvg introduced user-level differential privacy technology, complemented by adaptive clipping technology. To establish a data-privacy-preserving mechanism, Mahmood et al. [120] encrypted all data via a public key infrastructure (PKI) comprising a public key and a private key, achieving a BFL mechanism that preserved data privacy with multi-layered security.

3.2.5. Efficiency Enhancement

Lastly, to address the issue of inefficiency, BFL schemes often employ various methods to reduce the amount of data that need to be transmitted. The approach proposed in [82] stores specific related data in an off-chain distributed hash table, and only pointers are stored on the blockchain, thereby reducing the data transmission volume. Lu et al. [87] introduced an asynchronous FL scheme for the edge data learning model which further enhances the efficiency of FL by selecting participating nodes. Li et al. [30] introduced the committee consensus mechanism, which verifies local gradients before attaching them to the chain. Under this mechanism, only a few nodes are used to verify model updates, eliminating the need to broadcast to every node and reach a consensus and, thus, improving the efficiency of model verification. Kang et al. [88] described a gradient compression scheme, which can enhance the communication efficiency of blockchain-authorized federated edge learning without compromising learning accuracy. Furthermore, Kumar et al. [121] proposed a method that incorporates hyperparameter optimization and elastic weight consolidation into federated learning to enhance the accuracy and efficiency of the model training.

The integration of FL and blockchains makes the system a comprehensive closed-loop learning mechanism. On the one hand, FL technology provides a secure, cross-domain sharing solution for participants with private data. On the other hand, blockchain technology, serving as the core database, provides participants with application needs such as secure storage, trust management, fine-grained differentiation, and incentive returns, encouraging users with data to actively participate in data federation.

4. Applications

Currently, BFL technology has been applied in many industry areas. This article summarizes the application prospects of the current BFL technology in areas such as the Internet of Things (IoT), Industrial Internet of Things (IIoT), healthcare services, and Internet of Vehicles (IoV).

4.1. Internet of Things

In the realm of IoT, devices are decentralized, and consequently, conducting model training on these devices necessitates both timely and secure data access, as well as robust model generalization capabilities. The research pertaining to the application of BFL within the IoT domain predominantly centers on addressing concerns related to data security, resource allocation, communication protocols, and failure detection [27,71,108,122]. The overarching objective of these efforts is to empower IoT devices to collaboratively train models that exhibit high performance. Lu et al. [89] constructed a distributed multi-party data sharing model that further ensures the authenticity of data through differential privacy, allowing devices to retrieve data securely and accurately. Instead of the common PoW consensus algorithm, the proof of training quality (PoQ) consensus algorithm in [89] is used to verify training models, aiming to improve the utilization efficiency of computational resources. To help household appliance manufacturers improve service quality and optimize appliance functions, Zhao et al. [109] introduced a hierarchical crowdsourcing FL system, utilizing blockchain technology to prevent malicious model updates. To make the 6G network more secure and efficiently apply it to the IoT, Dai et al. [83] proposed a combination of a blockchain and FL, integrating mobile edge computing and device to device (D2D) communication, to address the challenges faced by the 6G network.

4.2. Industrial Internet of Things

The IIoT encompasses an intricate network of interconnected sensors, equipment, actuators, and other intelligent components. These components facilitate adaptive decision-making and continuous status tracking [123,124], playing a pivotal role in the digital transformation and intelligentization of the contemporary manufacturing industry. In a study conducted by Lu et al. [89], BlockFed was employed to facilitate data sharing within the domain of IIoT. The data-sharing challenge was approached by framing it as an ML problem, incorporating privacy-preserving FL, and integrating FL into the consensus mechanism of a permissioned blockchain. The computational effort required for the consensus was also utilized for federated training. In the context of fault detection scenarios in IIoT, Zhang et al. [91] proposed a federated averaging algorithm called Centroid Distance Weighted Federated Averaging. This algorithm takes into account the distance between negative and positive classes within each client dataset, thereby mitigating the impact of data heterogeneity challenges in IIoT device fault detection. Additionally, Lu et al. [92] recognized the challenges posed by unreliable communication channels, computational resource constraints, and the intricacies associated with establishing trust among users within the context of IIoT. To address these issues, they developed an FL framework for collaborative computation empowered by blockchain technology. This framework substantially elevated the system's reliability, security, and privacy.

4.3. Smart Healthcare

BFL can also bring significant advancements to healthcare services. Typically, remote patient monitoring or certain AI-assisted diagnoses require a large amount of patient disease information. However, many medical records contain sensitive information about the patient, and these data have high intrinsic value for certain attackers. As a result, BFL is gradually being applied to the medical field [75,107,125]. Passerat et al. [126] proposed a BFL scheme for healthcare alliances, establishing a set of enterprise-level blockchain components compatible with the Ethereum ecosystem and integrating a series of privacy protection techniques. It also introduced a new secure aggregation protocol designed to run within AMD's trusted hardware environment, secure encrypted virtualization (SEV), to ensure the security of private data. El Rifai et al. [127] introduced a BFL framework in the medical field, applying smart contracts to the data aggregation process of FL algorithms. This ensures transparency and permission during data sharing, predicting diabetes risk based on training with substantial patient information. Furthermore, Polap et al. [128] developed a lightweight security and privacy algorithm for Internet of Medical Things (IoMT) devices based on BFL. Rahman et al. [129] not only presented a trustworthy BFL framework applicable to the IoMT, but also designed a COVID-19 application for data classification by which we can learn about global models related to COVID-19 diagnoses. This scheme includes a trustworthy and tamper-proof gradient mining method and a decentralized consensus-based aggregator, and adds extra security for blockchain nodes responsible for aggregation. Aich et al. [130] also introduced a BFL scheme for healthcare, aiming to protect and share patients' medical information by building a real-time global application model. In addition, Kumar et al. [131] proposed a BFL framework that uses the latest data to segment and classify lung CT scans based on capsule networks, sharing data between hospitals to improve COVID-19 detection rates while ensuring patient privacy protection.

4.4. Internet of Vehicles

BFL solutions have been widely applied to the IoV to facilitate data sharing and autonomous driving [81,118,132]. Pokhrel et al. [81] proposed a fully decentralized BFL framework. This framework achieves end-to-end trustworthy communication within the IoV, and the communication latency remains within an acceptable range, thus promoting effective communication for automated vehicles. They use BFL to verify model updates in on-vehicle machine learning (oVML), enhancing the performance and privacy security of automated vehicles. Lu et al. [87] introduced a BFL framework composed of a primary permissioned blockchain maintained by roadside units and a local DAG run by vehicles, aiming for efficient data sharing in the IoV. Additionally, Lu et al. also proposed an asynchronous FL scheme based on edge data. By using the Delegated Proof of Stake (DPoS), it selects optimized participating nodes, thereby improving the efficiency of FL. In [133], a blockchain-based hierarchical FL algorithm is introduced which reduces storage consumption and improves training accuracy. The proposed knowledge-sharing method based on BFL enhances the reliability and security of in-vehicle networks. Using the proof of learning (PoL) consensus mechanism, a lightweight blockchain was realized, preventing the wastage of computational power.

Additionally, BFL is gradually being expanded to various domains. In the field of content caching, Cui et al. [134] presented a new algorithm called the blockchain-assisted compressed algorithm of FL, applied for content caching (CREAT). This blockchain-assisted FL algorithm aims to predict cache files and enhance the cache hit rate. In the domain of location prediction, the scheme proposed in [135] utilized BFL for local training on users' mobile devices. This approach safeguards user privacy while making better use of the data for more accurate location predictions. In the realm of mobile crowd sensing, Wang et al. [136] introduced the secure FL for an unmanned aerial vehicle (UAV)-assisted crowdsensing (SFAC) framework. This is a secure FL architecture for UAV-assisted mobile crowd sensing (MCS), employing local differential privacy to protect the privacy of data providers. Moreover, BFL has been applied to disaster response. The study in [137] proposed a blockchain-authorized BFL framework that will implement a disaster response system using wireless mobile modules on UAVs using future 6G networks. Additionally, BFL has also been adopted in the news recommendation field. Wang et al. [138] presented a cloud-edge collaborative filtering recommendation system based on FL. This system incorporates noise into the training model using differential privacy technology, further preventing data privacy exposure.

5. Challenges and Future Directions

The introduction of blockchains has helped address some of the significant issues in traditional FL. However, the integration of blockchains with FL also confronts challenges posed by blockchain technology itself, awaiting continuous exploration by researchers.

5.1. Privacy Concerns

The public blockchain ledger allows for secure and reliable data processing, but the collected FL training data can be accessed publicly and are available for all participants to use. This might lead to issues of circumventing privacy protection mechanisms. Furthermore, the ubiquitous sensing systems in the IoT continuously collect personal and sensitive data from consumers. Placing these data into an open ledger may lead to privacy concerns. Using a private blockchain ledger can ensure data privacy by enabling encryption and allowing controlled access to the ledger. However, such private blockchain platforms will limit the accuracy of processing and execution in the FL system, thereby affecting the access to and disclosure of vast amounts of data needed for decision making and analysis.

Most blockchain systems lack sufficiently robust privacy protection mechanisms. Therefore, BFL frameworks need to incorporate privacy protection technologies like differential privacy and homomorphic encryption to provide additional protection to the data placed on the blockchain. For instance, in the literature [89,111], differential privacy is employed during the model extraction process by adding noise to preserve the privacy of individual data. Shayan et al. [111] also introduced a verifiable secret-sharing scheme for secure model aggregation. In addition, Martinez et al. [116] used homomorphic encryption algorithms to encrypt training data for privacy protection. For existing BFL frameworks, striking a better balance between the cost of privacy protection and training accuracy remains a crucial issue to address.

5.2. Efficiency, Performance, Scalability

When incorporating specific privacy encryption algorithms into FL systems, there is a substantial deceleration in the system's processing speed. This has made the practical application of robust privacy protection mechanisms in FL systems particularly challenging. In the realm of blockchain systems, cryptocurrency platforms such as Bitcoin's blockchain can execute an average of four transactions per second, while Ethereum manages roughly twelve. When compared with VISA's capability to process millions of transactions every second, such a performance is obviously unsatisfactory. Current research focuses on side-chains (also known as off-chains) [139] to enhance blockchain performance, facilitating rapid settlements between parties outside the main chain, with daily consolidations on the primary chain. Emerging blockchain variants have considerably refined their consensus algorithms for mining nodes. Platforms like Algorand [140] and IOTA [141], for instance, offer superior performance compared to the Ethereum and Hyperledger blockchains. Nevertheless, there remains a pressing need to amplify scalability, address extant performance issues, and thereby elevate the integrated system's performance when paired with federated learning systems.

Additionally, the encryption/decryption processes inherent to blockchains, coupled with the PoW mechanism, substantially hamper the efficiency of model training due to their complexity. For more sophisticated models, encryption and the subsequent transmission of model parameters consume significant time. Furthermore, the storage of large-scale models during iterative processes in blockchains incurs elevated storage costs. Future iterations of BFL systems necessitate further enhancements to their practicality, striving to augment their tangible value in real-world applications.

5.3. Security Concerns

A BFL system may encounter issues related to the abuse of decentralized authority. While blockchain technology offers reliable solutions for protecting all parties involved in the federated learning system and parameter exchange during predictive analysis, the entire blockchain system is still vulnerable to network attacks like the 51% attack [142]. Furthermore, the consensus mechanism, depending on the mining power, may also be compromised, leading to a concentration of the originally decentralized platform around mining fields that control consensus and settlement. This security issue is more pronounced in public blockchains like Ethereum and Bitcoin, whereas private blockchain platforms are less affected because consensus protocols are predefined among the parties.

While BFL frameworks can offer some resistance against poisoning attacks through well-designed consensus mechanisms, many blockchain consensus algorithms themselves face security risks. For instance, in the most common Proof of Work (PoW) consensus algorithm, miners may experience delays in receiving blocks, which can lead to forking issues. In a recent study [80], the introduction of ACK (ACKnowledge character) was proposed to determine, within a waiting period, whether a fork has occurred. If a fork is detected, the mining process is restarted, mitigating the problem. Some recent research has put forward new consensus algorithms; however, the security of these algorithms often lacks theoretical proof and practical validation. Consequently, the challenge of developing provably secure BFL consensus algorithms remains an urgent issue to address.

6. Conclusions

This article elucidates the current state of the research domain that integrates blockchain technology with FL. Through an extensive survey of existing literature in the BFL realm, a comprehensive analysis and comparison was conducted across the foundational architecture, core technologies, and prospective applications. Currently, the BFL domain remains in its nascent stages. The majority of research endeavors merely integrate blockchain techniques to address the singular trust issue inherent to FL, lacking further exploration concerning privacy, efficiency, and security. Furthermore, a significant portion of the studies remains theoretical, and some proposed BFL frameworks are not exhaustive, thereby calling the practical applicability of the present BFL techniques into question. With the rapid advancements in both blockchain and FL, two pivotal domains, BFL, as their interdisciplinary junction, has the potential to distill the technical prowess of each, and further fosters innovative techniques that in turn nourish both fields. This paradigm establishes a trustworthy privacy-preserving learning model, heralding transformative changes for numerous application areas.

Author Contributions: Ideation, Y.H. and J.H.; literature research, L.W. and W.R.; writing-original draft, L.W.; writing-review and editing, W.R., J.H. and Y.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China, Joint Fund Project, U22B2021.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bourse, F.; Minelli, M.; Minihold, M.; Paillier, P. Fast Homomorphic Evaluation of Deep Discretized Neural Networks. In Proceedings of the Advances in Cryptology—CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2018; Proceedings, Part III. Springer-Verlag: Berlin/Heidelberg, Germany, 2018; pp. 483–512.
2. Shi, E.; Chan, T.-H.H.; Rieffel, E.; Song, D. Distributed Private Data Analysis: Lower Bounds and Practical Constructions. *ACM Trans. Algorithms* **2017**, *13*, 1–38. [CrossRef]
3. Albrecht, J.P. How the GDPR Will Change the World. *Eur. Data Prot. Law. Rev.* **2016**, *2*, 287–289. [CrossRef]
4. Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konečný, J.; Mazzocchi, S.; McMahan, B.; et al. Towards Federated Learning at Scale: System Design. *Proc. Mach. Learn. Syst.* **2019**, *1*, 374–388.
5. Zhao, L.; Ni, L.; Hu, S.; Chen, Y.; Zhou, P.; Xiao, F.; Wu, L. InPrivate Digging: Enabling Tree-Based Distributed Data Mining with Differential Privacy. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications, Honolulu, HI, USA, 16–19 April 2018; pp. 2087–2095.
6. Sprague, M.R.; Jalalirad, A.; Scavuzzo, M.; Capota, C.; Neun, M.; Do, L.; Kopp, M. Asynchronous Federated Learning for Geospatial Applications. In Proceedings of the ECML PKDD 2018 Workshops, Dublin, Ireland, 10–14 September 2018; Monreale, A., Alzate, C., Kamp, M., Krishnamurthy, Y., Paurat, D., Sayed-Mouchaweh, M., Bifet, A., Gama, J., Ribeiro, R.P., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 21–28.
7. Li, Q.; Wen, Z.; He, B. Practical Federated Gradient Boosting Decision Trees. *Proc. AAAI Conf. Artif. Intell.* **2020**, *34*, 4642–4649. [CrossRef]
8. Xie, C.; Koyejo, S.; Gupta, I. Asynchronous Federated Optimization. Available online: https://arxiv.org/abs/1903.03934v5 (accessed on 30 November 2023).
9. Bhowmick, A.; Duchi, J.; Freudiger, J.; Kapoor, G.; Rogers, R. Protection against Reconstruction and Its Applications in Private Federated Learning. Available online: https://arxiv.org/abs/1812.00984v2 (accessed on 10 October 2023).
10. Fredrikson, M.; Lantz, E.; Jha, S.; Lin, S.; Page, D.; Ristenpart, T. Privacy in Pharmacogenetics: An {End-to-End} Case Study of Personalized Warfarin Dosing. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 17–32.
11. Melis, L.; Song, C.; De Cristofaro, E.; Shmatikov, V. Exploiting Unintended Feature Leakage in Collaborative Learning. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 23 May 2019; pp. 691–706.

12. Hitaj, B.; Ateniese, G.; Perez-Cruz, F. Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 3 November 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 603–618.
13. Carlini, N.; Liu, C.; Erlingsson, Ú.; Kos, J.; Song, D. The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks. In Proceedings of the 28rd USENIX Security Symposium, Santa Clara, CA, USA, 14–16 August 2019.
14. Song, M.; Wang, Z.; Zhang, Z.; Song, Y.; Wang, Q.; Ren, J.; Qi, H. Analyzing User-Level Privacy Attack Against Federated Learning. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2430–2444. [CrossRef]
15. Geiping, J.; Bauermeister, H.; Dröge, H.; Moeller, M. Inverting Gradients—How Easy Is It to Break Privacy in Federated Learning? In Proceedings of the Advances in Neural Information Processing Systems, Online, 6–12 December 2020; Curran Associates, Inc.: New York, NY, USA, 2020; Volume 33, pp. 16937–16947.
16. Konečný, J.; McMahan, H.B.; Yu, F.X.; Richtárik, P.; Suresh, A.T.; Bacon, D. Federated Learning: Strategies for Improving Communication Efficiency. Available online: https://arxiv.org/abs/1610.05492v2 (accessed on 10 October 2023).
17. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
18. Wang, L.; Wang, W.; Li, B. CMFL: Mitigating Communication Overhead for Federated Learning. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–9 July 2019; pp. 954–964.
19. Li, L.; Fan, Y.; Tse, M.; Lin, K.-Y. A Review of Applications in Federated Learning. *Comput. Ind. Eng.* **2020**, *149*, 106854. [CrossRef]
20. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal. Process. Mag.* **2020**, *37*, 50–60. [CrossRef]
21. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 30 November 2023).
22. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain Challenges and Opportunities: A Survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
23. Toyoda, K.; Zhang, A.N. Mechanism Design for An Incentive-Aware Blockchain-Enabled Federated Learning Platform. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 395–403.
24. Hou, D.; Zhang, J.; Man, K.L.; Ma, J.; Peng, Z. A Systematic Literature Review of Blockchain-Based Federated Learning: Architectures, Applications and Issues. In Proceedings of the 2021 2nd Information Communication Technologies Conference (ICTC), Nanjing, China, 7–9 May 2021; pp. 302–307.
25. Wahab, O.A.; Mourad, A.; Otrok, H.; Taleb, T. Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1342–1397. [CrossRef]
26. Nguyen, D.C.; Ding, M.; Pham, Q.-V.; Pathirana, P.N.; Le, L.B.; Seneviratne, A.; Li, J.; Niyato, D.; Poor, H.V. Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges. *IEEE Internet Things J.* **2021**, *8*, 12806–12825. [CrossRef]
27. Issa, W.; Moustafa, N.; Turnbull, B.; Sohrabi, N.; Tari, Z. Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey. *ACM Comput. Surv.* **2023**, *55*, 191. [CrossRef]
28. Li, D.; Han, D.; Weng, T.-H.; Zheng, Z.; Li, H.; Liu, H.; Castiglione, A.; Li, K.-C. Blockchain for Federated Learning toward Secure Distributed Machine Learning Systems: A Systemic Survey. *Soft Comput.* **2022**, *26*, 4423–4440. [CrossRef]
29. Feng, L.; Zhao, Y.; Guo, S.; Qiu, X.; Li, W.; Yu, P. BAFL: A Blockchain-Based Asynchronous Federated Learning Framework. *IEEE Trans. Comput.* **2022**, *71*, 1092–1103. [CrossRef]
30. Li, Y.; Chen, C.; Liu, N.; Huang, H.; Zheng, Z.; Yan, Q. A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus. *IEEE Netw.* **2021**, *35*, 234–241. [CrossRef]
31. Lyu, L.; Yu, H.; Yang, Q. Threats to Federated Learning: A Survey. *arXiv* **2020**, *preprint*. arXiv:2003.02133.
32. Khan, L.U.; Saad, W.; Han, Z.; Hossain, E.; Hong, C.S. Federated Learning for Internet of Things: Recent Advances, Taxonomy, and Open Challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1759–1799. [CrossRef]
33. Sun, G.; Cong, Y.; Dong, J.; Wang, Q.; Lyu, L.; Liu, J. Data Poisoning Attacks on Federated Machine Learning. *IEEE Internet Things J.* **2022**, *9*, 11365–11375. [CrossRef]
34. Tolpegin, V.; Truex, S.; Gursoy, M.E.; Liu, L. Data Poisoning Attacks Against Federated Learning Systems. In Proceedings of the Computer Security—ESORICS 2020, Guildford, UK, 14–18 September 2020; Chen, L., Li, N., Liang, K., Schneider, S., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 480–501.
35. Chen, X.; Liu, C.; Li, B.; Lu, K.; Song, D. Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning. *arXiv* **2017**, *preprint*. arXiv:1712.05526.
36. Alfeld, S.; Zhu, X.; Barford, P. Data Poisoning Attacks against Autoregressive Models. In Proceedings of the AAAI Conference on Artificial Intelligence, Phoenix, AZ, USA, 12–17 February 2016; Volume 30.
37. Li, B.; Wang, Y.; Singh, A.; Vorobeychik, Y. Data Poisoning Attacks on Factorization-Based Collaborative Filtering. In Proceedings of the 30th Annual Conference on Neural Information Processing Systems 2016, Barcelona, Spain, 5–10 December 2016; Volume 29.
38. Caldas, S.; Konečny, J.; McMahan, H.B.; Talwalkar, A. Expanding the Reach of Federated Learning by Reducing Client Resource Requirements. Available online: https://arxiv.org/abs/1812.07210v2 (accessed on 10 October 2023).
39. Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D. Blockchain. *Bus. Inf. Syst. Eng.* **2017**, *59*, 183–187. [CrossRef]

40. Zheng, W.; Zheng, Z.; Chen, X.; Dai, K.; Li, P.; Chen, R. Nutbaas: A Blockchain-as-a-Service Platform. *IEEE Access* **2019**, *7*, 134422–134433. [CrossRef]
41. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain Technology Overview. Available online: https://arxiv.org/abs/1906.11078v1 (accessed on 10 October 2023).
42. Xu, L.; Shah, N.; Chen, L.; Diallo, N.; Gao, Z.; Lu, Y.; Shi, W. Enabling the Sharing Economy: Privacy Respecting Contract Based on Public Blockchain. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, United Arab Emirates, 2 April 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 15–21.
43. Jiao, Y.; Wang, P.; Niyato, D.; Suankaewmanee, K. Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks. *IEEE Trans. Parallel Distrib. Syst.* **2019**, *30*, 1975–1989. [CrossRef]
44. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain Technology: Beyond Bitcoin. *Appl. Innov.* **2016**, *2*, 71.
45. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
46. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3690–3700. [CrossRef]
47. Kang, J.; Xiong, Z.; Niyato, D.; Wang, P.; Ye, D.; Kim, D.I. Incentivizing Consensus Propagation in Proof-of-Stake Based Consortium Blockchain Networks. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 157–160. [CrossRef]
48. Xu, M.; Chen, X.; Kou, G. A Systematic Review of Blockchain. *Financ. Innov.* **2019**, *5*, 27. [CrossRef]
49. Yang, M.; Zhu, T.; Liang, K.; Zhou, W.; Deng, R.H. A Blockchain-Based Location Privacy-Preserving Crowdsensing System. *Future Gener. Comput. Syst.* **2019**, *94*, 408–418. [CrossRef]
50. Rouhani, S.; Deters, R. Performance Analysis of Ethereum Transactions in Private Blockchain. In Proceedings of the 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Piscataway, NJ, USA, 24–26 November 2017; pp. 70–74.
51. Dinh, T.T.A.; Wang, J.; Chen, G.; Liu, R.; Ooi, B.C.; Tan, K.-L. BLOCKBENCH: A Framework for Analyzing Private Blockchains. In Proceedings of the 2017 ACM International Conference on Management of Data, Chicago, IL, USA, 14–19 May 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1085–1100.
52. Iansiti, M.; Lakhani, K.R. The Truth about Blockchain. *Harv. Bus. Rev.* **2017**, *95*, 118–127.
53. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
54. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the Security and Performance of Proof of Work Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 3–16.
55. Nguyen, C.T.; Hoang, D.T.; Nguyen, D.N.; Niyato, D.; Nguyen, H.T.; Dutkiewicz, E. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access* **2019**, *7*, 85727–85745. [CrossRef]
56. Saad, S.M.S.; Radzi, R.Z.R.M. Comparative Review of the Blockchain Consensus Algorithm between Proof of Stake (POS) and Delegated Proof of Stake (DPOS). *Int. J. Innov. Comput.* **2020**, *10*, 1273–1282. [CrossRef]
57. Ailijiang, A.; Charapko, A.; Demirbas, M. Consensus in the Cloud: Paxos Systems Demystified. In Proceedings of the 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA, 1–4 August 2016; pp. 1–10.
58. Huang, D.; Ma, X.; Zhang, S. Performance Analysis of the Raft Consensus Algorithm for Private Blockchains. *IEEE Trans. Syst. Man. Cybern. Syst.* **2020**, *50*, 172–181. [CrossRef]
59. Sukhwani, H.; Martínez, J.M.; Chang, X.; Trivedi, K.S.; Rindos, A. Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric). In Proceedings of the 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 26 September 2017; pp. 253–255.
60. Bamakan, S.M.H.; Babaei Bondarti, A.; Babaei Bondarti, P.; Qu, Q. Blockchain Technology Forecasting by Patent Analytics and Text Mining. *Blockchain Res. Appl.* **2021**, *2*, 100019. [CrossRef]
61. Dos Santos, S.; Singh, J.; Thulasiram, R.K.; Kamali, S.; Sirico, L.; Loud, L. A New Era of Blockchain-Powered Decentralized Finance (DeFi)—A Review. In Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 27 June–1 July 2022; pp. 1286–1292.
62. Wu, H.; Cao, J.; Yang, Y.; Tung, C.L.; Jiang, S.; Tang, B.; Liu, Y.; Wang, X.; Deng, Y. Data Management in Supply Chain Using Blockchain: Challenges and a Case Study. In Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July–1 August 2019; pp. 1–8.
63. Wu, H.; Jiang, S.; Cao, J. High-Efficiency Blockchain-Based Supply Chain Traceability. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3748–3758. [CrossRef]
64. Yao, S.; Wang, M.; Qu, Q.; Zhang, Z.; Zhang, Y.-F.; Xu, K.; Xu, M. Blockchain-Empowered Collaborative Task Offloading for Cloud-Edge-Device Computing. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3485–3500. [CrossRef]
65. Liu, Y.; Lu, Q.; Chen, S.; Qu, Q.; O'Connor, H.; Raymond Choo, K.-K.; Zhang, H. Capability-Based IoT Access Control Using Blockchain. *Digit. Commun. Netw.* **2021**, *7*, 463–469. [CrossRef]
66. Lalitha, A.; Kilinc, O.C.; Javidi, T.; Koushanfar, F. Peer-to-Peer Federated Learning on Graphs. *arXiv* **2019**, *preprint*. arXiv:1901.11173.

67. Savazzi, S.; Nicoli, M.; Rampa, V. Federated Learning with Cooperating Devices: A Consensus Approach for Massive IoT Networks. *IEEE Internet Things J.* **2020**, *7*, 4641–4654. [CrossRef]
68. Hu, C.; Jiang, J.; Wang, Z. Decentralized Federated Learning: A Segmented Gossip Approach. *arXiv* **2019**, *preprint*. arXiv:1908.07782.
69. Abou El Houda, Z.; Hafid, A.S.; Khoukhi, L. Mitfed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using Sdn and Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 1985–2001. [CrossRef]
70. Moulahi, T.; Jabbar, R.; Alabdulatif, A.; Abbas, S.; El Khediri, S.; Zidi, S.; Rizwan, M. Privacy-preserving Federated Learning Cyber-threat Detection for Intelligent Transport Systems with Blockchain-based Security. *Expert. Syst.* **2023**, *40*, e13103. [CrossRef]
71. Huang, X.; Wu, Y.; Liang, C.; Chen, Q.; Zhang, J. Distance-Aware Hierarchical Federated Learning in Blockchain-Enabled Edge Computing Network. *IEEE Internet Things J.* **2023**, *10*, 19163–19176. [CrossRef]
72. Bao, X.; Su, C.; Xiong, Y.; Huang, W.; Hu, Y. Flchain: A Blockchain for Auditable Federated Learning with Trust and Incentive. In Proceedings of the 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), IEEE, Qingdao, China, 9–11 August 2019; pp. 151–159.
73. Baucas, M.J.; Spachos, P.; Plataniotis, K.N. Federated Learning and Blockchain-Enabled Fog-IoT Platform for Wearables in Predictive Healthcare. *IEEE Trans. Comput. Soc. Syst.* **2023**, *10*, 1732–1741. [CrossRef]
74. Ullah, I.; Deng, X.; Pei, X.; Jiang, P.; Mushtaq, H. A Verifiable and Privacy-Preserving Blockchain-Based Federated Learning Approach. *Peer Peer Netw. Appl.* **2023**, *16*, 2256–2270. [CrossRef]
75. Mohammed, M.A.; Lakhan, A.; Abdulkareem, K.H.; Zebari, D.A.; Nedoma, J.; Martinek, R.; Kadry, S.; Garcia-Zapirain, B. Energy-Efficient Distributed Federated Learning Offloading and Scheduling Healthcare System in Blockchain Based Networks. *Internet Things* **2023**, *22*, 100815. [CrossRef]
76. Fan, M.; Zhang, Z.; Li, Z.; Sun, G.; Yu, H.; Guizani, M. Blockchain-Based Decentralized and Lightweight Anonymous Authentication for Federated Learning. *IEEE Trans. Veh. Technol.* **2023**, *72*, 12075–12086. [CrossRef]
77. Zhang, J.; Liu, Y.; Qin, X.; Xu, X.; Zhang, P. Adaptive Resource Allocation for Blockchain-Based Federated Learning in Internet of Things. *IEEE Internet Things J.* **2023**, *10*, 10621–10635. [CrossRef]
78. Yang, F.; Abedin, M.Z.; Hajek, P. An Explainable Federated Learning and Blockchain-Based Secure Credit Modeling Method. *Eur. J. Oper. Res.* **2023**, *in press*. [CrossRef]
79. Singh, S.K.; Yang, L.T.; Park, J.H. FusionFedBlock: Fusion of Blockchain and Federated Learning to Preserve Privacy in Industry 5.0. *Inf. Fusion.* **2023**, *90*, 233–240. [CrossRef]
80. Kim, H.; Park, J.; Bennis, M.; Kim, S.-L. Blockchained On-Device Federated Learning. *IEEE Commun. Lett.* **2020**, *24*, 1279–1283. [CrossRef]
81. Pokhrel, S.R.; Choi, J. Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges. *IEEE Trans. Commun.* **2020**, *68*, 4734–4746. [CrossRef]
82. Qu, Y.; Gao, L.; Luan, T.H.; Xiang, Y.; Yu, S.; Li, B.; Zheng, G. Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing. *IEEE Internet Things J.* **2020**, *7*, 5171–5183. [CrossRef]
83. Awan, S.; Li, F.; Luo, B.; Liu, M. 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, London, UK, 11–15 November 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 2561–2563.
84. Hieu, N.Q.; Anh, T.T.; Luong, N.C.; Niyato, D.; Kim, D.I.; Elmroth, E. Resource Management for Blockchain-Enabled Federated Learning: A Deep Reinforcement Learning Approach. Available online: https://arxiv.org/abs/2004.04104v2 (accessed on 10 October 2023).
85. Majeed, U.; Hong, C.S. FLchain: Federated Learning via MEC-Enabled Blockchain Network. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.
86. Li, Z.; Liu, J.; Hao, J.; Wang, H.; Xian, M. CrowdSFL: A Secure Crowd Computing Framework Based on Blockchain and Federated Learning. *Electronics* **2020**, *9*, 773. [CrossRef]
87. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4298–4311. [CrossRef]
88. Kang, J.; Xiong, Z.; Jiang, C.; Liu, Y.; Guo, S.; Zhang, Y.; Niyato, D.; Leung, C.; Miao, C. Scalable and Communication-Efficient Decentralized Federated Edge Learning with Multi-Blockchain Framework. In Proceedings of the Blockchain and Trustworthy Systems, Dali, China, 6–7 August 2020; Zheng, Z., Dai, H.-N., Fu, X., Chen, B., Eds.; Springer: Singapore, 2020; pp. 152–165.
89. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT (Not Survey). *IEEE Trans. Ind. Inf.* **2020**, *16*, 4177–4186. [CrossRef]
90. ur Rehman, M.H.; Salah, K.; Damiani, E.; Svetinovic, D. Towards Blockchain-Based Reputation-Aware Federated Learning. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Online, 6–9 July 2020; pp. 183–188.
91. Zhang, W.; Lu, Q.; Yu, Q.; Li, Z.; Liu, Y.; Lo, S.K.; Chen, S.; Xu, X.; Zhu, L. Blockchain-Based Federated Learning for Device Failure Detection in Industrial IoT. *IEEE Internet Things J.* **2021**, *8*, 5926–5937. [CrossRef]
92. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5098–5107. [CrossRef]

93. Jiang, C.; Xu, C.; Cao, C.; Chen, K. GAIN: Decentralized Privacy-Preserving Federated Learning. *J. Inf. Secur. Appl.* **2023**, *78*, 103615. [CrossRef]
94. Ma, X.; Xu, D. TORR: A Lightweight Blockchain for Decentralized Federated Learning. *IEEE Internet Things J.* **2023**, 1. [CrossRef]
95. Zekiye, A.; Özkasap, Ö. Decentralized Healthcare Systems with Federated Learning and Blockchain. *arXiv* **2023**, *preprint*. arXiv:2306.17188.
96. Liu, S.; Wang, X.; Hui, L.; Wu, W. Blockchain-Based Decentralized Federated Learning Method in Edge Computing Environment. *Appl. Sci.* **2023**, *13*, 1677. [CrossRef]
97. Sharma, P.K.; Park, J.H.; Cho, K. Blockchain and Federated Learning-Based Distributed Computing Defence Framework for Sustainable Society. *Sustain. Cities Soc.* **2020**, *59*, 102220. [CrossRef]
98. Arachchige, P.C.M.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S.; Atiquzzaman, M. A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6092–6102. [CrossRef]
99. Wang, Z.; Hu, Q.; Li, R.; Xu, M.; Xiong, Z. Incentive Mechanism Design for Joint Resource Allocation in Blockchain-Based Federated Learning. *IEEE Trans. Parallel Distrib. Syst.* **2023**, *34*, 1536–1547. [CrossRef]
100. Park, M.; Chai, S. BTIMFL: A Blockchain-Based Trust Incentive Mechanism in Federated Learning. In Proceedings of the International Conference on Computational Science and Its Applications, Athens, Greece, 3–6 July 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 175–185.
101. Kim, H.; Park, J.; Bennis, M.; Kim, S.-L. On-Device Federated Learning via Blockchain and Its Latency Analysis. *arXiv* **2018**, arXiv:1808.03949.
102. Kang, J.; Xiong, Z.; Niyato, D.; Xie, S.; Zhang, J. Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory. *IEEE Internet Things J.* **2019**, *6*, 10700–10714. [CrossRef]
103. Weng, J.; Weng, J.; Zhang, J.; Li, M.; Zhang, Y.; Luo, W. DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-Based Incentive. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 2438–2455. [CrossRef]
104. Kim, Y.J.; Hong, C.S. Blockchain-Based Node-Aware Dynamic Weighting Methods for Improving Federated Learning Performance. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.
105. Zhan, Y.; Li, P.; Qu, Z.; Zeng, D.; Guo, S. A Learning-Based Incentive Mechanism for Federated Learning. *IEEE Internet Things J.* **2020**, *7*, 6360–6368. [CrossRef]
106. Dong, N.; Wang, Z.; Sun, J.; Kampffmeyer, M.; Wen, Y.; Zhang, S.; Knottenbelt, W.; Xing, E. Defending Against Malicious Behaviors in Federated Learning with Blockchain. *arXiv* **2023**, *preprint*. arXiv:2307.00543.
107. Kalapaaking, A.P.; Khalil, I.; Yi, X. Blockchain-Based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems. *IEEE Trans. Emerg. Top. Comput.* **2023**, 1–11. [CrossRef]
108. Prokop, K.; Połap, D.; Srivastava, G.; Lin, J.C.-W. Blockchain-Based Federated Learning with Checksums to Increase Security in Internet of Things Solutions. *J. Ambient. Intell. Hum. Comput.* **2023**, *14*, 4685–4694. [CrossRef]
109. Zhao, Y.; Zhao, J.; Jiang, L.; Tan, R.; Niyato, D.; Li, Z.; Lyu, L.; Liu, Y. Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices. *IEEE Internet Things J.* **2021**, *8*, 1817–1829. [CrossRef]
110. Zhang, K.; Huang, H.; Guo, S.; Zhou, X. Blockchain-Based Participant Selection for Federated Learning. In Proceedings of the Blockchain and Trustworthy Systems, Dali, China, 6–7 August 2020; Zheng, Z., Dai, H.-N., Fu, X., Chen, B., Eds.; Springer: Singapore, 2020; pp. 112–125.
111. Shayan, M.; Fung, C.; Yoon, C.J.M.; Beschastnikh, I. Biscotti: A Blockchain System for Private and Secure Federated Learning. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1513–1525. [CrossRef]
112. Chen, H.; Asif, S.A.; Park, J.; Shen, C.-C.; Bennis, M. Robust Blockchained Federated Learning with Model Validation and Proof-of-Stake Inspired Consensus. Available online: https://arxiv.org/abs/2101.03300v1 (accessed on 10 October 2023).
113. Ouyang, L.; Wang, F.-Y.; Tian, Y.; Jia, X.; Qi, H.; Wang, G. Artificial Identification: A Novel Privacy Framework for Federated Learning Based on Blockchain. *IEEE Trans. Comput. Soc. Syst.* **2023**, 1–10. [CrossRef]
114. Javed, L.; Anjum, A.; Yakubu, B.M.; Iqbal, M.; Moqurrab, S.A.; Srivastava, G. ShareChain: Blockchain-enabled Model for Sharing Patient Data Using Federated Learning and Differential Privacy. *Expert. Syst.* **2023**, *40*, e13131. [CrossRef]
115. Guduri, M.; Chakraborty, C.; Margala, M. Blockchain-Based Federated Learning Technique for Privacy Preservation and Security of Smart Electronic Health Records. *IEEE Trans. Consum. Electron.* **2023**, 1. [CrossRef]
116. Martinez, I.; Francis, S.; Hafid, A.S. Record and Reward Federated Learning Contributions with Blockchain. In Proceedings of the 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 17–19 October 2019; pp. 50–57.
117. Tao, R.E.N.; Ruochen, J.I.N.; Yongmei, L.U.O. Network Intrusion Detection Algorithm Integrating Blockchain and Federated Learning. *Netinfo Secur.* **2021**, *21*, 27. [CrossRef]
118. Qi, Y.; Hossain, M.S.; Nie, J.; Li, X. Privacy-Preserving Blockchain-Based Federated Learning for Traffic Flow Prediction. *Future Gener. Comput. Syst.* **2021**, *117*, 328–337. [CrossRef]
119. Zhang, J.; Zhou, J.; Guo, J.; Sun, X. Visual Object Detection for Privacy-Preserving Federated Learning. *IEEE Access* **2023**, *11*, 33324–33335. [CrossRef]
120. Mahmood, Z.; Jusas, V. Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy. *Electronics* **2022**, *11*, 1624. [CrossRef]

121. Kumar, S.; Dutta, S.; Chatturvedi, S.; Bhatia, M. Strategies for Enhancing Training and Privacy in Blockchain Enabled Federated Learning. In Proceedings of the 2020 IEEE Sixth International Conference on Multimedia Big Data (BigMM), New Delhi, India, 24–26 September 2020; pp. 333–340.
122. Kalapaaking, A.P.; Khalil, I.; Rahman, M.S.; Atiquzzaman, M.; Yi, X.; Almashor, M. Blockchain-Based Federated Learning with Secure Aggregation in Trusted Execution Environment for Internet-of-Things. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1703–1714. [CrossRef]
123. Zhang, P.; Hong, Y.; Kumar, N.; Alazab, M.; Alshehri, M.D.; Jiang, C. BC-EdgeFL: A Defensive Transmission Model Based on Blockchain-Assisted Reinforced Federated Learning in IIoT Environment. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3551–3561. [CrossRef]
124. Kang, J.; Ye, D.; Nie, J.; Xiao, J.; Deng, X.; Wang, S.; Xiong, Z.; Yu, R.; Niyato, D. Blockchain-Based Federated Learning for Industrial Metaverses: Incentive Scheme with Optimal AoI. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 22–25 August 2022; pp. 71–78.
125. Lian, Z.; Zeng, Q.; Wang, W.; Gadekallu, T.R.; Su, C. Blockchain-Based Two-Stage Federated Learning With Non-IID Data in IoMT System. *IEEE Trans. Comput. Soc. Syst.* **2023**, *10*, 1701–1710. [CrossRef]
126. Passerat-Palmbach, J.; Farnan, T.; Miller, R.; Gross, M.S.; Flannery, H.L.; Gleim, B. A Blockchain-Orchestrated Federated Learning Architecture for Healthcare Consortia. Available online: https://arxiv.org/abs/1910.12603v1 (accessed on 10 October 2023).
127. El Rifai, O.; Biotteau, M.; de Boissezon, X.; Megdiche, I.; Ravat, F.; Teste, O. Blockchain-Based Federated Learning in Medicine. In Proceedings of the Artificial Intelligence in Medicine, Minneapolis, MN, USA, 25–28 August 2020; Michalowski, M., Moskovitch, R., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 214–224.
128. Połap, D.; Srivastava, G.; Jolfaei, A.; Parizi, R.M. Blockchain Technology and Neural Networks for the Internet of Medical Things. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Online, 6–9 July 2020; pp. 508–513.
129. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef] [PubMed]
130. Aich, S.; Sinai, N.K.; Kumar, S.; Ali, M.; Choi, Y.R.; Joo, M.-I.; Kim, H.-C. Protecting Personal Healthcare Record Using Blockchain & Federated Learning Technologies. In Proceedings of the 24th International Conference on Advanced Communication Technology (ICACT), IEEE, Pyeongchang, Republic of Korea, 13–16 February 2022; pp. 109–112.
131. Kumar, R.; Khan, A.A.; Kumar, J.; Zakria; Golilarz, N.A.; Zhang, S.; Ting, Y.; Zheng, C.; Wang, W. Blockchain-Federated-Learning and Deep Learning Models for COVID-19 Detection Using CT Imaging. *IEEE Sens. J.* **2021**, *21*, 16301–16314. [CrossRef] [PubMed]
132. Hua, G.; Zhu, L.; Wu, J.; Shen, C.; Zhou, L.; Lin, Q. Blockchain-Based Federated Learning for Intelligent Control in Heavy Haul Railway. *IEEE Access* **2020**, *8*, 176830–176839. [CrossRef]
133. Chai, H.; Leng, S.; Chen, Y.; Zhang, K. A Hierarchical Blockchain-Enabled Federated Learning Algorithm for Knowledge Sharing in Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3975–3986. [CrossRef]
134. Cui, L.; Su, X.; Ming, Z.; Chen, Z.; Yang, S.; Zhou, Y.; Xiao, W. CREAT: Blockchain-Assisted Compression Algorithm of Federated Learning for Content Caching in Edge Computing. *IEEE Internet Things J.* **2022**, *9*, 14151–14161. [CrossRef]
135. Halim, S.M.; Khan, L.; Thuraisingham, B. Next—Location Prediction Using Federated Learning on a Blockchain. In Proceedings of the 2020 IEEE Second International Conference on Cognitive Machine Intelligence (CogMI), Atlanta, GA, USA, 28–31 October 2020; pp. 244–250.
136. Wang, Y.; Su, Z.; Zhang, N.; Benslimane, A. Learning in the Air: Secure Federated Learning for UAV-Assisted Crowdsensing. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1055–1069. [CrossRef]
137. Pokhrel, S.R. Federated Learning Meets Blockchain at 6G Edge: A Drone-Assisted Networking for Disaster Response. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, London, UK, 25 September 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 49–54.
138. Wang, Y.; Tian, Y.; Yin, X.; Hei, X. A Trusted Recommendation Scheme for Privacy Protection Based on Federated Learning. *CCF Trans. Netw.* **2020**, *3*, 218–228. [CrossRef]
139. Singh, A.; Click, K.; Parizi, R.M.; Zhang, Q.; Dehghantanha, A.; Choo, K.-K.R. Sidechain Technologies in Blockchain Networks: An Examination and State-of-the-Art Review. *J. Netw. Comput. Appl.* **2020**, *149*, 102471. [CrossRef]
140. Chen, J.; Micali, S. Algorand. Available online: https://arxiv.org/abs/1607.01341v9 (accessed on 11 October 2023).
141. Silvano, W.F.; Marcelino, R. Iota Tangle: A Cryptocurrency to Communicate Internet-of-Things Data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
142. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A Survey on the Security of Blockchain Systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.