applied sciences

MDPI

Review

Blockchain-Based Federated Learning: A Survey and New Perspectives

Weiguang Ning [1], Yingjuan Zhu [2], Caixia Song [3,*], Hongxia Li [3], Lihui Zhu [3], Jinbao Xie [3], Tianyu Chen [3], Tong Xu [3], Xi Xu [3] and Jiwei Gao [3]

[1] Qingdao Smart Village Development Service Center, Qingdao 266199, China
[2] College of Agronomy, Qingdao Agricultural University, Qingdao 266109, China
[3] College of Science and Information, Qingdao Agricultural University, Qingdao 266109, China
* Correspondence: cassiesong@qau.edu.cn

Abstract: Federated learning, as a novel distributed machine learning mode, enables the training of machine learning models on multiple devices while ensuring data privacy. However, the existence of single-point-of-failure bottlenecks, malicious threats, scalability of federated learning implementation, and lack of incentive mechanisms have seriously hindered the development of federated learning technology. In recent years, as a distributed ledger, blockchain has the characteristics of decentralization, tamper-proof, transparency, security, etc., which can solve the issues encountered in the above-mentioned federated learning. Particularly, the integration of federated learning and blockchain leads to a new paradigm, called blockchain-based federated learning (BFL), which has been successfully applied in many application scenarios. This paper aims to provide a comprehensive review of recent efforts on blockchain-based federated learning. More concretely, we propose and design a taxonomy of blockchain-based federated learning models, along with providing a comprehensive summary of the state of the art. Various applications of federated learning based on blockchain are introduced. Finally, we expand on current trends and provide new perspectives pertaining to this new and exciting development in the field.

Keywords: blockchain; federated learning; blockchain-based federated learning; distributed machine learning

Citation: Ning, W.; Zhu, Y.; Song, C.; Li, H.; Zhu, L.; Xie, J.; Chen, T.; Xu, T.; Xu, X.; Gao, J. Blockchain-Based Federated Learning: A Survey and New Perspectives. *Appl. Sci.* **2024**, *14*, 9459. https://doi.org/10.3390/app14209459

Academic Editor: Gianluca Lax

Received: 5 September 2024
Revised: 9 October 2024
Accepted: 10 October 2024
Published: 16 October 2024

1. Introduction

Federated learning (FL) [1] is a distributed machine learning approach to protecting privacy in distributed scenarios with edge intelligence, first proposed by Google in 2016 [2]. In traditional machine learning, all training data are collected by a centralized manager, which is prone to privacy and transmission problems. However, federated learning can prevent local data privacy disclosure to a large extent and reduce data transmission costs by allocating training work to users themselves [3]. Federated learning is a decentralized multi-user scenario $F_1, \ldots, F_N$, where each user client owns the current user's dataset $D_1, \ldots, D_N$. Traditional deep learning collects these data together to obtain an aggregated dataset $D = U_1 \cup \ldots \cup U_N$, and the model M_{SUM} is obtained after training. The federated learning method jointly trains a model M_{FED} with the participating users. At the same time, the user data D_i are kept locally and will not be transmitted externally. If there is a non-negative real number δ, the model accuracy V_{FED} of M_{FED} and the model accuracy V_{SUM} of M_{SUM} satisfy the following inequality:

$$|V_{FED} - V_{SUM}| < \delta \quad (1)$$

The federated learning algorithm achieves δ-precision loss.

Despite these advantages, federated learning still has some noticeable defects. First, federated learning lacks vetting of malicious trainers, and dishonest cooperation can inter-

fere with model training. In addition, federated learning is vulnerable to malicious servers, and huge threats are triggered by information leakage [4]. Meanwhile, the centralized parameter server is vulnerable to a single point of failure and can cost all trainers. Furthermore, the problem of insufficient incentive and lack of a certain reward distribution system for federated learning model training also needs to be solved. Therefore, it is critical to establish an open, auditable [5,6], decentralized [7], incentivized, and defensible [8] federated learning mechanism.

Blockchain, as the underlying technology underpinning Bitcoin, is essentially a decentralized database [9] capable of building ledgers in a secure and verifiable manner [10]. Moreover, consensus mechanisms, cryptography and smart contracts in blockchain enable secure transactions between participants without a central authority. The structure of blockchain is shown in Figure 1. Because of the advanced characteristics of blockchain, such as anonymity, tamper resistance, and decentralization, blockchain is widely used in fields such as in-vehicle networks [11,12], industrial Internet of Things [13,14], and medical networks [15].

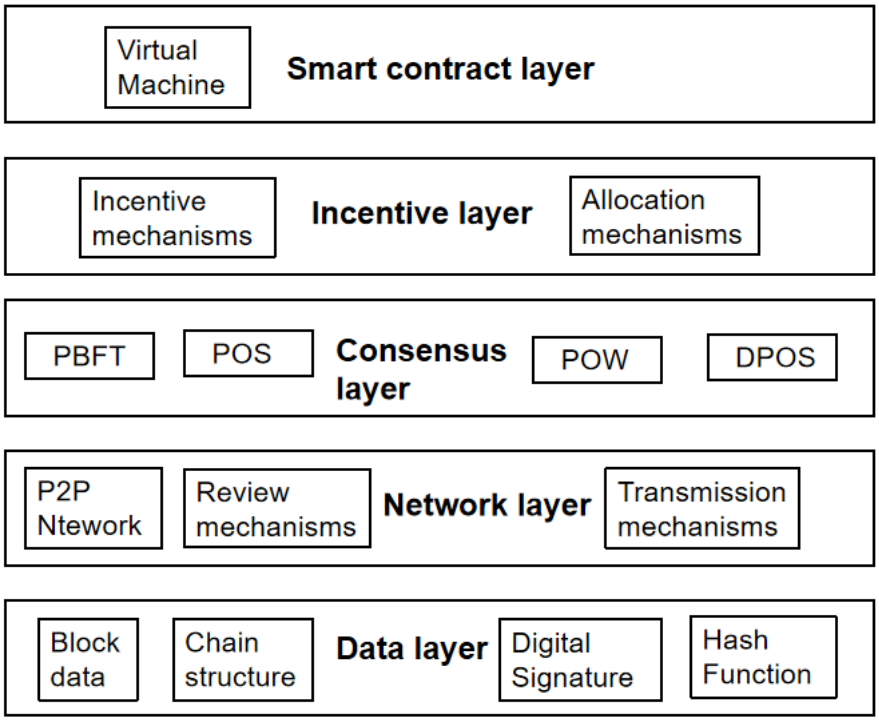

Figure 1. Blockchain architecture.

More importantly, blockchain-distributed trust provides a new approach for designing federated learning frameworks and paradigms. The main feature of blockchain is that it allows untrusted participants to communicate with each other and send status update messages in a secure manner without the involvement of a fully trusted third party or authorized central node. Therefore, blockchain can effectively solve the problems in federated learning, an approach called blockchain-based federated learning (BFL). Blockchain's central aggregator identifies malicious and unreliable actors by automating smart contract execution to defend against federated learning poisoning attacks [16,17]. Sun et al. [18] designed a new blockchain platform to manage reputation value in a decentralized manner, which can ensure accurate historical reputation, thus greatly improving the accuracy of FL. Wang et al. [19] proposed a blockchain-based encryption gradient audit method that uses the behavior chain to record the encryption gradient from the data owner to improve the security of FL. A blockchain-assisted federated learning (BC-FL) framework was developed to overcome the single point of failure caused by the FL central server.

Pervasiveness and ubiquity of blockchain in federated learning systems. In practical application scenarios, blockchain federated learning has been widely used in many fields. In the industrial Internet of Things (IIoT), the platform architecture of blockchain-based federated learning is used for failure detection in the IIoT for verifying the integrity of client data [20], safe model transfer and accelerated model training [21], and ensuring the security of industrial data transmission [22]. In the field of car networking, BFL can be used for promoting the dissemination of vehicle network information, which overcomes problems such as low data reception rate and privacy security [23,24]. Using a layered blockchain framework is proposed to enable vehicles to learn environmental data through machine learning methods and share learning knowledge with each other [25], addressing the privacy concerns of private data sharing [26]. In medical system networks, BFL is applied for privacy protection of electronic health records [27,28], sensitive healthcare data privacy protection in clinical institutions [29], and detecting COVID-19 with CT imaging [30].

What are the differences between this survey and former ones? In recent years, the number of research publications on blockchain-based federated learning has grown exponentially, strongly demonstrating the importance and ubiquity of blockchain in federated learning research, making this study more persuasive. However, to the best of our knowledge, few systematic reviews have sufficiently summarized the field, pinpointing existing work and current progress.

We conduct some surveys on traditional federated learning and blockchain technology and find that many papers lack a comprehensive and systematic review of blockchain-based federated learning. Although two papers are important to the field, they suffer from the disadvantages of few references and insufficient content [31,32]. Also, Hou et al. [31] highlight that there is neither an in-depth exploration of this area nor a comprehensive description of solutions to federated learning challenges from a blockchain perspective. More importantly, Li et al. [32] have less description of the blockchain-based federated learning model and lack a systematic description of the combination of the two technologies. Lastly, Internet of Things (IoT) security and digital twins are the main application directions in [33,34]. Although there exists research on specific models, there is a lack of investigation in other application fields with strong limitations.

Contributions of this survey. The purpose of this survey is to comprehensively review the research progress of blockchain-based federated learning. Although they are effective for preserving privacy, federated learning systems face limitations such as single points of failure, lack of incentives, and inadequate security. To address these challenges, blockchain technology is integrated into federated learning systems to provide stronger security, fairness, and scalability [35]. On the other hand, this review summarizes the technical framework integrating the two, and summarizes the application scenarios in healthcare [36,37], finance [38], industry [39], and so on. This review lays the foundation for promoting innovation in the field of federated learning and tapping into the richness of this research field. This review serves researchers, practitioners, and educators interested in federated learning, hoping that they will have a general guideline when choosing a blockchain to solve the federated learning task at hand. In summary, the main contributions of this survey are in four aspects: (1) To summarize the challenges of federated learning and propose the possibility of blockchain enabling federated learning; (2) To provide a new classification for FL supported by blockchain, taking into account the technical characteristics and architecture of blockchain; (3) To summarize the technical framework integrating the two, and classify and analyze the application direction of BFL; (4) To discuss the future development and application of blockchain-based federated learning, and identify new trends and future directions in this research field to share the vision of blockchain-based federated learning research and expand its application scenarios.

2. Research Methodology

With the continuous emergence of new research works, a new inclusive review framework is needed to better understand this research field. We have analyzed more than

100 research documents from different perspectives, and the technical characteristics of blockchain are fully studied. Based on the investigation of the combination of blockchain and federated learning, the feasibility of federated learning based on blockchain is systematically expounded in the form of tables according to the technical characteristics and application scenarios of the model. The application scenarios include the Internet of Things, medical systems, digital currency, Unmanned Aerial Vehicles (UAVs) and other specific scenarios. More importantly, we discuss the problem-solving of BFL in detail, and systematically study the enabling mechanism of blockchain on the challenges of federated learning. In addition, we have collected the literature published in recent years, focusing on the timeliness and scientific nature of the literature, in order to provide a broad and systematic exposition of federated learning based on blockchain.

2.1. Sample Extraction

Paper collection: In this survey, we use Google Scholar and CNKI (https://www.cnki.net/, accessed on 17 September 2024) as search engines for the initial paper screening. On the other hand, English databases, such as Web of Science and IEEE Xplore, are adopted for further paper screening to discover more related papers. In addition, we screened representative important journals and high-profile conferences in the field of blockchain-based federated learning. The technology mainly includes IEEE International Conference on Blockchain (Blockchain); International Conference on Mainstreaming Blockchain Implementation (ICOMBI); International Conference on Big Data and Blockchain; IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA); International Conference on Blockchain Computing and Applications (BCCA); IEEE International Conference on Cognitive Machine Intelligence (CogMI); and IEEE Access to understand the latest progress in related fields.

Time interval: From 2014 to 2024.

Major search keywords: The major search keywords are “blockchain”, “federated learning”, “federated learning algorithms”, “BFL”, “distributed machine learning”, “blockchain technology”, “blockchain-enabled federated learning”, “blockchain-empowered federated learning”, “blockchain-based federated learning”, “Hyperledger”, “Bitcoin”, “Ethereum”, “federated learning scheme”, “smart contracts”, “peer-to-peer”, “consensus algorithm”, “decentralized federated learning”, “reliable federated learning”, etc.

Determining the final research sample: Is it related to blockchain-based federated learning technology? If relevant, include it in the research sample; otherwise, discard it.

2.2. Content Analysis Coding

Blockchain-based federated learning is based on constructing content analysis coding, which is a research method that objectively and systematically describes the content to be studied. Furthermore, it is a scientific method that sees the essence through phenomena [40]. The paper mainly discusses blockchain-based federated learning recent efforts and proposes and designs a taxonomy of blockchain-based federated learning models, along with providing a comprehensive summary of the state-of-the-art. According to the research objectives of this paper, seven researchers discuss and set the analysis coding rule together.

Basic information from the papers: title, author, year of publication, the journal name, technology used, applied model and the specific content of the model study.

Research content analysis: The analysis of blockchain solutions for traceability problems, comparison of different blockchain models, contrast traditional traceability systems with blockchain traceability systems, analysis of advantages and disadvantages of blockchain technology, and analysis of blockchain technology traceability application for agricultural products.

2.3. Research Steps

Step one: According to the principle of sample extraction, the papers were extracted and screened; then, 756 initial samples were obtained.

Step two: Is the paper related to the blockchain-based federated learning technology? If yes, it is classified into the statistical sample. Otherwise, it is discarded.

Step three: Identify the technologies used in the papers and their application scenarios in various industries. This step was performed independently by four researchers.

Step four: The preliminary identification results of the four researchers were combined, and the identification results, which were controversial, were discussed and determined by seven researchers.

Step five: The preliminary classification was performed by five researchers.

Step six: The controversial classifications were discussed and determined by seven researchers; finally, the final research samples were obtained.

Based on the above content analysis method and research steps, the final number of sample papers was determined to be 135.

According to the design analysis above, the paper selection process is shown in Figure 2.

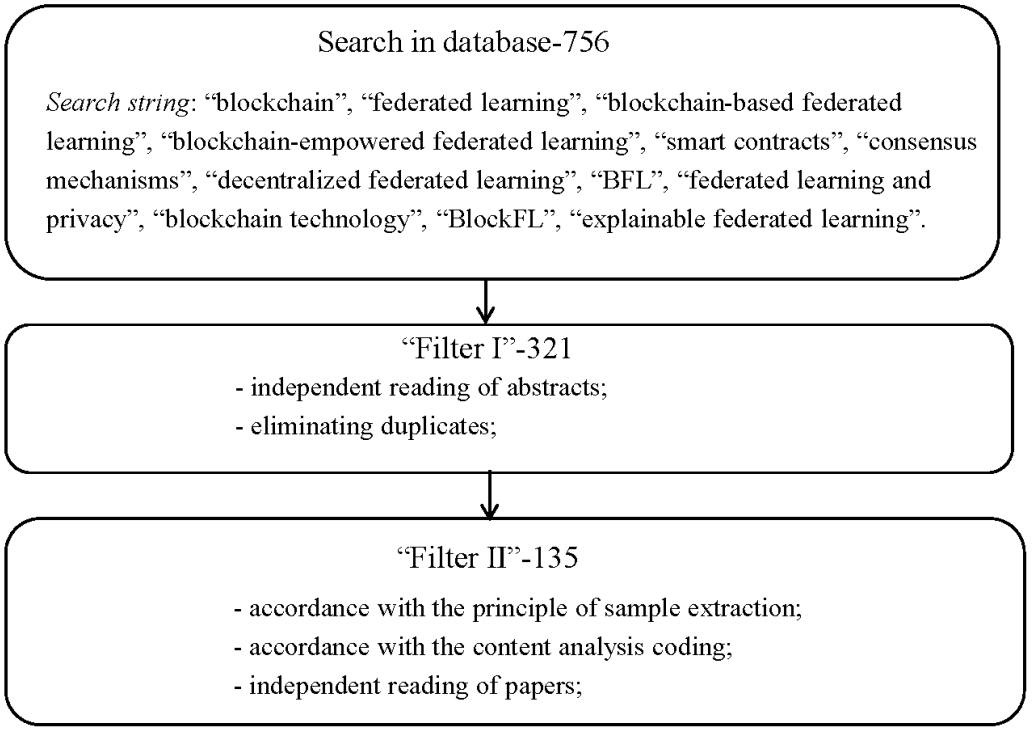

Figure 2. Methodology of research sample extraction process.

3. Blockchain vs. Federated Learning

3.1. Why Blockchain Empowers Federated Learning

Before introducing the combination of blockchain and federated learning, we first introduce the similarities and differences between blockchain and federated learning, as shown in the following Table 1:

Table 1. The similarities and differences between blockchain and federated learning.

	Blockchain	Federated Learning	References
Category of architecture	• Data structure	• Machine learning	[41,42]
Key technology	• Smart Contract • Consensus Algorithm • Hash Algorithm • Digital Signature	• Privacy protection technology • Distributed Computing • Machine Learning	[41,43]
Technical nature	• The data are consistent and form multi-party consensus.	• Data are complementary and private.	[37,44]
Data storage	• There is redundancy, each node records and stores the same data.	• There is no repetitive redundancy and each node has different feature dimensions.	[45,46]
Authentication mechanism	• Participants verify node transactions on the chain through a consensus algorithm, which has anonymity.	• The client can upload model updates without authentication, which has certain risks.	[47]
Target of application	• Build a decentralized, transparent and trusted platform to improve throughput while ensuring consensus.	• Under the premise of protecting data privacy and security, the robustness of the model is improved, and the high-quality model is trained.	[42,48]
Similarity	• Distributed structure Nodes participate equally Privacy risks. • Nodes participate equally • Privacy risks		

In short, blockchain and federated learning are different fields of computer technology. Each node of the blockchain stores the same data, which is consistent, the transaction of the node needs to be verified, and the anonymity is strong. However, too much node data can easily lead to throughput degradation. The dimensional characteristics of each node's data in federated learning are different. Node data are private and complementary to each other, but it is easy to cause a decrease in model training efficiency and data sharing obstacles as well as a series of problems caused by the central server. More importantly, FL nodes have no verification mechanism, making them prone to attack risks. Moreover, blockchain and federated learning have some similarities. Both are distributed structures and each node trades equally, and both have major flaws in privacy issues.

3.2. Drawbacks of Federated Learning

Although federated learning has many advantages, it still has some shortcomings that cannot be ignored, and more and more studies are being carried out in this area. In this part, we summarize and introduce the shortcomings of federated learning in detail so that readers can have the relevant knowledge reserve.

3.2.1. Privacy Protection

- **Privacy leakage:** In the FL framework, client devices upload raw data to the central server for model training, which may lead to the leakage of sensitive business data. In addition, if the central node obtains the information uploaded by other nodes to infer important information, it will also lead to data privacy leakage.
- **Poison attack**: Malicious actors corrupt machine learning predictions by uploading samples or models with viruses to a central server. Additionally, dishonest players

may delay transactions or terminate contracts for their own benefit at the expense of honest players, thus adversely affecting the global model [49].

3.2.2. Incentive Mechanism

- **Lack of motivation**: FL assumes that every local device voluntarily contributes data resources, but this is impractical. Participants lack motivation to perform model training as they apply their own data and computing resources. Selfish mobile devices will be unwilling to participate in model learning without fair financial compensation.
- **Improper incentive management**: Due to the decentralized nature of FL, workers may deviate from the agreement. In addition, there is a shortage of theoretical discussion on the distribution of rewards, there may be subjective judgment factors that lead to unfair distribution of profits, and the distribution of the behavior itself did not give specific rewards and punishment measures.

3.2.3. Robustness and Efficiency

- **Single-point failure**: FL relies on a central server that is vulnerable to malicious activity, causing global model updates to fail [50]. Moreover, if the central server is compromised, the entire system faces a collapse.
- **Barrier of defense**: Due to the lack of clear attack standards, FL frameworks lack defensive capability and are vulnerable to attacks, resulting in model updates being tampered by malicious agents. Likewise, FL lacks the ability to backtrack malicious clients, and the existence of malicious clients can also lead to model performance degradation and even training failure.
- **Not censoring**: Most existing federated learning systems are combined with centralized coordinators without providing any clear transparency and source mechanism for the generated models.
- **Robust performance**: Malicious or lazy devices in FL may migrate fake models or refuse to share models for profit, reducing the efficiency and reliability required for federated learning systems.
- **Network overload**: Federated learning (FL) is a decentralized learning method that breaks away from the traditional centralized learning. FL learns locally on each device and incrementally improves the learning model through interaction with a central server. However, it causes network overload due to the limited communication bandwidth and the participation of a large number of users [51].

3.3. Reasons Why Blockchain Enables Federated Learning

In summary, we have outlined the benefits of blockchain-based federated learning, which readers may keep in mind when trying to implement them.

3.3.1. Information Sharing

In blockchain-based federated learning, the consensus and incentive mechanism of the blockchain can use smart contracts and consensus algorithm technology to issue reward resources according to signed smart contracts after the federated learning model training is completed, and write the reward resources into the blockchain, effectively promoting the sharing and interaction of information in FL. For example, Liang et al. [52] proposed the use of smart contracts to realize the management of the entire federated reinforcement learning and realize the sharing and collaborative training of intelligent driving models among operators.

More importantly, P2P uses network edge resources such as storage and computing power to make the blockchain distributed, and the blockchain can further provide a shared storage system for federated learning. Therefore, BFL can store participant information in a distributed manner and realize distributed management of FL. For example, Lu et al. [24] proposed an asynchronous federated learning scheme using blockchain technology, and further improved the efficiency of federated learning information transfer by using DRL to

select optimized participating nodes. Rahmadika and Rhee [53] discussed the distributed storage of medical information obtained from multiple medical service providers by relying on blockchain technology in a peer-to-peer overlay network.

3.3.2. Privacy Storage

In blockchain-based federated learning, the digital records on the blockchain cannot be tampered with or forged and can form a new storage model. Therefore, taking advantage of the immutability of blockchain, FL can prevent malicious participants from tampering with model information to protect the global model from being destroyed [54]. The model parameters of federated learning are stored in the blockchain, which not only ensures the security and reliability of the model parameters, but also promotes participants to contribute data.

In addition, the blockchain provides a node data confidentiality mechanism. Zhang et al. [55] used the digital signature and smart contract technology of the blockchain and combined IPFS to propose a private blockchain federated learning (PriChainFL), which reduces the storage risk and risk of federated learning.

3.3.3. Reputation Incentives

The blockchain consensus mechanism provides a consensus protocol for the data stored on the chain, improving the efficiency of FL model training. The concept of blockchain-based reputation-aware fine-grained FL is proposed in [56] to ensure trusted collaborative training in mobile edge computing systems. Liu et al. [57] proposed a blockchain-based payment system for FL, where the contribution of each FL participant is evaluated through a Proof of Shapley (PoSap) consensus protocol. In addition, the characteristics of the blockchain itself can provide an incentive system for data and promote a reasonable distribution of rewards. In [29], Liu et al. discussed an incentive mechanism based on contribution points to fairly reward FL participants for contributing their local data, to achieve the authenticity of FL model aggregation and to provide incentives for FL participants. Ma et al. [58] proposed a blockchain-based federated learning framework and protocol to transparently evaluate the contribution of each participant. The framework preserves the privacy of all parties during the model building phase and transparently evaluates contributions based on model updates.

3.3.4. System Security

The blockchain has the characteristics of a stable FL model, such as digital signatures, hash algorithms, etc., and can further resist poison attacks. In [51], a consensus algorithm is used to propose a blockchain-based federated learning scenario, which can effectively avoid the problem of network overload. In terms of defense systems, Liu et al. [59] proposed a decentralized blockchain federated learning (BFL) framework with a simpler consensus mechanism, avoiding the risk of network paralysis caused by central equipment failure. In [60], authors utilized the characteristics of decentralization and anti-tampering of the blockchain to store data records and other important information on the blockchain, while the complete data are encrypted and stored in the distributed database to realize the safe storage of model data and prevent user privacy data leakage to ensure system security.

3.4. The Possibility of Combining Blockchain with Federated Learning

Blockchain is the core technology that underpins most digital cryptocurrencies since Bitcoin's launch in 2008. The combination of blockchain technology can effectively solve the challenges faced by FL. As a new decentralized and distributed computing paradigm, blockchain provides a suitable model aggregation framework for federated learning [61,62]. The P2P network in the blockchain structure will improve the fault tolerance of the FL system. Customized smart contracts not only motivate more users to participate in training but also automate the management and control of the federated learning process [63,64].

The integration of blockchain into the FL framework is widely regarded as a new basic technology for data updating and sharing, which is an inevitable trend in the future.

Technically, FL and blockchain are mutually beneficial and can therefore evolve together to form a complete solution that mines common value from distributed data owners and guarantees security and privacy controls. The mutual benefit is threefold [32]. First, the cooperation model is similar. Blockchain is a novel multi-party cooperative network architecture for distributed systems, while FL requires the participation of multiple entities and cooperative training models. Therefore, blockchain can be used as the basic architecture for FL. Secondly, they all have good security and privacy protection features. On the one hand, FL is designed to protect data privacy during distributed and collaborative data training. On the other hand, blockchain adopts a consensus mechanism and data verification mechanism in its accounting process, so that recorded transactions cannot be tampered with and denied. Thirdly, their applications can complement each other. The purpose of FL is to "create value", facilitate the complementarity of participant data and improve the validity of the model. Blockchain aims to "deliver value" by honestly documenting and rewarding the contributions of all participants [65].

4. Blockchain-Based Federated Learning: State-of-the-Art

In this section, we introduce the categories of blockchain-based federated learning and then highlight state-of-the-art research prototypes, aiming to identify the most notable and promising advancements in recent years. The purpose of this article is to present the latest progress in this area. However, the state of the art of the subject is temporary in nature, and periodic review is needed to maintain relevance and accuracy in the field of blockchain-based federated learning.

4.1. Model Classification for Blockchain-Based Federated Learning

Applying the key technologies of blockchain to federated learning is an important part of the federated learning model framework based on blockchain. In this part, we take the key technologies of blockchain as the main body and discuss the combination of key technologies of blockchain and federated learning in detail. Table 2 shows the key technologies of blockchain used to solve federated learning problems and methods, as well as the characteristics of the blockchain technology used.

Table 2. The technologies of blockchain-based federated learning.

Blockchain Technologies	Model	Solved Problem	Methods Described	Technical Characteristics	References
Smart Contract	BlockFLA FLChain SABlockFL	• The lack of trust between participants makes it impossible to establish a secure sharing mechanism.	• Proposing a new federated learning scheme based on blockchain architecture proposed, which is called federated learning data sharing.	Shareability	[66]
		• FL participants lack motivation to contribute their efforts.	• Proposing the point of contribution based on incentive mechanism to fairly reward FL participants for contributing their local data.	Anonymity and Authenticity	[29]
		• Uploading raw data to a central server for model training by client devices may lead to the disclosure of sensitive business data.	• Proposing a federated study method based on blockchain, guaranteeing the privacy of client data.	Decentralized	[20]
		• There is a lack of theoretical discussion about how rewards affect miners' behavior and how much to reward miners.	• Introducing the concept of competition into blockchain-based FL so that only workers who contribute well can be rewarded, achieving reasonable distribution of rewards.	Non-breach of contract	[63]
		• The traditional FL framework relies heavily on a centralized aggregation server, which can cause a system crash if the server is compromised.	• A blockchain-based secure FL framework is proposed to enable the creation of smart contracts prevent malicious or unreliable from participating in FL.	Non-tampering and non-breach of contract	[67]
		• Federated learning systems do not provide any standard transparency and provenance mechanisms for generated actors models.	• Proposing an integrated federated learning system "BassaML" based on blockchain and model card. The functions of model parameter sharing, local model generation, model averaging, and model sharing are realized through smart contract to enhance the transparency and trust of the model.	Transparency and auditability	[68]
Consensus Algorithm	DeepChain	• Issues of efficiency and reliability in federated learning systems.	• A model migration method based on blockchain is proposed to achieve secure model migration and accelerate model training, while minimizing computational cost.	Robustness	[21]
		• Privacy and security issues of federated learning system data.	• Proposing BLADE, an unbalanced federated learning (FL) model based on blockchain. With the help of blockchain, there is no need to worry about the failure of a single centralized server in FL, which enhances privacy protection of system data.	Decentralized	[69]

Table 2. *Cont.*

Blockchain Technologies	Model	Solved Problem	Methods Described	Technical Characteristics	References
Consensus Algorithm	DeepChain	• Data credibility and participant privacy protection. • The central node obtains information uploaded by other nodes and inferences important information, leading to data privacy disclosure. • Single point of failure due to centralized federated learning. • Due to the limited communication bandwidth and the participation of a large number of users, the network is overloaded.	• Proposing a privacy-preserving location proof mechanism using blockchain to meet these conditions and uses threshold identity-based encryption (TIBE) system to generate secret shares.	Privacy and anonymity	[70]
			• A completely decentralized federated learning framework based on blockchain is designed to avoid privacy risks of centralized structures.	Gradient inference attack audit	[71]
			• Proposing the blockchain federated learning (BlockFL) architecture is to realize machine learning on devices without any centralized training data or coordination by using the consensus mechanism in blockchain.	Decentralized	[61]
			• Proposing a local learning weighting method based on node identification, a node selection method according to the participation frequency and the amount of data, and a weighting method according to the participation frequency to converge fast and stable learning accuracy.	Locally weighted	[51]
Digital Signature	BlockFL BLADE-FL	• Data encryption makes it difficult to identify the quality of model updates, and malicious data owners can launch attacks such as data, poisoning and free-riding. • The traditional centralized machine learning management method cannot handle such a large data stream and the data privacy issue has attracted widespread attention.	• Proposing a blockchain-based cryptographic gradient audit method, which uses behavior chain to record the cryptography gradient from the data owner and uses audit chain to evaluate the quality of the gradient to achieve model security.	Gradient encryption audit	[18]
			• Based on the advantages of edge computing and federated learning, combined with the outstanding characteristics of blockchain, a secure data transmission method is proposed.	Transmission encryption	[22]

Table 2. *Cont.*

Blockchain Technologies	Model	Solved Problem	Methods Described	Technical Characteristics	References
Hash Algorithm	BAFL	• Model updates are easily tampered by malicious agents, leading to attacks on the federated learning framework.	• Proposing a novel chameleon hash scheme with variable trap gate (CHCT) for secure federated learning in IIoT Settings to enhance security.	Defensive	[54]
		• Federated learning has issues like data falsification and privacy leakage.	• In the local training stage, the PoF algorithm is designed to protect the privacy of the parameters of the local model by combining hash algorithm and differential privacy.	Audit	[72]
Peer-to-Peer Networking	ChainFL	• In a centralized central service, customer data are at risk of leakage. In addition, malicious clients can compromise model performance by performing poison attacks.	• Proposing Biscotti, a fully decentralized peer-to-peer (P2P) multi-party ML approach that uses blockchain and cryptographic primitives to implement privacy-preserving ML processes that coordinate peer-to-peer clients.	Expandability	[73]

4.1.1. Smart Contract

The smart contract technology of blockchain solves the trust problem between the participants of federated learning, the incentive management and allocation problem, the defense problem, and the data review problem. Through smart contracts, blockchains are able to manage interactions between participants without intermediaries or trusted third parties. In addition, smart contracts are decentralized, expanding the use of the underlying blockchain network [74]. In the distributed framework of BFL, the role of the central server is taken over by a smart contract to coordinate the workflow among all participating nodes. For example, it can publish modeling tasks and model training aggregation commands and validate updates sent by nodes. The node data are priced according to their contributions, and workers are rewarded or punished according to the content of contracts. It can also provide standards on where models come from and be transparent about the model training process.

Using smart contracts to manage federated learning training has many benefits. First, a copy of the global model and the associated computational state is maintained on the smart contract. Model selection and aggregation are performed in a completely decentralized manner, with user nodes making their own choices to build trust between nodes. In addition, smart contracts develop relevant protocols that, in addition to providing basic definitions of reward allocation, can also enhance trust among participants [66] and motivate participants in FL to contribute more data sets [29]. Furthermore, user nodes can use the global model copy to perform model aggregation steps in each round and update the global model independently, which can promote the development of global computing while defending against attacks from malicious participants [20]. Finally, smart contracts are backed by an underlying consensus protocol, helping to ensure transparency and a fair FL process [68].

Toyoda et al. [63] introduced the concept of competition into BFL, using the non-default nature of smart contracts to prevent workers from deviating from the agreement and to distribute rewards reasonably. Firdaus et al. [67] proposed a secure FL framework based on blockchain to prevent malicious participants from entering FL by creating smart contracts, so as to give full play to the non-tampering and non-breach properties of smart contracts.

The BlockFLA framework [75] uses smart contracts to automatically detect and punish attackers through fines, and retains the communication efficiency characteristics of FL. In addition, the framework can be inserted into any aggregation function and any attacker detection algorithm and provides experimental results that show that it can successfully punish attackers by using our new attacker detection algorithm.

In Flchain [76], global model updates were calculated, validated, validated, and stored by a blockchain network rather than a single central server. FLChain replaces the traditional FL parameter server, and its calculation results must be agreed on the chain. The participants realize the commercialization of the cooperative training model by providing a healthy market for the cooperative training model. The honest trainers obtain a fair share of the profits from the training model according to their own contributions, and the malicious trainers can be found in time and severely punished.

SABlockFL [77] is a blockchain-FL framework based on intelligent agent systems where intelligent agents act as both peers in the blockchain network and participants in FL tasks to achieve the effectiveness of data exchange between FL-trained models.

4.1.2. Consensus Algorithm

The process of selecting a billing node from a set of miner nodes through a variety of lead mechanisms [78], including voting-based, evidence-based, coalition-based, randomness-based, or other hybrid algorithms, is a key part of most blockchain consensus algorithms. The ongoing process of selecting an account node from a set of miner nodes is a key part of most blockchain consensus algorithms. One of the advantages of the blockchain consensus algorithm is that any completed request can be seen by subsequent requests but cannot be changed, so the blockchain has higher security.

There are many benefits to using consensus algorithms to facilitate federated learning training. Blockchain-based FL uses blockchain consensus mechanisms to select nodes to

participate in training, which can further improve the efficiency and robustness of FL. For example, a model migration method based on blockchain can achieve efficient model training [21]. Additionally, in BFL, we also need to consider other attributes of combined nodes and combine them with certain weights to select appropriate accounting nodes [32].

In an evidence-based mechanism, ledger nodes must demonstrate that their specific ability in each round of consensus is superior to other nodes. Inspired by this, some scholars also designed similar algorithms for BFL to ensure its robustness. For instance, honest nodes can earn equity awards more frequently, but the miner who makes the most contribution in each round of communication can create a legal block [79]. Moreover, the local weighting method of nodes [51] can be used to improve the accuracy of fast and stable learning of model convergence and achieve the robustness of BFL.

According to the characteristics of the coalition-based mechanism in which agent nodes alternately or elect to obtain the accounting authority of each block, researchers proposed to design a committee consensus mechanism to improve the training efficiency and optimize the training process [80].

By using blockchain, BFL can reduce the risk of a single point of failure through a decentralized data ledger without relying on any central server, and all network entities can transparently track any update events and user behavior.

DeepChain [49] provides blockchain-based value-driven incentives to force participants to behave correctly. At the same time, DeepChain guarantees the data privacy of each participant and provides auditability for the entire training process.

4.1.3. Digital Signature

In federated learning, data encryption makes it difficult to identify the quality of model updates, and malicious data owners may launch attacks such as data poisoning and free-riding. However, a blockchain is actually a form of blocks linked by hash values under the control of a consensus mechanism (such as Proof of Work (PoW)), mined by miners using digital signatures to make the linked blocks immune to modifications and changes [81]. Therefore, blockchain-based federated learning can realize data encryption and review, thereby ensuring data security.

In the digital signature, each node of the blockchain has a pair of public and private key pairs. During the transaction, the transaction content is first hashed at the point of transaction, and the private key is used to encrypt it to form a signature: The transaction party verifies the signature, and only after passing can the next transaction be carried out.

Data encryption makes it difficult for federated learning to identify the quality of these model updates. Therefore, Sun et al. [18] proposed a blockchain-based encryption gradient audit method to ensure the availability of aggregate gradients and achieve effective data protection. Moreover, Zhang et al. [22] adopted the distributed architecture of blockchain by taking advantage of edge computing and federated learning to upload data information to the blockchain for verification, effectively reducing the risk of information disclosure, ensuring the integrity of data transmission between devices and the security of high data communication. Using the advantages of edge computing and federated learning, the distributed architecture of blockchain is adopted to upload the data information to the blockchain for verification, effectively reducing the risk of information disclosure, ensuring the integrity of data transmission between devices and the security of high data communication.

BLADE-FL [82] is used to overcome the problem of centralized aggregation in traditional federated learning systems. Compared to traditional blockchain-enabled federated learning, BLADE-FL helps to improve privacy, prevent model leakage, and guarantee tamper-resistant model updates in a trusted blockchain network.

In BlockFL [61], local model updating is performed on data samples available on user devices. Local model updates accumulate on the blockchain in blocks. The global model update is also calculated by the user device based on the latest block, thereby

establishing the concept of federated learning on the device. The author considers the scalability, robustness and delay minimization of the global learning model.

4.1.4. Hash Algorithm

Transactions between each node in the blockchain are processed by a hashing algorithm. At the same time, SHA-256 is used to ensure the invariance of the blockchain, that is, the data in the blockchain cannot be modified or deleted. The hash indicator concatenates each block to the next block and preserves the previous hash data. Also, encrypted hash tables are often used in security protocols and applications to ensure the integrity of authentication files in a connection.

Using hashing algorithms has many benefits for federated learning. In blockchain-based federated learning, federated learning can prevent malicious actors from tampering with model information to protect the global model from being damaged by utilizing the immutability of blockchain [54]. In addition, the hash algorithm is used to encrypt the federated learning node data to protect data privacy [72].

Unlike traditional federated learning, the proposed BAFL [83] uses an asynchronous federated learning strategy that allows each device to upload a local model when global aggregation requires rapid convergence of global models. Blockchain prevents the failure of a single central server and ensures decentralized and secure data storage. Blockchain also incentivizes devices by rewarding them for participating in federated learning.

4.1.5. Peer-to-Peer Networking

P2P network is different from the centralized management of the traditional C/S framework; it breaks the centralized design mode, all participants are treated equally, and the transaction data can be spread throughout the network. In the blockchain-based federated learning system, the use of P2P network technology has many advantages for FL data dissemination. P2P networks can provide a shared storage system for FL. Therefore, the participant information can be distributed in BFL to realize the distributed management of FL. For example, Sandi et al. [53] proposed distributed storage of medical information, which is obtained from multiple medical service providers by relying on blockchain technology in peer-to-peer coverage networks. Further, P2P networks can use peer relationships to protect the privacy of clients in federated learning. For example, Shayan et al. [73] used blockchain and crypto-primitives to achieve privacy protection FL between coordinated peer-to-peer clients, and proposed Biscotti: a fully decentralized peer-to-peer (P2P) multi-party ML approach to address centralized infrastructure for central services without compromising customer privacy.

Chain FL [84] is a decentralized federated learning method that utilizes blockchain to delegate the responsibility of storing models to nodes on the network instead of centralized servers aggregating models so as to achieve federated learning with high security due to its embedded blockchain. Furthermore, ChainFL is compatible with both edge computing and blockchain technology, which can better support the embedding of security-centric offloading algorithms.

In summary, a combination of blockchain and federated learning can achieve a robust decentralized learning model for federated learning training, and the parameters of the trained learning model can be securely stored on the blockchain and protected against unauthorized access and malicious behavior to ensure the privacy of user data [85]. With the support of audit mechanisms, data sources and provenance can be managed transparently. In addition, the framework makes various constraints on the participants, realizes their honest participation in training, and provides reasonable rewards or punishments to the participants.

4.2. Application Direction of Blockchain-Enabled Federated Learning

From the previous sections on the shortcomings of federated learning and the possibility of combining blockchain with federated learning, we know that the shortcomings of federated learning can be compensated for by combining with blockchain. In this part, we introduce in detail the solutions to FL challenges from seven aspects, shown in Table 3.

Table 3. The solutions to federated learning challenges.

Solution	Blockchain Technology	Application Scenario	Problem to Be Solved	Method	Reference
• Incentive mechanism	• Smart contract	• Internet of Vehicles	• Lack of incentives	• A framework is proposed to realize the sharing and collaborative training of intelligent driving models between operators using technology, and to use smart contracts to realize the management of the entire federated reinforcement learning.	[52]
	• Consensus algorithm	• Autonomous driving, intelligent diagnosis, etc.	• Uneven distribution	• Using consensus algorithm, reputation value is calculated through model quality parameters to evaluate the reliability of workers so as to a achieve a tamper-proof and reasonable distribution of profits.	[17]
• Defense mechanism	• Smart contract	• Equipment failure	• Failure detection	• A platform architecture of federated learning based on blockchain is proposed for fault detection in IIoT, thus realizing the verifiable integrity of client data.	[20]
	• Hash algorithm	• Based on the interstellar file system	• Inference attacks	• IPFS is introduced to store training models and retrieve participants by unique hash values. In this way, the storage cost is reduced , and the model is protected from member inference attacks.	[55]
	• Consensus algorithm	• D2D communication	• Poison attack	• This paper proposes a deep enhanced FL (BDRFL) scheme based on a two-layer blockchain to achieve a privacy-preserving and cache-efficient D2D network.	[86]
		• Data storage	• Poison attack	• A blockchain-based federated learning security and privacy learning security and privacy to realize the security of models and data during training.	[87]
		• Electric system	• Attack tolerance	• In this paper, a blockchain-based federated system intelligence (BELIEFS) was proposed to realize the tolerance of malicious attacks under the consensus mechanism.	[88]
• Privacy mechanism	• Smart contract	• Medical system	• Decentralized privacy	• A new federated learning architecture based on blockchain is proposed, and a multi-module system is used to achieve the accessibility and privacy of medical data.	[89]
	• Consensus algorithm	• Internet of Vehicles	• Central privacy issues	• A fully decentralized machine learning system called Bift is proposed, which provides a consensus algorithm PoFL to resist possible adversaries and achieve privacy protection.	[90]
		• Malicious clients	• Attack backtracking	• This paper proposes a blockchain-based block federated learning scheme (BGFLS) to realize malicious client backtracking and improve the efficiency of model training.	[91]

Table 3. *Cont.*

Solution	Blockchain Technology	Application Scenario	Problem to Be Solved	Method	Reference
	• Hash algorithm	• Medical system	• Privacy protection failure	• Accessibility and security of health records are achieved through the use of a blockchain integrated with cryptography-based federated learning modules.	[27]
	• Digital signature	• Audit encrypted model	• Encryption audit lack	• This paper proposes a cryptographic gradient auditing method based on blockchain, which can audit the existence of malicious gradients without decrypting any individual cryptographic gradients.	[18]
• Robust mechanism	• Smart contract	• Network of Electric Vehicles	• Low robustness	• In this paper, a semi-decentralized robust network of electric vehicles (NoEV) integration system for power management in smart grid platform is proposed. The federated learning algorithm is used to predict power consumption and achieve a low latency rate, high security, and a high network efficiency.	[92]
	• Consensus algorithm	• Practical Byzantine fault tolerance consensus algorithm	• Low robustness	• The paper uses model compression to improve modeling efficiency, and practical Byzantine fault-tolerant algorithms commonly used in coalition chains are analyzed to realize the practicability of the model.	[93]
		• Infrastructure	• Low robustness	• Mitigating the impact of central and malicious clients by designing a blockchain-based privacy-preserving Byzantine robust federated learning (PBFL) scheme.	[94]
• Global mechanism	• Smart contract	• Coordinate the round delineation, model aggregation and update tasks	• Center aggregation	• This paper introduces an aggregator-free, blockchain-driven FL environment, BAFFLE, which uses smart contracts to coordinate the tasks of FL to achieve high scalability and computational efficiency.	[62]
	• Consensus algorithm	• Edge computing	• Single point of failure	• This paper proposes a novel decentralized secure multi-party learning system for blockchain authorization to solve the single-point failure problem.	[95]
		• Automatic modulation	• Single point of failure	• This paper proposes a decentralized blockchain federated learning (BFL) framework with simpler consensus which avoids the risk of network paralysis caused by the failure of central equipment.	[59]

Table 3. *Cont.*

Solution	Blockchain Technology	Application Scenario	Problem to Be Solved	Method	Reference
• Transmission mechanism	• Consensus algorithm	• Digital twin in IoT	• Network resource allocation	• A new digital two-sided network framework is proposed using blockchain to achieve flexible and secure digital two-sided structure.	[96]
		• Minimize the network load	• Network overload	• A federated learning scenario based on blockchain is proposed to make the model converge quickly and stably and avoid network overload.	[51]
• Audit mechanism	• Smart contract	• Machine learning system	• Not censorable	• This paper proposes an integrated federated learning system "BassaML" based on blockchain and model card, which provides strong transparency and trust for the model.	[68]

4.2.1. Incentive Mechanisms

Incentive mechanisms refer to the motivation of participants to participate in training tasks and the system of rational distribution of rewards. The goal of the incentive mechanism is to create and distribute value. Under the premise of sufficient incentive, participants are rewarded or punished according to their own contribution. The introduction of incentives is crucial to federated learning [97]. For those who do not have enough data to train the model themselves, using incentive mechanisms can motivate local data to participate in collaborative training, and the accuracy of model training will be greatly improved. Secondly, a reasonable reward and punishment system can ensure the honest behavior of participants in model training and gradient transactions and improve the application level of the model.

Fundamentally speaking, the blockchain is open and transparent. After the training of the federated learning model is completed, it can use smart contracts and consensus algorithm technology to allocate reward resources according to the quantity and quality of training data provided by each participant, and reward resources are written into the blockchain to bring in more participants and improve the cooperation of participants.

Existing studies on incentive mechanisms in federated learning mainly focus on one dimension and have some limitations [98]. For instance, Feng et al. [99] only considered the size of training data. Nevertheless, in blockchain-based federated learning, related problems are solved. For example, Kang et al. [100] took reputation as a fair indicator to select reliable employees, and employees with good reputation could obtain more rewards in model training. Dusit Niyato et al. [101] proposed an incentive mechanism based on contract theory aimed at obtaining hidden type information from users and maintaining long-term participation in healthcare applications. Liu et al. [57] presented a blockchain-based federated learning payment system, where the contribution of each FL participant is evaluated through the proof of the Shapley (PoSap) consensus protocol.

In particular, in order to ensure the transparency of the incentive mechanism and the practice of FL, Liu et al. [29] proposed that an incentive mechanism based on contribution points aims to fairly reward FL participants for contributing their local data, realize the authenticity of FL model aggregation and provide FL participants with the effectiveness of incentives. Weng et al. [102] provided an incentive mechanism based on Bayesian game theory to solve challenges in UAV-assisted wireless networks. Ma et al. [58] proposed a blockchain-based federated learning framework and protocol to transparently evaluate the contribution of each participant. The framework protects the privacy of all parties during the model building phase and transparently evaluates contributions based on model updates.

In addition, blockchain can also provide reasonable incentives and misconduct deterrence for collaborative models to facilitate alliance between customers [31]. If the local model update is successfully validated, the local device can be rewarded [79,80]. If the uploaded update is incorrect, the local device will also be penalized [76].

4.2.2. Defense Mechanisms

Defense mechanisms refer to the system of updating and verifying the model and attacking the confrontation. The solution of the defense mechanism plays an important role in improving the security of federated learning, and with the support of blockchain, federated learning realizes the improvement of defense capabilities.

The consensus mechanism of the blockchain can verify the model update to cope with the poison attack of federated learning. There are many application cases in blockchain-based federated learning. For example, Shayan et al. [73] proposed a completely decentralized peer-to-peer (P2P) multi-party ML method, developed Multi-Krum defense, and used Byzantine fault-tolerant aggregation scheme to verify local model updates and enhance FL defense capabilities. Peng et al. [103] proposed the VFChain system to prevent poison attacks by developing an effective committee selection scheme and blockchain authentication data structure.

Taking advantage of the immutable nature of blockchain records can improve the defense capability of federated learning. One of the current challenges faced by federated learning is the problem of countering attacks, such as the tampering of local data and model parameters, which will lead to the decline of model performance. However, current federated learning solutions, such as finding abnormal data or clients through anomaly detection, experience difficulties in effectively solving this problem. In this way, as long as one party's data or parameters are tampered with, its information will be judged to be invalid [104]. Alternatively, IPFS can be introduced to store the training model and retrieve participants by unique hash values. In this way, storage costs are reduced and the model is protected from member inference attacks [55]. Zhao et al. [87] presented a blockchain-based federated learning security and privacy protection framework (BFLSP) to achieve the security of models and data during training.

Blockchain can help federated learning to identify and defend against potential attacks, punishing malicious actors [75]. Additionally, due to the large number and dispersion of customer terminals, it is difficult for malicious clients to backtrack, and the traceability of blockchain can be used to trace and punish the participants who launch malicious attacks [91], improving the accuracy of model training in federated learning. Under a consensus mechanism, the blockchain-based federated system BELIEFS [88] achieves a tolerance for malicious attacks.

4.2.3. Privacy Mechanisms

Privacy mechanisms refer to participant authentication and node data storage, as well as distributed storage of data. The blockchain provides three mechanisms—identity authentication, node data confidentiality, and data storage—to achieve privacy protection in BFL. Therefore, blockchain-based federated learning has a strong privacy protection system.

Blockchain provides an identity authentication mechanism for on-chain data. Previously, federated learning clients did not require authentication to upload model updates, which was risky. Now, through the blockchain's authorization mechanism and identity management, untrusted users can be integrated as participants to establish a secure and trusted cooperation mechanism. Li Jiang et al. [96] introduced a model update chain to secure local model updates and global model updates by utilizing a directed acyclic graph (DAG) blockchain.

Blockchain provides a confidentiality mechanism for node data. In federated learning, although all participants exchange gradient information and do not expose their raw data to the outside world, there is still a risk of data inversion by opening the data gradient update process. Conversely, a blockchain-based federated learning framework avoids the privacy risks of centralized structures. Sun et al. [18] proposed a cryptography gradient audit method using two blockchains, which simultaneously realized privacy-preserving gradient recording and trusted quality audit.

Blockchain provides a data storage mechanism. Blockchain is essentially a distributed public ledger that connects blocks into a chain, which is actually a peer-to-peer accounting system on which every node can record information. The digital records on the blockchain cannot be tampered with or forged, which improves the efficiency of data flow and forms a new storage model. The model parameters of federated learning are stored in the blockchain, which not only ensures the safety and reliability of model parameters, but also promotes the contribution of data by participants. Frankly speaking, the superiority of blockchain-based federated learning in data storage and even data encryption has been significantly improved.

In addition, many BFL-based blockchain technologies cannot completely prevent privacy leaks, so it is best to incorporate differential privacy, homomorphic encryption, and other technologies with BFL. Homomorphic encryption [94] improves the security of node storage and computation in federated learning. It is important to process personal data by effectively encrypting it before it is shared on the blockchain. Wang et al. [105] proposed a blockchain-based privacy-preserving federated learning scheme called BPFL, which

combines homomorphic encryption and Multi-Krum technology to achieve ciphertext-level model aggregation and model filtering. In addition, Salim et al. [106] proposed an explainable FL (DP-BFL) framework based on differential privacy blockchain for data privacy. Wang et al. [107] integrate the blockchain's FL with the Wasserstein Generative Adversarial Network (WGAN) of Differential Privacy (DP) to protect the model parameters of edge devices in the Beyond-5G (B5G) network.

4.2.4. Robust Mechanisms

Robust mechanisms refer to system efficiency performance mechanisms. Federated learning is a machine learning framework specifically for data privacy protection. In traditional federated learning, the system cannot fully control the impact of client failures on model training, resulting in poor model training results. Existing research enhances the robustness of federated learning by leveraging the decentralization and immutability of blockchain.

With the support of blockchain, the efficiency and reliability of federated learning have been greatly improved. For example, the use of a trusted and efficient decentralized federated slicing architecture [108], combined with reinforcement learning to accelerate optimization of resource allocation, improves federated learning efficiency. In addition, leveraging model compression to improve modeling efficiency [93] can make the federated learning modeling process more robust. In [109], a blockchain-based federated learning parameter update architecture PUS-FL is proposed to solve the problem of model accuracy degradation caused by the existing traditional gradient filtering.

4.2.5. Global Mechanisms

Global mechanisms refer to mechanisms that replace FL central servers with distributed blockchain nodes or defend against malicious attacks against central servers. To address the single point of failure, FL's central server can be replaced with distributed blockchain nodes [110], model updates for local devices can be exchanged through miner nodes, and with the support of defense mechanisms, malicious attacks can be resisted. Bai et al. [111] proposed a privacy-preserving oriented no trusted third party federated learning system based on blockchain (NttpFL). Blockchain makes the whole process transparent and traceable, avoiding the single point of failure problem. In [112], the author analyzes the system delay and designs an algorithm to adjust the local iteration to solve the single point of failure problem and achieve better model performance for federated learning. In addition, Liu et al. [59] proposed a decentralized blockchain federated learning (BFL) framework with a simpler consensus mechanism, avoiding the risk of network paralysis caused by a central device failure.

However, there exists a possibility for malicious blockchain nodes using blockchain instead of central servers, so it is necessary to combine defense mechanisms and privacy mechanisms to make federated learning model training more secure and efficient.

4.2.6. Transmission Mechanisms

Transmission mechanisms refer to the system of network transmission and network resource allocation. Due to the limited communication bandwidth and the participation of a large number of users, federated learning can cause transmission barriers. However, blockchain-based federated learning can solve these two problems. Blockchain architecture can ensure the security and efficiency of data transmission over the network. Therefore, the transmission performance of federated learning based on blockchain is greatly improved.

One transmission obstacle problem is network overload, and the method to minimize network load is to make the model converge quickly and stably [51]. By virtue of its decentralized nature, blockchain stores data in a decentralized manner while reducing network overload. Thus, the BFL framework formed by federated learning under the support of blockchain can accelerate the model convergence and reduce the communication cost. Cui et al. [113] designed a CREAT algorithm and applied the auxiliary compression

algorithm to content cache or predictive cache files to alleviate the network overload problem. Furthermore, the blockchain stores all learning models for complete transmission, so local models cannot be adjusted, and network overload can be mitigated by accurate node identification of the blockchain [114].

In addition, to solve the network resource allocation problem, digital bilateral networks can be utilized to solve the optimal unified time problem of collaborative federated learning and local model update verification. Therefore, with the support of BFL, federated learning can utilize the bilateral network to update the local model to reduce the waste and insufficiency of network resources.

It is worth noting that the advantages of edge computing can be applied to BFL, combined with the outstanding features of blockchain, to better empower federated learning. Zhang et al. [22] combined edge computing and blockchain to propose a secure data transfer method. Lu et al. [115] proposed a digital twin wireless network (DTWN), and comprehensively considered the problems of digital twin association, datasets, and bandwidth; balanced the training accuracy and time cost of the scheme; and optimized the model.

4.2.7. Audit Mechanisms

Audit mechanisms perform transparent review of the source of the data and assess the traceability of the data on the chain. The distributed ledger feature of the blockchain ensures the consistency of model parameter data among multiple participants in federated learning, and the synchronization and sharing of model parameter data is safe and reliable, which can save node data. Moreover, the tamper-resistant nature of blockchain guarantees data transparency and traceability. Due to these two characteristics of blockchain, the censorship of blockchain-based federated learning data is realized.

Peng et al. proposed a verifiable and auditable federated learning framework named VFChain based on blockchain system [103]. Main process: First, the blockchain selects a committee to collectively aggregate models and record verifiable proofs in the blockchain, achieving verifiability. Then, a novel authentication data structure is proposed for blockchain to improve the search efficiency of verifiable proof and further enhance the auditability of the model.

4.3. Application Scenarios of Blockchain-Based Federated Learning

The BFL architecture has been applied to many services and domains, which are summarized and analyzed in this article. Table 4 lists the application scenarios and functions of BFL.

Table 4. Application directions of blockchain-based federated learning.

Application Direction	Goal	Method	Reference
IIoT	• Industrial data transmission	• Separate the local model updating process from the mobile device-independent process. • Add an edge server to make most of the computation on the server, which improves the learning efficiency. • Use a distributed architecture of the blockchain to protect data security and privacy.	[22]
	• Industrial data privacy protection	• Design the application model of blockchain-based federated learning in the industrial Internet of Things (IIoT) and develop our data protection aggregation scheme based on the model. • Give distributed K-means clustering, random forest, and AdaBoost to realize multiple data protection in data sharing and model sharing. • Integrate the methods with blockchain and federated learning and provide the complete security analysis.	[116]
	• Model tamper-resistant	• Propose an efficient chameleon hash scheme for secure federated learning in Industrial Internet of Things. • Limit the use of trapdoor. The data owner can choose the validity period of the trap in a flexible way to improve the security of the model.	[54]
Facility Internet of Things	• Model of migration	• Develop an incentive mechanism considering the economic benefits of fast devices. • Design a clustering-based algorithm for identifying malicious devices and preventing them from defrauding incentives. • Use blockchain to ensure trustworthiness in model migration and incentive processes.	[21]
	• Device failure detection	• Present a platform architecture of blockchain-based federated learning systems for failure detection in IIoT, which enables verifiable integrity of client data. • Propose a novel centroid distance weighted federated averaging (CDW-FedAvg) algorithm to address the data heterogeneity issue in IIoT failure detection.	[20]
Power Internet of Things	• Space-Air-Ground-Integrated	• The task offloading is decoupled from computing resource allocation through Lyapunov optimization. • The task offloading problem is solved by the proposed electromagnetic interference sensing task offloading algorithm (FDAC-EMI) based on federated deep participant critics. • Solve the resource allocation problem by smoothing approximation and Lagrangian optimization.	[117]
Internet of Vehicles	• Vehicle information dissemination	• Vehicles compete to become relay nodes (miners) by processing the proposed federated learning proof (PoFL) consensus embedded in the blockchain smart contract. • Develop a hybrid blockchain architecture to enhance the security and reliability of model parameters. In addition, propose an asynchronous federated learning scheme that uses Deep Reinforcement Learning (DRL) for node selection to improve efficiency.	[23,24]

Table 4. *Cont.*

Application Direction	Goal	Method	Reference
	• Knowledge sharing	• A hierarchical blockchain framework and hierarchical federated learning algorithm for knowledge sharing are proposed. Vehicles learn environment data through machine learning methods and share learning knowledge with each other. • Knowledge sharing is modeled as a trading market process to stimulate sharing behavior, and the trading process is formulated as a multi-leader and multi-player game.	[25]
	• Privacy data protection	• A framework called PPIoV is proposed, which is based on federated learning (FL) and blockchain technology to protect the privacy of vehicles in IoV. • PPIoV is built on the blockchain to establish trust across multiple communication nodes.	[26]
	• Privacy-aware and efficient communication	• A feedback learning (BFL) design based on autonomous blockchain is proposed for privacy-aware and efficient vehicle communication networks, in which local on Vehicle Machine Learning (oVML) model updates are exchanged and verified in a distributed manner. • Develop a mathematical framework that features controllable networks and BFL parameters to capture their impact on system-level performance.	[64]
Military systems	• Military defense system	• Use the characteristics of blockchain technology and federated learning to propose a distributed computing defense framework for sustainable society.	[118]
Medical system	• COVID-19 privacy data protection	• Describe various PPTs developed during COVID-19. These PPTs make use of emerging technologies, such as federated learning, blockchain, design privacy, and group learning.	[119]
	• Medical data protection	• A new technology using deep learning and blockchain technology to protect the privacy of electronic health records is proposed. The processed dataset uses the convolutional neural network (CNN) method to classify normal and abnormal users. • By using a blockchain integrated with a cryptography-based federated learning module, anomalous users have been processed and removed from the database, as well as accessibility of health records.	[27–29] [120,121]
	• CT imaging to detect COVID-19	• A data standardization technology is proposed that deals with the heterogeneity of data because data are collected from different hospitals with different types of computed tomography (CT) scanners. • Use segmentation and classification based on capsule networks to detect patients with novel coronary pneumonia. • Devise a method that can train global models using blockchain technology and federated learning collaboration while protecting privacy.	[30]
Digital currency system	• Transaction amount privacy protection	• Study the contradiction between privacy-preserving payment mechanisms, including controllable anonymity, and the penetration and regulation of digital currencies. • A solution based on homomorphic encryption and federated learning is proposed. • A digital currency prototype was implemented using the CORDA framework to validate our strategy.	[122]

Table 4. *Cont.*

Application Direction	Goal	Method	Reference
Beyond-5G applications	• Edge intelligence of UAV	• Focus on investigating the synergy between FL and blockchain to realize autonomous UAV edge intelligence. • The method includes multi-layer federated learning techniques and an efficient cooperative learning framework. • Use smart contracts for resource allocation to make decisions with specific objectives.	[123]
Digital twin edge network	• Efficient communication	• Combining digital twins with edge networks, digital twin edge networks (DITENs) are proposed to fill the gap between physical edge networks and digital systems. • A blockchain-authorized federated learning scheme is proposed to strengthen communication security and data privacy protection in DITEN. • An asynchronous aggregation scheme is proposed, and a digital double reinforcement learning authorization system is used to schedule relay users and allocate spectrum resources.	[124]
Fog computing	• Application privacy issues	• A new blockchain-based federated learning (FL-Block) scheme is proposed to bridge this gap. • FL-Block uses the blockchain's proof-of-work consensus mechanism so that autonomous machine learning does not require any centralized permissions to maintain global models and coordinates. • The latency performance of FL-Block is analyzed, and the optimal block generation rate is obtained considering communication, consensus delay, and computing overhead.	[125]
Unmanned Aerial Vehicle	• Mobile crowd perception	• Introduce a blockchain-based cooperative learning architecture for drones to securely exchange local model updates and verify contributions without a central administrator. • By applying local differential privacy, a privacy-preserving algorithm is designed to protect the privacy of drones and update the local model with ideal learning accuracy.	[126]
Prediction system	• Position prediction	• Use federated learning to conduct local training on users' mobile devices while identifying and combating the possibility of bad actors or adversaries who may intentionally report questionable data to harm the training process. • Use blockchain instead of centralized servers during training to ensure the security of the process.	[127]
Traffic flow prediction	• Prediction of traffic flow data	• Utilize federated learning and blockchain technology for a decentralized approach to ensuring the privacy and security of traffic data. • Analyze multi-source traffic data for traffic prediction, providing enhanced security for collaborative traffic management.	[128]

With the booming development in modern Information and Communications Technology (ICT), the fourth industrial revolution (Industry 4.0) has overturned the traditional industrial development model. Security requirements in IIoT are generally more stringent than those in typical IoT scenarios [129]. How to protect and use this valuable data in the IIoT to share it in an efficient, secure and cost-effective manner is an urgent issue that needs to be addressed. In the field of the industrial Internet of Things, federated learning based on blockchain provides a BFL framework for multi-party data sharing, which enables devices to safely retrieve data and ensures the accuracy of model training. Zhang et al. [22] proposed a secure data transmission method by taking advantage of edge computing and blockchain, using edge servers to improve the efficiency of federated learning, and utilizing the distributed architecture of blockchain to protect data security and privacy. Moreover, Lu et al. [130] presented using blockchain and federated learning to protect IIoT data privacy.

The Internet of Things (IoT) ecosystem connects physical devices to the Internet and offers significant advantages in terms of flexibility, responsiveness, and potential environmental benefits [33]. However, the current IoT paradigm relies on centralized storage and computation to operate deep learning algorithms. With the widespread application of blockchain, FL can be enabled in the entire IoT ecosystem.

Zhang et al. [20] proposed a blockchain-based federated learning platform architecture for fault detection in IIoT to achieve verifiable integrity of client data. In order to solve the problem of heterogeneous data in IIoT fault detection, a centroid distance-weighted federation average (CDW-FedAvg) algorithm is proposed. The model transfer method of federated learning based on blockchain [21] can achieve secure model transfer and accelerate model training on the resource-limited Internet of Things platform, while minimizing the computational cost. Blockchain records interactions between a central server and an IoT device without exposing the device's private data. In order to solve the security and delay problems of the existing power system, Liao et al. [117] proposed a secure and low-delay electromagnetic interference sensing computational off-loading algorithm (BRACE) based on blockchain and semi-distributed learning, which was used to realize the space-air-ground integrated PIoT (SAG-PIoT) and achieve high delay and security performance. More importantly, blockchain technology is a suitable platform to develop decentralized computing systems based on federated learning for military defense without the need for a central entity [125]. Thus, the integration of blockchain and FL is widely utilized in various IoT applications to enhance robustness, security, and privacy.

In the field of the Internet of Vehicles belonging to the Internet of Things, blockchain-based federated learning can be widely used. Encryption in the blockchain ensures data consistency, providing secure data transmission and storage. Under these conditions, the blockchain is able to monitor new device entrants through transaction record keeping [131], further guaranteeing data authorization and authentication. Blockchain also ensures secure communication between end devices by storing local training data for various transactions and performing transaction validation on each device [132]. The blockchain-based federated learning vehicle message propagation application proposed by Ayaz et al. [23] can produce more accurate models in less time, reduce consensus time delay, improve message delivery rate, and more effectively protect the privacy of neighboring vehicles. Lu et al. [24] introduced that blockchain empowers asynchronous federated learning, realizes secure data sharing of the Internet of Vehicles, reduces the transmission load and solves the privacy problems of providers, and ensures the reliability of data sharing. Chai et al. [25] proposed a hierarchical blockchain framework and hierarchical federated learning algorithm for knowledge sharing [133], and vehicles learn environmental data through machine learning methods and share learning knowledge with each other to meet the distributed mode and privacy protection requirements of IoV. Alotaibi et al. [25] proposed a framework for PPIoV, based on federated learning (FL) and blockchain technology to protect vehicle privacy in IoV. Pokhrel et al. [64] proposed an autonomous blockchain-based federated learning (BFL) design that integrates blockchain and FL to facilitate efficient communication of

autonomous vehicles, and validates on-vehicle machine learning model updates to enable privacy-aware and efficient in-vehicle communication networks.

In the healthcare system, Majeed et al. [119] conducted an extensive review of recently proposed privacy-preserving technologies to address various privacy concerns arising from the COVID-19 pandemic. Some scholars have developed lightweight security and privacy algorithms for Internet of Healthy Things (IoHT) devices based on BFL, using distributed and locally stored data to train intelligent systems to achieve privacy protection of medical data [120]. Kumar et al. [30] introduced the BFL framework to enable CT imaging to detect COVID-19 while protecting global data privacy. Besides, some scholars have proposed a framework for coordinated machine learning based on blockchain to achieve privacy protection of electronic health data [27–29].

Next, the application of BFL in some segments is introduced. In the digital currency system, the privacy of transaction amounts is achieved by using blockchain [122]. In Beyond-5G applications, Alsammi et al. [123] proposed a blockchain and FL synergy framework in UAV edge intelligence to achieve energy efficiency improvement. In digital twin edge networks, Lu et al. [124] combined digital twins with an edge network and proposed a blockchain-based federated learning scheme to strengthen communication security and data privacy protection in DITEN. In fog computing, in order to solve the potential defects of fog computing, Qu et al. [125] proposed a novel blockchain-enabled federated learning (FL-Block) scheme to realize the privacy protection and efficient computing of fog computing. In UAV applications, a safe federated learning framework for UAV-assisted MCS was proposed, and a new method of using unmanned aerial vehicle (UAV) and artificial intelligence (AI) to realize mobile crowd perception (MCS) was proposed [126]. In the prediction system, the privacy of sensitive location data is solved and the next position is predicted on the basis of BFL [127]. Additionally, Meese et al. [128] proposed a blockchain federated learning structure BFRT based on real-time data and edge computing for online traffic flow prediction, which can alleviate traffic congestion.

4.4. Potential Problems and Solutions

Are there really any drawbacks and limitations with using blockchain for federated learning? In this section, we aim to tackle several commonly cited arguments against the usage of blockchain for federated learning research.

4.4.1. How to Improve the Efficiency of Federated Learning in Blockchain

The high efficiency of the combination of blockchain and federated learning is the problem to improve the overall efficiency of the system. In this problem, the decentralized federated slicing architecture or federated learning model can be used to compress on-chain data to improve the training efficiency of the model [108]. Also, deep reinforcement learning (DRL) can be combined with node selection to improve the efficiency of BFL [24].

4.4.2. How to Reduce the Additional Communication Overhead Introduced by the Iterative Process of Federated Learning

To solve the communication cost problem, a distributed learning framework [64] can be considered to ensure end-to-end reliability and delay rate. Furthermore, digital twin reinforcement learning can also be used to schedule relay users and allocate spectrum resources to enhance communication efficiency while reducing communication costs [124].

4.4.3. How to Ensure the Privacy of Data Storage and Exchange on the Chain

In blockchain-based federated learning, the updated data from federated learning is stored on the blockchain, but the blockchain is not suitable for storing a large amount of data, and the on-chain data cannot be changed, so the aggregation model in FL may involve the privacy of users. To solve this problem, it is currently possible to construct editable blockchains using chameleon hashing for secure federated learning [54].

5. Discussion and Future Outlook

While existing works have established a solid foundation for BFL systems research, this section outlines several promising prospective research directions. We also elaborate on several open issues, which we believe is critical to the present state of the field.

5.1. Security of the BFL

As a new privacy-preserving machine learning technology, federated learning security is important. Due to its own centralized central server, there is a risk of privacy disclosure. Furthermore, the defense mechanism of federated learning also has notable defects which are prone to poison attacks and defense obstacles in the process of model training [134]. However, the distributed storage and transparent switching node single-point scheme provided by blockchain can effectively solve the problems arising in federated learning. The BFL framework mitigates external attacks and internal malicious servers to a certain extent, and there may be problems such as model efficiency degradation. Many scholars have suggested that the security of BFL supported by federated cryptography technology needs to be further developed.

5.2. The Incentive of BFL

As a new model training paradigm, federated learning combines the data of all parties to train the model on the premise of ensuring privacy security. The distribution and promotion of incentives in federated learning are flawed and lack the necessary supervision system and reward and punishment standards. With the support of blockchain, the BFL framework can use smart contracts to develop reward and punishment agreements, and the non-tamperability of blockchain can ensure that participants receive rewards or punishments reasonably. By using the consensus algorithm, participants are encouraged to contribute more data, which further improves the efficiency of BFL model training.

5.3. The Efficiency of BFL

The model training efficiency of federated learning is mainly related to the allocation of network resources and the reception efficiency of devices. A key aspect of federated learning (FL) is the need for a centralized aggregator to maintain and update the global model. However, orchestrating centralized aggregators is infeasible due to many operational constraints [62] and hinders model performance efficiency of federated learning. Model compression, slice transfer, etc., have been proposed to solve this problem [109], but it is unclear whether existing methods can achieve a balance between efficiency and accuracy of federated learning.

5.4. Advantages of Smart Contracts and Consensus Algorithm in BFL

Three articles [52,71,135] show the enhanced effect of smart contracts on incentives. Model selection and aggregation of smart contracts are performed in a fully decentralized manner, helping to build trust between nodes. In addition, smart contracts can formulate reward distribution provision protocols to enhance trust between participants and motivate participants in FL to contribute more datasets. Lastly, with the support of a basic consensus protocol, smart contracts help ensure the transparency and fairness of the FL process.

The proposed consensus algorithm provides selectivity for FL nodes, which can further improve the efficiency and robustness of BFL. Through the proposal of the committee consensus mechanism, the training efficiency of BFL can be improved, and the machine learning training process can be optimized. In addition, by using a decentralized data ledger with a consensus algorithm, BFL can reduce the risk of a single point of failure without any central server, and all network entities can transparently track any update events and user behavior.

In general, blockchain-based federated learning makes use of the inherent advantages of blockchain and federated learning itself, and combines them to a certain extent, which can make up for the defects of federated learning and strengthen the technological advantages

of blockchain, and fully promote the development of blockchain and federated learning on the basis of it.

6. Conclusions

In this paper, we provide an extensive review of the best-known works on blockchain-based federated learning to date. We propose the application direction of blockchain enabling federated learning while providing a comprehensive summary of blockchain addressing federated learning deficiencies. After that, the technical framework of the fusion of the two is summarized and the application of BFL is classified and analyzed. Finally, we discuss the future development and application expansion of blockchain-based federated learning. Both blockchain and federated learning have been hot research topics in recent decades, with a large number of new developments and emerging technologies each year. We hope that this survey will give readers a comprehensive understanding of the key aspects of this field, understand the most notable current advances in the field, and inform future research.

In view of the continuous development of this field, blockchain-based federated learning has been widely used in industrial Internet of Things, Internet of Vehicles, medical systems, and so on. The combination of blockchain and federated learning has been accepted by more and more scholars. Given the rising popularity and potential of blockchain applied in federated learning technology, future research will continue to conduct in-depth exploration around privacy and security protection mechanisms, global mechanisms, transmission mechanisms, and fairness, robustness, and personalized federated learning mechanisms to promote the deployment and application of federated learning technology.

Author Contributions: W.N., Y.Z., and C.S. studied the literature, conceived the study concepts, and led the entire manuscript. L.Z., J.X., T.C., T.X., X.X., and J.G. revised the manuscript, and the refinement of the article was completed under the supervision of H.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by Qingdao Science and Technology Demonstration project—New modern agriculture project in 2024 (No. 24-2-8-xdny-11-nsh).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created.

Acknowledgments: This work was supported in part by the Qingdao Science and Technology Demonstration project—New modern agriculture project in 2024 (No. 24-2-8-xdny-11-nsh), in part by the Shandong Smart Ocean Ranch Engineering Technology Collaborative Innovation Center, in part by the research fund for high-level talents of Qingdao Agricultural University (No. 1119048 and No. 1119041), in part by the Shandong Agricultural Science and Technology Service Project (No. 2019FW037-4), in part by Horizontal Project (No. 20193702010792), and in part by Experimental technical project of Qingdao Agricultural University (No. SYJK18-01).

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

References

1. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; y Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, Lauderdale, FL, USA, 20–22 April 2017; PMLR: London, UK, 2017; pp. 1273–1282. [CrossRef]
2. Konecny, J.; McMahan, H.; Yu, F.; Richtarik, P.; Suresh, A.; Bacon, D. Federated learning: Strategies for improving communication efficiency. *arXiv* **2016**, arXiv:1610.05492. [CrossRef]
3. AbdulRahman, S.; Tout, H.; Ould-Slimane, H.; Mourad, A.; Talhi, C.; Guizani, M. A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond. *IEEE Internet Things J.* **2020**, *8*, 5476–5497. [CrossRef]
4. Wen, J.; Zhang, Z.; Lan, Y.; Cui, Z.; Cai, J.; Zhang, W. A survey on federated learning: Challenges and applications. *Int. J. Mach. Learn. Cybern.* **2022**, *14*, 513–535. [CrossRef] [PubMed]
5. Saleh, A. Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain Res. Appl.* **2024**, *5*, 100193. [CrossRef]

6. Makridakis, S.; Christodoulou, K. Blockchain: Current Challenges and Future Prospects/Applications. *Future Internet* **2019**, *11*, 258. [CrossRef]
7. Gabrielli, E.; Pica, G.; Tolomei, G. A Survey on Decentralized Federated Learning. *arXiv* **2023**, arXiv:2308.04604. [CrossRef]
8. Narule, Y.S.; Thakre, K.S. Privacy preservation using optimized Federated Learning: A critical survey. *Intell. Decis. Technol.* **2024** *18*, 135–149. [CrossRef]
9. Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Trans. Industr. Inform.* **2017**, *13*, 3154–3164. [CrossRef]
10. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. p. 21260. Available online: https://cdn.nakamotoinstitute.org/docs/bitcoin.pdf (accessed on 14 September 2024).
11. Wang, X.; Zhu, H.; Ning, Z.; Guo, L.; Zhang, Y. Blockchain Intelligence for Internet of Vehicles: Challenges and Solutions. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 2325–2355. [CrossRef]
12. Singh, M.; Kim, S. Blockchain Based Intelligent Vehicle Data sharing Framework. *arXiv* **2017**, arXiv:1708.09721. [CrossRef]
13. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an Optimized BlockChain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, New York, NY, USA, 18–21 April 2017; ACM: New York, NY, USA, 2017; pp. 173–178. [CrossRef]
14. Nanda, S.; Panda, S.; Dash, M. Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. *Multimed Tools Appl.* **2023**, *82*, 32917–32939. [CrossRef] [PubMed]
15. Taherdoost, H. The Role of Blockchain in Medical Data Sharing. *Cryptography* **2023**, *7*, 36. [CrossRef]
16. Liu, Y.; Peng, J.; Kang, J.; Iliyasu, A.M.; Niyato, D.; El-Latif, A.A.A. A Secure Federated Learning Framework for 5G Networks. *IEEE Wirel. Commun.* **2020**, *27*, 24–31. [CrossRef]
17. Zhang, Q.; Ding, Q.; Zhu, J.; Li, D. Blockchain Empowered Reliable Federated Learning by Worker Selection: A Trustworthy Reputation Evaluation Method. In Proceedings of the 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Nanjing, China, 29 March 2021; IEEE: New York, NY, USA, 2021; pp. 1–6. [CrossRef]
18. Sun, Z.; Wan, J.; Yin, L.; Cao, Z.; Luo, T.; Wang, B. A blockchain-based audit approach for encrypted data in federated learning. *Digit. Commun. Netw.* **2022**, *8*, 614–624. [CrossRef]
19. Wang, Y.; Zhou, J.; Feng, G.; Niu, X.; Qin, S. Blockchain Assisted Federated Learning for Enabling Network Edge Intelligence. *IEEE Netw.* **2023**, *37*, 96–102. [CrossRef]
20. 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]
21. Zhang, C.; Xu, Y.; Elahi, H.; Zhang, D.; Tan, Y.; Chen, J.; Zhang, Y. A Blockchain-based Model Migration Approach for Secure and Sustainable Federated Learning in IoT Systems. *IEEE Internet Things J.* **2023**, *10*, 6574–6585. . [CrossRef]
22. 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. Industr. Inform.* **2022**, *18*, 3551–3561. [CrossRef]
23. Ayaz, F.; Sheng, Z.; Tian, D.; Guan, Y.L. A Blockchain Based Federated Learning for Message Dissemination in Vehicular Networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 1927–1940. [CrossRef]
24. 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]
25. 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]
26. Alotaibi, J.; Alazzawi, L. PPIoV: A Privacy Preserving-Based Framework for IoV-Fog Environment Using Federated Learning and Blockchain. In Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022; IEEE: New York, NY, USA, 2022; pp. 597–603. [CrossRef]
27. Alzubi, J.A.; Alzubi, O.A.; Singh, A.; Ramachandran, M. Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning. *IEEE Trans. Industr. Inform.* **2023**, *19*, 1080–1087. [CrossRef]
28. Passerat-Palmbach, J.; Farnan, T.; McCoy, M.; Harris, J.D.; Manion, S.T.; Flannery, H.L.; Gleim, B. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Toronto, ON, Canada, 3–6 May 2020; IEEE: New York, NY, USA, 2020; pp. 550–555. [CrossRef]
29. Liu, Y.; Yu, W.; Ai, Z.; Xu, G.; Zhao, L.; Tian, Z. A Blockchain-empowered Federated Learning in Healthcare-based Cyber Physical Systems. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 2685–2696. [CrossRef]
30. 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]
31. 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. [CrossRef]
32. Li, C.; Yuan, Y.; Wang, F.Y. Blockchain-enabled Federated Learning: A Survey. In Proceedings of the 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI), Beijing, China, 15 July–15 August 2021; IEEE: New York, NY, USA, 2021; pp. 286–289.

33. 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.* **2022**, *55*, 1–43. [CrossRef]
34. Liu, K.; Liang, X.; Kantola, R.; Hu, C. A survey on blockchain-enabled federated learning and its prospects with digital twin. *Digit. Commun. Netw.* **2022**, *10*, 248–264. [CrossRef]
35. Zhu, J.; Cao, J.; Saxena, D.; Jiang, S.; Ferradi, H. Blockchain-empowered Federated Learning: Challenges, Solutions, and Future Directions. *ACM Comput. Surv.* **2023**, *55*, 1–31. [CrossRef]
36. Rani, S.; Kataria, A.; Kumar, S.; Tiwari, P. Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. *Know.-Based Syst.* **2023**, *274*, 110658. [CrossRef]
37. Ali, A.; Al-rimy, B.A.S.; Tin, T.T.; Altamimi, S.N.; Qasem, S.N.; Saeed, F. Empowering Precision Medicine: Unlocking Revolutionary Insights through Blockchain-Enabled Federated Learning and Electronic Medical Records. *Sensors* **2023**, *23*, 7476. [CrossRef]
38. Zheng, W.; Yan, L.; Gou, C.; Wang, F.Y. Federated meta-learning for fraudulent credit card detection. In Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence, New York, NY, USA, 7 January 2021; ACM: New York, NY, USA, 2021.
39. Zeng, S.; Li, Z.; Yu, H.; Zhang, Z.; Luo, L.; Li, B.; Niyato, D. HFedMS: Heterogeneous Federated Learning with Memorable Data Semantics in Industrial Metaverse. *arXiv* **2022**, arXiv:2211.03300 [CrossRef]
40. Cohen, L.; Manion, L.; Morrison, K. *Research Methods in Education*; Routledge: London, UK, 2018; pp. 668–685. [CrossRef]
41. Wang, H.; Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
42. Li, L.; Fan, Y.; Tse, M.; Lin, K.Y. A review of applications in federated learning. *Comput. Ind. Eng.* **2020**, *149*, 106854. [CrossRef]
43. 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]
44. Jagarlamudi, G.K.; Yazdinejad, A.; Parizi, R.M.; Pouriyeh, S. Exploring privacy measurement in federated learning. *J. Supercomput.* **2023**, *80*, 10511–10551. [CrossRef]
45. Musa, H.S.; Krichen, M.; Altun, A.A.; Ammi, M. Survey on Blockchain-Based Data Storage Security for Android Mobile Applications. *Sensors* **2023**, *23*, 8749. [CrossRef] [PubMed]
46. Silva, P.R.; Vinagre, J.; Gama, J. Towards federated learning: An overview of methods and applications. *WIREs Data Min. Knowl. Discov.* **2023**, *13*, e1486. [CrossRef]
47. Ji, S.; Zhang, J.; Zhang, Y.; Han, Z.; Ma, C. LAFED: A lightweight authentication mechanism for blockchain-enabled federated learning system. *Future Gener. Comput. Syst.* **2023**, *145*, 56–67. [CrossRef]
48. Gourisetti, S.N.G.; Mylrea, M.; Patangia, H. Evaluation and Demonstration of Blockchain Applicability Framework. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1142–1156. [CrossRef]
49. 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 Secure Comput.* **2021**, *18*, 2438–2455. [CrossRef]
50. Feng, C.; Liu, B.; Yu, K.; Goudos, S.K.; Wan, S. Blockchain-Empowered Decentralized Horizontal Federated Learning for 5G-Enabled UAVs. *IEEE Trans. Industr. Inform.* **2022**, *18*, 3582–3592. [CrossRef]
51. 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; IEEE: New York, NY, USA, 2019; pp. 1–4. [CrossRef]
52. Liang, H.; Zhang, Y.; Xiong, H. A Blockchain-based Model Sharing and Calculation Method for Urban Rail Intelligent Driving Systems. In Proceedings of the 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 20–23 September 2020; ACM: New York, NY, USA, 2020; pp. 1–5. [CrossRef]
53. Rahmadika, S.; Rhee, K.H. Blockchain technology for providing an architecture model of decentralized personal health information. *Int. J. Eng. Bus. Manag.* **2018**, *10*, 1847979018790589. [CrossRef]
54. Wei, J.; Zhu, Q.; Li, Q.; Nie, L.; Shen, Z.; Choo, K.K.R.; Yu, K. A Redactable Blockchain Framework for Secure Federated Learning in Industrial Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 17901–17911. [CrossRef]
55. Zhang, P.; Liu, G.; Chen, Z.; Guo, J.; Liu, P. A study of a federated learning framework based on the interstellar file system and blockchain: Private Blockchain Federated Learning. In Proceedings of the 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), Changchun, China, 20–22 May 2022; IEEE: New York, NY, USA, 2022; pp. 267–273. [CrossRef]
56. 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), Toronto, ON, Canada, 6–9 July 2020; IEEE: New York, NY, USA, 2020; pp. 183–188. [CrossRef]
57. Liu, Y.; Ai, Z.; Sun, S.; Zhang, S.; Liu, Z.; Yu, H. FedCoin: A Peer-to-Peer Payment System for Federated Learning. In *Federated Learning: Privacy and Incentive*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 125–138. ._9. [CrossRef]
58. Ma, S.; Cao, Y.; Xiong, L. Transparent Contribution Evaluation for Secure Federated Learning on Blockchain. In Proceedings of the 2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW), Chania, Greece, 19–22 April 2021; IEEE: New York, NY, USA, 2021; pp. 88–91. [CrossRef]
59. Liu, Z.; Mu, J.; Lv, W.; Jing, Z.; Zhou, Q.; Jing, X. A Distributed Attack-Resistant Trust Model for Automatic Modulation Classification. *IEEE Commun. Lett.* **2022**, *27*, 145–149. [CrossRef]

60. Feng, T.; Jiao, Y.; Fang, J.; Tian, Y. Medical health data security model based on alliance blockchain. *Comput. Sci.* **2020**. *47*, 305–311. [CrossRef]
61. Kim, H.; Park, J.; Bennis, M.; Kim, S.L. Blockchained On-Device Federated Learning. *IEEE Commun. Lett.* **2020**, *24*, 1279–1283. [CrossRef]
62. Ramanan, P.; Nakayama, K. BAFFLE: Aggregator Free Federated Learning. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; IEEE: New York, NY, USA, 2020; pp. 72–81. [CrossRef]
63. Toyoda, K.; Zhao, J.; Zhang, A.N.S.; Mathiopoulos, P.T. Blockchain-Enabled Federated Learning With Mechanism Design. *IEEE Access* **2020**, *8*, 219744–219756. [CrossRef]
64. Pokhrel, S.R.; Choi, J. Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges. *IEEE Trans. Commun.* **2020**, *68*, 4734–4746. [CrossRef]
65. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538. [CrossRef]
66. Wang, Z.; Yan, B.; Dong, A. Blockchain Empowered Federated Learning for Data Sharing Incentive Mechanism. *Procedia Comput. Sci.* **2022**, *202*, 348-353. [CrossRef]
67. Firdaus, M.; Larasati, H.T.; Rhee, K.H. A Secure Federated Learning Framework using Blockchain and Differential Privacy. In Proceedings of the 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom), Xi'an, China, 25–27 June 2022; IEEE: New York, NY, USA, 2022; pp. 18–23. [CrossRef]
68. Bandara, E.; Shetty, S.; Rahman, A.; Mukkamala, R.; Zhao, J.; Liang, X. Bassa-ML—A Blockchain and Model Card Integrated Federated Learning Provenance Platform. In Proceedings of the 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2022; IEEE: New York, NY, USA, 2022; pp. 753–759. [CrossRef]
69. Cheng, X.; Tian, W.; Shi, F.; Zhao, M.; Chen, S.; Wang, H. A Blockchain-Empowered Cluster-Based Federated Learning Model for Blade Icing Estimation on IoT-Enabled Wind Turbine. *IEEE Trans. Industr. Inform.* **2022**, *18*, 9184–9195. [CrossRef]
70. Kong, Q.; Yin, F.; Xiao, Y.; Li, B.; Yang, X.; Cui, S. Achieving Blockchain-based Privacy-Preserving Location Proofs under Federated Learning. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; IEEE: New York, NY, USA, 2021; pp. 1–6. [CrossRef]
71. Wu, X.; Wang, Z.; Zhao, J.; Zhang, Y.; Wu, Y. FedBC: Blockchain-based Decentralized Federated Learning. In Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Beijing, China, 23–25 October 2020; IEEE: New York, NY, USA, 2020; pp. 217–221. [CrossRef]
72. Qu, Y.; Gao, L.; Xiang, Y.; Shen, S.; Yu, S. FedTwin: Blockchain-Enabled Adaptive Asynchronous Federated Learning for Digital Twin Networks. *IEEE Netw.* **2022**, *36*, 183–190. [CrossRef]
73. Shayan, M.; Fung, C.; Yoon, C.J.; Beschastnikh, I. Biscotti: A blockchain system for private and secure federated learning. *IEEE Trans. Parallel Distrib. Syst.* **2020**, *32*, 1513–1525. [CrossRef]
74. Imran, B. *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*; PACKT Publishing: Birmingham, UK, 2018.
75. Desai, H.B.; Ozdayi, M.S.; Kantarcioglu, M. BlockFLA:Accountable Federated Learning via Hybrid Blockchain Architecture. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual Event, USA, 26–28 April 2021; ACM: New York, NY, USA, 2021; pp. 101–112. [CrossRef]
76. 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), Qingdao, China, 9–11 August 2019; IEEE: New York, NY, USA, 2019; pp. 151–159. [CrossRef]
77. Zhang, Z.; Yang, T.; Liu, Y. SABlockFL: A blockchain-based smart agent system architecture and its application in federated learning. *Int. J. Crowd Sci.* **2020**, *4*, 133–147. [CrossRef]
78. Fu, X.; Wang, H.; Shi, P. A survey of Blockchain consensus algorithms: Mechanism, design and applications. *Sci. China Inf. Sci.* **2021**, *64*, 1–15. [CrossRef]
79. 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. *arXiv* **2021**, arXiv:2101.03300. [CrossRef]
80. 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]
81. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain. *IEEE Internet Things J.* **2021**, *8*, 11743–11757. [CrossRef]
82. Li, J.; Shao, Y.; Wei, K.; Ding, M.; Ma, C.; Shi, L.; Han, Z.; Poor, H.V. Blockchain Assisted Decentralized Federated Learning (BLADE-FL): Performance Analysis and Resource Allocation. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *33*, 2401–2415. [CrossRef]
83. 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]

84. Korkmaz, C.; Kocas, H.E.; Uysal, A.; Masry, A.; Ozkasap, O.; Akgun, B. Chain FL: Decentralized Federated Machine Learning via Blockchain. In Proceedings of the 2020 Second International Conference on Blockchain Computing and Applications (BCCA), Antalya, Turkey, 2–5 November 2020; IEEE: New York, NY, USA, 2020; pp. 140–146. [CrossRef]
85. Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and Open Research Challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
86. Cheng, R.; Sun, Y.; Liu, Y.; Xia, L.; Feng, D.; Imran, M.A. Blockchain-Empowered Federated Learning Approach for an Intelligent and Reliable D2D Caching Scheme. *IEEE Internet Things J.* **2022**, *9*, 7879–7890. [CrossRef]
87. Zhao, S.; Wu, Y.; Sun, R.; Qian, X.; Zi, D.; Xie, Z.; Tong, E.; Niu, W.; Liu, J.; Han, Z. Blockchain-based decentralized federated learning: A secure and privacy-preserving system. In Proceedings of the 2021 IEEE 23rd International Conference on High Performance Computing & Communications; 7th International Conference on Data Science & Systems; 19th International Conference on Smart City; 7th International Conference on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Haikou, China, 20–22 December 2021; IEEE: New York, NY, USA, 2021; pp. 941–948. [CrossRef]
88. Chen, S.; Zhang, J.; Bai, Y.; Xu, P.; Gao, T.; Jiang, H.; Gao, W.; Li, X. Blockchain Enabled Intelligence of Federated Systems (BELIEFS): An attack-tolerant trustable distributed intelligence paradigm. *Energy Rep.* **2021**, *7*, 8900–8911. [CrossRef]
89. Mehta, J.; Desai, R.; Mehta, J.; Gandhi, D.; D'Mello, L. Towards a Multi-Modular Decentralized System for Dealing with EHR Data. In Proceedings of the 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 25–26 March 2022; IEEE: New York, NY, USA, 2022; pp. 567–572.
90. He, Y.; Huang, K.; Zhang, G.; Li, J.; Chen, J.; Leung, V.C.M. A Blockchain-Enabled Federated Learning System with Edge Computing for Vehicular Networks. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021; IEEE: New York, NY, USA, 2021; pp. 1–6. [CrossRef]
91. Guo, H.; Mao, Y.; He, X.; Nie, H. A Blockchain-based Grouped Federated Learning Scheme Against Malicious Clients. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021; IEEE: New York, NY, USA, 2021; pp. 1–6. [CrossRef]
92. Wang, Z.; Ben Abdallah, A. A Robust Multi-Stage Power Consumption Prediction Method in a Semi-Decentralized Network of Electric Vehicles. *IEEE Access* **2022**, *10*, 37082–37096. [CrossRef]
93. Chen, Y.; Chen, Q.; Xie, Y. A Methodology for High-efficient Federated-learning with Consortium Blockchain. In Proceedings of the 2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2), Wuhan, China, 31 October–1 November 2020; IEEE: New York, NY, USA, 2020; pp. 3090–3095. [CrossRef]
94. Miao, Y.; Liu, Z.; Li, H.; Choo, K.K.R.; Deng, R.H. Privacy-Preserving Byzantine-Robust Federated Learning via Blockchain Systems. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 2848–2861. [CrossRef]
95. Wang, Q.; Guo, Y.; Wang, X.; Ji, T.; Yu, L.; Li, P. AI at the Edge: Blockchain-Empowered Secure Multiparty Learning with Heterogeneous Models. *IEEE Internet Things J.* **2020**, *7*, 9600–9610. [CrossRef]
96. Jiang, L.; Zheng, H.; Tian, H.; Xie, S.; Zhang, Y. Cooperative Federated Learning and Model Update Verification in Blockchain-Empowered Digital Twin Edge Networks. *IEEE Internet Things J.* **2022**, *9*, 11154–11167. [CrossRef]
97. Xu, Y.; Lu, Z.; Gai, K.; Duan, Q.; Lin, J.; Wu, J.; Choo, K.K.R. BESIFL: Blockchain Empowered Secure and Incentive Federated Learning Paradigm in IoT. *IEEE Internet Things J.* **2021**, *10*, 6561–6573. [CrossRef]
98. Ding, N.; Fang, Z.; Huang, J. Incentive Mechanism Design for Federated Learning with Multi-Dimensional Private Information. In Proceedings of the 2020 18th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT), Volos, Greece, 15–19 June 2020; IEEE: New York, NY, USA, 2020; pp. 1–8.
99. Feng, S.; Niyato, D.; Wang, P.; Kim, D.I.; Liang, Y.C. Joint Service Pricing and Cooperative Relay Communication for Federated Learning. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; IEEE: New York, NY, USA, 2019; pp. 815–820. [CrossRef]
100. 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]
101. Lim, W.Y.B.; Garg, S.; Xiong, Z.; Niyato, D.; Leung, C.; Miao, C.; Guizani, M. Dynamic Contract Design for Federated Learning in Smart Healthcare Applications. *IEEE Internet Things J.* **2021**, *8*, 16853–16862. [CrossRef]
102. Weng, J.; Weng, J.; Huang, H.; Cai, C.; Wang, C. FedServing: A Federated Prediction Serving Framework Based on Incentive Mechanism. In Proceedings of the IEEE INFOCOM 2021—IEEE Conference on Computer Communications, Vancouver, BC, Canada, 10–13 May 2021; IEEE: New York, NY, USA, 2021; pp. 1–10. [CrossRef]
103. Peng, Z.; Xu, J.; Chu, X.; Gao, S.; Yao, Y.; Gu, R.; Tang, Y. VFChain: Enabling Verifiable and Auditable Federated Learning via Blockchain Systems. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 173–186. [CrossRef]
104. 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. Industr. Inform.* **2022**, *19*, 1703–1714. [CrossRef]
105. Wang, N.; Yang, W.; Guan, Z.; Du, X.; Guizani, M. BPFL: A Blockchain Based Privacy-Preserving Federated Learning Scheme. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; IEEE: New York, NY, USA, 2021; pp. 1–6. [CrossRef]

106. Salim, S.; Turnbull, B.; Moustafa, N. A Blockchain-Enabled Explainable Federated Learning for Securing Internet-of-Things-Based Social Media 3.0 Networks. *IEEE Trans. Comput. Soc. Syst.* **2021**, 4681–4697. [CrossRef]
107. Wan, Y.; Qu, Y.; Gao, L.; Xiang, Y. Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing. *Comput. Netw.* **2022**, *204*, 108671. [CrossRef]
108. Hu, Q.; Wang, W.; Bai, X.; Jin, S.; Jiang, T. Blockchain Enabled Federated Slicing for 5G Networks with AI Accelerated Optimization. *IEEE Netw.* **2020**, *34*, 46–52. [CrossRef]
109. Liu, S.; Shang, Y. Federated Learning with Anomaly Client Detection and Decentralized Parameter Aggregation. In Proceedings of the 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Baltimore, MD, USA, 27–30 June 2022; IEEE: New York, NY, USA, 2022; pp. 37–43. [CrossRef]
110. Ma, C.; Li, J.; Shi, L.; Ding, M.; Wang, T.; Han, Z.; Poor, H.V. When Federated Learning Meets Blockchain: A New Distributed Learning Paradigm. *IEEE Comput. Intell. Mag.* **2022**, *17*, 26–33. [CrossRef]
111. Bai, S.; Yang, G.; Liu, G.; Dai, H.; Rong, C. NttpFL: Privacy-Preserving oriented No Trusted Third Party Federated Learning System based on Blockchain. *IEEE Trans. Netw. Service Manag.* **2022**, *19*, 3750–3763. [CrossRef]
112. Wang, Q.; Meng, H. Blockchain-based Federated Learning with Limited Resources. In Proceedings of the 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), Changchun, China, 20–22 May 2022; IEEE: New York, NY, USA, 2022; pp. 449–452. [CrossRef]
113. 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]
114. Liu, L.; Wu, C.; Xiao, J. Blockchain-Based platform for Distribution AI. *EasyChair Prepr.* **2019**. [CrossRef]
115. 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]
116. Jia, B.; Zhang, X.; Liu, J.; Zhang, Y.; Huang, K.; Liang, Y. Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT. *IEEE Trans. Industr. Inform.* **2022**, *18*, 4049–4058. [CrossRef]
117. Liao, H.; Wang, Z.; Zhou, Z.; Wang, Y.; Zhang, H.; Mumtaz, S.; Guizani, M. Blockchain and Semi-Distributed Learning-Based Secure and Low-Latency Computation Offloading in Space-Air-Ground-Integrated Power IoT. *IEEE J. Sel. Top. Signal Process* **2022**, *16*, 381–394. [CrossRef]
118. 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]
119. Majeed, A.; Hwang, S.O. A Comprehensive Analysis of Privacy Protection Techniques Developed for COVID-19 Pandemic. *IEEE Access* **2021**, *9*, 164159–164187. [CrossRef]
120. 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), Toronto, ON, Canada, 6–9 July 2020; IEEE: New York, NY, USA, 2020; pp. 508–513. [CrossRef]
121. 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]
122. Xu, B.; Chen, H.; Jin, S.; Jiao, Q. A Digital Currency System with Transaction Amount Privacy Protection. In Proceedings of the 2021 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Virtual, AB, Canada, 25–28 October 2021; IEEE: New York, NY, USA, 2021; pp. 535–540. [CrossRef]
123. Alsamhi, S.H.; Almalki, F.A.; Afghah, F.; Hawbani, A.; Shvetsov, A.V.; Lee, B.; Song, H. Drones' Edge Intelligence Over Smart Environments in B5G: Blockchain and Federated Learning Synergy. *IEEE Trans. Green. Commun. Netw.* **2022**, *6*, 295–312. [CrossRef]
124. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Communication-Efficient Federated Learning and Permissioned Blockchain for Digital Twin Edge Networks. *IEEE Internet Things J.* **2021**, *8*, 2276–2288. [CrossRef]
125. 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]
126. 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]
127. 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; IEEE: New York, NY, USA, 2020; pp. 244–250. [CrossRef]
128. Meese, C.; Chen, H.; Asif, S.A.; Li, W.; Shen, C.C.; Nejad, M. BFRT: Blockchained Federated Learning for Real-time Traffic Flow Prediction. In Proceedings of the 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid), Taormina, Italy, 16–19 May 2022; IEEE: New York, NY, USA, 2022; pp. 317–326. [CrossRef]
129. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [CrossRef]

130. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Trans. Industr. Inform.* **2020**, *16*, 4177–4186. [CrossRef]
131. Tseng, L.; Wong, L.; Otoum, S.; Aloqaily, M.; Othman, J.B. Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture. *IEEE Netw.* **2020**, *34*, 16–23. [CrossRef]
132. Rathee, G.; Sharma, A.; Iqbal, R.; Aloqaily, M.; Jaglan, N.; Kumar, R. A Blockchain Framework for Securing Connected and Autonomous Vehicles. *Sensors* **2019**, *19*, 3165. [CrossRef] [PubMed]
133. Ai, B.; Cheng, X.; Kurner, T.; Zhong, Z.D.; Guan, K.; He, R.S.; Xiong, L.; Matolak, D.W.; Michelson, D.G.; Briso-Rodriguez, C. Challenges Toward Wireless Communications for High-Speed Railway. *IEEE Trans. Intell. Transp. Syst.* **2014**, *15*, 2143–2158. [CrossRef]
134. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Nitin Bhagoji, A.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and Open Problems in Federated Learning. *Found. Trends Mach. Learn.* **2021**, *14*, 1–210. [CrossRef]
135. Zhu, S.; Li, R.; Cai, Z.; Kim, D.; Seo, D.; Li, W. Secure verifiable aggregation for blockchain-based federated averaging. *High-Confid. Comput.* **2022**, *2*, 100046. [CrossRef]