Blockchained Federated Learning for Internet of Things: A Comprehensive Survey

YANNA JIANG, University of Technology Sydney, Broadway, Australia
BAIHE MA, University of Technology Sydney, Broadway, Australia
XU WANG, University of Technology Sydney, Broadway, Australia
GUANGSHENG YU, CSIRO, Sydney, Australia
PING YU, Harbin Institute of Technology, Harbin, China
ZHE WANG, Xidian University, Xian, China
WEI NI, CSIRO, Sydney, Australia
REN PING LIU, University of Technology Sydney, Broadway, Australia

The demand for intelligent industries and smart services based on big data is rising rapidly with the increasing digitization and intelligence of the modern world. This survey comprehensively reviews Blockchained Federated Learning (BlockFL) that joins the benefits of both Blockchain and Federated Learning to provide a secure and efficient solution for the demand. We compare the existing BlockFL models in four Internet-of-Things (IoT) application scenarios: Personal IoT (PIoT), Industrial IoT (IIoT), Internet of Vehicles (IoV), and Internet of Health Things (IoHT), with a focus on security and privacy, trust and reliability, efficiency, and data diversity. Our analysis shows that the features of decentralization and transparency make BlockFL a secure and effective solution for distributed model training, while the overhead and compatibility still need further study. It also reveals the unique challenges of each domain presents unique challenges, e.g., the requirement of accommodating dynamic environments in IoV and the high demands of identity and permission management in IoHT, in addition to some common challenges identified, such as privacy, resource constraints, and data heterogeneity. Furthermore, we examine the existing technologies that can benefit BlockFL, thereby helping researchers and practitioners to make informed decisions about the selection and development of BlockFL for various IoT application scenarios.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Computing methodologies** → **Machine learning**; • **Computer systems organization** → *Distributed architectures;*

Additional Key Words and Phrases: Federated learning, blockchain, blockfl, internet of things

Yanna Jiang and Baihe Ma contributed equally to this research.

Authors' Contact Information: Yanna Jiang, University of Technology Sydney, Broadway, New South Wales, Australia; email: Yanna.Jiang@student.uts.edu.au; Baihe Ma, University of Technology Sydney, Broadway, New South Wales, Australia; e-mail: Baihe.Ma@uts.edu.au; Xu Wang, University of Technology Sydney, Broadway, New South Wales, Australia; e-mail: Xu.Wang-1@uts.edu.au; Guangsheng Yu, CSIRO, Sydney, New South Wales, Australia; e-mail: Saber.Yu@data61.csiro.au; Ping Yu (Corresponding author), Harbin Institute of Technology, Harbin, Heilongjiang, China; e-mail: yuping0428@hit.edu.cn; Zhe Wang, Xidian University, Xian, Shaanxi, China; e-mail: wz201018@163.com; Wei Ni, CSIRO, Sydney, New South Wales, Australia; e-mail: wei.ni@data61.csiro.au; Ren Ping Liu, University of Technology Sydney, Broadway, New South Wales, Australia; e-mail: renping.liu@uts.edu.au.

ACM 0360-0300/2024/06-ART258
https://doi.org/10.1145/3659099

ACM Reference Format:
Yanna Jiang, Baihe Ma, Xu Wang, Guangsheng Yu, Ping Yu, Zhe Wang, Wei Ni, and Ren Ping Liu. 2024. Blockchained Federated Learning for Internet of Things: A Comprehensive Survey. *ACM Comput. Surv.* 56, 10, Article 258 (June 2024), 37 pages. https://doi.org/10.1145/3659099

1 INTRODUCTION

The **Internet of Things** (**IoT**), comprising smartphones, laptops, vehicles, and smartwatches, is ubiquitous and equipped with sensing and computing capabilities that enable accurate and effective data analysis and decision-making based on massive data and advanced models [2]. **Artificial Intelligence** (**AI**) disciplines, especially the field of **Machine Learning** (**ML**), have been rapidly growing and widely applied to enhance the performance of these devices and drive the evolution of related industries [38, 87]. However, big-data-based applications bring significant risks and challenges, particularly in traditional centralized storage and computing approaches. The data collected by mobile devices and containing sensitive information is growing at an unprecedented rate, leading to a development bottleneck in cloud-based data processing.

Various approaches have been proposed to meet the requirements of new-generation data storage, data processing, and privacy protection. One such approach is **Federated Learning** (**FL**), a distributed ML approach introduced in 2016 by McMahan et al. [80]. In the FL model, training data is kept locally on edge devices, instead of being uploaded to a central server. By only sharing the model parameters for aggregation, FL mitigates the risk of privacy leakage during raw training data transmission, relieves the burden of centralized data storage and computation, and aligns well with the IoT development trend. FL empowers devices to collaboratively learn a shared model while maintaining data locally, thereby circumventing the centralization of sensitive information and further addressing the concerns over data privacy and security in the IoT ecosystem [13].

There is a growing focus on research in FL, recognizing the specific challenges and problems related to FL, such as heterogeneity and trust issues of the central server [60, 152]. To address these concerns and further advance development, Blockchain technology [86], which enables safe data storage and sharing, is introduced as an alternative to classical the central server of FL. Blockchain is a distributed and immutable ledger, consisting of blocks of data that are linked and secured using cryptography [113]. It ensures data consistency, integrity and trustworthiness across Blockchain peers, fostering a secure environment for decentralized systems [32]. The integration of FL and Blockchain technology can leverage their strengths and enable the training of distributed models in a secure and decentralized way. The advent of Blockchain technology as a complement to FL introduces an unprecedented level of security and trust. By decentralizing the management of model updates and data exchanges, Blockchain ensures that the learning process within FL is immutable and transparent [97].

In this article, we explore the synergistic integration of FL and Blockchain technologies, commonly referred to as BlockFL, across various domains of the IoT. The IoT landscape is vast and diverse, encompassing a range of application areas, each with its unique challenges and requirements. To provide a structured and in-depth analysis, we focus on four specific application areas of IoT, selected for their distinct characteristics and the unique benefits they can derive from BlockFL technologies:

— **Personal Internet of Things** (**PIoT**): PIoT enhances the connectivity and automation of daily-use objects, using data from individual sensors and devices to drive personalization and convenience [34]. The integration of BlockFL in PIoT is crucial for ensuring data privacy and security in personal applications [58].

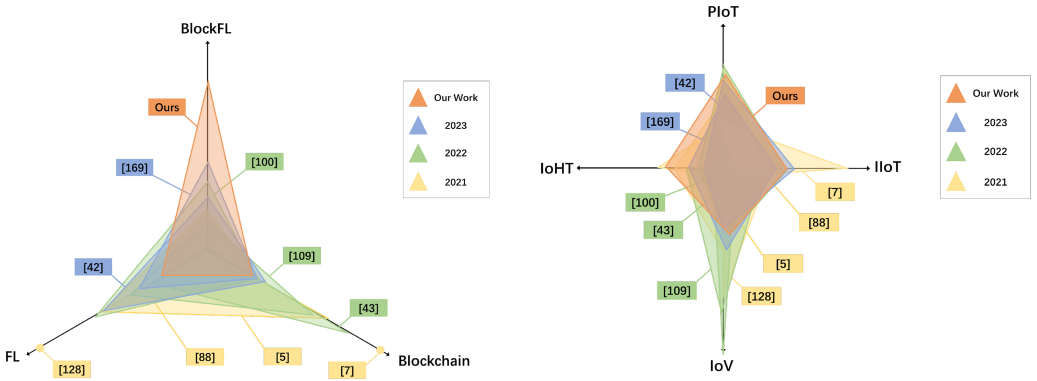

Fig. 1. This figure presents a taxonomy of recent studies on Blockchained FL. It is based on a statistical analysis of references, categorized by their technological focus and IoT application domains. Our study stands out as it concentrates on BlockFL, differentiating it from research that mainly focuses on either FL or Blockchain separately. Moreover, our work provides a broader analysis of applications and development in diverse IoT fields, surpassing studies confined to one or two domains.

— **Industrial Internet of Things (IIoT)**: IIoT is geared toward revolutionizing industrial processes through intelligent manufacturing and smart factories [110]. In IIoT, BlockFL is instrumental in ensuring secure, efficient, and transparent industrial operations, enhancing productivity and process optimization [53].
— **Internet of Vehicles (IoV)**: IoV focuses on vehicle-related aspects of IoT, providing real-time traffic information and enhancing in-vehicle services [21]. The role of BlockFL in IoV is vital for managing vast amounts of vehicular data securely and efficiently, improving transportation systems and vehicle-to-infrastructure communication [108].
— **Internet of Health Things (IoHT)**: IoHT connects patients and healthcare providers, utilizing biomedical sensors for improved healthcare services [104]. The application of BlockFL in IoHT is paramount for safeguarding sensitive health data, ensuring data integrity, and facilitating secure health data exchange [19].

By categorizing these IoT domains, we aim at highlighting the distinct challenges each faces and how the convergence of FL and Blockchain can offer tailored solutions. The criteria for selecting these domains include the sensitivity and volume of data involved, the criticality of data security and privacy, the need for efficient data processing, and the potential for enhancing overall system efficiency and user experience. This categorization allows for a focused examination of BlockFL's role in addressing the unique needs of each domain, paving the way for innovative applications and advancements in IoT.

As shown in Figure 1, our work focuses on BlockFL tailored to various IoT applications with the collation and analysis of the latest research. In contrast, prior works like [42, 88], and [5] focus more on separate discussions of FL and Blockchain, while [169] pays less attention to specific IoT scenarios, emphasizing theoretical analysis. In [100], authors discuss Blockchain as a solution to existing FL issues, focusing more on how to optimize the performance of FL rather than discussing the development of BlockFL. Research in [109] and [43] are concerned with specific domains within IoT, and [7] and [128] only consider either Blockchain or FL aspects alone, which seem limited compared to our work. Our research highlights the role of BlockFL in security and privacy, trust and reliability, efficiency, and data diversity within four IoT domains: PIoT, IIoT, IoV, and IoHT. We

analyze the distinct needs and challenges in those IoT domains, with the different development focuses of BlockFL under different application areas.

BlockFL has shown growing popularity and potential as a novel solution in recent years. Further survey work is necessary to synthesize current research and inform future developments. The four IoT domains we discussed cover a broad spectrum, addressing the primary concerns of relevant stakeholders and researchers. The challenges we pay attention to are the most mentioned in the current research, which can not be ignored in future applications and developments related to BlockFL. Issues of privacy and security are most frequently discussed in FL and Blockchain, hence critical in BlockFL. Trust and reliability are emerging as new focus areas with increasing system demands. Efficiency in learning and resource allocation is an ongoing challenge for BlockFL, especially in IoV scenarios, while addressing data diversity is crucial for practical applications in PIoT and IoHT. Our analyses provide targeted insights into the future development and optimization of BlockFL in different application scenarios, including enhancing security and privacy, building trust and reliability, improving efficiency, and addressing data diversity.

Moreover, our work discusses the potential integration of other learning frameworks, such as Split Learning, Transfer Learning, and Continuous Learning with BlockFL, which have not been explored in other articles. By leveraging the techniques of these learning frameworks, BlockFL can be further optimized in terms of efficiency and scalability, providing a more robust and feasible application across various IoT scenarios. This integration paves the way for tailored solutions that cater to specific needs within the diverse landscape of IoT applications, thereby enhancing the practical utility and implementation success of BlockFL models.

The key contributions of this article are summarized as follows:

— We conduct a detailed analysis of BlockFL in four common scenarios, i.e., PIoT, IIoT, IoV, and IoHT, and highlight the challenges faced by BlockFL in these contexts. We also examine the advantages and disadvantages of BlockFL concerning these challenges comprehensively.
— We present an overview of the relationship between BlockFL, FL, and Blockchain, and perform a comparative classification of existing BlockFL applications and features in various scenarios, focusing on four essential aspects: security and privacy, trust and reliability, efficiency, and data heterogeneity.
— We analyze the common challenges and unique needs of BlockFL across different application domains and find that combining existing technologies (including cryptography, anomaly detection, compression techniques, and normalization) and enhancing the exploration of Blockchain components can drive the development of BlockFL.

Our analysis reveals that features of decentralization and transparency make BlockFL a secure and effective solution for distributed model training, while the overhead and compatibility still need further investigation for the fruition of BlockFL. Considering diverse application domains, our analysis also indicates that, besides the universal considerations of privacy protection, resource constraints and data heterogeneity, each domain presents unique challenges, e.g., the requirement of accommodating dynamic environments in IoV and the high demands of identity and permission management in IoHT. It is anticipated that this article can serve as an informative guide for future research efforts.

The rest of this article is organized as shown in Figure 2. Section 2 introduces the concepts and definitions of FL, Blockchain, and BlockFL. Section 3 describes the different application scenarios of BlockFL. Sections 4 – 7 illustrate the latest application BlockFL models focusing on these different scenarios. The most prominent features of each reference are highlighted to show their advantages and limitations. Section 8 summarizes the key lessons learned from the previous sections and puts

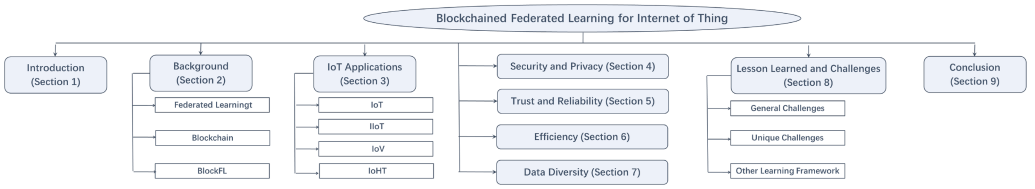

Fig. 2. Overall structure of this article.

forward future research directions. Finally, the conclusion of this article and suggestions for the follow-up works are presented in Section 9.

2 FEDERATED LEARNING, BLOCKCHAIN, AND BLOCKFL

This section introduces important concepts and models of FL and Blockchain, and analyzes the basic framework of BlockFL that combines FL and Blockchain technologies.

2.1 FL

FL is a distributed ML framework [80] involving N training participants and an aggregator. Participants, such as mobile devices, utilize their local datasets $\mathcal{D}$ for the training process and share their model parameters instead of their raw data. Meanwhile, the aggregator, such as a server, aggregates the shared local models as a global model. The central aggregator acts as a model coordinator rather than a data repository for the local data of the participants, preserving data privacy [152]. The structure allows the global model to benefit from diverse data sources without learning individual datasets, as raw data is never shared.

In a typical FL process, there are four steps involved. By using $\{P_1, \ldots, P_i, \ldots, P_N\}$ to denote the N training participants, the typical FL process is shown in the Figure 3 and divided into the following parts:

— First, the aggregator initializes the model and distributes it to all the participants;
— Next, the ith participant P_i trains the model using its local dataset D_i. The participant then obtains an improved model with an update w_i, which is achieved by minimizing a loss function $\mathcal{F}(w_i)$ as given by: $w_i^* = \arg\min \mathcal{F}(w_i), i \in N$, where the loss function $\mathcal{F}(w_i)$ is chosen differently depending on the FL algorithm to meet the model requirements of different scenarios;
— After local training, P_i transmits updated parameters to the aggregator for subsequent optimization;
— Finally, the aggregator calculates the shared parameters with the aggregation algorithm and updates the model according to the calculation results.

Then, the updated model is returned to the participants, and the next round of training begins. These processes continue to loop until the model reaches the expected performance.

The model update in each loop is determined by the choice of the aggregation algorithm used in the FL process. One of the most commonly used aggregation algorithms is FedAvg [80], which performs aggregation by computing the average during the FL process. Specifically, FedAvg calculates the shared parameters w_G as follows:

$$w_G = \frac{1}{\sum_{i \in N} |D_i|} \sum_{i=1}^{N} |D_i| w_i, \tag{1}$$

where $|D_i|$ represents the number of local training data in the dataset D_i of participant P_i.

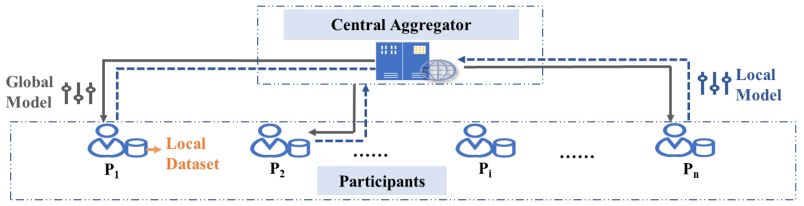

Fig. 3. Traditional FL process: Firstly, participants download the global model from the central aggregator. Then, participants perform local model training in parallel. Thirdly, participants upload their local models. Finally, the aggregator performs global model aggregation. The process repeats until the global model converges.

The FedAvg algorithm has limitations, such as the need to synchronize all updated parameters at each iteration and the consideration of dataset size in weight calculation. To address the limitations, several variants of FedAvg have been proposed to improve the effectiveness of aggregation. Reisizadeh et al. [103] introduce FedPAQ, which allows for multiple local updates before sharing parameters and controls participant selection. Li et al. [61] develop the FedProx algorithm, which uses a proximal term to reduce the computing consumption of heterogeneous data. Wang et al. [129] improve the FedMA algorithm, which applies a Bayesian non-parametric mechanism to adjust the model size based on distribution heterogeneity.

2.2 Blockchain

As the underlying support of Bitcoin, Blockchain is a distributed ledger technology that uses cryptographic techniques to secure and maintain a decentralized database [48]. Blockchain is designed to provide independent internal verification, communication, transmission, and storage while maintaining a reliable and transparent environment [156]. This technique has the potential to meet various data requirements as it allows any peer to add new data and maintain synchronized information according to specific rules.

The Blockchain is structured as a series of blocks that store transactional information. Each block is comprised of two parts, i.e., the header and the body, as shown in Figure 4. The block header includes hash values of the previous block and its own, enabling the blocks to link and form a continuous chain [111]. The Merkle Root Hash locks all the transactions in the block such that the transactions cannot be tampered without changing the root hash. The Nonce field reflects the Blockchain consensus works. The body of the Blockchain holds detailed information about transactions, which are cryptographically secured, ensuring the data it contains is immutable and tamper-resistant once a block is added to the chain [123].

The features of Blockchain [81] have led to rapid development in existing industries, which can be described as follows:

— Decentralization is the most significant feature of Blockchain. With the consensus algorithm, Blockchain can verify and execute information transactions without requiring a trusted third party.
— Immutability is an essential trait of Blockchain, as all peers approve the information newly added through a decentralized consensus. Hence, it is difficult and expensive to change the record of the Blockchain, which requires the consent of the majority.
— Auditability is also an important feature of Blockchain. Each transaction in the Blockchain is accompanied by a unique hash and timestamp, and a copy of the Blockchain is held by all peers, allowing every peer to audit any specific transaction.

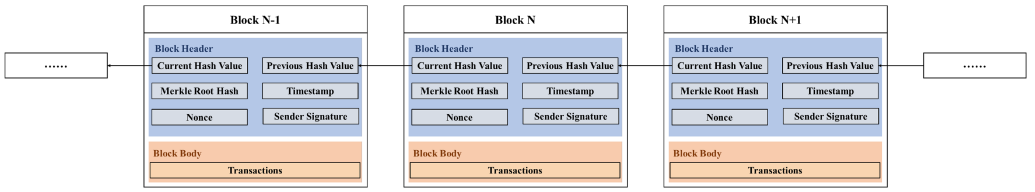

Fig. 4. The Structure of Blockchain Blocks.

— Blockchain is autonomous. With smart contracts, Blockchain can realize trust in physical machines, not bothered by anyone's interference.

Blockchains have already demonstrated their usefulness in the context of IoT [74, 75, 135], and the capacity of Blockchains has been analyzed in [132, 133, 153] for IoT applications. According to the application scenario, the Blockchain can be classified into three types [6], as follows:

— Public Blockchain: In the public Blockchain, all nodes participate in the consensus process and have the right to publish new blocks and access the whole Blockchain. The public Blockchain is the most completely decentralized, and most of the familiar Blockchain entities belong to this category, such as Bitcoin and Ether.
— Private Blockchain: The nodes in a private Blockchain need permission to join the network and participate in Blockchain activities. This type of Blockchain is suitable and often used for a single organization or enterprise, which has control over the consensus process, and thus, private Blockchain is not truly decentralized. Compared with public Blockchain, private Blockchain is generally smaller in scale and controllable in access, making transactions faster to process and the system easier to implement.
— Consortium Blockchain: Consortium Blockchain is based on the private Blockchain and built a consortium network across multiple organizations. Permission is also necessary for the nodes in the consortium Blockchain to become members of the Blockchain. The scale of the consortium Blockchain can be larger and involves more participating nodes than that of the private Blockchain, but in other performance characteristics, it is still consistent with the private Blockchain.

A detailed comparison between the three Blockchain types is shown in Table 1. In terms of the consensus process, all nodes of a public Blockchain can participate, while the consensus of a private Blockchain is controlled by a single organization. A consortium Blockchain expands on the private Blockchain to include multiple organizations. Correspondingly, a public Blockchain has complete decentralization, and its access is public without requiring permission. By contrast, private and consortium Blockchains, on the other hand, are only partially decentralized and more controlled, where nodes need permission to access.

2.3 BlockFL

The BlockFL model combines FL and Blockchain technologies, which can offer innovative solutions in various sectors [42]. By monitoring, recording, certifying, and coordinating the FL process, BlockFL offers the following advantages:

— Decentralization: Blockchain enables decentralized FL [59], where Blockchain consensus mechanisms ensure consistent views across FL participants, and Blockchain smart contracts can coordinate distributed learning processes in a decentralized way.
— Scalability and Robustness: BlockFL achieves high scalability and robustness by removing the central aggregator [5]. BlockFL allows multiple FL tasks to run simultaneously and

Table 1. Comparison of Different Blockchains

Feature	Consensus Participant	Decentralization	Access	Permission Required	Transactions Procession
Public Blockchains	All nodes	Complete	Public	No	Slow
Private Blockchains	Single Organization	Partial	Controllable	Yes	Fast
Consortium Blockchains	Multiple Organizations	Partial	Controllable	Yes	Fast

asynchronously and eliminate the single point of failure, leveraging Blockchain-based robust distributed infrastructure.
— Traceability and Auditability: Blockchain records the entire FL process immutable [50], enabling rollbacks to any point and providing a comprehensive audit trail for review.
— Anonymity and Privacy: The pseudo-anonymous mechanisms and privacy-preserving advances of Blockchain can break the link between FL updates and real identities of participants, enhancing the anonymity and privacy protection for FL tasks [14].
— Credibility and Trustworthiness: Blockchain provides tamper-resistant records of contributions in FL and Proof of Learning [57], ensuring transparency in reflecting the contributions from each participant and fostering openness and trust in FL actions.

FL also enhances Blockchain by contributing crucially to its consensus algorithms. The models and training data shared through FL, as detailed in sources [17, 136], improve the incentive structures of Blockchain. Additionally, the way of securing raw training data in FL increases the data privacy aspect of Blockchain technology.

Architecture. A BlockFL system model [50] consists of two parts: the local learning process (running on mobile devices) and the integrated calculation process (implemented on the Blockchain). In the BlockFL system, there are two main actors: participants (i.e., mobile devices) who use their local datasets to learn preliminary models, and miners in the Blockchain who verify models and facilitate aggregate calculations. The participants and miners can be either the same or different entities. The process of a BlockFL model is shown in Figure 5. Compared to traditional FL, BlockFL introduces a more complex process by adding miner validation and leader election, leveraging Blockchain technology to replace the role of traditional aggregators. The uploaded and downloaded global models in BlockFL are stored in secure blocks, and model aggregations are completed through miner campaigns. This eliminates the dependence on unreliable aggregators in FL, reducing associated risks and improving the security and trustworthiness of the overall process. The BlockFL system can be described as follows:

— Once an expected model is requested, a crowdsourcing task is created on the Blockchain. Interested participants begin the local learning process by downloading the initial model from the Blockchain and training their local model with their respective datasets. The progress of the training process depends on the factors, such as the amount of data and computing power available to the participants. With multiple training rounds, participants can get their local models that achieve high performance on their local datasets. Then, participants sign the hash values of their models with their private keys and send their models to the Blockchain for privacy protection and security, which is different from the traditional FL process.
— The BlockFL system operates within the Blockchain, which serves as permanent and immutable storage for machine learning models. Transactions processed by the miners include verifying the related signatures of the submitted model and scoring its contribution. In verification, the miners are responsible for rejecting the fake data from adversaries in the submitted models. The score of the model is a comprehensive parameter that considers both the

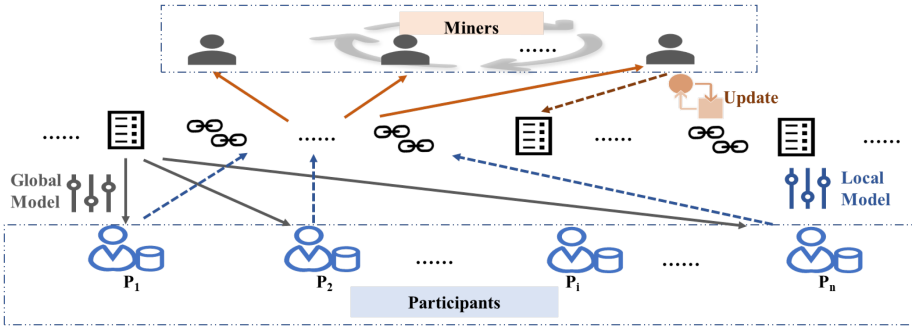

Fig. 5. BlockFL Process: First, participants download the global model from Blockchain; Then, participants perform local model training. Thirdly, participants upload their local models to Blaockchain; Next, miners process transactions to verify and score; After that, miners conduct a leadership competition; Finally, the leader elected generates a new block with the updated global model.

accuracy of the model and the size of the training dataset. The score affects the rewards of participants who submit the model and is used to determine the weight of the global aggregation. The miners compete to be the leader who generates a new block for the integrated global model. The elected leader calculates the global model parameters based on the submitted local models and their corresponding scores. The leader creates a new block consisting of the calculated global model and the signatures and agreements of other participants. The consensus protocol is based on Proof-of-X [155] or **Byzantine Fault Tolerance** (**BFT**) [15], which ensures the security of the system by assuming that more than 1/2 or 2/3 of miners are trustworthy, respectively.

— The global model in the Blockchain is regularly updated, prompting participants to download and train it with their local datasets repeatedly. The iterative process of local learning and integrated calculation continues until the global model researches the expected level of accuracy and convergence.

Why BlockFL. BlockFL is a pioneering approach that integrates the privacy-preserving structure of FL with the secure and transparent ledger system of Blockchain. While FL decentralizes model training across various nodes, ensuring data privacy by keeping it local, it typically relies on a central server for model aggregation, which can be a bottleneck [65]. Blockchain, known for its immutable and auditable transaction records, provides a secure and decentralized system but can be limited by scalability and energy consumption [25]. BlockFL capitalizes on the strengths of both, utilizing the decentralized ledger of Blockchain to enhance the security and trustworthiness of decentralized model training in FL. As shown in Table 2, we observe distinct tradeoffs across efficiency, storage, communication, and computational overhead in FL, Blockchain, and BlockFL. FL offers efficient local computations but faces limitations during global aggregation, while the efficiency of Blockchain is dependent on post-mining processes. BlockFL achieves a balance by integrating both the efficiency of FL and the overhead of Blockchain.

The storage, communication, and computation costs are evaluated in Table 2 following the BlockFL architecture, in which each local model is certified via a single Blockchain transaction. This could be done by saving the local model in the **InterPlanetary File System** (**IPFS**) and then embedding the hash and reference of the local model in a transaction. We also consider a synchronized FL process with R iteration. In each interaction, every FL participant contributes a local model by training on the local dataset, and then the local models are aggregated. The storage costs of FL, Blockchain and BlockFL are $O(N_F D + N_F M)$, $O(N_B T S)$, and $O(N_F D + N_F R M + N_B T N_F R)$,

Table 2. A Comparison of FL, Blockchain and BlockFL

	FL	Blockchain	BlockFL
Characteristics	Distributed model training on local datasets.	Decentralized ledger; Immutable transactions.	Combines FL with Blockchain; Decentralized and secure collaborative model training.
Advantages	Enhanced privacy; Reduced central data storage [128].	Enhanced security; Transparency; Auditability [7].	Decentralization; Enhanced security and privacy [100].
Limitations	Dependent on central aggregator [65]; Potential biases.	Scalability issues; Energy-intensive [25].	Increased computational and storage requirements
Efficiency	Medium (Efficient local computations, limited by aggregation)	Medium to High (Post-mining efficiency)	Medium (Balance of FL efficiency and Blockchain overhead)
Storage	$O(N_F D + N_F M)$	$O(N_B TS)$	$O(N_F D + N_F MR + N_B TN_F R)$
Communication	$O(N_F MR)$	$O(N_B TS + f(N_B)S)$	$O(N_B N_F MR + N_B TN_F R + f(N_B)N_F R)$
Computation	$O(N_F RC_L + RC_A)$	$O(N_B S + g(N_B)S)$	$O(N_F RC_L + N_B RC_A + N_B N_F R + g(N_B)N_F R)$

N_F and N_B are the numbers of FL participants and Blockchain peers, respectively. D, M, and T are the sizes of a local dataset, an FL model, and a Blockchain transaction, respectively. R is the number of FL iterations, S is the number of transactions in the Blockchain, and $S = N_F R$ for synchronized BlockFL, assuming every local model update is certified by one transaction. C_L and C_A are the computation costs of local training and FL aggregation, respectively. $f(N_B)$ and $g(N_B)$ are the communication and computation costs of a transaction, respectively, and vary according to the Blockchain consensus protocols.

respectively, where N_F is the number of FL participants, D is the average size of a local dataset, M is the size of an FL model, N_B is the number of Blockchain peers, T is the average transaction size, S is the number of transactions on the Blockchain. In the case of BlockFL, all $N_F R$ local models are logged, i.e., $S = N_F R$, leading to $O(N_F RM)$ model storage and $O(N_B TN_F R)$ Blockchain transaction storage costs across Blockchain peers. The communication costs of FL, Blockchain and BlockFL are $O(N_F MR)$, $O(N_B TS + f(N_B)S)$, and $O(N_B N_F RM + N_B TN_F R + f(N_B)N_F R)$, respectively, where $f(N_B)$ is the consensus communication cost of a transaction among N_B Blockchain peers (which varies according to the consensus protocol). In FL, $N_F R$ local models are transferred to the aggregator. In BlockFL, N_B Blockchain peers need to learn $N_F R$ models and model transactions and then run consensus on the transactions. The computation costs of FL, Blockchain and BlockFL are $O(N_F RC_L + RC_A)$, $O(N_B S + g(N_B)S)$, and $O(N_F RC_L + N_B RC_A + N_B N_F R + g(N_B)N_F R)$, respectively, where C_L is the local learning cost, C_A is the aggregation costs, $g(N_B)$ is the consensus computation cost of a transaction among N_B Blockchain peers depending on the consensus protocol. In BlockFL, the local training process is similar to the local training in FL, but the aggregation is independently executed by N_B peers with an aggregation cost of $O(N_B RC_A)$. Blockchain peers also need to verify and run consensus on $N_F R$ transactions.

Technical Features. Table 3 provides a comprehensive summary of the technical features of various BlockFL models, analyzing and comparing them based on factors such as training synchronization, chain structure, consensus mechanisms, and permission. This analysis offers valuable insights into the current state of development of popular BlockFL models.

However, the integration of Blockchain and FL introduces new security and privacy challenges. Unlike traditional FL, where local models are only shared between participants and the central aggregator, BlockFL allows all participants to access local models from each other, essentially elevating the knowledge of the participants to the level of the central aggregator. Consequently, FL participants can launch attacks that were previously exclusive to central aggregators in traditional FL, such as attacks based on consensus algorithms [35] and inference attacks [115], where attackers infer training data from model updates. The open network also raises concerns about **Intellectual Property** (**IP**) protection. Participants can learn from the local models of others and then manipulate theirs to falsely claim learning contributions. Moreover, Byzantine failures, a common threat in distributed systems, persist in BlockFL systems. For example, malicious participants may vote on FL model updates in a biased manner, either independently or collusively [147].

Table 3. Comparison of Technical Features of BlockFL Models

BlockFL Models	Data Sharing	FL System	FL Architectures	Synchronization	Chain Structure	Permission	Consensus	Application	Features
Autonomous BFL [94]	Model Sharing	Open	Distributed	Sync	Blockchain	Public	PoW	IoV	End-to-end trustworthiness assurance; Delay minimization and block arrival rate optimization.
BAFL [27]	Model Sharing	Open	Distributed	Async	Blockchain	Public	PoW	PIoT	Faster convergence of the global model; Score for secure evaluation;Dual strategy tradeoff parameters.
ChainsFL [158]	Model Sharing	Closed	Centralized	Sync + Async	Blockchain +DAG	Public	Raft + Tangle Consensus	PIoT	Two-layer Blockchain for security and scalability enhancement; Synchronous and asynchronous training combination for efficiency.
FedAC [66]	Model Sharing	Open	Centralized	Async	Blockchain	Public	PoW	PIoT	Considering a staleness coefficient; Avoidance of single-point failures; Protection for cyberattacks.
FL-Block [98]	Model Sharing	Closed	Centralized	Sync	Blockchain	Public	PoW	IIoT	Only global updates pointer saved on-chain; Prevention of single point failure; Elimination of poisoning attacks; Optimal block generation rate analysis.
Hierarchical BlockFL [16]	Knowledge Sharing	Open	Centralized	Sync	Hierarchical Blockchain	Public	PoK	IoV	Knowledge sharing with one top chain and multiple ground chains; Hierarchical FL with a bottom knowledge aggregation middle layer.
MAS BlockFL [95]	Model Sharing	Closed	Centralized	Sync	Blockchain	Authorized	PoW	IoHT	Parallel training of IoHT classifiers; Private Blockchain for secure data sharing and privacy; Allow tasks assigned to agents.
PermiDAG [71]	Model Sharing	Open	Centralized	Async	Blockchain +DAG	Authorized	DPoS + Simplified PoW	IoV	Hybrid scheme for efficiency; DRL algorithm for participant selection; Two-stage quality verification.
Secure Data Sharing Scheme [70]	Computed Results Sharing	Closed	Centralized	Sync	Blockchain	Authorized	PoQ	IIoT	Permissioned Blockchain for data sharing; Integration of differential privacy to FL; Improved resources utilization and efficiency.
VFChain [92]	Model Sharing	Open	Centralized	Sync	Blockchain	Public	PBFT	PIoT	Committee for verifiable proofs; DSC for effective data authentication; Multiple-model tasks DSC optimization.

Moreover, the additional computational and storage demands of Blockchain lead to efficiency issues for BlockFL [159]. Energy consumption and new control costs arise from coordinating Blockchain operations with FL processes, as shown in Table 2. From the learning efficiency standpoint, empirical studies indicate that the convergence speed of BlockFL models slightly lags behind traditional FL [152], signaling opportunities for further optimization. Ongoing research is increasingly focused on enhancing the operational efficiency of BlockFL across various domains, which is anticipated to augment its practical utility significantly.

3 APPLICATIONS OF BLOCKFL IN IOT

The BlockFL framework has been widely implemented in various scenarios to enhance security, privacy, reliability, and efficiency. We analyze the key indicators and challenges based on the development of BlockFL in different application domains. Existing studies on the integration of FL and Blockchain are divided into four parts based on their application scenarios: PIoT, IIoT, IoV, and IoHT, as shown in Figure 6.

Table 4 presents a comparative analysis of the varying scenarios within the IoT domain: PIoT, IIoT, IoV, and IoHT. It outlines the differences in security and privacy requirements, data processing needs, network environments, device diversity, and the key challenges faced by each scenario.

— For PIoT, security and privacy requirements range from medium to high, data processing involves handling numerous small items, and it operates over both public internet and local networks [23]. Device diversity is high, including simple sensors to smartphones, presenting challenges such as complex smart services, large data volume, data heterogeneity, varying capabilities, data sensitivity, and the need for privacy protection.

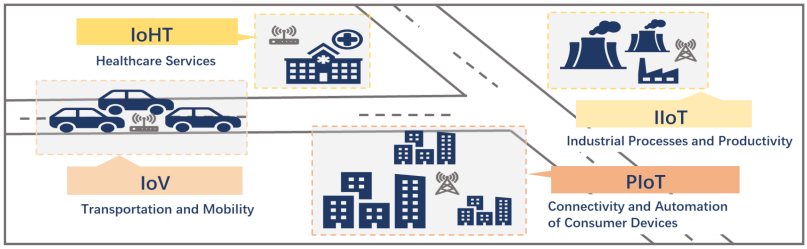

Fig. 6. Application scenarios of BlockFL: PIoT, IIoT, IoV, and IoHT. PIoT focuses on improving connectivity and automation of everyday objects, while IIoT focuses on industrialized processes and productivity improvements. IoV focuses on transportation, and IoHT focuses on medical health. All aspects of life and work are encompassed by these four areas.

Table 4. Distinguishing IoT Scenarios: A Comparative Analysis of PIoT, IIoT, IoV, and IoHT

Scenario	PIoT	IIoT	IoV	IoHT
Security and Privacy Requirements	Medium to high (Depending on the application)	High (Especially regarding the impact of production processes)	High (For driving safety)	High (Dealing with sensitive personal health information)
Data Processing	Handling a massive number of small items.	Processing complex datasets; Real-time requirements could be low.	Real-time data processing is crucial.	Heterogeneous data integration; High privacy protection.
Network Environment	Both public internet and local networks	Mostly closed networks	Dynamic networks	Secure and controllable networks
Device Diversity	High (From simple sensors to smartphones)	Low (Industrial-specific devices)	Medium to high (In-vehicle devices and sensors)	High (Including wearable devices and medical monitor equipment)
Key Challenges	Complex smart services; Large amount of small data; Complex in data processing; Data heterogeneity; Varying capabilities; Data sensitivity; Privacy protection.	Complex intelligent collaboration; Closed environment; Reliability and stability of the system; Scalability; Data security.	High delay; Dynamic nature of the network; Timeliness of the data; Dynamic data flow.	Difficult identity management; Privacy protection; Data Security; Trust.

— IIoT has high-security needs, especially considering the complex production processes [124]. It requires processing complex datasets and real-time responses within mostly closed network environments. Device diversity is low, focused on industrial-specific devices. The challenges in IIoT encompass complex intelligent collaboration, the need for closed and stable system environments, and issues related to scalability and data security.
— The IoV scenario, crucial for driving safety, demands high levels of security. It is characterized by the need for real-time data processing within dynamic networks. Device diversity is medium to high, with in-vehicle devices and sensors [85]. The key challenges include high delay, the dynamic nature of the network, ensuring timeliness of data, and managing dynamic data flow.
— IoHT, dealing with sensitive personal health information, has high security and privacy demands. Data processing in IoHT involves heterogeneous data integration within secure and controllable network environments. Device diversity is high, ranging from wearable devices to medical monitoring equipment [77]. The challenges faced by IoHT are managing complex identities, protecting privacy, ensuring security, and maintaining trust.

4 SECURITY AND PRIVACY OF BLOCKFL FOR IOT

Security and privacy are crucial elements when it comes to FL and Blockchain technology, and this importance carries over to BlockFL as well, making them areas of significant interest and

concern. This section presents an analysis and comparison of BlockFL models from various application domains with a focus on security and privacy. Compared to traditional FL, the integration of Blockchain offers BlockFL a stronger and more scalable solution to support security and privacy protection without depending on any centralized server.

4.1 PIoT

As PIoT applications become more widespread, the massive amounts of sensitive information used for training models pose significant challenges to privacy protection. In recent years, data security and privacy protection have garnered increased attention from researchers, particularly in relation to data generated during the sensing, communication, and computation processes of PIoT.

FL is at risk of data leakage when facing adversaries with an honest-but-curious server [8] or with **Generative Adversarial Network** (**GAN**) technology [37]. Although Blockchain can promote the development of decentralized and data-intensive applications [22], FL still relies on the honesty of miners as all raw data are public. Therefore, traditional FL and separate Blockchain technologies cannot satisfy the security and privacy requirements of PIoT scenarios. Hence, the BlockFL, which combines the advantages of FL and Blockchain, has become a new research direction to solve security and privacy issues in the PIoT.

A number of researchers have proposed different solutions for addressing the challenges of security and privacy in FL with the integration of Blockchain technology. Awan et al. [10] present a Blockchain-based PPFL model, which combines the FL framework with the decentralized trust of Blockchain to ensure privacy preservation. To achieve this, the authors enhance a variant of the Paillier cryptosystem to implement homomorphic encryption. Yin et al. [150] propose an FDC framework based on FL and Blockchain, which leverages multiparty secure computation technologies to ensure data security. Wang et al. [131] discuss the Security Parameter Aggregation Mechanisms in detail in their BlockFedML model. Furthermore, Ma et al. [72] propose a new group-based Shapley value computation framework that is compatible with secure aggregation in a Blockchain-based FL model. The approaches aim at addressing the privacy and security concerns in FL by integrating Blockchain technology and novel cryptographic methods.

4.2 IIoT

The proliferation of IIoT has resulted in an exponential increase in the volume of data generated by devices equipped by various industries. The value of the data, because of the sensitive information it contains, has gained rise to concerns about data security. The leakage of IIoT data could result in significant financial losses for the company, as well as disruption and disorder within the industry.

Ensuring data security is a crucial factor in determining the utility of the IIoT model. Wang et al. [118] identify the security requirements for IIoT and investigate the advantages of integrating Blockchain technology into IIoT applications. In a separate study, Blockchain is leveraged in edge intelligence to optimize resource allocation in IIoT [163]. Additionally, FL has also been highlighted in IIoT applications [149].

To satisfy differential privacy, Geyer et al. [31] propose a method to conceal the contribution of each client during the training process. In the pursuit of safer data sharing, Lu et al. [70] build data models with BlockFL structures, where only FL-generated data models are shared by Blockchain. And thus, the model reduces the risk of raw data leakage and effectively protects data security. By using homomorphic encryption and secure multi-party computation, the authors ensure that the privacy of the raw data is maintained while enabling collaborative learning. Furthermore, Yazdinejad et al. [149] develop a block hunter framework based on cluster detection to automatically search for attacks and threat risks in BlockFL networks.

4.3 IoV

In IoV, practical models require large amounts of data sharing, which can include sensitive private information such as frequently visited addresses, real-time road conditions, driving routes, and driving preferences. Protecting privacy while participating in model training and sharing information with others is important and necessary in IoV applications [162], where the BlockFL framework could play an influential role.

Liu et al. [64] improve an optimized mask noise model upload algorithm for secure secret sharing of model parameters. The authors also introduce a two-stage **Intrusion Detection System** (**IDS**) utilizing the combination of FL and Blockchain in vehicles and roadside units to ensure data security and privacy protection in IoV. Chen et al. [18] propose a novel Byzantine-fault-tolerant Blockchain-based FL method named BDFL, which implements a publicly verifiable secret sharing scheme to address privacy concerns in IoV. The experimental results on actual datasets demonstrate the practicality of multi-object recognition while preserving privacy.

4.4 IoHT

In the IoHT, a large amount of sensitive information poses a significant risk of privacy breaches. To address the issue and enable secure data sharing, BlockFL has been introduced as a promising approach for IoHT applications. Passerat-Palmbach et al. [91] propose a basic structure of Blockchain-orchestrated FL and identify six critical elements of privacy and security requirements in IoHT models:

— Ensuring data security sharing and processing in the Blockchain while maintaining privacy;
— refusing to generate data or fabricate value effectively;
— ensuring computation with FL and advanced cryptography;
— ensuring privacy through both software and hardware cryptography;
— establishing a suitable incentive mechanism to evaluate data quality;
— preventing poisoning attacks and mitigating the impact of poor data.

The requirements provide a comprehensive framework for developing secure and privacy-preserving IoHT applications using Blockchain-orchestrated FL.

Based on the requirements, Połap et al. [95] develop a multi-agent system that divides specific medical tasks into agent units for parallel training of classifiers with FL and uses Blockchain to share and protect private data. Similarly, Aich et al. [1] design a BlockFL-based solution for the secure sharing of healthcare data to address the fragmented nature of personal medical data. However, the approach has only been theoretically analyzed without using practical applications yet.

El Rifai et al. [26] conduct experiments on a diabetes dataset to evaluate the effectiveness of their model, which utilizes BlockFL for secure knowledge sharing between medical centers while preventing attackers from accessing the raw records of the patients. The experimental results demonstrate the ability of the proposed approach to ensure data security and privacy protection. A hybrid Blockchain-based FL framework [101] has been tested in the context of COVID-19 clinical trials, which ensures the complete privacy of training data and supports reputation management, making it more relevant to current healthcare applications. Another privacy-preservation framework proposed by Singh et al. [117] also illustrates that the BlockFL technology can mitigate the risk of exposing patient medical data, creating a transparent and secure environment for data sharing and model training

4.5 Conclusion

Table 5 highlights models for IoT security and privacy in PIoT, IIoT, IoV, and IoHT. In PIoT, BC-based PPFL [10] focuses on privacy with enhancements like a Paillier cryptosystem variant, facing

Table 5. Comparison of BlockFL across IoT Domains for Security and Privacy

	Domains	Model	Objective	Features	Advantages	Limitations
Security and Privacy	PIoT	BC-based PPFL [10]	Privacy preserving	Malicious client assumption; Enhanced Paillier cryptosystem variant.	Protecting data privacy; Overcome random client dropouts; Identify and exclude malicious client updates.	Parallelism issues; Non-IID partitioned data challenges.
		FDC [150]	Secure multiparty data computation	Divide into private and public data centers; Support scattered data fragments.	Secure collaboration; Flexible and efficient access control.	Efficiency; Challenges for complex tasks and large models.
		Block-FedML [131]	Secure aggregation	Immutable audit trail; Encrypted communications.	Defend against model input integrity attacks; Protecting data privacy.	Lack of experimental validation.
	IIoT	BlockFL Data Models [70]	Secure data sharing	Data model sharing instead of data sharing; Integrate differential privacy.	Privacy-preserving data sharing; Collaboration among multiple untrusted parties.	Utility optimization of data map.
		Block Hunter [149]	Threat hunting	Cluster-based anomaly detection architecture.	Implementation of various anomaly detection algorithms.	Limited resource challenges; Evolving attack.
	IoV	Two-stage IDS [64]	Autonomous Driving Safety	Mask noise model upload algorithm; Trust evaluation algorithm.	Edge vehicles and roadside facilities collaborate; Secure model sharing.	Limited resource challenges.
		BDFL [18]	Autonomous Vehicles Privacy-preservation	Extended HydRand protocol; Publicly verifiable secret sharing.	Byzantine-fault-tolerant; High fidelity to models' parameters.	Limited resource challenges; Model stealing threat.
	IoHT	Multi-agent System [95]	Private Data Security	Division of complicated tasks into individual objects; Agent with a consortium mechanism.	Process medical data in real time; Task segregation.	High latency; Classifier optimization.
		Lightweight hybrid BlockFL [101]	Privacy preserving	Multiple encryption methods; Lightweight differential privacy.	Target IoHT-powered edge devices; Full encryption of dataset, model training, and inferencing process.	Limited resource challenges.
		Secure System in Smart Healthcare [117]	Privacy preserving	Distributed secure environment; Cloud computing service.	Lightweight; Scalable; Supports interoperability.	High latency; Limited resource challenges.

parallelism and non-IID data challenges. FDC [150] offers secure multiparty data computation with flexible access control, though with efficiency concerns. BlockFedML [131] provides secure aggregation with audit trails and encrypted communications but lacks experimental validation. For IIoT, BlockFL Data Models [70] enhance secure data sharing with differential privacy but struggle with utility optimization. Block Hunter [149] employs cluster-based anomaly detection for threat hunting, constrained by resource limitations. In IoV, a two-stage IDS [64] ensures safety in autonomous driving with a mask noise model, limited by resources. BDFL [18] aims at privacy preservation in autonomous vehicles using the HyRand protocol, facing scalability challenges. In IoHT, a multi-agent system [95] secures medical data processing with real-time capabilities, hindered by latency. A hybrid BlockFL [101] preserves privacy with encryption methods, yet with resource constraints. Secure Architecture in Smart Healthcare [117] maintains privacy in a distributed environment, dealing with latency and resource issues.

As shown in Figure 7, BlockFL models are making substantial strides in enhancing security and privacy across various IoT domains, addressing specific challenges and pertinent objectives. In PIoT, the emphasis is on preserving the privacy of vast amounts of sensitive consumer information, while in IIoT, the focus shifts to securing corporate data to ensure industry stability [63]. For IoV, the critical concern is secure information sharing to maintain the integrity of autonomous driving safety, and in IoHT, the models underscore the need to protect sensitive healthcare information, which is vital for maintaining patient trust and adhering to regulatory standards. Particularly in IoHT, where the stakes are incredibly high due to the involvement of personal medical data, BlockFL models are not only safeguarding privacy but also ensuring the security of data, which directly impacts the quality of healthcare services [119]. By leveraging the inherent properties of blockchain, such as immutability and decentralized consensus, along with the data localization of FL, these models foster innovation in healthcare technologies by enabling secure data sharing without compromising on privacy.

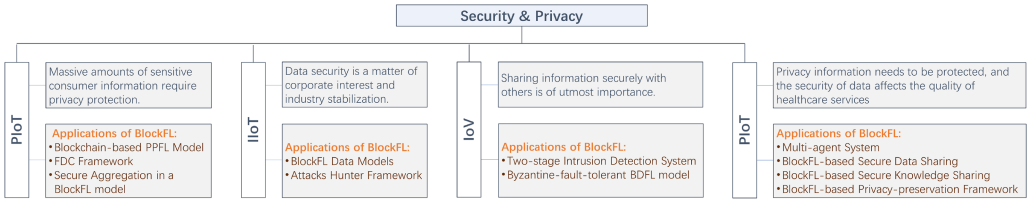

Fig. 7. Application of BlockFL: Security and Privacy. The models applied in PIoT and IoHT place greater emphasis on privacy protection, while those used in IIoT and IoV prioritize security. This reflects the different priorities and concerns of each domain, highlighting the need for tailored approaches to security and privacy protection in BlockFL.

5 TRUST AND RELIABILITY OF BLOCKFL FOR IOT

Apart from the improved security and privacy protection, the characteristics of immutability and auditability in Blockchain provide a sense of trust and reliability to the BlockFL process. In this section, we delve into the ways in which BlockFL addresses the trust and reliability problems and examine the specific features of BlockFL-based models that are tailored to meet the unique needs and characteristics of various application domains.

5.1 PIoT

The PIoT model has to ensure the trust and availability of information, and services to enable its practical application. To avoid errors and losses in data transmission and communication, which can have catastrophic consequences (e.g., the risk of poisoning attacks), [12] has demonstrated the possibility of malicious workers manipulating model results by injecting poisonous data or tampering with training data.

Existing studies have been developed to tackle the challenge of information errors and losses during traditional FL training. Zhao et al. [166] design a method to address the issue by minimizing the influence of low-quality participants. VerifyNet [143] introduces a verifiable framework that verifies the integrity of the aggregated results of FL. However, the framework faces the problem of susceptibility to single-point attacks due to its reliance on the central server.

The combination of Blockchain and FL technologies improves the reliability of PIoT models because of the auditability and decentralization provided by Blockchain. Peng et al. [92] improve the VFChain system, enabling verification for the FL training process and recording verifiable proofs in the Blockchain. Preuveneers et al. [96] introduce an anomaly detection model into the FL process and utilize Blockchain technology to record its incremental updates. Kang et al. [47] propose a metric called "reputation" to support reliable-worker selection, ensuring data integrity and preventing tampering. By reducing the impact of adversarial data corruption, integrating Blockchain and FL technologies can improve the robustness and stability of PIoT models. The work in [127] applies the concept of reputation in a Blockchain-based fine-grained FL model to facilitate trustworthy collaborative training. The experiment in [120] shows that implementing the Blockchain in FL improves the performance when adopting various types of corruption to the dataset of the end-point adversary, including salt and pepper noise and circle occlusion. The FLchain scheme developed by Majeed et al. [73] outperforms traditional FL models in robustness as the provenance of data is auditable.

5.2 IIoT

Real-world industries require reliable and stable IIoT models that can withstand environmental disturbances and attacks. However, data flaws are common in the FL process as local datasets

are easily disturbed by environmental factors [36]. The usage of Blockchain for the underlying mechanism of the IIoT model can ensure the regular operation of the entire system so that the machines can work honestly and normally [112].

To detect device failures and attacks in IIoT applications, Zhang et al. [164] introduce an optimization of an averaging algorithm called CDW-FedAvg that calculates the distance between positive and negative class data. By combining the advantages of both FL and Blockchain, the developed approach reduces the impact of device failures and improves the stability of the IIoT system. Similarly, Qu et al. [99] develop a D2C paradigm for the IIoT model and a modified Markovian decision process to enhance performance when facing poisoning attacks.

Stability is a crucial advantage of industrial automation, enabling control and prediction of the operational status of machines. In Industry 4.0, researchers aim at enhancing the stability of IIoT models by combining FL and Blockchain technologies. Hua et al. [39] conduct experiments on heavy haul rail applications, replacing manual operation with intelligent control using a Blockchain-based asynchronous FL system. The simulation results demonstrated that the proposed BlockFL system effectively achieves stable and smart control in real heavy-haul rail applications.

5.3 IoV

The high mobility of vehicles in IoV introduces dynamically and rapidly changing environments, leading to crucial timeliness of decisions, as autonomous driving and intelligent transportation systems require vehicles to respond quickly to real-world situations. Therefore, improving the speed of vehicles' model learning and information communication is a key issue in practical applications and a prominent topic in research.

To accelerate model learning and information communication in the IoV, Pokhrel et al. [94] develop a mathematical analysis to identify the delay in the BlockFL model, where participating vehicles share their on-vehicle machine learning model updates via Blockchain and cooperate to complete the FL process. The vehicles calculate the total end-to-end latency, including communication and consensus delays, and an online algorithm is proposed to adjust parameters in real time to minimize the model delay.

To improve the intelligence of vehicles, different models are needed to process, analyze, and respond to different application scenarios. Each model in the IoV requires diverse and vast data that is collected from the vehicles, the neighbors, and the roadside units. Due to the variability of the IoV, neighboring vehicles are in a constant state of flux, so vehicles in the IoV are often unfamiliar with their surroundings. It is, therefore, essential to evaluate the credibility of the data and identify any malicious attempts to compromise it.

Blockchain has been seen as an effective tool to integrate with FL as BlockFL to manage participants and improve system reliability [148] to address the trustworthiness issue in the IoV. PermiDAG model developed by Lu et al. [71] uses a hybrid Blockchain with a directed acyclic graph to perform asynchronous FL. The quality of shared parameters is verified to detect false information and malicious data. Kang et al. [45] introduce a reputation system to judge participant trustworthiness and design a distributed reputation calculation scheme for selecting trustworthy participants. The authors present a stable many-to-one matching model for task assignment to achieve a trusted win-win situation.

5.4 IoHT

In the realm of IoHT, trust and reliability are paramount, with the sector demanding robust frameworks to guarantee data privacy and secure sharing of sensitive health information. This need

has been accentuated by the challenges posed by the COVID-19 pandemic [107], where concerns about misinformation and malicious behavior have become rife. Moreover, the growing demand for personalized medicine presents new challenges to traditional healthcare systems, requiring innovations to accommodate individual patient needs [52].

In this context, the BlockFL model has gained attention for its potential to foster trust and reliability in healthcare data management. Samuel et al. have illustrated this by proposing a BlockFL-based infrastructure that not only enhances the dissemination of authentic COVID-19 information but also offers a robust infrastructure against security attacks [107]. Similarly, Moulahi et al. create a trusted Blockchain-based FL system capable of predicting diabetes risk, achieving significant accuracy in their results and demonstrating the resilience of the system against cyberattacks [82]. Some work focuses on the trustworthiness, accountability, and fairness of FL systems in IoHT. A BlockFL architecture is proposed in [68] design to improve these aspects by employing smart contracts and a fair data sampler algorithm. It is demonstrated to be feasible, enabling accountability and improving fairness in a COVID-19 X-ray detection use case.

Personalized precision medicine as a transformative approach to healthcare, which focuses on customizing treatments and therapies for individual patients based on their unique medical data [52], requires a high level of trust and reliability in managing sensitive health information, facilitated by advanced technologies like Blockchain and FL. Ali et al. have explored the transformative potential of Blockchain-enabled FL for precision medicine with a representative dataset of **electronic medical records** (**EMRs**) [4]. They emphasize the importance of trust and decentralized data sharing and demonstrate the feasibility of BlockFL by simulating an EMRs system. To address the need for personalized healthcare models and the challenges of potential risks, Lian et al. propose a Blockchain-based personalized FL system for IoHT with personalization layers to capture personalized features, which shows better results on heterogeneous medical data than a one-size-fits-all global model [62].

5.5 Conclusion

Table 6 shows the comparative analysis of BlockFL across various IoT domains for Trust and Reliability, which reveals distinct approaches tailored to the unique challenges of each sector. In the realm of PIoT, models like VFChain [92] prioritize verifiability and auditability to enhance data integrity, whereas IIoT solutions like the D2C paradigm [99] focus on resistance to sophisticated cyber threats, reflecting the critical need for robust defense mechanisms in industrial settings. For IoV, the BFL model underscores the importance of minimizing delays and ensuring data reliability to support the dynamic nature of autonomous vehicles [94]. In the healthcare sector, IoHT, the sensitivity of data in IoHT necessitates models that not only bolster system security but also address the pressing need for accountable and fair data handling, as demonstrated by the COVID-19 X-ray Detection [68] and Personalized Healthcare models [62]. These innovations collectively underscore the pivotal role of BlockFL in fortifying trust and reliability, with each domain benefiting from bespoke features that address their specific security challenges and operational demands.

BlockFL models are crucial in reinforcing trust and reliability within the IoT sphere, as shown in Figure 8. The models cater to the unique demands of each domain: PIoT focuses on data transmission accuracy, IIoT on correcting data flaws due to environmental impacts, IoV on timely decision-making for mobile units, and IoHT on safeguarding sensitive health data. Particularly in IIoT, where uninterrupted operation in harsh conditions is common, the reliability requirements highlight the importance of BlockFL models. The robust BlockFL frameworks counteract exploitation threats and ensure continuous industrial activities, playing a key role in protecting against economic and safety risks.

Table 6. Comparison of BlockFL across IoT Domains for Trusty and Reliability

	Domains	Model	Objective	Features	Advantages	Limitations
Trust and Reliability	PIoT	VFChain [92]	Verifiability and Auditability	Selected committee for aggregation ; Novel authenticated data structure.	High efficiency; Secure committee rotation.	Time-consuming; Limited resource challenges.
		Chained Anomaly Detection [96]	Anomaly Detection	Permissioned Blockchain-based; Audit of ML models.	Transparency over the distributed training; Flexibility to apply different frameworks.	Validity threats; Global network-level attack
		Flchain [73]	Robust	Integrated Multi-access edge computing; Introduce the global model state trie.	Ensure provenance; Maintain auditable.	High latency; Limited resource challenges.
	IIoT	CDW-FedAvg [164]	Failure Detection	Custom Merkle tree for data record; Centroid distance weighted federated averaging.	Enable verifiable integrity; High detection accuracy.	Limited resource challenges.
		D2C paradigm [99]	Attack Resistance	Modified Markovian decision process; Industry 4.0 model.	Improves the accuracy and robustness against poisoning attacks.	Attacker assumption; Performance indexes optimization.
		Railway Control [39]	Intelligent Control	SVM-based model; Mixing kernel function.	Asynchronous collaborative ML; High accuracy with dynamic weight factor changing.	Scalability challenges.
	IoV	BFL for AVs [94]	Delay Reduction	Controllable network and BFL parameters; Exploit channel dynamics to minimize delay.	Quantify the end-to-end delay; Derive optimal block arrival rate.	Packet-level loss issues; Limited resource challenges.
		Hybrid PermiDAG [71]	Reliability	Two-stage verification; Node selection to minimize costs.	Guarantee the reliability of shared data; High efficiency.	Limited resource challenges.
		Matching Model [45]	Task Assignment	Distributed reputation calculation scheme based on subjective logic model.	No risk of a single point of failure; Win-win for both worker and task publisher.	Many-to-many matching problem; Limited resource challenges.
	IoHT	X-ray Detection [68]	Accountability and Fairness	Smart contract-based data-model provenance registry; Weighted fair data sampler algorithm.	Enable accountability; Improve fairness; High generalization and accuracy.	Scalability challenges.
		Persona lized Healthcare [62]	System Security	Divide the model into base layers and personalization layers.	Achieve personalized models; Avoid single point of failure.	Vulnerable to inference attacks and model inversion attacks.

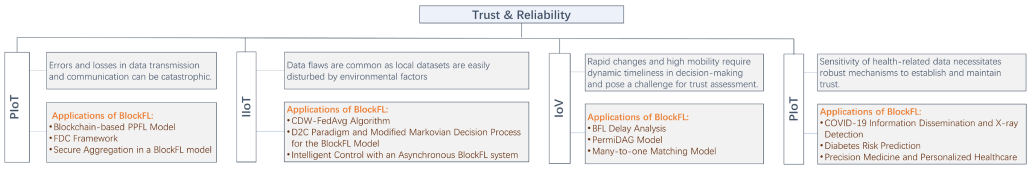

Fig. 8. Application of BlockFL: Trust and Reliability. The high-speed changing environment of IoV requires application models to have higher requirements for trust and stability. At the same time, models in PIoT and IIoT also have specific demands for trust and stability. The sensitivity of health-related data necessitates robust mechanisms to establish and maintain trust in IoHT.

6 EFFICIENCY OF BLOCKFL FOR IOT

In practical application scenarios, realistic conditions such as limited resources and restricted costs must be taken into account, unlike in theoretical analysis. As a result, adjusting various factors and seeking efficient solutions under limited conditions is a crucial topic in the development of BlockFL. Because BlockFL comprises the resource-intensive learning process of FL and the block generation process of Blockchain, balancing these two parts to achieve optimal system performance requires careful consideration of multiple factors. This section focuses on the efforts of BlockFL to balance efficiency within resource constraints in various application domains through analysis and discussion.

6.1 PIoT

The practicality of the PIoT model is to enable intelligent PIoT devices and offer advanced services. To accomplish this ambition, the PIoT model should exhibit high accuracy and efficiency when executing tasks, which means optimizing algorithms and designing models for improving performance under the condition of limited resources.

Accuracy is a key metric for model evaluation in PIoT models. Existing works have demonstrated that BlockFL models integrating Blockchain and FL technologies outperform traditional FL and separate Blockchain in various tasks. Liu et al. [66] proposed the FedAC model, which combines asynchronous FL and Blockchain technologies, and achieved impressive accuracy rates of 98.96% in horizontal data distribution and 95.84% in vertical data distribution, outperforming the accuracy of its counterparts.

Efficiency is also an important metric for evaluating BlockFL models. To improve efficiency, Ramanan et al. [102] present the BAFFLE model by using smart contracts in Blockchain to coordinate the round delineation, model aggregation, and update tasks in FL. The model significantly reduces the computational cost of the model because smart contracts are computerized transaction protocols [122] that automatically execute the contractual terms. Feng et al. [27] develop two complementary policies to ensure efficiency, i.e., controlling the block generation rate and dynamically adjusting the number of training times in asynchronous FL. In ChainsFL [158], synchronous and asynchronous training are combined to improve the efficiency of the model.

6.2 IIoT

In research and analysis, the existing studies assume that devices participating in model training have unlimited energy and ample computing power. However, in the real-world, industrial machines used in manufacturing often fall short of theoretical ideals. Due to the cost considerations, such equipment is subject to constraints on capacity, energy, communication ability, and other aspects. For instance, machines with limited computing power require more time to train and update the model, while those with poor wireless channel conditions take longer to transmit information. Therefore, it is essential to flexibly adjust model parameters based on actual conditions and enhance model performance under resource limitations.

To address the problem of resource constraints, Nishio et al. [89] develop the FedCS model, which selects suitable training participants. By excluding unqualified machines, as many participants as possible can join the training process under limited conditions, making it suitable for actual industrial applications. In addition to participant selection, adjusting other model parameters is also effective. Qu et al. [98] consider a range of factors, including communication, delays, and computation cost, to determine the optimal block generation rate in FL-Block, an autonomous FL system based on Blockchain.

Reducing energy consumption can be utilized to address the resource issues in BlockFL training. Lu et al. [69] improve a compression technique to reduce communication costs without sacrificing performance. The authors consider the instability and complexity of the network connections in the IIoT model, allowing machines to join or leave the training process more freely. Kang et al. [44] employ a gradient compression scheme to replace complete gradients with sparse but important gradients, effectively reducing communication overhead.

6.3 IoV

The dynamic nature of vehicular networks introduces a challenge in resource allocation. Despite the advancements in in-vehicle computing and communication technologies, there still exists a gap in achieving optimal solutions for model learning in theory. This is especially true in the

case of BlockFL, where vehicles need to conduct multiple rounds of communication and require high computational power. Hence, exploring ways to adjust parameters effectively to meet the requirements under limited resources is an important research direction in IoV.

Chai et al. [16] improve a hierarchical FL algorithm that leverages Blockchain technology to include multiple ground chains and one top chain, resulting in reduced computation and sharing consumption. The experimental results show the effectiveness of the hierarchical structure. Pokhrel et al. [93] introduce a Blockchain-empowered FL system for drones in 6G networks aimed at disaster response systems. The authors focus on the impact of transmission parameters such as power and the number of miners on energy consumption through modeling and simulation that offer valuable insights and potential research directions for future work in this field. The negative impact of the energy limitation problem of drones on the service time is also discussed in a data collection BlockFL scheme [41].

6.4 IoHT

Efficiency and resource management emerge as non-negligible concerns in IoHT, underscoring the need for solutions that optimize data processing and minimize energy consumption. The dynamic and distributed nature of IoHT devices, which collect vast amounts of patient data, poses significant challenges in terms of bandwidth usage, storage capacity, and computational load [161].

Traditional centralized data processing models often struggle with these challenges, leading to inefficiencies and potential risks. The application of Blockchain-empowered FL addresses these issues by decentralizing data analysis, thus reducing the need for data to be transmitted to a central server for processing. Lakhan et al. [56] introduce an FL-based Blockchain system to minimize energy consumption and delay in healthcare applications, showcasing the potential of BlockFL in meeting the stringent requirements of healthcare workloads with resource constraints. While Muazu et al. [83] demonstrate how edge computing, combined with BlockFL, can optimize resource management in IoHT, reducing computing costs while enhancing security and privacy. The above studies collectively underscore the transformative impact of BlockFL on IoHT, highlighting the role of BlockFL in achieving efficiency within the healthcare domain, especially with the rapid development of healthcare-based cyber-physical systems [67].

6.5 Conclusion

Table 7 presents models designed to boost efficiency in four domains. In PIoT, the BAFFLE model [102] enhances computational performance by segmenting parameter space, reducing costs but grappling with complexities in large models. BAFL [27] intertwines power with model utility for learning efficiency, though optimization remains a challenge. For IIoT, ChainsFL [158] uses a DAG-based network for better efficiency and scalability, despite resource limitations. FL-Block [98] leverages fog computing for cost-effective communication and consensus, yet faces stability issues. PAFLM [69] optimizes utility via edge network ML, with synchronization hurdles. In IoV, Hierarchical BlockFL [16] and BlockFL for Drones [93] focus on knowledge sharing and efficient consensus in IoT drones, contending with scalability in dynamic environments. For IoHT, FL-BETS [56] addresses task scheduling with risk quantification, balancing resource allocation and fraud vulnerability. Edge-empowered BlockFL [83] aims at resourcing optimization through mixed-model programming, improving allocation and reducing consumption, yet faces scalability issues.

BlockFL is instrumental in enhancing efficiency across IoT applications, with a notable impact in the IoV domain. As shown in Figure 9, BlockFL models in PIoT aim for high efficiency within limited resources to unlock advanced consumer services [3], while stakeholders and researchers in the IIoT focus on tackling cost-related performance gaps in manufacturing [28]. The IoV sector benefits from the ability of BlockFL to manage dynamic network resources effectively, optimizing

Table 7. Comparison of BlockFL Across IoT Domains for Efficiency

	Domains	Model	Objective	Features	Advantages	Limitations
Efficiency	PIoT	BAFFLE [102]	Computational Performance Improvement	Decompose parameter space into distinct chunks.	Boost computational performance; Reduce the gas costs.	Privacy Risk; Challenges for complex task.
		BAFL [27]	Learning Efficiency	Entropy weight method; Model the energy consumption and delay as a Pareto problem.	High efficiency; High performance; Preventing poisoning attacks.	Challenges in deploying to real-world.
		ChainsFL [158]	Efficiency and Scalability	Raft-based shard networks and Refined DAG-based main chain; Combinition of synchronous and asynchronous training.	High scalability; High FL efficiency; Eliminate the impact of stale models.	Limited resource challenges.
	IIoT	FL-Block [98]	Effective Fog Computing	Consider communication, consensus delays, and computation cost.	Derive the optimal block generation rate; Resistance to poisoning attacks.	Scalability challenges.
		PAFLM [69]	Effective ML for Edge Network	Compress the communications; Allow the node to join or quit; Data dual-weights correction.	Low communication costs; Low risk of privacy breach; High flexibility	Asynchronous optimization.
	IoV	Hierarchical BlockFL [16]	Effective Knowledge Sharing	Light-weight PoK consensus; Multi-leader and multi-player non-cooperative game.	Reduce the computation consumption; Suitable for the dynamic vehicular scenarios.	Challenges in deploying to real-world; Scalability challenges.
		BLockFL for Drones [93]	Energy Calculation	Quantify the probability of occurrence of forking events.	Pragmatic analyses of the expected energy consumption.	Performance optimization; Scalability challenges.
	IoHT	FL-BETS [56]	Task Scheduling	Execution on the distributed fog and cloud nodes; Consider both hard and soft constraint.	Minimize energy consumption and delay; Satisfy the deadlines of healthcare workloads.	Vulnerable to mobility fraud.
		Edge-empowered BlockFL [83]	Resource Management	Paillier encryption; Mixed integer nonlinear programming .	Maximize resource allocation; Minimize energy consumption and transmission delay.	Scalability challenges.

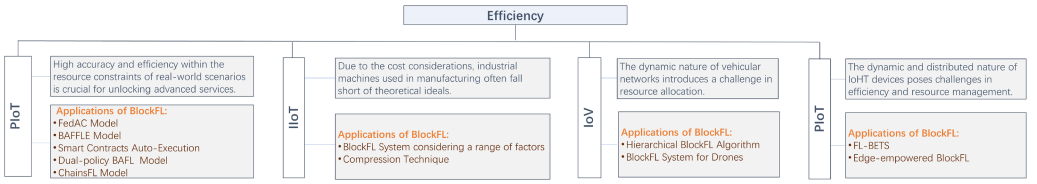

Fig. 9. Application of BlockFL: Efficiency. In PIoT, IIoT, and IoV, a variety of resource and economic factors may limit the implementation of BlockFL models. Therefore, it is crucial for application models, particularly those used in IIoT, to consider the balance and optimization between model performance and resources for efficiency.

real-time data processing for safer and more efficient transportation. Unlike its counterparts, BlockFL for IoV distinctly targets the swift allocation of resources amidst the dynamism of the network. This precision in IoV allows quick data handling and optimizes the decision-making process for safer and more efficient traffic systems [141]. In the realm of the IoHT, BlockFL is critical for managing the efficiency of distributed devices, ensuring swift data handling while conserving resources. The unique challenges of each domain are addressed through the collaborative model training in BlockFL, demonstrating the versatility and necessity of BlockFL in achieving efficiency and resource management capability in the IoT ecosystem.

7 DATA DIVERSITY OF BLOCKFL FOR IOT

The quality and quantity of training data are crucial factors determining the performance of any data-driven ML model, making the expansion of training data richness and diversity an essential issue that cannot be overlooked in model optimization, including BlockFL. This section emphasizes the efforts made by BlockFL to increase the diversity of training data for performance improvement.

These efforts include establishing an effective incentive mechanism to encourage more participants in model training, as well as addressing heterogeneous problems to enhance the capability.

7.1 PIoT

Accurate judgments and correct decisions rely on the large amount and diversity of data. So increasing the enthusiasm of devices for participation in the model training is an effective action for optimizing the accuracy of PIoT models, which requires the model to have a reasonable incentive mechanism.

The Blockchain has shown its ability to provide an effective incentive mechanism based on the performance of participants. More and more recent research works have been done to implement Blockchain into PIoT applications, especially with the FL that can safely combine massive devices to train a model. Without requiring honest participants, Short et al. [116] offer rewards on a Blockchain network according to the quality of contributions in FL. Martinez et al. [79] propose an in-depth workflow to record and reward the contributions of participants. In the work of Kim et al. [51], Blockchain is used to separate participating users as nodes and induce them to join the FL efficiently.

Besides, in order to attract more participants to join BlockFL to improve data diversity and model performance, more work is devoted to designing more reasonable and attractive incentive mechanisms. An effective incentive mechanism combining reputation management with smart contracts is proposed by Kang et al. [46] to motivate high-quality devices to join the model learning process. Zhao et al. [167] design an incentive mechanism to award participants with a novel normalization technique. Weng et al. [139] propose a DeepChain framework with a value-driven incentive mechanism to force the participants to train the model following the rules. Kumar et al. [55] also develop a value-driven incentive mechanism to encourage the positive actions of the contributors by introducing Blockchain technology via Ethereum.

Introducing repeated competition for FL is also feasible [125] as rational participants want to maximize their profits. Also, based on the hypothesis of rational man, Xuan et al. [146] propose a double-layer FL platform based on Blockchain with an incentive mechanism to ensure that rational workers can gain the maximum benefit by remaining honest. Desai et al. [24] create a general Blockchain-based FL framework to detect and punish attackers automatically. An honest trainer [11] is presented to gain fairly partitioned profit, rewarding contributions, and punishing the malicious.

7.2 IIoT

In the realm of IIoT, the diversity of training data plays a pivotal role in enhancing model performance, particularly in applications that demand high precision and reliability across various industrial sectors. The application of BlockFL emerges as a powerful solution, as it provides incentives for IIoT data owners, encouraging participation and thereby enriching the diversity and quantity of training data.

Recent research highlights the significance of incentive mechanisms in enhancing the diversity of training data for IIoT systems, addressing a critical challenge for the deployment of BlockFL. The blockchain and FL-based secure data-sharing scheme introduced in [144], incorporating model parameter validation and incentives into the consensus algorithm, directly addresses the challenge of data diversity by encouraging a broader participation base. Wang et al. have introduced an incentive mechanism for resource allocation in Blockchain-based FL, facilitating optimal participation by rewarding training and mining efforts [137]. The mechanism addresses the dual challenges of encouraging participation and managing resource constraints, thereby supporting the collection of diverse training data across IIoT devices.

The studies present innovative solutions that not only incentivize participation but also ensure the security and fairness of data contributions, crucial for the IIoT environment where data originates from a vast and varied array of sources. A Blockchain-based FL system, FGFL [30], focuses on a fair incentive mechanism, designed to attract high-quality workers and deter malicious actors by rewarding substantial and genuine contributions. Similarly, the Blockchain-enabled FL framework proposed by Witt et al. [140] aims at balancing contributions fairly, tackling the diversity challenge by ensuring that a wide range of participants are motivated to contribute their unique data. This framework uses Federated Knowledge Distillation with compressed soft-labels to promote honest participation through an incentive-compatible ecosystem.

7.3 IoV

In addressing the challenge of enhancing the diversity of training data within IoV, integrating BlockFL has proven to be a promising solution. The methodologies and frameworks developed in recent research focus on leveraging BlockFL to overcome data silos while promoting the diversity and quality of the data involved in training ML models.

For instance, frameworks like IoV-SFL [126] introduce secure and efficient data-sharing mechanisms, utilizing advanced encryption techniques and ML models to process diverse and heterogeneous data types while enhancing model performance. Fu et al. have incorporated a supervision game into a hierarchical Blockchain-supported FL architecture for autonomous driving, which demonstrates a significant stride in managing heterogeneous data within the IoV ecosystem [29].

Other studies emphasize the importance of incentive mechanisms to attract quality data contributions. Wang et al. have proposed BPFL, a Blockchain-based privacy-preserving FL scheme for IoV, enhancing Multi-Krum technology with homomorphic encryption [130]. Additionally, a reputation-based incentive mechanism is developed to encourage honest participation and data sharing. Similarly, BESIFL is introduced by Xu et al. [145], leveraging Blockchain for decentralization, integrating mechanisms for malicious node detection and incentive management, thereby improving FL performance by ensuring the participation of credible nodes. The paradigm underscores the importance of a secure and incentivized environment for handling diverse data and enhancing the overall efficacy of federated learning in IoV.

7.4 IoHT

When discussing how to enrich the diversity of training data, the heterogeneity of healthcare data is a significant issue in the context of IoHT due to the diversity of medical equipment and the complexity of application scenarios. Because of the variability in data format and characteristics across different medical institutions, it is impractical to enforce a standardized structure for all data in IoHT. For example, **Computed Tomography** (**CT**) images may vary in size, pixel density, and data format, so addressing the heterogeneity of healthcare data is an important consideration for developing effective IoHT solutions.

To address the challenge of heterogeneity in healthcare data, Kumar et al. [54] improve a Blockchain-empowered FL model with the data normalization technique. The authors utilize capsule-network-based segmentation and classification to detect patterns of COVID-19 from various types of lung CT scans. By leveraging the Blockchain and FL technologies, the presented BlockFL model caters to the particularities of the IoHT.

7.5 Conclusion

Table 8 provides an assessment of BlockFL applications across various IoT sectors, highlighting their role in managing data diversity. DeepChain [139] in PIoT incentivizes nodes for collaborative training, ensuring fairness but facing synchronization issues. DAM-SE [146] promotes honesty

Table 8. Comparison of BlockFL across IoT Domains for Data Diversity

	Domains	Model	Objective	Features	Advantages	Limitations
Data Diversity	PIoT	DeepChain [139]	Encouraging Participation	Incentive mechanism and transaction processing for collaborative training. Non-interactive zero-knowledge for auditability.	Confidentiality, auditability, and fairness; Compatibility and liveness properties.	Limited resource challenge; Efficiency issues.
		DAM-SE [146]	Encouraging Honesty	Double-layer aggregation based on security evaluation; Maximum benefit for remaining honest.	Low communication cost; Defend against poisoning attacks and free-rider attacks.	Scalability challenges; Efficiency issues.
		BlockFLA [24]	Punishment for Malicious	Automatically detect attacker with monetary penalties.	High generalizability; Successfully penalize attackers.	Limited resource challenges.
		Flchain [11]	Fair Incentive	Distributed trust and incentive among trainers; Reward for misbehavior detector and compensation for affected trainers.	Fair profit partition; Timely misbehavior detection and model purchase.	Time-consuming; Privacy risk.
	IIoT	Secured Data Sharing [144]	Encouraging Participation	PoC consensus mechanism; Adaptive differential privacy.	Encourage contribution of local privacy data and computing power; Identify poisoning attacks.	Scalability challenges.
		FGFL [30]	Fair Incentive	Reputation and contribution indicators; Punishment and elimination mechanisms.	Assess the trustworthiness and utilities in real time; Attack-resistance and profit-sharing.	Limited resource challenges.
	IoV	BPFL [130]	Encouraging Participation	Reputation-based incentive mechanism; Multi-Krum combined with holomorphic encryption.	Encourage honest participation; Achieve ciphertext-level model aggregation and model filtering.	Efficiency issues.
		BESIFL [145]	Encouraging Participation	Contribution-based incentive mechanism with a token-based reward scheme; Accuracy-based malicious node detection.	Improve performance through incentive and credible nodes selection; Enhance security.	Privacy risk; Efficiencyissues.
	IoHT	COVID-19 Detection [54]	Heterogeneous Data Processing	Data normalization technique; Capsule Network-based segmentation and classification.	High detection accuracy; Better generalization; Secure data sharing.	Limited resource challenges.

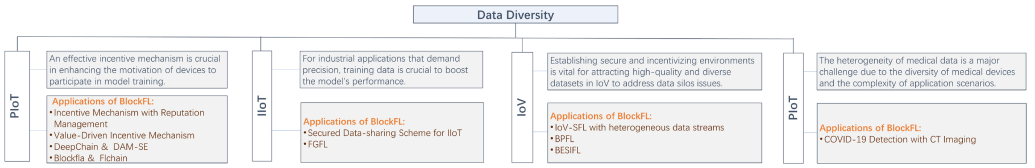

Fig. 10. Application of BlockFL: Data Diversity. In order to increase data diversity and optimize BlockFL, the PIoT model should consider incentives to encourage greater participation, while the IoHT domain presents a challenge with regard to heterogeneous problems that require more attention from the model. The importance of data diversity in IIoT and IoV is to help improve model accuracy and address data silos issues.

with a cost-effective aggregation model, balancing strong data privacy against scalability and delay challenges. Blockfla [24] combats malicious intent by building trust indices, trading off with potential system overhead. FleChain [11] ensures equitable participation yet deals with model convergence. In IIoT, Secured Data-sharing [144] and FGFL [30] focus on fair compensation and attack resilience, respectively, each facing overhead and resource scalability issues. For IoV, BPFL [130] and BESIFL [145] use reputation-based and contribution-based incentives to enhance participation and data security, confronting node failure and efficiency impacts. In IoHT, COVID-19 Detection [54] employs a Capsule Network for secure data sharing in medical contexts, with limitations in resource availability.

Figure 10 delineates a structured analysis of the impact of data diversity on the effectiveness of BlockFL across varied IoT domains. Within PIoT, the framework emphasizes the critical role of incentive mechanisms in model training processes. In the realm of IIoT, the precision and

performance of models are of utmost importance, thereby requiring the implementation of secured data-sharing schemes, maintaining data integrity, and improving operational efficiency. The IoV sector seeks to establish secure and incentivizing environments, aiming at attracting a rich variety of datasets and address the challenges of data silos. In the domain of IoHT, the focus shifts to tackling the heterogeneity of medical data, with sophisticated applications such as processing CT Imaging, developed to navigate the diversity of medical devices and the intricacies of healthcare application scenarios.

8 LESSON LEARNED AND OPEN CHALLENGES OF BLOCKFL FOR IOT

The combination of FL and Blockchain has demonstrated significant potential in advancing next-generation digital developments. Through theoretical analysis and related experiments, existing studies confirm the application value of integrating BlockFL technologies in various fields. But the works are limited and remain largely theoretical. The throughout review of the BlockFL in IoT reveals several essential challenges and unresolved issues when considering the implementation and development of BlockFL.

This section will highlight potential future research directions for BlockFL, exploring both general open issues faced across all application domains, as well as domain-specific challenges.

8.1 General Challenges of BlockFL in Different Application Scenarios

In the 5G/6G era, BlockFL is set to thrive due to unprecedented data speeds, lower latency, and higher reliability [106]. These advanced networks enhance real-time interactions between Blockchain nodes and FL participants, contributing to more efficient data exchange, model updating, and consensus. The increased data transmission speeds also aid in the quick synchronization of Blockchain ledgers and fast sharing of FL model updates, bolstering the scalability and efficiency of BlockFL systems. With the evolution of 5G and the advent of 6G technologies, however, BlockFL faces new challenges in maintaining efficiency and security. The ultra-low latency of these networks demands real-time data processing and decision-making in BlockFL systems [20]. For instance, autonomous driving requires millisecond-precise decision-making utilizing the low latency of these networks. Additionally, the higher data throughput of 5G/6G networks increases resource demands, necessitating more efficient BlockFL algorithms [152], especially in contexts like smart cities where vast sensor data needs to be managed without overwhelming network nodes.

As BlockFL navigates these technological advancements, it also encounters universal challenges in IoT scenarios, underscoring the need for tailored solutions in various applications. While each considered IoT scenario has its unique characteristics, they share foundational challenges in data security, privacy, resource limitation, scalability, and data diversity. All scenarios involve data collection, transmission, and processing, often with sensitive information, necessitating robust security and evolving privacy protection [9]. The limited computing power and energy resources of IoT devices pose scalability challenges as the IoT ecosystem expands. Moreover, data diversity in terms of device capabilities and communication protocols requires intelligent processing techniques for efficient BlockFL deployment [40]. These challenges vary significantly across scenarios. For example, IoHT involves health-related data requiring strict compliance with healthcare regulations [49], while IIoT might focus more on protecting industrial processes and proprietary information [78]. The degree of resource limitation and scalability requirements can differ. PIoT devices might be more constrained in terms of battery life and processing power [114], whereas IIoT settings might prioritize the scalability of solutions across vast industrial networks with varying computational capacities [142]. The type and level of heterogeneity can vary widely; IoV deals with mobility-related data and connectivity challenges unique to vehicular networks [84], while IIoT must accommodate a wide range of industrial equipment and operational technologies.

Table 9. Potential Synergies between BlockFL and Related Technologies

Technology	Description	Challenges Solved by Combining with BlockFL	Example	Features and Benefits
Cryptography	Mathematical algorithms for security and sensitive information protection.	Data Security and Privacy	PPFL Model [10]	Enhance a variant of the Paillier cryptosystem to implement homomorphic encryption.
			FDC Framework [150]	Leverages multiparty secure computation technologies to ensure data security.
			Fed-DFE Model [121]	Uses the interactive key generation algorithm to avoid collusion attack.
Anomaly Detection	Techniques to identify unusual patterns or outliers in data.	Data Security and Privacy, Reliability	Block Hunter Framework [149]	Based on cluster detection to automatically search for attacks and threat risks.
			Anomaly Detection [96]	Utilizes Blockchain to record the incremental updates of anomaly detection.
			CDW-FedAvg Algorithm[164]	Calculates the distance between positive and negative class data to detect failures and attacks.
Optimization	Methods for finding the best solution for a given problem and conditions.	Resource Limitation	Dual-policy BAFL Model [27]	Develops two complementary policies to control block-generation rate and adjust training rounds.
			FL-Block Scheme [98]	Considers delays, communication and computation cost to determine the optimal block generation rate.
			Disaster ResponseSystem [93]	Discusses the effect of the number of miners, computing power, transmission capacity, and channel dynamics.
Compression Technique	Techniques for reducing data size while maintaining integrity and usefulness.	Resource Limitation, Scalability	PAFLM [69]	Reduces communication costs without sacrificing performance.
			Decentralized FEL Model [44]	Replaces complete gradients with sparse but important gradients to reduce communication overhead.
Data Normalization	Techniques for transforming data into a standardized form.	Heterogeneity	Pathological Detection [54]	Deals with the data collected by different kinds of CT scanners effectively.

Table 9 summarizes potential technologies for future BlockFL development. In terms of security enhancement and privacy protection, the integration of encryption and secure computing technologies has been effective [10, 121, 150]. Combining BlockFL with various encryption algorithms and noise addition methods [154, 160] or multi-party security technologies can further enhance Blockchain-based FL models. Additionally, data processing techniques like compression [44, 69] and normalization [54], along with smart contracts [76] and sharding mechanisms [151, 165], are suggested to address resource limitations and data heterogeneity, enhancing the capabilities of BlockFL.

Furthermore, ongoing research is needed to delve deeper into combining Blockchain and FL. Current BlockFL models mainly employ Blockchain for aggregation in the FL process, with less emphasis on enhancing Blockchain through FL. Intermediate results in BlockFL, such as the quality of local models, could be utilized in the consensus calculations of Blockchain [70], thus reducing the costs of computational and communication resources. Exploring new consensus methods and smart contract technologies based on BlockFL presents promising avenues for further development. This research should also address issues typically associated with Blockchain, such as the collusion of the miners and the challenges of hybrid-Blockchain structures [134, 157].

8.2 Unique Challenges of BlockFL in Different Application Scenarios

The integration of BlockFL across different IoT applications presents unique challenges due to the distinct nature of each field. Table 10 summarizes these challenges and their solutions. In PIoT, the complexity arising from personalized smart services is addressed using transfer and split learning technologies to enhance personalization and privacy. IIoT leverages transfer learning to improve intelligent collaboration, boosting efficiency and cutting costs. For IoV, high latency is tackled through online and continuous learning technologies, enhancing safety and traffic flow. In IoHT, the focus is on handling sensitive medical data securely, utilizing consortium Blockchains and split

Table 10. Unique Challenges of BlockFL in Different Application Scenarios

Scenario	Unique Challenges	Reasons	Solutions	Key Insights
PIoT	Complex smart services	Personalized needs	Transfer learning technology; Split learning technology.	Enhances personalization; Adapts to user preferences; Preserves privacy.
IIoT	Complex intelligent collaboration	Automation	Transfer learning technology.	Improves multitask efficiency; Reduces costs; Shares knowledge across domains.
IoV	Long delay	Real-time changing traffic environments	Continuous learning technology.	Enables real-time adaptation; Optimizes traffic flows; Ensures safety and efficiency.
IoHT	Challenging identity management	Permission requirements for access to medical data	Consortium Blockchains; Split learning technology.	Restricts access; Secures medical data; Supports collaborative healthcare research.

learning for secure data handling and collaborative research. This table encapsulates the diverse challenges and innovative solutions tailored to the unique needs of different IoT scenarios.

In large-scale PIoT and IIoT, collaborative intelligence and meeting personalized needs have emerged as a new research direction. As existing studies have focused on optimizing a single task, the increasing demand for multitasking collaboration and cooperation requires a complex system to analyze and coordinate the relationship and connection of multitasking and multi-objective. To enable intelligent coordination, the models should explore transfer learning technology and other related novel technologies in combination with BlockFL models. In particular, the process of industrialization requires more consideration of the costs of large-scale implementation.

In IoV, ensuring the stability of the system in high-speed movement is a crucial research direction. A large number of vehicles in the IoV application scenarios are constantly moving at high speeds and changing positions in real time, which poses a considerable challenge to the stability and reliability of the network and connection. To address this issue, researchers can increase the calculation effectiveness, reduce model delay, and consider optimizing and innovating BlockFL models by imitating online learning algorithms. Moreover, future vehicles in 6G are expected to support cross-domain communication across the ground, underwater and air [33], so stability in combination with new devices and technologies, such as over-the-air computing, should also be taken into account [168].

In IoHT, permission and identity management of participants are critical challenges due to the high sensitivity of medical data. Consortium Blockchains are more suitable for implementation in IoHT, with the high professional knowledge required by participants to analyze and manage medical-related data. The involvement of medical organizations can make the management of IoHT models highly controllable and convenient, and multiple participation can improve the accuracy and other performance of IoHT models. Thus, researchers should explore how to incentivize participation in BlockFL while considering the problem of membership management.

8.3 Other Learning Framework as Solution for BlockFL

In addressing future research on BlockFL, it is imperative to broaden the scope to include various frameworks of distributed learning, such as split learning, transfer learning, and continuous learning. This expansion is crucial for offering a holistic view of the distributed learning landscape, enabling the identification of synergies and potential integrations that could further enhance the capabilities and applications of BlockFL across diverse IoT scenarios.

Integrating learning frameworks like Split Learning, Transfer Learning, and Continuous Learning with BlockFL offers the potential to leverage the strengths of both FL and Blockchain

technologies while addressing their respective weaknesses. By doing so, we can create a learning ecosystem that is robust against data privacy issues, adaptable to new data, and capable of continuous improvement without centralized data storage.

Split Learning is a distributed learning framework that divides a neural network model between client and server sides [105]. Clients compute with local data and send intermediate results to a server for further processing. This method, combined with BlockFL, enhances privacy and efficiency. Clients handle initial training stages and only transfer intermediate results to a Blockchain-based server, which aggregates them securely and updates the Blockchain ledger with the enhanced model. This integration with BlockFL offers scalable, privacy-preserving solutions in IoT environments, benefiting from the security and transparency of Blockchain.

Transfer Learning applies knowledge from one domain to solve problems in another and is particularly useful in PIoT and IIoT within BlockFL contexts [138]. By incorporating it into BlockFL, pre-trained models on Blockchain nodes can be refined by new participants using their data, thus reducing training time while maintaining privacy. This approach also facilitates cross-domain applications, allowing knowledge transfer from one IoT sector to another (e.g., from IoHT to IoV), accelerating intelligent system deployment across varied IoT ecosystems.

Continuous Learning focuses on systems that learn and evolve over time, accumulating and adapting to new data while retaining previous knowledge [90]. Incorporating this into the BlockFL framework could enhance adaptability. The approach involves regularly updating Blockchain models with insights from client data. Clients contribute to ongoing learning, facilitating continuous model evolution, which ensures data integrity and lineage for auditing purposes. In dynamic IoT settings, this enables BlockFL systems to adapt to new patterns and changes, maintaining relevance and effectiveness in applications such as IoV and IoHT, where continuous learning and updating are essential.

9 CONCLUSION AND FUTURE WORK

In this article, we have divided the different application scenarios for the conjunction of FL and Blockchain into four important IoT domains: PIoT, IIoT, IoV, and IoHT. We have introduced the status quo and current requirements in each application field and classified the different models according to the solved issues. In addition, we have summarized the common challenges in these areas, such as outstanding issues in privacy security, system scalability, and data heterogeneity, and provided several possible future research directions for different fields. The specific challenges encountered by BlockFL development in various application domains have been also highlighted, along with some recommendations for further investigation. Our research has shown that BlockFL, as a highly secure and efficient approach for distributed model training, offers superior performance compared to traditional FL in all IoT application domains thanks to its decentralized structure and transparency.

In our future work, we plan to do further research on optimizing the performance of existing models and improving the practicability of applications. Designing new types of Blockchain-based FL model with high privacy security and high accuracy is also a feasible direction for our follow-up works.

REFERENCES

[1] Satyabrata Aich, Nday Kabulo Sinai, Saurabh Kumar, Mohammed Ali, Yu Ran Choi, Moon-IL Joo, and Hee-Cheol Kim. 2021. Protecting personal healthcare record using blockchain and federated learning technologies. In *Proceedings of the 2021 23rd International Conference on Advanced Communication Technology*. IEEE, 109–112.

[2] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials* 17, 4 (2015), 2347–2376.

[3] Yasser Alharbi. 2022. A novel federated learning based lightweight sustainable IoT approach to identify abnormal traffic. *International Journal of Pervasive Computing and Communications* (2022).
[4] Aitizaz Ali, Bander Ali Saleh Al-Rimy, Ting Tin Tin, Saad Nasser Altamimi, Sultan Noman Qasem, and Faisal Saeed. 2023. Empowering precision medicine: Unlocking revolutionary insights through blockchain-enabled federated learning and electronic medical records. *Sensors* 23, 17 (2023), 7476.
[5] Mansoor Ali, Hadis Karimipour, and Muhammad Tariq. 2021. Integration of blockchain and federated learning for internet of things: Recent advances and future challenges. *Computers and Security* 108 (2021), 102355.
[6] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. 2018. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys and Tutorials* 21, 2 (2018), 1676–1717.
[7] Omar Ali, Ashraf Jaradat, Atik Kulakli, and Ahmed Abuhalimeh. 2021. A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* 9 (2021), 12730–12749.
[8] Yoshinori Aono, Takuya Hayashi, Lihua Wang, and Shiho Moriai. 2017. Privacy-preserving deep learning via additively homomorphic encryption. *IEEE Transactions on Information Forensics and Security* 13, 5 (2017), 1333–1345.
[9] Hany F. Atlam and Gary B. Wills. 2020. IoT security, privacy, safety and ethics. *Digital Twin Technologies and Smart Cities* (2020), 123–149.
[10] Sana Awan, Fengjun Li, Bo Luo, and Mei Liu. 2019. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2561–2563.
[11] Xianglin Bao, Cheng Su, Yan Xiong, Wenchao Huang, and Yifei Hu. 2019. 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*. IEEE, 151–159.
[12] Arjun Nitin Bhagoji, Supriyo Chakraborty, Prateek Mittal, and Seraphin Calo. 2019. Analyzing federated learning through an adversarial lens. In *Proceedings of the International Conference on Machine Learning*. PMLR, 634–643.
[13] Franziska Boenisch, Adam Dziedzic, Roei Schuster, Ali Shahin Shamsabadi, Ilia Shumailov, and Nicolas Papernot. 2023. When the curious abandon honesty: Federated learning is not private. In *Proceedings of the 2023 IEEE 8th European Symposium on Security and Privacy*. IEEE, 175–199.
[14] Jorge Castillo, Phillip Rieger, Hossein Fereidooni, Qian Chen, and Ahmad Sadeghi. 2023. Fledge: Ledger-based federated learning resilient to inference and backdoor attacks. In *Proceedings of the 39th Annual Computer Security Applications Conference*. 647–661.
[15] Miguel Castro and Barbara Liskov. 1999. Practical byzantine fault tolerance. In *Proceedings of the OsDI*. 173–186.
[16] Haoye Chai, Supeng Leng, Yijin Chen, and Ke Zhang. 2020. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems* 22, 7 (2020), 3975–3986.
[17] Hang Chen, Syed Ali Asif, Jihong Park, Chien-Chung Shen, and Mehdi Bennis. 2021. Robust blockchained federated learning with model validation and proof-of-stake inspired consensus. arXiv:2101.03300. Retrieved from https://arxiv.org/abs/2101.03300
[18] Jin-Hua Chen, Min-Rong Chen, Guo-Qiang Zeng, and Jia-Si Weng. 2021. BDFL: A byzantine-fault-tolerance decentralized federated learning method for autonomous vehicle. *IEEE Transactions on Vehicular Technology* 70, 9 (2021), 8639–8652.
[19] Qiuling Chen, Ayong Ye, Qiang Zhang, and Chuan Huang. 2023. A new edge perturbation mechanism for privacy-preserving data collection in IoT. *Chinese Journal of Electronics* 32, 3 (2023), 1–10.
[20] Wanshi Chen, Xingqin Lin, Juho Lee, Antti Toskala, Shu Sun, Carla Fabiana Chiasserini, and Lingjia Liu. 2023. 5G-advanced toward 6G: Past, present, and future. *IEEE Journal on Selected Areas in Communications* 41, 6 (2023), 1592–1619.
[21] JiuJun Cheng, JunLu Cheng, MengChu Zhou, FuQiang Liu, ShangCe Gao, and Cong Liu. 2015. Routing in internet of vehicles: A review. *IEEE Transactions on Intelligent Transportation Systems* 16, 5 (2015), 2339–2352.
[22] Marco Conoscenti, Antonio Vetro, and Juan Carlos De Martin. 2016. Blockchain for the internet of things: A systematic literature review. In *Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications*. IEEE, 1–6.
[23] Jonathan Cook, Sabih Ur Rehman, and M. Arif Khan. 2023. Security and privacy for low power IoT devices on 5G and beyond networks: Challenges and future directions. *IEEE Access* 11 (2023), 39295–39317.
[24] Harsh Bimal Desai, Mustafa Safa Ozdayi, and Murat Kantarcioglu. 2021. Blockfla: Accountable federated learning via hybrid blockchain architecture. In *Proceedings of the 11th ACM Conference on Data and Application Security and Privacy*. 101–112.
[25] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. 2017. Towards an optimized blockchain for IoT. In *Proceedings of the 2nd International Conference on Internet-of-Things Design and Implementation*. 173–178.

[26] Omar El Rifai, Maelle Biotteau, Xavier de Boissezon, Imen Megdiche, Franck Ravat, and Olivier Teste. 2020. Blockchain-based federated learning in medicine. In *Proceedings of the International Conference on Artificial Intelligence in Medicine*. Springer, 214–224.

[27] Lei Feng, Yiqi Zhao, Shaoyong Guo, Xuesong Qiu, Wenjing Li, and Peng Yu. 2021. BAFL: A blockchain-based asynchronous federated learning framework. *IEEE Transactions on Computers* 71, 5 (2021) 1092–1103.

[28] Luca Franceschini and Alberto Midali. 2020. Industrial IoT: A cost-benefit analysis of predictive maintenance service. (2020). Available: https://hdl.handle.net/10589/167108

[29] Yuchuan Fu, Changle Li, F. Richard Yu, Tom H. Luan, and Pincan Zhao. 2023. An incentive mechanism of incorporating supervision game for federated learning in autonomous driving. *IEEE Transactions on Intelligent Transportation Systems* 24, 12 (2023), 14800–14812.

[30] Liang Gao, Li Li, Yingwen Chen, ChengZhong Xu, and Ming Xu. 2022. FGFL: A blockchain-based fair incentive governor for federated learning. *Journal of Parallel and Distributed Computing* 163 (2022), 283–299.

[31] Robin C. Geyer, Tassilo Klein, and Moin Nabi. 2017. Differentially private federated learning: A client level perspective. arXiv:1409.0473. Retrieved from https://arxiv.org/abs/1701.00133

[32] Vinay Gugueoth, Sunitha Safavat, Sachin Shetty, and Danda Rawat. 2023. A review of IoT security and privacy using decentralized blockchain techniques. *Computer Science Review* 50 (2023), 100585.

[33] Hongzhi Guo, Xiaoyi Zhou, Jiajia Liu, and Yanning Zhang. 2022. Vehicular intelligence in 6G: Networking, communications, and computing. *Vehicular Communications* 33 (2022), 100399.

[34] Ankur Gupta, Purnendu Prabhat, and Bisma Gulzar. 2022. Personal-internet-of-things (PIoT): A vision for hyper-personalization delivered securely. In *Proceedings of the 2022 IEEE Delhi Section Conference*. IEEE, 1–6.

[35] Malka N. Halgamuge. 2022. Estimation of the success probability of a malicious attacker on blockchain-based edge network. *Computer Networks* 219 (2022), 109402.

[36] Yufei Han and Xiangliang Zhang. 2020. Robust federated learning via collaborative machine teaching. In *Proceedings of the AAAI Conference on Artificial Intelligence*. 4075–4082.

[37] Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz. 2017. Deep models under the GAN: Information leakage from collaborative deep learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 603–618.

[38] Shuyan Hu, Xiaojing Chen, Wei Ni, Ekram Hossain, and Xin Wang. 2021. Distributed machine learning for wireless communication networks: Techniques, architectures, and applications. *IEEE Communications Surveys and Tutorials* 23, 3 (2021), 1458–1493.

[39] Gaofeng Hua, Li Zhu, Jinsong Wu, Chunzi Shen, Linyan Zhou, and Qingqing Lin. 2020. Blockchain-based federated learning for intelligent control in heavy haul railway. *IEEE Access* 8 (2020), 176830–176839.

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

[41] Anik Islam, Ahmed Al Amin, and Soo Young Shin. 2022. FBI: A federated learning-based blockchain-embedded data accumulation scheme using drones for internet of things. *IEEE Wireless Communications Letters* 11, 5 (2022), 972–976. DOI: https://doi.org/10.1109/LWC.2022.3151873

[42] Wael Issa, Nour Moustafa, Benjamin Turnbull, Nasrin Sohrabi, and Zahir Tari. 2023. Blockchain-based federated learning for securing internet of things: A comprehensive survey. *Computing Surveys* 55, 9 (2023), 1–43.

[43] Abdul Rehman Javed, Muhammad Abul Hassan, Faisal Shahzad, Waqas Ahmed, Saurabh Singh, Thar Baker, and Thippa Reddy Gadekallu. 2022. Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey. *Sensors* 22, 12 (2022), 4394.

[44] Jiawen Kang, Zehui Xiong, Chunxiao Jiang, Yi Liu, Song Guo, Yang Zhang, Dusit Niyato, Cyril Leung, and Chunyan Miao. 2020. Scalable and communication-efficient decentralized federated edge learning with multi-blockchain framework. In *Proceedings of the International Conference on Blockchain and Trustworthy Systems*. Springer, 152–165.

[45] Jiawen Kang, Zehui Xiong, Xuandi Li, Yang Zhang, Dusit Niyato, Cyril Leung, and Chunyan Miao. 2021. Optimizing task assignment for reliable blockchain-empowered federated edge learning. *IEEE Transactions on Vehicular Technology* 70, 2 (2021), 1910–1923.

[46] Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. 2019. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal* 6, 6 (2019), 10700–10714.

[47] Jiawen Kang, Zehui Xiong, Dusit Niyato, Yuze Zou, Yang Zhang, and Mohsen Guizani. 2020. Reliable federated learning for mobile networks. *IEEE Wireless Communications* 27, 2 (2020), 72–80.

[48] Jiawen Kang, Rong Yu, Xumin Huang, Sabita Maharjan, Yan Zhang, and Ekram Hossain. 2017. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics* 13, 6 (2017), 3154–3164.

[49] Shwet Ketu and Pramod Kumar Mishra. 2021. Internet of healthcare things: A contemporary survey. *Journal of Network and Computer Applications* 192 (2021), 103179.
[50] Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. 2019. Blockchained on-device federated learning. *IEEE Communications Letters* 24, 6 (2019), 1279–1283.
[51] You Jun Kim and Choong Seon Hong. 2019. 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*. IEEE, 1–4.
[52] Michael R. Kosorok and Eric B. Laber. 2019. Precision Medicine. *Annual Review of Statistics and its Application* 6 (2019), 263–286.
[53] Kottilingam Kottursamy, Banupriya Sadayapillai, Ahmad Ali AlZubi, and Ali Kashif Bashir. 2023. A novel blockchain architecture with mutable block and immutable transactions for enhanced scalability. *Sustainable Energy Technologies and Assessments* 58 (2023), 103320.
[54] Rajesh Kumar, Abdullah Aman Khan, Jay Kumar, A Zakria, Noorbakhsh Amiri Golilarz, Simin Zhang, Yang Ting, Chengyu Zheng, and WenYong Wang. 2021. Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. *IEEE Sensors Journal* 21, 14 (2021), 16301–16314.
[55] Swaraj Kumar, Sandipan Dutta, Shaurya Chatturvedi, and MPS Bhatia. 2020. Strategies for enhancing training and privacy in blockchain enabled federated learning. In *Proceedings of the 2020 IEEE 6th International Conference on Multimedia Big Data*. IEEE, 333–340.
[56] Abdullah Lakhan, Mazin Abed Mohammed, Jan Nedoma, Radek Martinek, Prayag Tiwari, Ankit Vidyarthi, Ahmed Alkhayyat, and Weiyu Wang. 2022. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE Journal of Biomedical and Health Informatics* 27, 2 (2022), 664–672.
[57] Yixiao Lan, Yuan Liu, Boyang Li, and Chunyan Miao. 2021. Proof of learning (PoLe): Empowering machine learning with consensus building on blockchains. In *Proceedings of the AAAI Conference on Artificial Intelligence*. 16063–16066.
[58] Daoxing Li, Kai Xiao, Xiaohui Wang, Pengtian Guo, and Yong Chen. 2023. Towards sparse matrix operations: Graph database approach for power grid computation. *Global Energy Interconnection* 6, 1 (2023), 50–63.
[59] Jun Li, Yumeng Shao, Kang Wei, Ming Ding, Chuan Ma, Long Shi, Zhu Han, and H. Vincent Poor. 2021. Blockchain assisted decentralized federated learning (BLADE-FL): Performance analysis and resource allocation. *IEEE Transactions on Parallel and Distributed Systems* 33, 10 (2021), 2401–2415.
[60] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. 2020. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine* 37, 3 (2020), 50–60.
[61] Xiang Li, Kaixuan Huang, Wenhao Yang, Shusen Wang, and Zhihua Zhang. 2019. On the convergence of fedavg on non-iid data. *International Conference on Learning Representations*. Retrieved from https://arxiv.org/abs/1907.02189
[62] Zhuotao Lian, Weizheng Wang, Zhaoyang Han, and Chunhua Su. 2023. Blockchain-based personalized federated learning for internet of medical things. *IEEE Transactions on Sustainable Computing* 8, 4 (2023), 694–702.
[63] Chun-Cheng Lin, Ching-Tsorng Tsai, Yu-Liang Liu, Tsai-Ting Chang, and Yung-Sheng Chang. 2023. Security and privacy in 5G-IIoT smart factories: Novel approaches, trends, and challenges. *Mobile Networks and Applications* (2023), 1–16.
[64] Hong Liu, Shuaipeng Zhang, Pengfei Zhang, Xinqiang Zhou, Xuebin Shao, Geguang Pu, and Yan Zhang. 2021. Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing. *IEEE Transactions on Vehicular Technology* 70, 6 (2021), 6073–6084.
[65] Wei Liu, Li Chen, and Wenyi Zhang. 2022. Decentralized federated learning: Balancing communication and computing costs. *IEEE Transactions on Signal and Information Processing over Networks* 8 (2022), 131–143.
[66] Yinghui Liu, Youyang Qu, Chenhao Xu, Zhicheng Hao, and Bruce Gu. 2021. Blockchain-enabled asynchronous federated learning in edge computing. *Sensors* 21, 10 (2021), 3335.
[67] Yuan Liu, Wangyuan Yu, Zhengpeng Ai, Guangxia Xu, Liang Zhao, and Zhihong Tian. 2022. A blockchain-empowered federated learning in healthcare-based cyber physical systems. *IEEE Transactions on Network Science and Engineering* 10, 5 (2022), 2685–2696.
[68] Sin Kit Lo, Yue Liu, Qinghua Lu, Chen Wang, Xiwei Xu, Hye-Young Paik, and Liming Zhu. 2022. Toward trustworthy AI: Blockchain-based architecture design for accountability and fairness of federated learning systems. *IEEE Internet of Things Journal* 10, 4 (2022), 3276–3284.
[69] Xiaofeng Lu, Yuying Liao, Pietro Lio, and Pan Hui. 2020. Privacy-preserving asynchronous federated learning mechanism for edge network computing. *IEEE Access* 8 (2020), 48970–48981.
[70] Yunlong Lu, Xiaohong Huang, Yueyue Dai, Sabita Maharjan, and Yan Zhang. 2019. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics* 16, 6 (2019), 4177–4186.

[71] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. 2020. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology* 69, 4 (2020), 4298–4311.

[72] Shuaicheng Ma, Yang Cao, and Li Xiong. 2021. Transparent contribution evaluation for secure federated learning on blockchain. In *Proceedings of the 2021 IEEE 37th International Conference on Data Engineering Workshops*. IEEE, 88–91.

[73] Umer Majeed and Choong Seon Hong. 2019. FLchain: Federated learning via MEC-enabled blockchain network. In *Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium*. IEEE, 1–4.

[74] Imran Makhdoom, Mehran Abolhasan, Haider Abbas, and Wei Ni. 2019. Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications* 125 (2019), 251–279.

[75] Imran Makhdoom, Mehran Abolhasan, and Wei Ni. 2018. Blockchain for IoT: The challenges and a way forward. In *ICETE 2018-Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*.

[76] Imran Makhdoom, Ian Zhou, Mehran Abolhasan, Justin Lipman, and Wei Ni. 2019. PrivySharing: A blockchain-based framework for integrity and privacy-preserving data sharing in smart cities.. In *Proceedings of the ICETE*. 363–371.

[77] Moustafa Mamdouh, Ali Ismail Awad, Hesham F. A. Hamed, and Ashraf A. M. Khalaf. 2020. Outlook on security and privacy in IoHT: Key challenges and future vision. In *Proceedings of the International Conference on Artificial Intelligence and Computer Vision*. Springer, 721–730.

[78] Soujanya Mantravadi, Reto Schnyder, Charles Møller, and Thomas Ditlev Brunoe. 2020. Securing IT/OT links for low power IIoT devices: Design considerations for industry 4.0. *IEEE Access* 8 (2020), 200305–200321.

[79] Ismael Martinez, Sreya Francis, and Abdelhakim Senhaji Hafid. 2019. Record and reward federated learning contributions with blockchain. In *Proceedings of the 2019 International Conference on Cyber-enabled Distributed Computing and Knowledge Discovery*. IEEE, 50–57.

[80] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y. Arcas. 2017. Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the Artificial Intelligence and Statistics*. PMLR, 1273–1282.

[81] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* 7 (2019), 117134–117151.

[82] Wided Moulahi, Imen Jdey, Tarek Moulahi, Moatsum Alawida, and Abdulatif Alabdulatif. 2023. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Computers in Biology and Medicine* 167 (2023), 107630.

[83] Tasiu Muazu, Mao Yingchi, Abdullahi Uwaisu Muhammad, Muhammad Ibrahim, Omaji Samuel, and Prayag Tiwari. 2023. IoMT: A medical resource management system using edge empowered blockchain federated learning. *IEEE Transactions on Network and Service Management* 21, 1 (2023), 517–534.

[84] Salahadin Seid Musa, Marco Zennaro, Mulugeta Libsie, and Ermanno Pietrosemoli. 2022. Mobility-aware proactive edge caching optimization scheme in information-centric IoV networks. *Sensors* 22, 4 (2022), 1387.

[85] Mohamed Nahri, Azedine Boulmakoul, Lamia Karim, and Ahmed Lbath. 2018. IoV distributed architecture for real-time traffic data analytics. *Procedia Computer Science* 130 (2018), 480–487.

[86] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.

[87] Dinh C. Nguyen, Peng Cheng, Ming Ding, David Lopez-Perez, Pubudu N. Pathirana, Jun Li, Aruna Seneviratne, Yonghui Li, and H. Vincent Poor. 2020. Enabling AI in future wireless networks: A data life cycle perspective. *IEEE Communications Surveys and Tutorials* 23, 1 (2020), 553–595.

[88] Dinh C. Nguyen, Ming Ding, Quoc-Viet Pham, Pubudu N. Pathirana, Long Bao Le, Aruna Seneviratne, Jun Li, Dusit Niyato, and H. Vincent Poor. 2021. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal* 8, 16 (2021), 12806–12825.

[89] Takayuki Nishio and Ryo Yonetani. 2019. Client selection for federated learning with heterogeneous resources in mobile edge. In *Proceedings of the ICC 2019-2019 IEEE International Conference on Communications*. IEEE, 1–7.

[90] German I. Parisi, Ronald Kemker, Jose L. Part, Christopher Kanan, and Stefan Wermter. 2019. Continual lifelong learning with neural networks: A review. *Neural Networks* 113 (2019), 54–71.

[91] Jonathan Passerat-Palmbach, Tyler Farnan, Mike McCoy, Justin D. Harris, Sean T. Manion, Heather Leigh Flannery, and Bill Gleim. 2020. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In *Proceedings of the 2020 IEEE International Conference on Blockchain*. IEEE, 550–555.

[92] Zhe Peng, Jianliang Xu, Xiaowen Chu, Shang Gao, Yuan Yao, Rong Gu, and Yuzhe Tang. 2021. VFchain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Transactions on Network Science and Engineering* 9, 1 (2021), 173–186.

[93] Shiva Raj Pokhrel. 2020. Federated learning meets blockchain at 6G edge: A drone-assisted networking for disaster response. In *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*. 49–54.

[94] Shiva Raj Pokhrel and Jinho Choi. 2020. Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Transactions on Communications* 68, 8 (2020), 4734–4746.
[95] Dawid Połap, Gautam Srivastava, and Keping Yu. 2021. Agent architecture of an intelligent medical system based on federated learning and blockchain technology. *Journal of Information Security and Applications* 58 (2021), 102748.
[96] Davy Preuveneers, Vera Rimmer, Ilias Tsingenopoulos, Jan Spooren, Wouter Joosen, and Elisabeth Ilie-Zudor. 2018. Chained anomaly detection models for federated learning: An intrusion detection case study. *Applied Sciences* 8, 12 (2018), 2663.
[97] Attia Qammar, Ahmad Karim, Huansheng Ning, and Jianguo Ding. 2023. Securing federated learning with blockchain: A systematic literature review. *Artificial Intelligence Review* 56, 5 (2023), 3951–3985.
[98] Youyang Qu, Longxiang Gao, Tom H. Luan, Yong Xiang, Shui Yu, Bai Li, and Gavin Zheng. 2020. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal* 7, 6 (2020), 5171–5183.
[99] Youyang Qu, Shiva Raj Pokhrel, Sahil Garg, Longxiang Gao, and Yong Xiang. 2020. A blockchained federated learning framework for cognitive computing in industry 4.0 networks. *IEEE Transactions on Industrial Informatics* 17, 4 (2020), 2964–2973.
[100] Youyang Qu, Md Palash Uddin, Chenquan Gan, Yong Xiang, Longxiang Gao, and John Yearwood. 2022. Blockchain-enabled federated learning: A survey. *Computing Surveys* 55, 4 (2022), 1–35.
[101] Mohamed Abdur Rahman, M. Shamim Hossain, Mohammad Saiful Islam, Nabil A. Alrajeh, and Ghulam Muhammad. 2020. Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. *Ieee Access* 8 (2020), 205071–205087.
[102] Paritosh Ramanan and Kiyoshi Nakayama. 2020. Baffle: Blockchain based aggregator free federated learning. In *Proceedings of the 2020 IEEE International Conference on Blockchain*. IEEE, 72–81.
[103] Amirhossein Reisizadeh, Aryan Mokhtari, Hamed Hassani, Ali Jadbabaie, and Ramtin Pedarsani. 2020. Fedpaq: A communication-efficient federated learning method with periodic averaging and quantization. In *Proceedings of the International Conference on Artificial Intelligence and Statistics*. PMLR, 2021–2031.
[104] Joel J. P. C. Rodrigues, Dante Borges De Rezende Segundo, Heres Arantes Junqueira, Murilo Henrique Sabino, Rafael Maciel Prince, Jalal Al-Muhtadi, and Victor Hugo C. De Albuquerque. 2018. Enabling technologies for the internet of health things. *Ieee Access* 6 (2018), 13129–13141.
[105] Jihyeon Ryu, Dongho Won, and Youngsook Lee. 2021. A study of split learning model to protect privacy. *Convergence Security Journal* 21, 3 (2021), 49–56.
[106] Adeeb Salh, Lukman Audah, Nor Shahida Mohd Shah, Abdulraqeb Alhammadi, Qazwan Abdullah, Yun Hee Kim, Samir Ahmed Al-Gailani, Shipun A. Hamzah, Bashar Ali F. Esmail, and Akram A. Almohammedi. 2021. A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems. *IEEE Access* 9 (2021), 55098–55131.
[107] Omaji Samuel, Akogwu Blessing Omojo, Abdulkarim Musa Onuja, Yunisa Sunday, Prayag Tiwari, Deepak Gupta, Ghulam Hafeez, Adamu Sani Yahaya, Oluwaseun Jumoke Fatoba, and Shahab Shamshirband. 2022. IoMT: A COVID-19 healthcare system driven by federated learning and blockchain. *IEEE Journal of Biomedical and Health Informatics* 27, 2 (2022), 823–834.
[108] Najam U. Saqib, Saif U. R. Malik, Adeel Anjum, Madiha Haider Syed, Syed Atif Moqurrab, Gautam Srivastava, and Jerry Chun-Wei Lin. 2023. Preserving privacy in the internet of vehicles (IoV): A novel group leader-based shadowing scheme using blockchain. *IEEE Internet of Things Journal* 10, 24 (2023), 21421–21430.
[109] Deepti Saraswat, Ashwin Verma, Pronaya Bhattacharya, Sudeep Tanwar, Gulshan Sharma, Pitshou N. Bokoro, and Ravi Sharma. 2022. Blockchain-based Federated Learning in UAVs Beyond 5G Networks: A Solution Taxonomy and Future Directions. *IEEE Access* 10 (2022), 33154–33182. DOI: https://doi.org/10.1109/ACCESS.2022.3161132
[110] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications* 149 (2020), 102481.
[111] Byoungjin Seok, Jinseong Park, and Jong Hyuk Park. 2019. A lightweight hash-based blockchain architecture for industrial IoT. *Applied Sciences* 9, 18 (2019), 3740.
[112] Sreenivas Sudarshan Seshadri, David Rodriguez, Mukunda Subedi, Kim-Kwang Raymond Choo, Sara Ahmed, Qian Chen, and Junghee Lee. 2020. Iotcop: A blockchain-based monitoring framework for detection and isolation of malicious devices in internet-of-things systems. *IEEE Internet of Things Journal* 8, 5 (2020), 3346–3359.
[113] Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, and Simon Duquennoy. 2017. Towards blockchain-based auditable storage and sharing of IoT data. In *Proceedings of the 2017 on Cloud Computing Security Workshop*. 45–50.
[114] Syed Waqas Haider Shah, Adnan Noor Mian, Adnan Aijaz, Junaid Qadir, and Jon Crowcroft. 2021. Energy-efficient MAC for cellular IoT: State-of-the-art, challenges, and standardization. *IEEE Transactions on Green Communications and Networking* 5, 2 (2021), 587–599.

[115] Meng Shen, Huan Wang, Bin Zhang, Liehuang Zhu, Ke Xu, Qi Li, and Xiaojiang Du. 2020. Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing. *IEEE Internet of Things Journal* 8, 4 (2020), 2265–2275.

[116] Andrew Ronald Short, Helen C. Leligou, Michael Papoutsidakis, and Efstathios Theocharis. 2020. Using blockchain technologies to improve security in federated learning systems. In *Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference*. IEEE, 1183–1188.

[117] Saurabh Singh, Shailendra Rathore, Osama Alfarraj, Amr Tolba, and Byungun Yoon. 2022. A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology. *Future Generation Computer Systems* 129 (2022), 380–388.

[118] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. 2018. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics* 14, 11 (2018), 4724–4734.

[119] Ekta Soni and Khyati Chopra. 2023. IoHT: Healthcare with the internet of things. In *Proceedings of the IoT and Cloud Computing-based Healthcare Information Systems*. Apple Academic Press, 65–82.

[120] Yuwei Sun, Hiroshi Esaki, and Hideya Ochiai. 2020. Blockchain-based federated learning against end-point adversarial data corruption. In *Proceedings of the 2020 19th IEEE International Conference on Machine Learning and Applications*. IEEE, 729–734.

[121] Zhe Sun, Jiyuan Feng, Lihua Yin, Zixu Zhang, Ran Li, Yu Hu, and Chongning Na. 2022. Fed-DFE: A decentralized function encryption-based privacy-preserving scheme for federated learning. *CMC-Computers Materials and Continua* 71, 1 (2022), 1867–1886.

[122] Nick Szabo. 1997. Formalizing and securing relationships on public networks. *First Monday* 2, 9 (1997).

[123] Mohammad Hossein Tabatabaei, Roman Vitenberg, and Narasimha Raghavan Veeraragavan. 2023. Understanding blockchain: Definitions, architecture, design, and system comparison. *Computer Science Review* 50 (2023), 100575.

[124] Soo Fun Tan and Azman Samsudin. 2021. Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (IIoT): A survey. *Sensors* 21, 19 (2021), 6647.

[125] Kentaroh Toyoda and Allan N. Zhang. 2019. Mechanism design for an incentive-aware blockchain-enabled federated learning platform. In *Proceedings of the 2019 IEEE International Conference on Big Data*. IEEE, 395–403.

[126] Irshad Ullah, Xiaoheng Deng, Xinjun Pei, Husnain Mushtaq, and Muhammad Uzair. 2023. IoV-SFL: A blockchain-based federated learning framework for secure and efficient data sharing in the internet of vehicles. (2023). DOI : https://doi.org/10.21203/rs.3.rs-3648280/v1

[127] Muhammad Habib ur Rehman, Khaled Salah, Ernesto Damiani, and Davor Svetinovic. 2020. Towards blockchain-based reputation-aware federated learning. In *Proceedings of the IEEE Infocom 2020-IEEE Conference on Computer Communications Workshops*. IEEE, 183–188.

[128] Omar Abdel Wahab, Azzam Mourad, Hadi Otrok, and Tarik Taleb. 2021. Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. *IEEE Communications Surveys and Tutorials* 23, 2 (2021), 1342–1397.

[129] Hongyi Wang, Mikhail Yurochkin, Yuekai Sun, Dimitris Papailiopoulos, and Yasaman Khazaeni. 2020. Federated learning with matched averaging. *International Conference on Learning Representations*. Retrieved from https://arxiv.org/abs/2002.06440

[130] Naiyu Wang, Wenti Yang, Xiaodong Wang, Longfei Wu, Zhitao Guan, Xiaojiang Du, and Mohsen Guizani. 2022. A blockchain based privacy-preserving federated learning scheme for internet of vehicles. *Digital Communications and Networks* 10, 1 (2022), 126–134.

[131] Shufen Wang. 2019. BlockFedML: Blockchained federated machine learning systems. In *Proceedings of the 2019 International Conference on Intelligent Computing, Automation and Systems*. IEEE, 751–756.

[132] Xu Wang, Wei Ni, Xuan Zha, Guangsheng Yu, Ren Ping Liu, Nektarios Georgalas, and Andrew Reeves. 2021. Capacity analysis of public blockchain. *Computer Communications* 177 (2021), 112–124.

[133] Xu Wang, Guangsheng Yu, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Kangfeng Zheng, and Xinxin Niu. 2019. Capacity of blockchain based internet-of-things: Testbed and analysis. *Internet of Things* 8 (2019), 100109.

[134] Xu Wang, Ping Yu, Guangsheng Yu, Xuan Zha, Wei Ni, Ren Ping Liu, and Y. Jay Guo. 2019. A high-performance hybrid blockchain system for traceable IoT applications. In *Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings 13*. Springer, 721–728.

[135] Xu Wang, Xuan Zha, Guangsheng Yu, Wei Ni, and Ren Ping Liu. 2020. Blockchain for internet of things. In *Proceedings of the Blockchains for Network Security: Principles, Technologies and Applications*. The Institution of Engineering and Technology.

[136] Yuntao Wang, Haixia Peng, Zhou Su, Tom H. Luan, Abderrahim Benslimane, and Yuan Wu. 2022. A platform-free proof of federated learning consensus mechanism for sustainable blockchains. *IEEE Journal on Selected Areas in Communications* 40, 12 (2022), 3305–3324.

[137] Zhilin Wang, Qin Hu, Ruinian Li, Minghui Xu, and Zehui Xiong. 2023. Incentive mechanism design for joint resource allocation in blockchain-based federated learning. *IEEE Transactions on Parallel and Distributed Systems* 34, 5 (2023), 1536–1547.

[138] Karl Weiss, Taghi M Khoshgoftaar, and DingDing Wang. 2016. A survey of transfer learning. *Journal of Big Data* 3, 1 (2016), 1–40.

[139] Jiasi Weng, Jian Weng, Jilian Zhang, Ming Li, Yue Zhang, and Weiqi Luo. 2019. Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing* 18, 5 (2019), 2438–2455.

[140] Leon Witt, Usama Zafar, KuoYeh Shen, Felix Sattler, Dan Li, Songtao Wang, and Wojciech Samek. 2023. Decentralized and incentivized federated learning: A blockchain-enabled framework utilising compressed soft-labels and peer consistency. *IEEE Transactions on Services Computing* (2023), 1–16.

[141] Lang Wu, Weijian Ruan, Jinhui Hu, and Yaobin He. 2023. A survey on blockchain-based federated learning. *Future Internet* 15, 12 (2023), 400.

[142] Yulei Wu, Hong-Ning Dai, and Hao Wang. 2020. Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal* 8, 4 (2020), 2300–2317.

[143] Guowen Xu, Hongwei Li, Sen Liu, Kan Yang, and Xiaodong Lin. 2019. Verifynet: Secure and verifiable federated learning. *IEEE Transactions on Information Forensics and Security* 15 (2019), 911–926.

[144] Guangxia Xu, Zhaojian Zhou, Jingnan Dong, Lejun Zhang, and Xiaoling Song. 2023. A blockchain-based federated learning scheme for data sharing in industrial internet of things. *IEEE Internet of Things Journal* 10, 24 (2023), 21467–21478.

[145] Yajing Xu, Zhihui Lu, Keke Gai, Qiang Duan, Junxiong Lin, Jie Wu, and Kim-Kwang Raymond Choo. 2021. BESIFL: Blockchain-empowered secure and incentive federated learning paradigm in IoT. *IEEE Internet of Things Journal* 10, 8 (2021), 6561–6573.

[146] Shichang Xuan, Ming Jin, Xin Li, Zhaoyuan Yao, Wu Yang, and Dapeng Man. 2021. DAM-SE: A blockchain-based optimized solution for the counterattacks in the internet of federated learning systems. *Security and Communication Networks* 2021 (2021), 1–14.

[147] Zhanpeng Yang, Yuanming Shi, Yong Zhou, Zixin Wang, and Kai Yang. 2022. Trustworthy federated learning via blockchain. *IEEE Internet of Things Journal* 10, 1 (2022), 92–109.

[148] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, and Victor C. M. Leung. 2018. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal* 6, 2 (2018), 1495–1505.

[149] Abbas Yazdinejad, Ali Dehghantanha, Reza M. Parizi, Mohammad Hammoudeh, Hadis Karimipour, and Gautam Srivastava. 2022. Block hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks. *IEEE Transactions on Industrial Informatics* 18, 11 (2022), 8356–8366.

[150] Bo Yin, Hao Yin, Yulei Wu, and Zexun Jiang. 2020. FDC: A secure federated deep learning mechanism for data collaborations in the internet of things. *IEEE Internet of Things Journal* 7, 7 (2020), 6348–6359.

[151] Guangsheng Yu, Xu Wang, Kan Yu, Wei Ni, J. Andrew Zhang, and Ren Ping Liu. 2020. Survey: Sharding in blockchains. *IEEE Access* 8 (2020), 14155–14181.

[152] Guangsheng Yu, Xu Wang, Caijun Sun, Qin Wang, Ping Yu, Wei Ni, and Ren Ping Liu. 2023. Ironforge: An open, secure, fair, decentralized federated learning. *IEEE Transactions on Neural Networks and Learning Systems* (2023), 1–15.

[153] Guangsheng Yu, Xu Wang, Kan Yu, Wei Ni, J. Andrew Zhang, and Ren Ping Liu. 2020. Blockchains for network security: Principles, technologies and applications. *Institution of Engineering and Technology*.

[154] Guangsheng Yu, Xu Wang, Ping Yu, Caijun Sun, Wei Ni, and Ren Ping Liu. 2022. Dataset obfuscation: Its applications to and impacts on edge machine learning. arXiv:2208.03909. Retrieved from https://arxiv.org/abs/2208.03909

[155] Guangsheng Yu, Xuan Zha, Xu Wang, Wei Ni, Kan Yu, J. Andrew Zhang, and Ren Ping Liu. 2020. A unified analytical model for proof-of-x schemes. *Computers and Security* 96 (2020), 101934.

[156] Guangsheng Yu, Xuan Zha, Xu Wang, Wei Ni, Kan Yu, Ping Yu, J. Andrew Zhang, Ren Ping Liu, and Y. Jay Guo. 2020. Enabling attribute revocation for fine-grained access control in blockchain-IoT systems. *IEEE Transactions on Engineering Management* 67, 4 (2020), 1213–1230.

[157] Guangsheng Yu, Litianyi Zhang, Xu Wang, Kan Yu, Wei Ni, J. Andrew Zhang, and Ren Ping Liu. 2021. A novel dual-blockchained structure for contract-theoretic LoRa-based information systems. *Information Processing and Management* 58, 3 (2021), 102492.

[158] Shuo Yuan, Bin Cao, Mugen Peng, and Yaohua Sun. 2021. ChainsFL: Blockchain-driven federated learning from design to realization. In *Proceedings of the 2021 IEEE Wireless Communications and Networking Conference*. IEEE, 1–6.

[159] Shuo Yuan, Bin Cao, Yao Sun, Zhiguo Wan, and Mugen Peng. 2024. Secure and efficient federated learning through layering and sharding blockchain. *IEEE Transactions on Network Science and Engineering* 11, 3 (2024), 3120–3134.

[160] Xin Yuan, Wei Ni, Ming Ding, Kang Wei, Jun Li, and H. Vincent Poor. 2023. Amplitude-varying perturbation for balancing privacy and utility in federated learning. *IEEE Transactions on Information Forensics and Security* 18 (2023), 1884–1897.

[161] Umar Zaman, Imran, Faisal Mehmood, Naeem Iqbal, Jungsuk Kim, and Muhammad Ibrahim. 2022. Towards secure and intelligent internet of health things: A survey of enabling technologies and applications. *Electronics* 11, 12 (2022), 1893.

[162] Xuan Zha, Xu Wang, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu, and Kangfeng Zheng. 2017. Analytic model on data security in VANETs. In *Proceedings of the 2017 17th International Symposium on Communications and Information Technologies*. IEEE, 1–6.

[163] Ke Zhang, Yongxu Zhu, Sabita Maharjan, and Yan Zhang. 2019. Edge intelligence and blockchain empowered 5G beyond for the industrial internet of things. *IEEE Network* 33, 5 (2019), 12–19.

[164] Weishan Zhang, Qinghua Lu, Qiuyu Yu, Zhaotong Li, Yue Liu, Sin Kit Lo, Shiping Chen, Xiwei Xu, and Liming Zhu. 2020. Blockchain-based federated learning for device failure detection in industrial IoT. *IEEE Internet of Things Journal* 8, 7 (2020), 5926–5937.

[165] Zixu Zhang, Xu Wang, Guangsheng Yu, Wei Ni, Ren Ping Liu, Nektarios Georgalas, and Andrew Reeves. 2022. A community detection-based blockchain sharding scheme. In *Blockchain–ICBC 2022: 5th International Conference, Held as part of the Services Conference Federation, SCF 2022, Honolulu, HI, USA, December 10–14, 2022, Proceedings*. Springer, 78–91.

[166] Lingchen Zhao, Qian Wang, Qin Zou, Yan Zhang, and Yanjiao Chen. 2019. Privacy-preserving collaborative deep learning with unreliable participants. *IEEE Transactions on Information Forensics and Security* 15 (2019), 1486–1500.

[167] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. 2020. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet of Things Journal* 8, 3 (2020), 1817–1829.

[168] Jingheng Zheng, Hui Tian, Wanli Ni, Wei Ni, and Ping Zhang. 2022. Balancing accuracy and integrity for reconfigurable intelligent surface-aided over-the-air federated learning. *IEEE Transactions on Wireless Communications* 21, 12 (2022), 10964–10980.

[169] Juncen Zhu, Jiannong Cao, Divya Saxena, Shan Jiang, and Houda Ferradi. 2023. Blockchain-empowered federated learning: Challenges, solutions, and future directions. *Computing Surveys* 55, 11 (2023), 1–31.

Received 18 April 2023; revised 13 March 2024; accepted 9 April 2024