Journal on
Internet of Things

Tech Science Press

https://doi.org/10.32604/jiot.2026.073962

REVIEW

From Trust to Efficiency: Challenges, Optimizations, and the Hyper-Learning Framework for IoT Ecosystems

Priyanka Halder and Gopikrishnan Sundaram*

School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India

*Corresponding Author: Gopikrishnan Sundaram. Email: gopikrishnan.s@vitap.ac.in

Received: 29 September 2025; Accepted: 30 January 2026; Published: 29 May 2026

ABSTRACT: The need for intelligent learning frameworks that can function under stringent limitations relating to privacy, energy, scalability, and trust has increased due to the Internet of Things' (IoT) and the Internet of Artificial Things' (IoAT) explosive expansion. Federated Learning (FL), which allows collaborative model training without sharing raw data, has become a potential approach. Non-IID data delivery, inconsistent client engagement, vulnerability to poisoning assaults, and low resource knowledge are among of the significant obstacles that FL alone must overcome. Blockchain integration adds extra overhead in terms of latency, energy consumption, and scalability, but it has been suggested to address trust, auditability, and integrity through decentralised validation and immutable logging. DRL, on the other hand, has demonstrated a great deal of promise for adaptive decision-making, but it is frequently researched separately from blockchain and FL systems. With an emphasis on the function of DRL in enhancing system performance, this survey offers a thorough and organised analysis of blockchain-enabled federated learning for IoT and IoAT ecosystems. We methodically examine current consensus protocols, DRL-driven optimisation techniques, blockchain-based security measures, and distributed learning architectures. In a variety of IoT situations, such as healthcare, industrial IoT, UAV networks, and smart cities, important issues pertaining to energy efficiency, communication overhead, incentive mechanisms, block size management, and participant trust are critically explored. Additionally, a comparison of privacy-preserving methods like Homomorphic Encryption and Differential Privacy is given, emphasising their trade-offs and appropriateness for contexts with limited resources. This survey presents a Hyper-Learning Framework that tightly integrates FL, blockchain, and DRL inside a single control loop based on the gaps found. The system seeks to maintain efficiency and privacy while facilitating scaled learning, secure collaboration, and adaptive resource management. In order to steer the creation of reliable, sustainable, and intelligent IoT learning systems, open research directions and upcoming difficulties are finally discussed.

KEYWORDS: Federated learning (FL); blockchain; internet of artificial things (IoAT); distributed computing; deep reinforcement learning (DRL); security

1 Introduction

With billions of connected devices in healthcare, business, transportation, and smart cities, the Internet of Things (IoT) has created new demands for safe and private intelligence. This is made possible by Federated Learning (FL), which allows for remote model training without the need to share raw data. However, FL still has issues with non-IID data, device heterogeneity, inconsistent participation, and threats like poisoning and inference leakage. Blockchain-FL systems still have issues with scalability, latency, high energy consumption, and privacy related to traceability, despite the introduction of blockchain to improve trust and auditability through immutable logging and decentralised validation. Surveys that are now available usually look at FL,

blockchain, or DRL separately, providing little information about how these technologies can work together in IoAT. This paper offers an integrated Hyper-Learning perspective that combines deep reinforcement learning (DRL), blockchain, and FL to close this gap. The study explains how they interact, emphasizes DRL's function in adaptive optimisation, and lists unresolved issues including cross-domain interoperability, energy-aware consensus, and incentive design.

In light of these opportunities and gaps, a structured examination of how federated learning and blockchain can be combined within IoT and IoAT ecosystems is essential. This review fulfills that need by surveying distributed learning architectures, assessing blockchain's contributions to strengthening FL, and outlining optimization methods based on deep reinforcement learning. The work is driven by the urgent requirement to design learning systems for IoT that are secure, scalable, and energy efficient while operating under tight resource and privacy constraints.

This review is guided by the following research questions (RQs):

- **RQ1:** What are the existing frameworks and methodologies for distributed and federated learning in IoT/IoAT environments?
- **RQ2:** How can blockchain enhance the security, trust, and reliability of federated learning in IoT?
- **RQ3:** What role can deep reinforcement learning play in optimizing blockchain-enabled federated learning?
- **RQ4:** What are the key challenges, open issues, and future research directions in this domain?

The remainder of this paper is organized as follows: Section 2 presents a survey of distributed learning frameworks for IoT. Section 3 discusses blockchain-enabled federated learning in IoT. Section 4 reviews consensus mechanisms and resource optimization strategies. Section 5 explores deep reinforcement learning for FL optimization. Section 6 highlights research gaps and open challenges, while Section 7 outlines future directions. Finally, Section 7 concludes the paper with closing remarks.

2 Survey of Distributed Learning in IoT

Federated learning, a form of distributed learning, provides a promising solution for running ML on IoT systems while reducing privacy risks and coping with resource constraints. FL enables local training with aggregated updates, protecting sensitive information and matching use cases where logs are scattered among diverse tools and platforms [1]. This approach enables edge-based learning so sensitive user data stays on devices rather than being sent to the cloud, only model updates are exchanged between smart endpoints and the central server. Embedding FL into IoT therefore brings both benefits and limitations although it improves privacy compared with centralized ML, privacy risks persist. For example, adversaries can mount inference attacks on the shared model updates to recover private information [2]. To address these problems, academics have introduced multiple methods. FedADA for instance, applies adversarially guided federated training to harmonize distributional differences among diverse data origins, thereby boosting performance on novel target domains. Complementary approaches use knowledge-transfer within FL to mitigate the effects of heterogeneity and outdated gradients in low-resource distributed environments [3].

Fig. 1 illustrates the proposed IoAT architecture combining federated learning, blockchain, and DRL. Edge devices perform privacy-preserving local training and send compressed updates, while a DRL-based controller enables energy-aware aggregation. The blockchain layer ensures secure logging, trust, and auditability, and the global model is redistributed for continuous learning.

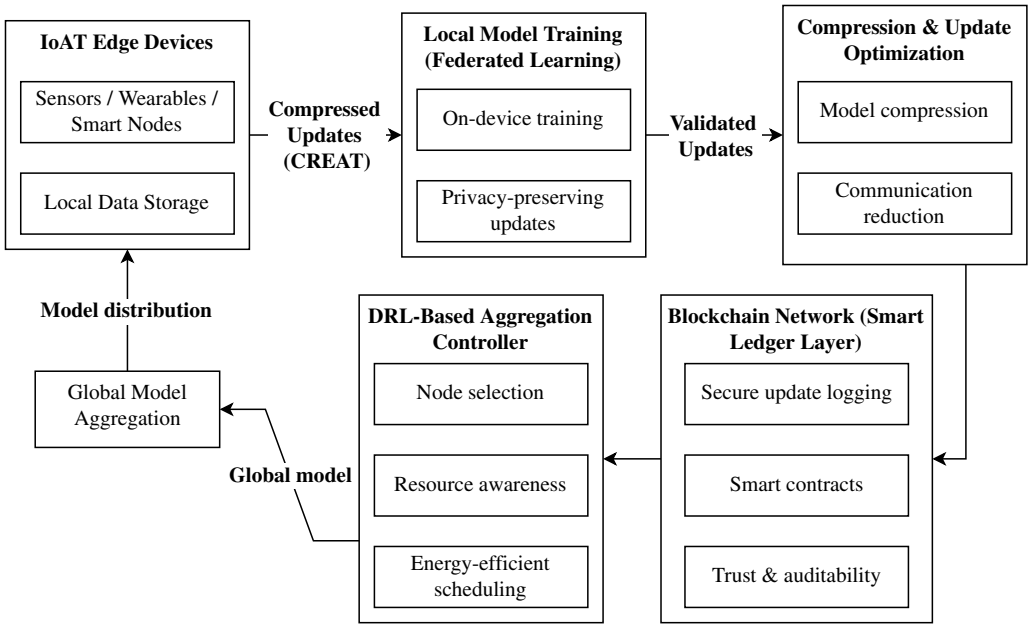

Figure 1: IoT flowchart.

Applications of FL within IoT extend to areas like healthcare services, advanced mobility, drone technology, smart urban infrastructures, and next-generation industrial systems [4]. The strength of FL lies in delivering smart services without compromising privacy, yet its adoption within IoT is challenged by hardware limitations. Autonomous machines, drones, and lightweight computing devices typically face issues such as low computational ability, weak connectivity, restricted battery life, and constrained storage [5]. Researchers have explored several approaches to address these challenges. One such method in vehicular IoT involves edge assisted networking and communication strategies, where vehicles operate as FL clients to optimize local models also serving as relay nodes for data exchange [6]. One promising option is multilayer blockchain integrated cloud edge orchestrated FL (HBCE-FL), delivering decentralized and resilient IoT data evaluation alongside precise, fine-grained privacy safeguards [7]. To conclude, FL provides a viable pathway for secure and efficient learning in IoT environments. However, its adoption is limited by resource bottlenecks, privacy concerns, and diverse device settings. Promising research avenues include better communication protocols, methods for handling non-IID data, and improved privacy safeguards [8]. As shown in Table 1, traditional FL provides basic privacy protection but struggles with threats, scalability issues, and the absence of incentive mechanisms. Blockchain integration addresses many of these shortcomings by enabling stronger accountability, though at the cost of energy and latency. The trend reflects an evolution toward Hyper-learning, designed for secure, scalable, and resource-aware learning.

Table 1: Comparison of federated learning frameworks and their characteristics.

S. No.	Aspect	Traditional FL	Blockchain-Based FL	Features Required
1.	Data Privacy	Medium (no raw data sharing, but vulnerable to inference attacks)	High (immutability, tamper resistance, smart contracts)	Very High (privacy-preserving with DP, SMPC, homomorphic encryption, and adaptive DRL scheduling)

(Continued)

Table 1 (continued)

S. No.	Aspect	Traditional FL	Blockchain-Based FL	Features Required
2.	Security Threats	Susceptible to poisoning, gradient leakage, Sybil attacks	Mitigated via blockchain audit logs, authentication, incentives	Further reduced via DRL-based threat detection, adaptive trust scoring, and intelligent anomaly monitoring
3.	Scalability	Moderate, limited by device heterogeneity and communication cost	Limited by block size, consensus latency, and energy overhead	High, enabled by lightweight consensus, hierarchical FL aggregation, and DRL-based adaptive resource allocation
4.	Incentive Mechanism	Mostly absent or static reward policies	Token-based or score-based incentives for honest participation	Adaptive DRL-driven incentives considering data quality, contribution reliability, and energy costs
5.	Resource Awareness	Low, ignores device battery and bandwidth limitations	Medium, partial consideration of resource consumption	High, energy-efficient block selection, dynamic node participation, and DRL-optimized scheduling
6.	Consensus Mechanism	Not applicable (central server-based aggregation)	PoS, DPoS, PBFT variants integrated with FL	Adaptive, lightweight, DRL-integrated consensus protocols tailored for IoT constraints
7.	Inter Operability	Limited, often domain-specific FL frameworks	Moderate, blockchain ensures integrity but lacks cross-domain standards	High, standardized hyper-learning architecture supporting heterogeneous IoT ecosystems with cross-platform operability
8.	Application Domains	Smart healthcare, finance, IoT sensing	Secure IoT/IIoT, edge intelligence	Broad: healthcare, autonomous vehicles, industrial IoT, smart cities, and safety-critical IoT domains

2.1 Existing FL Frameworks for IoT

As IoT ecosystems create immense data streams, FL offers an effective way to manage and analyze them. To address the constraints of centralized data handling in IoT networks, the community has released multiple open-source FL platforms [9]. By analyzing input streams directly on devices and federating results, these frameworks support privacy preservation and low latency [10]. Yet, IoT-focused FL implementations still struggle with issues of robustness, efficiency, and security. To mitigate these problems, novel solutions have been introduced, such as blockchain-enabled asynchronous FL scheme that verifies information accuracy, avoids dependence on vulnerable nodes, and boosts system productivity [11]. An additional approach combines blockchain with federated learning to obscure shared training parameters and enhance privacy protection in IoT environments [12]. To refine FL operations in IoT scenarios, several frameworks have been proposed. One such method, FedEAFO, optimizes performance by simultaneously reducing parameters and incorporating local updates, thereby balancing the trade-offs across data processing, connectivity, and accuracy [13]. For image recognition tasks in IoT, researchers have proposed a federated unsupervised

learning approach capable of managing the difficulties created by non-IID logs among diverse clients [14]. SemiFL further integrates centralized and federated paradigms to support large-scale IoT systems, with notable benefits in settings that include computation restricted sensor devices [15].

AsyFed addresses device heterogeneity and resulting stragglers by clustering clients into gears based on comparable training performance and introducing a T step protocol that reduces the contribution of lagging gears [16]. In IoT environments, a streamlined hybrid federated learning framework employs blockchain-based smart contracts to ensure authentication, distribute models, and maintain trust [17]. FL has shown potential as a resource-efficient replacement for centralized intrusion detection in IoT environments. Studies employing shallow artificial neural networks and different aggregation methods confirmed that FL based IDSs can achieve competitive prediction accuracy, reliable response behavior, robust sensitivity, and solid F1-score [18]. To better preserve confidentiality with digital medical systems, studies have merged privacy-enhancing technologies and blockchain with federated learning. These combined methods tackle critical technological requirements for healthcare data protection, such as blockchain-enabled model repositories, protected aggregation procedures, and immutable gradient uploads [19]. Current FL frameworks for IoT show strong potential in addressing distributed data handling, privacy protection, and rapid model training. Yet, ongoing research continues to refine these systems, aiming to boost efficiency, robustness, and security while aligning with the evolving needs of IoT applications across various industries [20].

2.2 Security Vulnerabilities and Model Poisoning in FL

As a cooperative learning paradigm, FL supports the protection of user data, yet it simultaneously opens the door to specific security threats that malicious entities can leverage [21]. A significant risk arises from model poisoning, in which hostile participants manipulate local contributions to corrupt the shared model and disrupt its consistency [22]. Among the most severe risks in FL is model poisoning, in which attackers alter personalized updates to damage the shared model's effectiveness. An advanced threat called the Sybil collusion attack has been identified in IIoT-FL setting. In this method, adversaries inject malicious updates by combining label flipping techniques with the creation of multiple Sybil nodes. This increases the likelihood that corrupted updates will be accepted during aggregation, leading to misclassification of targeted samples while the accuracy on other classes remains largely unaffected [23]. This approach introduces a verifiable incentive mechanism designed to encourage collaboration among decentralized participants while addressing persistent challenges in federated learning.

To mitigate poisoning threats, the DeMAC framework has been proposed as a tailored defense strategy. It leverages a metric known as GradScore, which assesses the gradient norms of client updates, thereby distinguishing malicious actors from legitimate contributors during training. A key advantage of this approach is its ability to automatically detect adversarial activity without manual parameter tuning, and empirical studies show it significantly reduces attack success rates across diverse poisoning strategies [24]. Security architectures supported by blockchain [25]. Homomorphic encryption-based federated learning models provide another method for achieving privacy preservation [26]. Despite existing efforts, it is still difficult to reconcile privacy; studies may explore enhanced federated learning architectures that tackle both privacy and security challenges concurrently [27,28].

2.3 Motivation for Integrating Blockchain and Federated Learning

Federated learning reduces data exposure, but it still depends on a central server, which poses issues with poisoning, integrity, and trust. FL-only systems struggle to confirm whether client updates are accurate or unaffected, and trust-scoring methods often lack robustness. However, blockchain offers decentralized auditability and immutable validation, but it does not provide efficient model aggregation, customization,

or large-scale distributed learning. We combine the benefits of FL and blockchain by doing the following: Blockchain ensures verifiable, tamper-resistant update provenance and transparent incentive mechanisms, while FL minimizes data transfer and permits scalable, privacy-preserving training across heterogeneous IoT devices. This combination is becoming more and more popular in research on trustworthy FL [29] and decentralized federated learning frameworks that stress auditability and transparency [30].

2.4 Blockchain-Based Counter Measures

This survey presents a succinct taxonomy based on attack surface, attacker type, and target layer because security risks in blockchain-assisted federated learning are still dispersed across layers. Gradient-based inference, which can extract secret data from shared updates [31], backdoor insertion, where hidden triggers are implanted during training, and Byzantine poisoning, where corrupted updates deteriorate model integrity [32], are important attack surfaces. Even in lightweight systems, dangers like ledger-state manipulation and consensus manipulation exist at the blockchain layer [33]. These risks target IoT devices, the FL aggregation pipeline, or the blockchain ledger and come from external adversaries, Sybil-style attackers, or malicious insiders. This cohesive framework replaces previous disjointed explanations and explains why blockchain-only or FL-only defenses are insufficient. Blockchain is increasingly recognized as a vital tool for boosting cybersecurity in diverse industries such as retail. Its immutable and distributed architecture provides a strong basis for mitigating prevalent security risks. Through distributed ledger mechanisms, blockchain also facilitates decentralized data governance while reinforcing integrity and trust [34]. The application of blockchain within retail settings has introduced stronger mechanisms for supply chain transparency, secure transactions, and reliable data handling. Because of the technology's traceability features, product sources can be verified, which lowers fraud associated with counterfeit goods and improves vendor management. Moreover, blockchain enabled transaction frameworks, together with fraud monitoring solutions, add an extra shield of trust to financial operations in this sector [35]. Blockchain excels in protecting data by applying privacy controls, enforcing consent protocols, and maintaining permanent, unalterable records. Such capabilities are crucial for industries that manage sensitive datasets, including medical services. To advance biomedical security in this area, the BDL-IBS (Blockchain and distributed Ledger based improved Biomedical security) solution integrates blockchain with distributed lrdger systems, delivering enhanced safeguards for medical data [36]. Although blockchain first emerged in the financial sector, its applications have since broadened into multiple domains, including supply chain management, IoT, governance, and manufacturing. In recent years, adoption has grown steadily across these areas, with the banking industry witnessing some of the fastest advancements [37]. Despite its advantages, blockchain continues to encounter obstacles including scalability limitations, security vulnerabilities, and unresolved regulatory issues. Addressing these challenges is essential to achieving large scale deployment of blockchain based systems [38]. Even with existing hurdles, blockchain stands out as a powerful tool for advancing cybersecurity practices in multiple industries. By enabling secure, transparent, and distributed frameworks, it strengthens resilience against cyberattacks. Ongoing research and adoption are likely to foster novel blockchain based protection strategies in the coming years [39]. Table 2 explains how the main attack types in federated learning relate to the defence measures in blockchain-enabled frameworks. The table illustrates how security against model poisoning, Sybil attacks, inference assaults, and Byzantine behaviour is strengthened by blockchain characteristics like immutable logging, decentralised identity management, and transparent validation. The particular security benefits offered by blockchain-based federated learning under various attack scenarios are made clear by this mapping.

Table 2: Mapping of security attacks to defense mechanisms in blockchain-enabled federated learning.

Attack Type	Threat Description	Defense Mechanisms	Role of Blockchain
Model Poisoning	Malicious clients manipulate local updates to degrade global model accuracy	Robust aggregation, reputation-aware client selection	Immutable logging of updates and accountability of contributors
Sybil Attack	Adversary creates multiple fake identities to dominate aggregation	Identity verification, stake-based participation	Decentralized identity management and Sybil resistance
Inference Attack	Sensitive training data inferred from shared gradients	Differential privacy, homomorphic encryption	Auditable enforcement of privacy-preserving mechanisms
Byzantine Attack	Arbitrary or faulty updates disrupt convergence	Byzantine-robust aggregation rules	Transparent validation and traceable update history
Backdoor Attack	Hidden triggers embedded during training	Update validation, anomaly detection	Tamper-proof record of model updates and auditability

3 Blockchain-Enabled Federated Learning in IoT

Traditional federated learning is based on strong trust assumptions, including a trustworthy central aggregator, genuine client participation, and unverifiable model aggregation. These assumptions become fragile in open, large-scale IoT environments. Blockchain reconstructs these trust requirements by offering decentralised coordination, unchangeable model update tracking, and visible incentive systems independent of a trustworthy server. Although techniques like differential privacy and homomorphic encryption increase confidentiality, they are not sufficient to ensure auditability, accountability, or fair reward distribution. The basic requirement for a decentralised trust mechanism to overcome these fundamental challenges of federated learning is what motivates the inclusion of blockchain [40].

A blockchain enabled FL framework offers a strong, privacy respecting model for cooperative learning across IoT networks. The fusion of blockchain's distributed trust and FL's local training capability helps mitigate privacy leakage, enhance security, and ensure the integrity of the aggregated model [41]. For IoT applications, federated learning makes it possible for IoT entities to co-train machine learning models without disclosing original datasets, and blockchain complements this by offering a reliable, auditable ledger for secure data transactions [42]. The combination proves highly beneficial for contexts such as medical systems, intelligent industrial IoT, and connected vehicles, where safeguarding confidential records is critical and privacy concerns dominate [43]. The fusion of blockchain and FL for IoAT applications delivers several strengths, particularly in privacy protection, where edge devices perform local training and share solely model updates instead of sensitive data [44].

In addition, blockchain provides data integrity for model updates through its immutable nature, while maintaining a complete and traceable history of the federated learning process [45]. Blockchain-enabled

smart contracts also facilitate autonomous aggregation of models, regulate reward distribution, and impose access limitations, ensuring secure collaboration [46]. The optimization of speed and scalability in blockchain enabled federated learning for IoAT continues to pose difficulties. Scalability and speed remain unresolved challenges in applying blockchain to federated learning within IoAT environments. Researchers are therefore exploring lightweight consensus mechanisms, improved ledger storage techniques, and flexible security frameworks designed for devices with restricted resources [47]. These innovations create opportunities to advance secure and privacy-focused distributed learning. Looking forward, merging FL and blockchain with breakthroughs in quantum technology and advanced communication systems could provide long-term solutions to IoT's persistent privacy and security limitations [48,49]. The ongoing improvements in these technologies are projected to drive resilient, high performance, and privacy conscious distributed learning solutions for critical IoT applications like healthcare and smart grid networks [50].

3.1 Fundamentals of Federated Learning

As a collaborative learning method, FL allows devices or organizations to train a common model collectively without transmitting their sensitive source data [51]. This method allows training to take place across multiple distributed nodes while ensuring robust safeguards for both privacy and data security [52]. In federated learning, computation is divided between edge devices and a coordinating server. Each device processes its local data and produces updates, which are then merged at the central node through an aggregation step [53]. A key difficulty in federated learning arises from the presence of non-independent and identically distributed datasets among clients, leading to heterogeneous learning contexts [54]. In response, tailored FL methods have been developed to produce client specific models, ensuring that the learning outcomes better reflect diverse user demands [55]. The combination of federated learning and blockchain is also under study, aiming to provide more secure, decentralized, and incentive driven collaborative systems [56]. To put in briefly, federated learning offers a powerful framework for safe AI development, particularly beneficial in domains like healthcare and financial services, where data transfer is prohibited [57]. As federated learning progresses, efforts are being directed towards enhancing communication efficiency, optimizing model aggregation techniques, and reinforcing defenses to ensure stronger and more scalable systems [58]. The design of effective FL systems plays a vital role in supporting algorithm deployment and overcoming challenges tied to accuracy, resource utilization, and data confidentiality [59].

3.2 Security and Privacy Challenges in FL

While FL offers a valuable pathway for secure and distributed predictive learning, it continues to encounter challenges in safeguarding privacy and maintaining data reliability. The decentralized setup leaves room for malicious actors to exploit framework weaknesses [60]. Backdoor attacks and malicious exploitation pose a significant threat to FL, as they allow attackers to alter the shared model by injecting harmful inputs or poisoned updates [61]. Privacy can also be compromised through inference attacks, which make it possible for attackers to deduce original data by analyzing the parameters communicated during training [62]. Because of its distributed design, FL is exposed to several other attack surfaces that malicious actors can exploit to target the global model. Paradoxically, while FL aims to enhance confidentiality, studies have demonstrated that it is not fully immune to privacy related attacks [63]. This paradox highlights the necessity of integrating stronger defense strategies into FL frameworks. Researchers have proposed countermeasures applied at different stages prior to aggregation, during the process, and after model updates are combined [64]. Researchers are examining approaches like encrypted computation, privacy preserving anonymization, and blockchain assisted models to reinforce the confidentiality and resilience of FL [65].

To effectively tackle the privacy and security challenges in federated learning, comprehensive and multi-layered strategies are required. Future frameworks should embed the core strength of FL: its ability to protect sensitive data [66]. Future research should focus on balancing privacy, model accuracy, and stronger security.

Table 3 compares differential privacy, homomorphic encryption, and hybrid privacy-preserving models for IoT-based federated learning. The comparison shows that while DP-based methods are lightweight, they suffer from accuracy loss, whereas HE-based solutions offer stronger confidentiality at the cost of higher computation and latency. Hybrid and adaptive approaches attempt to balance these trade-offs, motivating the need for intelligent coordination in the proposed Hyper-Learning Framework.

Table 3: Comparative view of differential privacy and homomorphic encryption for IoT-FL.

Technique/Model Type	Representative Models	Strengths	Limitations	Suitable IoT Devices
Local Differential Privacy (LDP)	Local DP-FL, DP-SGD at client side	Lightweight, scalable, low computation overhead	Accuracy loss due to noise, weak against inference attacks	Wearables, sensors, smart home nodes
Central Differential Privacy (CDP)	DP-FedAvg, server-side noise injection	Better utility than LDP, simple aggregation	Requires trusted aggregator, single-point risk	Smart gateways, edge nodes
Adaptive Differential Privacy	Budget-aware DP-FL, dynamic noise scaling	Balances privacy and accuracy dynamically	Privacy-budget tuning complexity	Moderate-capability edge devices
Homomorphic Encryption (HE)	Encrypted aggregation FL	Strong confidentiality, encrypted model updates	High CPU/memory cost, increased latency	MEC servers, industrial controllers
Packed/Partial HE (PHE)	Batched encrypted aggregation	Reduced overhead compared to full HE	Still expensive for end devices	Gateways, edge servers
Fully Homomorphic Encryption (FHE)	Fully encrypted FL pipelines	End-to-end encryption, strongest privacy	Impractical for IoT due to extreme computation cost	Cloud servers, powerful edge nodes
Secure Aggregation (Non-HE)	Mask-based secure aggregation	Lightweight, avoids heavy cryptography	Vulnerable to collusion attacks	Resource-constrained IoT devices
Hybrid DP + HE	Client-side DP with encrypted aggregation	Balanced privacy and efficiency	Multi-layer coordination complexity	Mixed IoT hierarchies
Blockchain-Assisted Privacy FL	Encrypted model logging, on-chain verification	Tamper resistance, auditability, trust enforcement	Added latency and energy overhead	Industrial IoT, smart infrastructure
DRL-Optimized Privacy FL	Adaptive DP/HE selection via DRL	Context-aware privacy and energy optimization	Increased system complexity	Heterogeneous IoT environments

Since privacy-preserving strategies in FL are frequently given inconsistently, this study groups them around two fundamental methods: Homomorphic Encryption (HE) and Differential Privacy (DP). Although DP can decrease accuracy under non-IID data, it is lightweight enough for IoT devices and adds calibrated noise to updates. HE prevents sensitive gradients from being exposed and maintains model changes encrypted throughout aggregation, but it adds significant computation and communication overhead and is mostly appropriate for gateways or edge servers. According to recent IEEE research, combining HE at aggregation nodes with DP at the device level can balance resource restrictions and privacy strength in heterogeneous IoT environments. The best times to use each method in blockchain-enabled FL systems are made clear by this methodical comparison. Despite the fact that FL employs a number of privacy-preserving techniques, their discussion in the literature is frequently dispersed and lacks a comparison framework. In order to solve this, we take a narrow emphasis on two popular methods: Homomorphic Encryption (HE) and Differential Privacy (DP). By adding calibrated noise to gradients prior to upload, DP protects user

data and provides low computational overhead appropriate for IoT devices with limited resources. However, under non-IID settings, it increases accuracy loss [67]. HE is more suitable for gateways and MEC nodes since it allows encrypted model updates to be aggregated without decryption, offering high confidentiality assurances but imposing a substantial computational and communication expense [68]. According to recent research, hybrid designs can balance accuracy and overhead in heterogeneous IoT installations by combining DP at the edge with HE at intermediate nodes to provide layered safety [69]. This comparative viewpoint makes the privacy design decisions more understandable and in line with the real-world limitations of blockchain-assisted FL.

Table 4: Comparative review of blockchain-integrated federated learning methods in IoT environments.

S. No.	Title	Findings	Research Directions	Limitations	Advantages
1	BDIM: A Blockchain-Based Decentralized Identity Management Scheme for Large-Scale IoT [70]	BDIM ensures fast, scalable, and secure IoT identity management with smart contracts.	Enhance scalability, security, interoperability, and real-world application.	Scalability limits, performance issues under high load, blockchain dependency, and user experience challenges.	Enhances security and trust, offers low gas costs and fast response time.
2	FabricFL: Blockchain in the Loop Federated Learning for Trusted Decentralized Systems [71]	Integrates blockchain and FL to improve security and trust using credibility scoring.	Improve scalability, reduce latency, enhance privacy and user experience.	High complexity, latency, and integration cost.	Boosts privacy, performance, and accuracy (+10%).
3	Comments on LPBFL for Blockchained Federated Learning in IoT [72]	Addresses signature vulnerabilities and proposes improved LPBFL.	Focus on cryptography, attack resilience, and implementation.	CDH reliance, lack of real-world evidence.	Strengthens verification, uses Paillier encryption, improves efficiency.
4	RL-FL-BC: RL-Based Federated Learning over Blockchain [73]	Combines RL, FL, blockchain for cost savings and privacy.	Optimize protocol efficiency, latency, and testing.	Latency, cost, and scalability concerns.	Enhances collaboration and privacy, especially for healthcare.
5	Decentralized FL on Edge over Wireless Mesh Networks [74]	Achieves 93% accuracy, ensures privacy via local training.	Explore blockchain and protocol optimization.	Underutilization of edge devices.	Improves resilience and privacy.
6	Differentially Private Federated Multi-Task Learning for HDT [75]	Enhances privacy, connectivity, and cost-efficiency in HDT.	Optimize scalability and blockchain integration.	Privacy-accuracy tradeoff, synchronization issues.	Boosts adaptability, task optimization, and validation.
7	Blockchain-Based Hierarchical FL for UAV-IoT [76]	Improves latency, accuracy, and trust in UAV-enabled networks.	Study consensus, resilience, and resource allocation.	Centralized UAVs, high overhead, security issues.	Trustworthy with non-i.i.d. data handling.
8	Resource-Efficient FL with DAG Blockchain for IIoT [77]	Integrates FL, DAG blockchain, and digital twins for secure IIoT.	Improve sharding, consensus, and performance evaluation.	Latency, resource limits, MAPPO complexity.	Enhances adaptability, verification, and error handling.
9	Blockchain-Enabled FL Model with Multisignature [78]	Addresses FL vulnerabilities and adversarial risks.	Enhance security, blockchain integration, and speed.	Costly and complex encryption.	Improves IoT security and reduces resource needs.
10	FL-Based Task Offloading in UAV-Aided MEC [79]	DFedAvg optimizes UAV paths, reducing delay by 16.7%.	Focus on mobility, bandwidth, and real-world validation.	High demands, scalability and privacy concerns.	Reduces latency, improves offloading.

In the proposed Hyper-Learning Framework, the selection between Differential Privacy (DP) and Homomorphic Encryption (HE) is guided by a DRL-based control mechanism. The DRL agent observes device-level states such as computational capacity, energy availability, latency constraints, and communication reliability. Based on these observations, resource-constrained IoT devices are dynamically assigned

DP-based protection to ensure lightweight privacy preservation, while more capable nodes such as gateways and edge servers employ HE for stronger confidentiality during aggregation. This adaptive selection enables a balance between privacy strength and system efficiency under heterogeneous IoT conditions [80]. By warping shared updates, Differential Privacy (DP) mainly thwarts inference-based attacks like membership inference and gradient inversion. Nevertheless, malevolent clients are still able to deliver poisoned model modifications thanks to DP. Conversely, Homomorphic Encryption (HE) protects against honest-but-curious aggregators by allowing encrypted aggregation, but it does not reduce poisoning, Sybil, or backdoor assaults. Because of this, neither DP nor HE by itself provides total protection against all attack surfaces, highlighting the need for other procedures like blockchain-based verification and trust management [81].

3.3 Role of Blockchain in FL: Model Security, Integrity, and Trust

The use of blockchain within federated learning strengthens guarantees of trust, safety, and fairness. Decentralized consensus and validation protocols address potential weaknesses during training, particularly when dealing with unreliable or adversarial nodes. Through tamper-proof logging of model updates and user activities, blockchain ensures both integrity and privacy in distributed learning environments. With immutable tracking of model changes and participant actions, blockchain becomes a key enabler for secure and confidential collaborative learning [82]. By requiring organised involvement and public update validation, blockchain might lessen the influence of non-IID data, which is still a major problem in FL. In order to prevent excessive bias from highly skewed nodes, smart contract-based selection can provide preference to clients with trustworthy or balanced data [83]. Immutable on-chain logging aids in identifying aberrant gradient variance and local drifts in diverse environments [84], while blockchain-based reputation scores deter updates that consistently deviate from expected gradient behaviour [85]. These processes stabilise aggregation and enhance convergence among many IoT devices, even when blockchain does not completely eradicate non-IID distributions. While blockchain-assisted mechanisms such as reputation-based client selection and immutable update logging can alleviate the impact of non-IID data, they do not eliminate it entirely. In highly skewed data distributions, trusted clients may still contribute biased updates, and reputation scores may converge slowly in dynamic IoT environments. Moreover, blockchain-based validation increases latency and may limit rapid adaptation when data distributions shift abruptly. These limitations indicate that blockchain can mitigate, but not fully resolve, non-IID challenges, especially under strict resource and real-time constraints [64].

A key strength of blockchain lies in its immutability, ensuring that model updates remain permanent once committed, thus safeguarding the system from manipulation attempts. This feature provides strong guarantees in multi-party settings where stakeholders may not fully trust one another and where transparent auditing is necessary. Through consensus driven verification, blockchain enhances the protection and trustworthiness of federated learning systems. Given that FL relies on distributed clients who share only model updates, such mechanisms are critical for securing the joint model-building process. The Table 4 summarizes the recent works in blockchain based federated learning.

Through an immutable, verifiable record of model changes and contributor data, blockchain prevents falsification and markedly improves security guarantees [86]. The permanence of blockchain entries ensures that stored model updates cannot be rolled back, protecting the system from manipulation during training. This property proves critical when contributors may not fully trust one another or when transparency in auditing is required [87]. Ensuring the uniformity of operations in federated learning is a concern, and blockchain offers a solution. By leveraging smart contracts, it becomes possible to automate the enforcement of rules, making sure every participant abides by the established protocols [88]. Such a mechanism secures the correctness of the trained model and acts as a barrier against malicious actions like tampering with

updates. Moreover, the decentralized validation offered by blockchain allows independent nodes to confirm the authenticity of updates before they affect the overall system [89]. Apart from enhancing protection and verifying the integrity of shared models, blockchain provides a foundation for transparent contribution tracking and fair incentive allocation among participants.

Ten representative studies that show how blockchain-enhanced FL has developed in various IoT scenarios are summarised in Table 5. Our explanation of safe participant authentication in Section 3.3 is reinforced by BDIM's identity-management focus whereas the claims of cryptographic verification, tamper resistance, and trust formation are directly supported by FabricFL and LPBFL. The hierarchical UAV-IoT frameworks and RL-FL-BC are in line with Sections 5 and 5.1, showing how reinforcement learning enhances resource allocation, adaptive coordination, latency handling, and blockchain and FL. The paper's focus on privacy protection, robustness, and non-IID data management is reinforced by edge-centric and multi-task learning contributions, such as decentralised FL over mesh networks and differentially private HDT systems. The scalability, security, and reliability issues examined in Sections 4 and 6 are substantiated by DAG-based blockchain for IIoT and multisignature-assisted FL. Lastly, our system-level discussions on mobility-aware optimisation and energy-efficient training directly relate to UAV-assisted MEC offloading. When taken as a whole, the works in Table 2 demonstrate the technical reasons for moving closer to the suggested Hyper-Learning Framework and confirm the main points made throughout the survey.

Table 5: Summary of models, datasets, and performance across blockchain-enabled federated learning studies.

Paper/Framework	Model Used	Dataset	Performance Summary
BDIM: Blockchain-Based Decentralized Identity Management for Large-Scale IoT	4-layer FNN (Hierarchical FL), centralized aggregation	General IoT classification tasks	Hierarchical FL accuracy ≈92%; centralized FL ≈94%; standard FL ≈88%–89%
FabricFL: Blockchain-in-the-Loop Federated Learning for Trusted Systems	ResNet, DNN	X-ray, CIFAR, IoT-IDS	Robustness of 70%–90% under poisoning and inference attacks
LPBFL: Lightweight Privacy-Preserving Blockchain FL for IoT	Conceptual FL architecture	Not explicitly reported	Qualitative evaluation of privacy preservation and secure aggregation
RL-FL-BC: RL-Based Federated Learning over Blockchain	FL with DRL-based controller	Benchmark simulation datasets	Near-optimal convergence; accuracy approaching centralized FL
Decentralized FL on Edge over Wireless Mesh Networks	MLP, CNN, VGG	MNIST, CIFAR	Centralized > FedAvg > Mesh-based FL in accuracy and convergence

(Continued)

Table 5 (continued)

Paper/Framework	Model Used	Dataset	Performance Summary
Differentially Private Federated Multi-Task Learning	DPML, DP-FedAvg	CelebA	DPML achieves highest utility; DP-FedAvg shows higher noise sensitivity
Hierarchical FL for UAV-IoT Learning	4-layer FNN	IoT sensor data	Centralized FL ≈ 94%; Hierarchical FL ≈ 92%
Resource-Efficient FL with DAG Blockchain for IIoT	4-layer FNN	Industrial IoT sensors	Proposed scheme achieves >91% accuracy with reduced latency
Blockchain-Enabled FL Model with Multisignature Verification	LeNet	MNIST, FMNIST	Accuracy drop limited to 1%–2% under strong security constraints
FL-Based Task Offloading in UAV-Assisted MEC	DDPG, FedAvg	Simulated MEC workloads	Delay reduced by ≈ 17%; energy savings of 25%–35%

The verifiable nature of blockchain records allows the establishment of fair payment schemes, reinforcing trust and accountability among FL participants [90]. It is important to note that integrating blockchain and FL is not straightforward, since transaction costs and bottlenecks may arise, requiring thorough study in environments with constrained devices [91]. While blockchain enhances transparency, mishandling its design may put privacy at risk. Storing sensitive data or participant identifiers directly on an immutable ledger could inadvertently expose confidential information [92]. By combining blockchain with federated learning, researchers aim to build systems that are more secure, transparent, and dependable. Blockchain's ability to keep permanent records, apply smart contracts automatically, and manage rewards fairly makes it a strong complement to FL. In the future, this integration is expected to produce hybrid models that offer both resilience and efficiency in collaborative learning [93].

The combined table and graph demonstrate that FedAvg stays close with little loss while centralised training provides the best accuracy. While expected decreases occur, more decentralised techniques like FedDec and MeshFedAvg continue to work reliably across datasets. Accuracy trade-offs are introduced by privacy and security-enhanced FL techniques, however these are greatly mitigated by optimized variations. The best adaptive performance is attained by RL-based FL, which frequently matches or surpasses baseline FL. Overall, the combined findings show that federated learning can continue to be precise, safe, and scalable, and the additional quantitative comparison enhances the suggested framework's technical validity.

4 Consensus Mechanisms and Resource Optimization in Blockchain FL

Blockchain enhanced federated learning has shown promise in addressing key challenges of traditional FL, including security weaknesses, lack of decentralization, and limited scalability. Nevertheless, which consensus algorithm is used significantly influences the operational behavior and resource demands of the resulting system [94]. Traditional consensus algorithms like Proof of Work (PoW) impose heavy

computational costs and are unsuitable for FL, particularly in scenarios involving wireless devices with limited resources [95]. In pursuit of optimized resource usage and higher efficiency, multiple innovative designs have been explored. The Directed Acyclic Graph approach to federated learning (DAG-FL) stands out by providing improved predictive reliability and effectiveness over standard hardware integrated FL implementations [96]. Similarly, the ChainsFL architecture leverages a hybrid structure, merging Raft enabled shard management with a DAG backed central blockchain, to better accommodate the demands of large federated learning deployments [97]. Such methods work to mitigate delays from slow participants and strengthen parallel training efficiency. Thus, the synergy between blockchain and federated learning highlights new avenues and challenges in resource allocation, with innovative mechanisms like proof of federated learning turning idle processing into meaningful tasks [40]. Moreover, the use of adaptive scheduling policies combined with deep reinforcement learning is being examined to improve spectrum efficiency, block sizing, and block generation rates in blockchain supported mobile edge computing environments [98]. These advancements demonstrate ongoing efforts to maintain security equilibrium, efficiency, and scalability in the blockchain-FL framework. This survey uses a single analytical approach that divides limits into three interrelated dimensions: computation, communication, and storage in order to address the fragmented debate of resource limitations [99]. IoT nodes must employ low-power processors for local training and blockchain verification, which leads to computation limitations [100]. Unstable links, large upload costs during model exchange, and consensus overhead that increases with dense deployments are examples of communication limitations. Maintaining model parameters, blockchain metadata, and historical updates on devices with limited memory capacity results in storage limitations [101]. When these limitations are taken as a whole, it becomes clear that inefficiencies in any one area spread throughout the system, which encourages integrated optimisation techniques like lightweight aggregation, hierarchical blockchain storage, and DRL-based scheduling to ensure sustained FL in IoT.

4.1 Consensus Algorithms in Blockchain for IoT

In blockchain based IoT applications, consensus mechanisms play a crucial role, and different approaches are being assessed for their performance and applicability. Notably, three well known algorithms such as custom proof-of-work, PBFT, and two valued consensus have delivered promising results in IoT settings by achieving consensus in less than one second [102]. In IoT environments, legacy consensus approaches like Proof of Work are limited by the modest processing strength of IoT nodes. Since PoW is highly computationally intensive, it proves unsuitable for devices with restricted energy and processing resources [103]. Addressing this concern, researchers have introduced more appropriate consensus protocols for IoT systems. Proof of Stake, in particular, has gained attention as it minimizes computational demands while significantly improving energy efficiency relative to PoW [104]. Practical Byzantine Fault Tolerance (PBFT) stands out as a reliable consensus framework for IoT, demonstrating compatibility with devices that have limited computational capacity [105]. The convergence of blockchain and IoT creates a dual scenario in which blockchain strengthens trust and security within IoT networks, the limited resources of IoT nodes highlight the necessity for optimized, resource efficient consensus mechanisms [106]. As innovations continue, specialized consensus protocols for IoT will likely evolve, crafted to overcome device constraints yet maximize the benefits blockchain contributes to distributed systems [107]. The summary of consensus mechanisms in IoT has been presented in Table 6. The degree to which the consensus techniques in Table 6 are appropriate for IoT environments varies significantly. Although they provide robust security, PoW and PoS are too hefty for low-power systems. When the number of nodes increases, PBFT and related protocols perform badly, but they are effective in small, permissioned groups. Although they can be less resilient to attacks, IoT-oriented and DAG-based techniques lower delay and energy consumption. The requirement

for an adaptable, learning-driven consensus layer in the Hyper-Learning Framework is highlighted by the fact that no current architecture successfully combines trust, responsiveness, energy efficiency, and widespread participation.

Table 6: Comparison of consensus mechanisms for IoT applications.

S. No.	Consensus Mechanism	Energy Efficiency	Scalability	Suitability for IoAT	Notes
1	Proof of Work (PoW)	Very Low	High	Poor	Too resource-intensive for IoT
2	Proof of Stake (PoS)	Moderate	High	Limited	Better than PoW, but still demands constant availability
3	Delegated PoS (DPoS)	High	High	Suitable	Reduces burden by limiting active participants
4	PBFT	High	Limited	Good for permissioned IoT systems	Communication overhead increases with nodes
5	Proof of Authentication (PoAh)	Very High	Limited	Designed for IoT	Lightweight and secure
6	PoDL (Proof of Deep Learning)	Moderate	Moderate	Emerging	Integrates model performance into consensus

4.2 Challenges of IoT Resource Limitations in Blockchain Operations

Integrating blockchain within IoT networks faces major obstacles because of the restricted capabilities of IoT devices. Constraints in computing resources, limited memory, and high energy demands often hinder the efficient execution of blockchain-based operations in such environments [108]. Since IoT hardware generally offers minimal computational power and limited storage, these devices struggle to participate in conventional blockchain networks that demand intensive resources for consensus and mining [109]. The challenge is most apparent in edge nodes with limited capacity, where the high algorithmic load of blockchain proves difficult to manage [110]. Several solutions have been put forward, including the development of streamlined blockchain frameworks and mechanisms for balancing workloads across devices with varying resource availability [111]. A creative solution introduced in literature is the sliding window blockchain, where earlier block data supports the hashing of subsequent blocks, coupled with a simplified proof of work mechanism, making it more feasible for IoT use cases [112]. A different solution leverages the Proof of Authority mechanism in Ethereum which has been applied to show the viability of blockchain within IoT networks by mitigating both delay and scalability issues [113]. Overall, the combination of blockchain and IoT opens doors to improved decentralization, transparency, and security, but faces obstacles due to the limited resources of IoT hardware. Researchers are focusing on developing efficient blockchain and consensus mechanisms tailored for such environments ensuring the feasibility and scalability of blockchain driven IoT ecosystems [114].

4.3 Dynamic Node Selection and Energy-Efficient Strategies

Energy efficient allocation methods combined with dynamic node selection are instrumental in refining wireless network operations, notably in varied and device to device communication scenarios. Within heterogeneous networks, applying these techniques leads to marked gains in energy efficiency [115]. Attention is given to power reduction mechanisms and conflict mitigation for co-channel Single-RAT HetNets, underlining the necessity of flexible, energy optimized resource control frameworks [116]. An energy conscious staged allocation model for HetNets is proposed, incorporating fractional frequency reuse to both conserve resources and ensure stable connectivity at the network boundary. Through adaptive center edge partitioning, time slot planning, and optimized power management, the system secures notable improvements in efficiency and lower outage probability.

Leveraging direct D2D connectivity creates opportunities to implement power optimized strategies in wireless networks [117]. Research highlights that embedding D2D communication into dynamic TDD frameworks can boost energy efficiency by coordinating mode choice, slot allocation, and power usage. Such designs demonstrate improved spectral performance and reduced energy consumption over standard cellular methods [118]. It presents a new framework that improves D2D energy performance in HetNets by dynamically determining communication modes via fuzzy clustering. It further highlights that intelligent, dynamic selection of nodes within Cloud RANs is key to achieving better energy efficiency [119]. It highlights an integrated framework for heterogeneous C-RANs that unifies RRH activation, user association, and resource scheduling. Using a greedy activation policy and channel-driven pairing, the scheme achieves significant energy efficiency improvements. Ensuring network performance further requires dynamic node selection and energy optimized designs. Extending these methods to HetNets D2D links, and C-RANs strengthens both spectrum efficiency and overall performance. Additional measures such as sleep/wake cycles, interference reduction, and dynamic resource distribution contribute to building more sustainable and high performing wireless networks [120].

5 Deep Reinforcement Learning for FL Optimization

In recent years, DRL has been explored as a way to strengthen FL in environments where devices face strict resource limitations, such as drone assisted wireless systems and IIoT. DRL not only guides the placement of UAVs but also manages resource sharing, which leads to improved connectivity and higher throughput. Within IIoT, it supports stable load distribution across devices while preserving accuracy and training speed. When used together, FL and DRL enable networks to adapt in real time, ultimately achieving better scalability, efficiency, and reliability [121]. The proposed method enhances the long term effectiveness of FL by addressing critical resource constraints, including harvested energy, bandwidth availability, and UAV energy capacity. Using a Markov Decision Process formulation, a DRL based solution manages these challenges to achieve energy efficient operation while remaining responsive to dynamic network conditions. Within IIoT environments, this strategy is further refined through a DRL driven joint policy for resource allocation and device coordination. As a result, hierarchical FL systems supported by MEC can maintain high model accuracy while lowering both computation and communication burdens [122]. The method focuses on reducing delay, improving energy efficiency, and preserving model accuracy in constrained edge environments. Using the Deep Deterministic Policy Gradient approach, it demonstrates strong performance across these dimensions. Evaluating DRL with federated learning also addresses decentralized optimization challenges effectively. The Fed-MARL framework exemplifies this by arranging channel selection and power allocation in vehicle-to-vehicle communications, enhancing both efficiency and network reliability [123]. Leveraging DRL in combination with FL, this approach enhances consistency and minimizes lag while improving cellular link performance. Federated learning balances cooperative multi agent training

and speeds up convergence, while DRL efficiently optimizes resource distribution, communication, and adaptation to evolving IoT network topologies [124].

Fig. 2 presents the DRL-driven optimization framework for federated learning, where the DRL agent observes system states and selects actions such as client selection, aggregation strategy, and update frequency. The reward reflects energy efficiency, communication cost, and model performance, enabling adaptive and optimized FL operation.

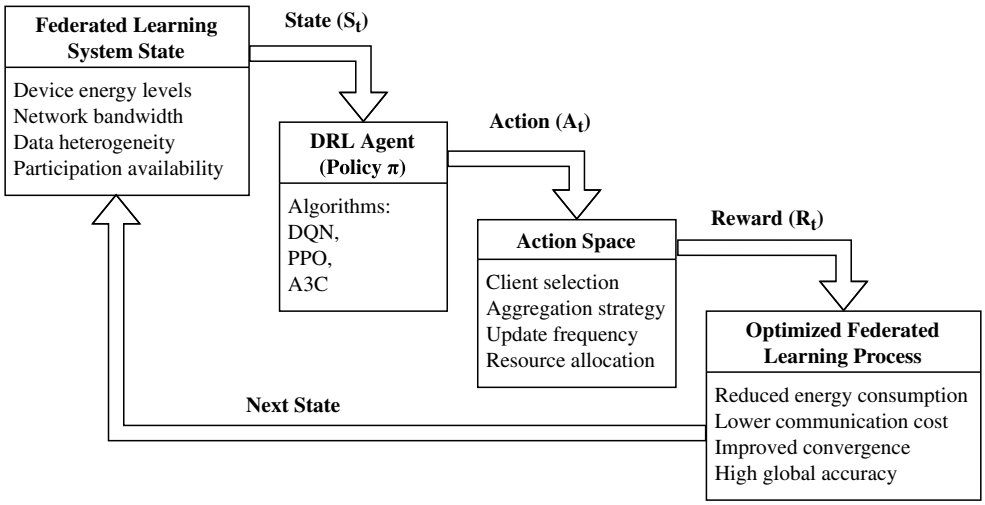

Figure 2: Hyper-learning framework: closed-loop interaction of FL, blockchain, and DRL.

5.1 Adaptive Resource Allocation in FL Using DRL

In FL, DRL serves as an effective approach to improve resource allocation, particularly in wireless environments where energy and bandwidth are limited. DRL-based strategies have been designed to identify optimal UAV placement and manage resource distribution in UAV-assisted networks. By accounting for the limited energy harvested by user devices, these methods help ensure the long term sustainability of FL operations [125]. The goal of this model is to improve the long-term effectiveness of federated learning systems in environments with limited resources, where obstacles include constrained bandwidth, harvested energy, and UAV power budgets. Energy constraints are transformed into a deterministic structure through the use of stability based optimization, which makes it possible for a DRL-based Markov Decision Process to direct effective system operation. There is room for more balanced designs, though, as the majority of the current research still focuses on either single control or fully distributed DRL approaches [126], A hybrid system known as federated deep reinforcement learning has been suggested to provide performance close to centralized training while decreasing information exchange and user privacy protection in wireless networks. In this setup, a central unit coordinates training but limits the scope of data sharing, making it highly suitable for federated learning environments. DRL-driven adaptive resource allocation further improves this approach by optimizing energy, bandwidth, and device deployment under restricted conditions, all while preserving privacy. Looking ahead, advancing specialized DRL algorithms tailored for secure and efficient FL remains an important direction for future research [127].

5.2 Minimizing Energy Consumption while Maintaining Accuracy

Because edge devices have limited battery capacity, compute power, and communication bandwidth, energy economy is a significant difficulty in federated learning for IoT systems. Energy consumption is

greatly increased by frequent model updates, blockchain-related validation processes, and repeated local training, especially in large-scale and heterogeneous IoT implementations. Recent research focusses on energy-aware federated learning techniques that both maximise accuracy and resource utilisation to address these issues. By adjusting client participation, transmission power, update frequency, and aggregation intervals based on current device and network conditions, deep reinforcement learning has become a useful tool for dynamically managing energy consumption. IoT devices with limited resources can selectively participate in training thanks to this kind of adaptive control without compromising the overall performance of the model. By synchronising compute offloading, communication time, and device activation, DRL-based scheduling algorithms further enhance energy efficiency in edge-assisted and UAV-enabled IoT systems. These methods retain a reasonable convergence speed and learning accuracy while cutting down on pointless transmissions and avoiding overloading low-energy nodes. By moving intensive processing away from devices with limited resources, hierarchical FL architectures enabled by MEC nodes also aid in balancing energy consumption. In general, adaptive, context-aware techniques that concurrently take into account device heterogeneity, network dynamics, and learning objectives are needed for IoT-specific energy optimisation in federated learning. A viable technique to accomplish sustainable FL operation in IoT systems without sacrificing accuracy or scalability is through DRL-driven energy management.

6 Research Gaps and Open Challenges

Notable advantages include upgraded data integrity, more reliable privacy protection, and shared decision making when blockchain and federated learning (FL) are combined in Internet of Things systems. Despite these advantages, a number of obstacles still stand in the way of the creation of effective and scalable blockchain FL frameworks. Key challenges hindering widespread adoption of these systems include inadequate incentive and trust mechanisms, excessive energy consumption, restricted block sizes, and inherent limitations in existing models. Resolving these issues is essential for achieving scalable and sustainable deployment across large scale IoT ecosystems.

Different IoT scenarios provide different issues related to limited involvement, high energy use, and security risks. Battery-limited wearables in healthcare IoT often stop training, which reduces client diversity and slows convergence. Because blockchain validation and repeated FL rounds must function under stringent real-time limitations, industrial IoT faces significant energy and latency overhead. UAV-assisted networks have even more severe energy restrictions; lightweight consensus is crucial because drones must balance training, communication, and flight stability. Healthcare systems are more susceptible to inference assaults, whereas smart city installations are more susceptible to poisoning and Sybil attacks because of open public networks. These variations emphasise the necessity of flexible, situation-specific mitigation techniques. By combining FL for privacy, blockchain for trust, and DRL for dynamic optimisation of participation, block size, and communication scheduling, the suggested Hyper-Learning Framework facilitates such adaptability.

Another major issue with blockchain-assisted federated learning for IoT is interoperability. Single-chain architectures are frequently used in current solutions, which restricts cooperation between many administrative domains and application platforms. Cross-domain learning is challenging in large-scale IoAT setups because devices and edge networks may run on distinct blockchain frameworks. Relay-based bridges, side-chain coordination, and cross-chain communication protocols are examples of emerging interoperability techniques that present promising paths for enabling safe model update exchange and trust verification across various ledgers. However, there are new latency, synchronisation, and security consistency issues when combining these approaches with federated learning. For actual blockchain-FL deployment, addressing interoperability in a lightweight and scalable way is still an open research challenge.

6.1 Challenges of Blockchain-Assisted Federated Learning in IoT Systems

While combining blockchain with FL strengthens data security and trust in IoT networks, deploying such systems at scale remains difficult. Resource constrained devices struggle to participate fully, and differences in hardware, connectivity instability, and communication delays hinder synchronous training. These factors collectively slow convergence, reduce model accuracy, and impair overall efficiency across heterogeneous IoT environments.

Managing resources and communication remains a major challenge for blockchain enabled FL in IoT networks. Systems can experience sharp performance drops under fluctuating network conditions and heterogeneous device capabilities. Adaptive mechanisms that can dynamically balance training loads and optimize communication schedules are essential. Additionally, blockchain integration imposes extra energy and computational demands, which can overwhelm low power devices. The choice of block sizes leads to frequent validation cycles, increasing energy usage and communication overhead.

In blockchain supported federated learning, energy consumption is a critical concern. Even supposedly low power consensus protocols like PoS still require significant computation, and multiple rounds of model training amplify the energy burden. Most current models neglect energy efficiency in key operations such as block generation, participant selection, and aggregation, resulting in fast battery drain and reduced sustainability for IoT devices. On the security side, FL remains exposed to threats including model poisoning, Sybil attacks, and privacy leakage. Malicious participants can manipulate model updates or incentive systems, and existing verification or reputation mechanisms often fall short in scalability and resilience against collusion. Furthermore, static approaches to selecting nodes for block creation and model aggregation increase vulnerability to rogue participants and compromise the integrity of the global model.

6.2 Issues with Block Size, Energy Efficiency, and Security

The integration of blockchain in federated learning creates extra strain on energy use and computational efficiency, which limits its suitability for constrained IoT systems. Among the most decisive issues is block size control. Poorly managed block sizes affect the overall network by influencing latency, throughput, and storage capacity. Small block sizes shorten consensus intervals but lead to higher communication load and energy costs, while large blocks delay consensus due to increased propagation delays. Beyond block size, the energy demand of consensus itself is a key obstacle. Even energy optimized mechanisms such as Proof of Stake still consume considerable resources. Since federated learning relies on frequent training and communication, the cumulative energy efficiency considerations in block production, aggregation design, and the process of selecting participating nodes.

Network stability is difficult to maintain since sensor-driven and mobile IoT devices often experience quick energy depletion. Security risks add another layer of concern. While blockchain offers some protection against tampering, federated learning is still exposed to threats such as data inference, Sybil behavior, and poisoned model updates. Attackers may deliberately inject false contributions or manipulate the incentive structure. Approaches like verification checks and reputation models have been proposed, but they typically fail to scale and are ineffective when multiple attackers act together. Moreover, node selection during block generation or model integration is usually fixed or handled without trust based evaluation, which leaves the system open to adversarial behavior. The lack of robust trust and security mechanisms raises the likelihood of corruption in the global model.

6.3 Need for Dynamic Incentive Mechanisms and Participant Trust Evaluation

Sustaining reliability and active engagement in blockchain driven FL requires incentive mechanisms that can adapt to changing conditions. Many existing designs still depend on basic contribution based rewards, which overlook the complexity of IoT environments. Improved incentive frameworks should consider not only how often or how much a node contributes, but also the value and stability of those contributions, the efficiency of resource usage, communication reliability, and device readiness. In addition, robust trust evaluation is essential to reduce the impact of malicious or underperforming participants. Leveraging machine learning or reinforcement learning for trust assessment can help flag harmful nodes while gradually reinforcing cooperative and beneficial behavior.

Addressing the shortcomings of current designs requiers moving toward smarter, context aware blockchain FL frameworks tailored for IoT. DRL offers a promising pathway by dynamically coordinating operations such as channel distribution, block leader selection, and block size tuning in response to device capabilities and current network status. Pairing layered blockchain structures with hybrid consensus mechanisms can also enhance both scalability and energy performance. Incorporating private or consortium blockchains with edge based aggregators also reduces consensus workload and delays while preserving decentralization and security. Despite its strong potential, blockchain FL integration still demands further exploration to address its open challenges and to create IoT systems that balance privacy, performance, affordability, and long term sustainability.

7 Conclusion and Future Directions

In conclusion, by combining security, privacy, optimisation, and trust viewpoints under a single analytical framework, this review unifies disparate studies on blockchain-enabled federated learning. This article describes a closed-loop Hyper-Learning architecture for IoAT systems and emphasises the interdependencies between FL, blockchain, and DRL, in contrast to previous surveys that examine them separately. These contributions serve as a foundation for upcoming system-level design as well as an organised reference for ongoing research. Merging blockchain with federated learning (FL) has shifted IoT research towards decentralized, privacy oriented, and secure intelligence. This survey provided a comprehensive review of blockchain FL integration, outlining its strengths, weaknesses, and emerging opportunities for adaptive IoT ecosystems. Based on the research questions stated in Section 1 guided this study to maintain coherence and focus. For **RQ1**, the survey focused on FL and distributed learning models for IoT showing how they enable privacy and efficient bandwidth use but also bring difficulties tied to device heterogeneity, data imbalance, and possible leakage. For **RQ2**, blockchain was evaluated as a means of establishing immutability, trust, and accountability, although scalability concerns and the energy costs of consensus algorithms remain unsolved. In **RQ3**, we explored how DRL strengthens FL by dynamically managing device participation, communication scheduling, and block optimization, supporting both accuracy and resource savings. Addressing **RQ4**, we pointed to unresolved challenges such as interoperability, flexible incentive mechanisms, domain-specific safeguards, and energy efficient cryptography. Overall, this review delivers an integrated perspective on blockchain, FL, and DRL in IoT, identifies ongoing limitations, and proposes pathways toward secure, efficient, and sustainable distributed intelligence.

7.1 Future Directions: Toward a Hyper-Learning Framework

For safe, flexible, and resource-efficient intelligence in IoAT systems, the suggested Hyper-Learning Framework combines Federated Learning (FL), blockchain, and Deep Reinforcement Learning (DRL) into a single control loop. In this approach, the blockchain layer guarantees integrity, auditability, and incentive management through verifiable update recording, while FL permits privacy-preserving local training.

In response to current network and device conditions, such as energy availability, update quality, and consensus delay, a DRL controller dynamically modifies system parameters like client participation, aggregation intervals, block configuration, and resource allocation. Actions alter FL and blockchain parameters, and rewards represent trade-offs between accuracy, communication overhead, and energy consumption. The interaction is based on a closed-loop decision process. The closed-loop optimization in the proposed Hyper-Learning Framework follows the DRL-driven control process illustrated in Fig. 2, where system states, actions, and rewards jointly guide adaptive federated learning and blockchain operations.

Future research should concentrate on adaptive incentive models appropriate for heterogeneous IoT contexts, scalable FL architectures, and lightweight consensus procedures. Real-world implementation requires enhanced interoperability and standardised assessment. Future studies might investigate DRL-driven incentive models, for instance, in which incentives are dynamically modified according to client dependability, energy contribution, and update quality. High-quality and energy-efficient participants are rewarded more in such a system, whereas malicious or unreliable nodes are gradually penalised. Using DRL to adjust incentive mechanisms across heterogeneous IoT domains—for example, giving priority to energy-aware rewards in wearable healthcare systems and latency-sensitive awards in industrial IoT—is another interesting avenue. These illustrations show how clever incentive design can enhance sustainability, equity, and participation in federated learning enabled by blockchain technology. All things considered, the Hyper-Learning Framework offers a useful path towards obtaining scalable and secure distributed intelligence in IoAT systems.

Acknowledgement: We acknowledge that the assistance provided by VIT-AP University on the aspect of getting subscribed journal and conference articles to complete the review.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Priyanka Halder: Conceptualization, methodology, investigation, writing—original draft, review & editing. Gopikrishnan Sundaram: Conceptualization, supervision, methodology, review & editing. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors.

Ethics Approval: Not applicable.

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

References

1. Chen J, Wang Q, Cao X. FedTHQ: tensor-assisted heterogeneous model with quality-based aggregation for federated learning integrated IoT. IEEE Internet Things J. 2025;12(8):10453–62. doi:10.1109/JIOT.2024.3511635.
2. Khan LU, Saad W, Han Z, Hossain E, Hong CS. Federated learning for internet of things: recent advances, taxonomy, and open challenges. IEEE Commun Surv Tutor. 2021;23(3):1759–99. doi:10.1109/COMST.2021.3090430.
3. Chen Z, Tian P, Liao W, Chen X, Xu G, Yu W. Resource-aware knowledge distillation for federated learning. IEEE Trans Emerg Top Comput. 2023;11(3):706–19. doi:10.1109/TETC.2023.3252600.
4. Duan Q, Huang J, Hu S, Deng R, Lu Z, Yu S. Combining federated learning and edge computing toward ubiquitous intelligence in 6G network: challenges, recent advances, and future directions. IEEE Commun Surv Tutor. 2023;25(4):2892–950. doi:10.1109/COMST.2023.3316615.
5. Xu W, Yang Z, Ng DWK, Levorato M, Eldar YC, Debbah M. Edge learning for B5G networks with distributed signal processing: semantic communication, edge computing, and wireless sensing. IEEE J Select Top Signal Process. 2023;17(1):9–39. doi:10.1109/JSTSP.2023.3239189.

6. Bao W, Wu C, Guleng S, Zhang J, Yau KLA, Ji Y. Edge computing-based joint client selection and networking scheme for federated learning in vehicular IoT. China Commun. 2021;18(6):39–52. doi:10.23919/JCC.2021.06.004.
7. Wang J, Li J. Blockchain and access control encryption-empowered IoT knowledge sharing for cloud-edge orchestrated personalized privacy-preserving federated learning. Appl Sci. 2024;14(5):1743. doi:10.3390/app14051743.
8. Li R, Shu Y, Cao Y, Luo Y, Zuo Q, Wu X, et al. Federated cross-view e-commerce recommendation based on feature rescaling. Sci Rep. 2024;14(1):1–19. doi:10.1038/s41598-024-81278-1.
9. Zhang H, Bosch J, Olsson HH. Enabling efficient and low-effort decentralized federated learning with the EdgeFL framework. Inf Softw Tech. 2025;178(3):107600. doi:10.1016/j.infsof.2024.107600.
10. Zhao J, Zhu H, Wang F, Lu R, Liu Z, Li H. PVD-FL: a privacy-preserving and verifiable decentralized federated learning framework. IEEE Trans Inf Forensics Secur. 2022;17:2059–73. doi:10.1109/TIFS.2022.3176191.
11. Alam T, Gupta R, Ullah A, Qamar S. Blockchain-enabled federated reinforcement learning (B-FRL) model for privacy preservation service in IoT systems. Wirel Pers Commun. 2024;136(4):2545–71. doi:10.1007/s11277-024-11411-w.
12. Orabi MM, Emam O, Fahmy H. Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review. J Big Data. 2025;12(1):55. doi:10.1186/s40537-025-01099-5.
13. Chen Z, Cui H, Wu E, Yu X. Computation and communication efficient adaptive federated optimization of federated learning for internet of things. Electronics. 2023;12(16):3451. doi:10.3390/electronics12163451.
14. Zhao C, Gao Z, Yang Y, Wang Q, Mo Z, Yu X. FedUSC: collaborative unsupervised representation learning from decentralized data for internet of things. IEEE Internet Things J. 2023;10(15):13601–11. doi:10.1109/JIOT.2023.3262669.
15. Ni W, Zheng J, Tian H. Semi-federated learning for collaborative intelligence in massive IoT networks. IEEE Internet Things J. 2023;10(13):11942–3. doi:10.1109/JIOT.2023.3253853.
16. Li Z, Huang C, Gai K, Lu Z, Wu J, Chen L, et al. AsyFed: accelerated federated learning with asynchronous communication mechanism. IEEE Internet Things J. 2023;10(10):8670–83. doi:10.1109/JIOT.2022.3231913.
17. Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access. 2020;8:205071–87. doi:10.1109/ACCESS.2020.3037474.
18. Lazzarini R, Tianfield H, Charissis V. Federated learning for IoT intrusion detection. AI. 2023;4(3):509–30.
19. Alharbey RA, Jamil F. Federated learning framework for real-time activity and context monitoring using edge devices. Sensors. 2025;25(4):1266. doi:10.3390/s25041266.
20. Alam T, Gupta R. Federated learning and its role in the privacy preservation of IoT devices. Future Internet. 2022;14(9):246. doi:10.3390/fi14090246.
21. Nair AK, Raj ED, Sahoo J. A robust analysis of adversarial attacks on federated learning environments. Comput Stand Interfaces. 2023;86:103723. doi:10.1016/j.csi.2023.103723.
22. Bahadoripour S, Karimipour H, Jahromi AN, Islam A. An explainable multi-modal model for advanced cyber-attack detection in industrial control systems. Internet Things. 2024;25(4):101092. doi:10.1016/j.iot.2024.101092.
23. Xiao X, Tang Z, Li C, Xiao B, Li K. SCA: sybil-based collusion attacks of IIoT data poisoning in federated learning. IEEE Trans Ind Inform. 2023;19(3):2608–18.
24. Yang H, Gu D, He J. DeMAC: towards detecting model poisoning attacks in federated learning system. Internet Things. 2023;23(2):100875. doi:10.1016/j.iot.2023.100875.
25. Chatterjee P, Das D, Rawat DB. Digital twin for credit card fraud detection: opportunities, challenges, and fraud detection advancements. Future Gener Comput Syst. 2024;158(1):410–26. doi:10.1016/j.future.2024.04.057.
26. Liu X, Li H, Xu G, Chen Z, Huang X, Lu R. Privacy-enhanced federated learning against poisoning adversaries. IEEE Trans Inf Forensics Secur. 2021;16:4574–88. doi:10.1109/TIFS.2021.3108434.
27. Ren C, Yu H, Peng H, Tang X, Zhao B, Yi L, et al. Advances and open challenges in federated foundation models. IEEE Commun Surv Tutor. 2025;28(1):2087–126. doi:10.1109/comst.2025.3552524.
28. Kausar F, Deo S, Hussain S, Ul Haque Z. Federated deep learning model for false data injection attack detection in cyber physical power systems. Energies. 2024;17(21):5337. doi:10.3390/en17215337.

29. Yang Z, Shi Y, Zhou Y, Wang Z, Yang K. Trustworthy federated learning via blockchain. IEEE Internet Things J. 2023;10(1):92–109. doi:10.1109/JIOT.2022.3201117.
30. Witt L, Zafar U, Shen K, Sattler F, Li D, Wang S, et al. Decentralized and incentivized federated learning: a blockchain-enabled framework utilising compressed soft-labels and peer consistency. IEEE Trans Serv Comput. 2024;17(4):1449–64.
31. Ye Z, Luo W, Zhou Q, Zhu Z, Shi Y, Jia Y. Gradient inversion attacks: impact factors analyses and privacy enhancement. IEEE Trans Pattern Anal Mach Intell. 2024;46(12):9834–50. doi:10.1109/TPAMI.2024.3430533.
32. García-Márquez M, Rodríguez-Barroso N, Luzón MV, Herrera F. Improving (α, f)-Byzantine resilience in federated learning via layerwise aggregation and cosine distance. Knowl Based Syst. 2025;326:114004. doi:10.1016/j.knosys.2025.114004.
33. Kandah F, Mendis T, Medury L, Sherawat H, Wang H. Navigating IoT security: architectures, emerging threats, and adaptive countermeasures. IEEE Access. 2025;13(7):98888–908. doi:10.1109/ACCESS.2025.3576355.
34. Minoli D. Positioning of blockchain mechanisms in IoT-powered smart home systems: a gateway-based approach. Internet Things. 2020;10(2):100147. doi:10.1016/j.iot.2019.100147.
35. Aslam J, Lai KH, Hanbali AA, Khan NT. Blockchain solution for supply chains & logistics challenges: an empirical investigation. Transp Res Part E Logist Transp Rev. 2025;198:104134. doi:10.1016/j.tre.2025.104134.
36. Pradeep Kumar K, Prathap BR, Thiruthuvanathan MM, Murthy H, Jha Pillai V. Secure approach to sharing digitized medical data in a cloud environment. Data Sci Manag. 2024;7(2):108–18. doi:10.1016/j.dsm.2023.12.001.
37. Idrees SM, Nowostawski M, Jameel R, Mourya AK. Security aspects of blockchain technology intended for industrial applications. Electronics. 2021;10(8):951. doi:10.3390/electronics10080951.
38. An M, Zhang X, Wang J, Fan Q, Gao C, Li L, et al. RLChain: a DRL approach for blockchain performance optimization toward IIoT. IEEE Trans Netw Serv Manag. 2025;22(2):1629–45. doi:10.1186/s40537-025-01099-5.
39. Wen B, Wang Y, Ding Y, Zheng H, Qin B, Yang C. Security and privacy protection technologies in securing blockchain applications. Inf Sci. 2023;645(2):119322. doi:10.1016/j.ins.2023.119322.
40. Wang Y, Peng H, Su Z, Luan TH, Benslimane A, Wu Y. A platform-free proof of federated learning consensus mechanism for sustainable blockchains. IEEE J Select Areas Commun. 2022;40(12):3305–24.
41. Mahmood Z, Jusas V. Blockchain-enabled: multi-layered security federated learning platform for preserving data privacy. Electronics. 2022;11(10):1624.
42. Jia B, Zhang X, Liu J, Zhang Y, Huang K, Liang Y. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Trans Ind Inform. 2022;18(6):4049–58. doi:10.1109/TII.2021.3085960.
43. Ferrag MA, Friha O, Maglaras L, Janicke H, Shu L. Federated deep learning for cyber security in the internet of things: concepts, applications, and experimental analysis. IEEE Access. 2021;9:138509–42. doi:10.1109/access.2021.3118642.
44. Ghimire B, Rawat DB. Secure, privacy preserving, and verifiable federating learning using blockchain for internet of vehicles. IEEE Consum Electron Mag. 2022;11(6):67–74. doi:10.1109/MCE.2021.3097705.
45. Ouyang L, Wang FY, Tian Y, Jia X, Qi H, Wang G. Artificial identification: a novel privacy framework for federated learning based on blockchain. IEEE Trans Comput Soc Syst. 2023;10(6):3576–85. doi:10.1109/TCSS.2022.3226861.
46. Li D, Luo Z, Cao B. Blockchain-based federated learning methodologies in smart environments. Clust Comput. 2022;25(4):2585–99. doi:10.1007/s10586-022-03548-3.
47. Al Asqah M, Moulahi T. Federated learning and blockchain integration for privacy protection in the Internet of Things: challenges and solutions. Future Internet. 2023;15(6):203. doi:10.3390/fi15060203.
48. Cui L, Qu Y, Xie G, Zeng D, Li R, Shen S, et al. Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. IEEE Trans Ind Inform. 2022;18(5):3492–500. doi:10.1109/TII.2021.3107783.
49. Xu Y, Lu Z, Gai K, Duan Q, Lin J, Wu J, et al. BESIFL: blockchain-empowered secure and incentive federated learning paradigm in IoT. IEEE Internet Things J. 2023;10(8):6561–73. doi:10.1109/JIOT.2021.3138693.
50. Liu P, Li X, Zang B, Diao G. Privacy-preserving sports data fusion and prediction with smart devices in distributed environment. J Cloud Comput. 2024;13(1):106. doi:10.1186/s13677-024-00478-9.

51. Saidi A, Amira A, Nouali O. Securing decentralized federated learning: cryptographic mechanisms for privacy and trust. Clust Comput. 2025;28(2):1–17. doi:10.1007/s10586-024-04890-1.
52. Alwabli A. Federated learning for privacy-preserving air quality forecasting using IoT sensors. Eng Technol Appl Sci Res. 2024;14(4):16069–76. doi:10.48084/etasr.6625.
53. Long G, Tan Y, Jiang J, Zhang C. Federated learning for open banking. In: Jiang J, Zhang C, editors. Federated learning: privacy and incentive. Cham, Switzerland: Springer; 2020. p. 240–54. doi:10.1007/978-3-030-47682-8_14.
54. Shu J, Yang T, Liao X, Chen F, Xiao Y, Yang K, et al. Clustered federated multitask learning on Non-IID Data with enhanced privacy. IEEE Internet Things J. 2023;10(4):3453–67. doi:10.1109/JIOT.2022.3228893.
55. Cao X, Sun G, Yu H, Guizani M. PerFED-GAN: personalized federated learning via generative adversarial networks. IEEE Internet Things J. 2023;10(5):3749–62. doi:10.1109/JIOT.2022.3172114.
56. Korkmaz C, Kocas HE, Uysal A, Masry A, Ozkasap O, Akgun B, et al. Chain FL: decentralized federated machine learning via blockchain. In: 2020 Second International Conference on Blockchain Computing and Applications (BCCA). Piscataway, NJ, USA: IEEE; 2020. p. 140–6. doi:10.1109/BCCA50787.2020.9274451.
57. Kundroo M, Kim T. Federated learning with hyper-parameter optimization. J King Saud Univ Comput Inf Sci. 2023;35(9):101740. doi:10.1016/j.jksuci.2023.101740.
58. Fu L, Zhang H, Gao G, Zhang M, Liu X. Client selection in federated learning: principles, challenges, and opportunities. IEEE Internet Things J. 2023;10(24):21811–9.
59. Ficco M, Guerriero A, Milite E, Palmieri F, Pietrantuono R, Russo S. Federated learning for IoT devices: enhancing TinyML with on-board training. Inf Fusion. 2024;104:102189. doi:10.1016/j.inffus.2023.102189.
60. Bouacida N, Mohapatra P. Vulnerabilities in federated learning. IEEE Access. 2021;9:63229–49. doi:10.1109/access.2021.3075203.
61. Yaacoub JPA, Noura HN, Salman O. Security of federated learning with IoT systems: issues, limitations, challenges, and solutions. Internet Things Cyber Phys Syst. 2023;3:155–79. doi:10.1016/j.iotcps.2023.04.001.
62. Aziz R, Banerjee S, Bouzefrane S, Le Vinh T. Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm. Future Internet. 2023;15(9):310. doi:10.3390/fi15090310.
63. Yin X, Wu X, Zhang X. A trusted federated learning method based on consortium blockchain. Information. 2025;16(1):14. doi:10.3390/info16010014.
64. Yang Z, Cheng C, Li Z, Wang R, Zhang X. Reliable federated learning based on delayed gradient aggregation for intelligent connected vehicles. Eng Appl Artif Intell. 2025;140:109719. doi:10.1016/j.engappai.2024.109719.
65. Begum K, Mozumder MAI, Joo MI, Kim HC. BFLIDS: blockchain-driven federated learning for intrusion detection in IoMT networks. Sensors. 2024;24(14):4591. doi:10.3390/s24144591.
66. Yang Q, Huang A, Fan L, Chan CS, Lim JH, Ng KW, et al. Federated learning with privacy-preserving and model IP-right-protection. Mach Intell Res. 2023;20(1):19–37. doi:10.1007/s11633-022-1343-2.
67. Li Y, Wang S, Chi CY, Quek TQS. Differentially private federated clustering over non-IID data. IEEE Internet Things J. 2024;11(4):6705–21. doi:10.1109/JIOT.2023.3312852.
68. Castro F, Impedovo D, Pirlo G. An efficient and privacy-preserving federated learning approach based on homomorphic encryption. IEEE Open J Comput Soc. 2025;6:336–47. doi:10.1109/OJCS.2025.3536562.
69. Li Y, Yan N, Chen J, Wang X, Hong J, He K, et al. FedPHE: a secure and efficient federated learning via packed homomorphic encryption. IEEE Trans Dependable Secur Comput. 2025;22(5):5448–63. doi:10.1109/TDSC.2025.3567301.
70. Xiong R, Ren W, Hao X, He J, Choo KKR. BDIM: a blockchain-based decentralized identity management scheme for large scale internet of things. IEEE Internet Things J. 2023;10(24):22581–90. doi:10.1109/JIOT.2023.3303922.
71. Mothukuri V, Parizi RM, Pouriyeh S, Dehghantanha A, Choo KKR. FabricFL: blockchain-in-the-loop federated learning for trusted decentralized systems. IEEE Syst J. 2022;16(3):3711–22. doi:10.1109/JSYST.2021.3124513.
72. Fan M, Ji K, Zhang Z, Yu H, Sun G. Lightweight privacy and security computing for blockchained federated learning in IoT. IEEE Internet Things J. 2023;10(18):16048–60. doi:10.1109/JIOT.2023.3267112.
73. Riahi A, Mohamed A, Erbad A. RL-based federated learning framework over blockchain (RL-FL-BC). IEEE Trans Netw Serv Manag. 2023;20(2):1587–99. doi:10.1109/TNSM.2023.3241437.

74. Salama A, Stergioulis A, Zaidi SAR, McLernon D. Decentralized federated learning on the edge over wireless mesh networks. IEEE Access. 2023;11(21):124709–24. doi:10.1109/ACCESS.2023.3329362.
75. Okegbile SD, Cai J, Zheng H, Chen J, Yi C. Differentially private federated multi-task learning framework for enhancing human-to-virtual connectivity in human digital twin. IEEE J Select Areas Commun. 2023;41(11):3533–47. doi:10.1109/JSAC.2023.3310106.
76. Tong Z, Wang J, Hou X, Chen J, Jiao Z, Liu J. Blockchain-based trustworthy and efficient hierarchical federated learning for UAV-enabled IoT networks. IEEE Internet Things J. 2024;11(21):34270–82. doi:10.1109/JIOT.2024.3370964.
77. Jiang L, Liu Y, Tian H, Tang L, Xie S. Resource-efficient federated learning and DAG blockchain with sharding in digital-twin-driven industrial IoT. IEEE Internet Things J. 2024;11(10):17113–27. doi:10.1109/JIOT.2024.3357827.
78. Kalapaaking AP, Khalil I, Atiquzzaman M. Blockchain-enabled and multisignature-powered verifiable model for securing federated learning systems. IEEE Internet Things J. 2023;10(24):21410–20. doi:10.1109/JIOT.2023.3289832.
79. Agarwal N, Joshi S. Federated learning-based task offloading in a UAV-aided cloud computing mobile network. IEEE Trans Veh Technol. 2024;73(10):15751–6. doi:10.1109/TVT.2024.3404223.
80. Truhn D, Tayebi Arasteh S, Saldanha OL, Müller-Franzes G, Khader F, Quirke P, et al. Encrypted federated learning for secure decentralized collaboration in cancer image analysis. Med Image Anal. 2024;92:103059. doi:10.1016/j.media.2023.103059.
81. Zhou M, Yang Z, Yu H, Yu S. VDFChain: secure and verifiable decentralized federated learning via committee-based blockchain. J Netw Comput Appl. 2024;223(3):103814. doi:10.1016/j.jnca.2023.103814.
82. Sameera KM, Nicolazzo S, Arazzi M, Nocera A, Rafidha Rehiman KA, Vinod P, et al. Privacy-preserving in blockchain-based federated learning systems. Comput Commun. 2024;222(4):38–67. doi:10.1016/j.comcom.2024.04.024.
83. Tariq A, Serhani MA, Sallabi FM, Barka ES, Qayyum T, Khater HM, et al. Trustworthy federated learning: a comprehensive review, architecture, key challenges, and future research prospects. IEEE Open J Commun Soc. 2024;5:4920–98. doi:10.1109/OJCOMS.2024.3438264.
84. Kasyap H, Manna A, Tripathy S. An efficient blockchain assisted reputation aware decentralized federated learning framework. IEEE Trans Netw Serv Manag. 2023;20(3):2771–82. doi:10.1109/TNSM.2022.3231283.
85. Huang X, Han L, Li D, Xie K, Zhang Y. A reliable and fair federated learning mechanism for mobile edge computing. Comput Netw. 2023;226(22):109678. doi:10.1016/j.comnet.2023.109678.
86. Milne AJM, Beckmann A, Kumar P. Cyber-physical trust systems driven by blockchain. IEEE Access. 2020;8:66423–37. doi:10.1109/ACCESS.2020.2984675.
87. Rouhani S, Deters R. Data trust framework using blockchain technology and adaptive transaction validation. IEEE Access. 2021;9:90379–91. doi:10.1109/ACCESS.2021.3091327.
88. Gong Q, Zhang J, Wei Z, Wang X, Zhang X, Yan X, et al. SDACS: blockchain-based secure and dynamic access control scheme for internet of things. Sensors. 2024;24(7):2267. doi:10.3390/s2407226.
89. Xu M, Zhao F, Zou Y, Liu C, Cheng X, Dressler F. BLOWN: a blockchain protocol for single-hop wireless networks under adversarial SINR. IEEE Trans Mob Comput. 2023;22(8):4530–47. doi:10.1109/TMC.2022.3162117.
90. Liu H, Crespo RG, Martínez OS. Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. Healthcare. 2020;8(3):243. doi:10.3390/healthcare8030243.
91. Yadav AS, Singh N, Kushwaha DS. Evolution of Blockchain and consensus mechanisms & its real-world applications. Multimed Tools Appl. 2023;82(22):34363–408. doi:10.1007/s11042-023-14624-6.
92. Daah C, Qureshi A, Awan I, Konur S. Enhancing zero trust models in the financial industry through blockchain integration: a proposed framework. Electronics. 2024;13(5):865. doi:10.3390/electronics13050865.
93. Jamil H, Qayyum F, Iqbal N, Khan MA, Naqvi SSA, Khan S, et al. Secure hydrogen production analysis and prediction based on blockchain service framework for intelligent power management system. Smart Cities. 2023;6(6):3192–224. doi:10.3390/smartcities6060142.
94. Cao M, Zhang L, Cao B. Toward on-device federated learning: a direct acyclic graph-based blockchain approach. IEEE Trans Neural Netw Learn Syst. 2021;34(4):2028–42. doi:10.1109/TNNLS.2021.3083508.

95. Yang G, Lee K, Lee K, Yoo Y, Lee H, Yoo C. Resource analysis of blockchain consensus algorithms in Hyperledger Fabric. IEEE Access. 2022;10:74902–20. doi:10.1109/ACCESS.2022.3190979.
96. Xu S, Liu S, He G. A method of federated learning based on blockchain. In: Proceedings of the 5th International Conference on Computer Science and Application Engineering. New York, NY, USA: Association for Computing Machinery; 2021. p. 1–8. doi:10.1145/3487075.3487143.
97. Yuan S, Cao B, Peng M, Sun Y. ChainsFL: blockchain-driven federated learning from design to realization. In: 2021 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway, NJ, USA: IEEE; 2021. p. 1–6. doi:10.1109/WCNC49053.2021.9417299.
98. Alhartomi MA, Salh A, Audah L, Alzahrani S, Alzahmi A, Altimania MR, et al. Sustainable resource allocation and reduce latency based on federated-learning-enabled digital twin in IoT devices. Sensors. 2023;23(16):7262. doi:10.3390/s23167262.
99. Chen Z, Cui H, Luan Q, Xi Y. Efficient adaptive federated learning in resource-constrained IoT environments. In: GLOBECOM 2023—2023 IEEE Global Communications Conference. Piscataway, NJ, USA: IEEE; 2023. p. 1896–901.
100. Kably S, Arioua M, Alaoui N. Lightweight direct acyclic graph blockchain for enhancing resource-constrained IoT environment. Comput Mater Contin. 2022;70(2):2801–19. doi:10.32604/cmc.2022.0208335.
101. Wankhede SB, Patel D. Federated learning and blockchain approach for securing IoT data. Discov Internet Things. 2025;5(1):116. doi:10.1007/s43926-025-00234-1.
102. Alsunaidi SJ, Alhaidari FA. A survey of consensus algorithms for blockchain technology. In: 2019 International Conference on Computer and Information Sciences (ICCIS). Piscataway, NJ, USA: IEEE; 2019. p. 1–6.
103. Bach LM, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Piscataway, NJ, USA: IEEE; 2018. p. 1545–50.
104. Ahn J, Yi E, Kim M. Blockchain consensus mechanisms: a bibliometric analysis (2014–2024) using vosviewer and R bibliometrix. Information. 2024;15(10):644. doi:10.3390/info15100644.
105. Meshcheryakov Y, Melman A, Evsutin O, Morozov V, Koucheryavy Y. On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices. IEEE Access. 2021;9(1):80559–70. doi:10.1109/access.2021.3085405.
106. Chaudhry N, Yousaf MM. Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST). Piscataway, NJ, USA: IEEE; 2018. p. 54–63.
107. Li W, He M, Sang H. An overview of blockchain technology: applications, challenges and future trends. In: 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC). Piscataway, NJ, USA: IEEE; 2021. p. 31–9.
108. Bataineh MR, Mardini W, Khamayseh YM, Yassein MMB. Novel and secure blockchain framework for health applications in IoT. IEEE Access. 2022;10(7):14914–26. doi:10.1109/access.2022.3147795.
109. Adhikari N, Ramkumar M. IoT and blockchain integration: applications, opportunities, and challenges. Network. 2023;3(1):115–41. doi:10.3390/network3010007.
110. Honar Pajooh H, Rashid M, Alam F, Demidenko S. Hyperledger fabric blockchain for securing the edge internet of things. Sensors. 2021;21(2):359. doi:10.3390/s21020359.
111. Wang Y, Wu Z. Blockchain-based multidimensional trust management in edge computing. IEEE Access. 2023;11(3):122736–48. doi:10.1109/ACCESS.2023.3329126.
112. Shelke K, Dakshayani G. A sliding window blockchain architecture for the internet of things. In: 2022 5th International Conference on Advances in Science and Technology (ICAST); 2022 Dec 2–3; Mumbai, India. p. 45–8. doi:10.1109/ICAST55766.2022.10039664.
113. Alrubei SM, Ball EA, Rigelsford JM, Willis CA. Latency and performance analyses of real-world wireless IoT-blockchain application. IEEE Sens J. 2020;20(13):7372–83. doi:10.1109/JSEN.2020.2983861.
114. Singh M, Singh A, Kim S. Blockchain: a game changer for securing IoT data. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT); 2018 Feb 5–8; Singapore. p. 51–5. doi:10.1109/WF-IoT.2018.8355182.

115. Tayade SN, Gulhane VA. Designing of macro-femto heterogeneous network for improving energy efficiency of cellular system. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET); 2016 Mar 23–25; Chennai, India. p. 695–8. doi:10.1109/WiSPNET.2016.7566222.
116. Coskun CC, Davaslioglu K, Ayanoglu E. Three-stage resource allocation algorithm for energy-efficient heterogeneous networks. IEEE Trans Veh Technol. 2017;66(8):6942–57. doi:10.1109/TVT.2016.2633970.
117. Della Penda D, Fu L, Johansson M. Energy efficient D2D communications in dynamic TDD systems. IEEE Trans Commun. 2016;65(3):1260–73. doi:10.1109/TCOMM.2016.2637354.
118. Algedir AA, Refai HH. Energy efficiency optimization and dynamic mode selection algorithms for D2D communication under HetNet in downlink reuse. IEEE Access. 2020;8:95251–65. doi:10.1109/ACCESS.2020.2995541.
119. Lee YL, Wang LC, Chuah TC, Loo J. Joint resource allocation and user association for heterogeneous cloud radio access networks. In: 2016 28th International Teletraffic Congress (ITC 28). Piscataway, NJ, USA: IEEE; 2016. p. 87–93. doi:10.1109/ITC-28.2016.120.
120. Sukanesh R, Edsor E, Aarthylakshmi M. Energy efficient malicious node detection scheme in wireless networks. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO). Piscataway, NJ, USA: IEEE; 2016. p. 1–6. doi:10.1109/ISCO.2016.7726997.
121. Do QV, Pham QV, Hwang WJ. Deep reinforcement learning for energy-efficient federated learning in UAV-enabled wireless powered networks. IEEE Commun Lett. 2022;26(1):99–103. doi:10.1109/LCOMM.2021.3122129.
122. Zhao T, Li F, He L. DRL-based joint resource allocation and device orchestration for hierarchical federated learning in NOMA-enabled industrial IoT. IEEE Trans Ind Inform. 2023;19(6):7468–79. doi:10.1109/TII.2022.3170900.
123. Ahmed TH, Tiang JJ, Mahmud A, Do DT, Tran T, Mumtaz S. V2V communications using blockchain-enabled 6G technology and federated learning. In: GLOBECOM 2023—2023 IEEE Global Communications Conference. Piscataway, NJ, USA: IEEE; 2023. p. 1302–7. doi:10.1109/GLOBECOM54140.2023.10437406.
124. Soykan B, Rabadi G. Optimizing multi commodity flow problem under uncertainty: a deep reinforcement learning approach. In: 2023 International Conference on Machine Learning and Applications (ICMLA). Piscataway, NJ, USA: IEEE; 2023. p. 1267–72. doi:10.1109/ICMLA58977.2023.00191.
125. Hou X, Wang J, Jiang C, Zhang X, Ren Y, Debbah M. UAV-enabled covert federated learning. IEEE Trans Wirel Commun. 2023;22(10):6793–809. doi:10.1109/TWC.2023.3245621.
126. Lu Z, Zhong C, Gursoy MC. Dynamic channel access and power control in wireless interference networks via multi-agent deep reinforcement learning. IEEE Trans Veh Technol. 2022;71(2):1588–601. doi:10.1109/TVT.2021.3131534.
127. Gu X, Wu Q, Fan P, Fan Q, Cheng N, Chen W, et al. DRL-based resource allocation for motion blur resistant federated self-supervised learning in IoV. IEEE Internet Things J. 2025;12(6):7067–85. doi:10.1109/JIOT.2024.3492326.