International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

Decentralized Federated Learning Framework with Blockchain-based Incentive and Reputation Mechanism

Tushar Waykole[1], Deven Randhir[2], Mrunal Patil[3], Swapnil Durafe[4]
[1,2,3,4]Dept. of Computer Engineering, Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra, India.
Email ID: *tushar.waykole@nmiet.edu.in[1], devenrandhir9821@gmail.com[2], mrunalp220@gmail.com[3], swapnildurafe1702@gmail.com[4]*

Abstract
Federated Learning (FL) enables collaborative model training while preserving data privacy but relies on centralized aggregation servers, leading to issues such as lack of transparency, vulnerability to malicious updates, and single points of failure. This paper proposes a decentralized federated learning framework integrating blockchain technology and the InterPlanetary File System (IPFS) to eliminate central authority and enhance trust. Smart contracts deployed on the Ethereum Sepolia testnet manage model submission, validation, incentive distribution, and reputation tracking. Model updates are stored off-chain using IPFS, while their hashes are recorded on the blockchain to ensure integrity and immutability. A staking and slashing mechanism is introduced to encourage honest participation, where valid contributions are rewarded and malicious updates are penalized. A reputation system further evaluates participant reliability over time. The system is implemented using PyTorch, Solidity, Web3.py, and React.js. Experimental results demonstrate improved security, transparency, and efficient decentralized coordination, highlighting the feasibility of integrating federated learning with blockchain and decentralized storage for scalable and trustworthy machine learning applications.

Keywords: *Blockchain, Federated Learning, Artificial Intelligence, Collaborative Machine Learning.*

1. Introduction
Machine learning has become a core component of modern intelligent systems, supporting applications in healthcare, finance, autonomous systems, and smart cities. These models typically require large and diverse datasets, which are traditionally collected and processed on centralized servers. However, this approach raises significant concerns related to data privacy, security, and regulatory compliance. To address these challenges, Federated Learning (FL) has emerged as a decentralized paradigm that enables multiple clients to collaboratively train a global model without sharing raw data. Initially introduced by McMahan et al. (2017), FL allows participants to train models locally and share only model updates with a central aggregator. While this approach improves privacy, it still relies on a centralized server, leading to issues such as single points of failure, lack of transparency, and vulnerability to malicious updates. Blockchain technology provides a promising solution by offering a decentralized, immutable, and transparent ledger. Blockchain provides a decentralized and immutable ledger for secure transactions (Zheng et al., 2017; Casino et al., 2019). Integrating blockchain with federated learning eliminates the need for a central authority and ensures that operations such as model submission, validation, and reward distribution are recorded in a tamper-proof manner. Smart contracts further automate these processes, enabling trustless and fair interactions (Nakamoto, 2008; Buterin, 2014). However, storing model parameters directly on-chain is impractical due to high computational and storage costs. To overcome this limitation, decentralized storage systems such as the InterPlanetary File System (IPFS) are used to store model updates off-chain, while only their hashes are recorded on the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

blockchain to ensure data integrity. In this paper, we propose a decentralized federated learning framework that integrates blockchain and IPFS with incentive and reputation mechanisms. The system incorporates staking and slashing to promote honest participation and penalize malicious behavior, along with a reputation system to evaluate participant reliability. The key contributions of this work are:

- Design and implementation of a decentralized federated learning architecture using blockchain.
- Integration of IPFS for scalable storage of model updates.
- Development of a smart contract-based incentive mechanism with staking and rewards.
- Implementation of a reputation system for participant evaluation.
- Demonstration of a working prototype using PyTorch, Solidity, Web3.py, and React.js

The remainder of the paper is organized as follows: Section 2 reviews related work, Section 3 describes the system architecture, Section 4 explains the methodology, Section 5 presents implementation details, Section 6 discusses results, and Section 7 concludes the paper.[1]

2. Literature Review

Federated Learning (FL) has emerged as a privacy-preserving machine learning paradigm that enables collaborative model training without sharing raw data. In this approach, clients train models locally and share updates with a central server for aggregation. Foundational work by McMahan et al. (2017) introduced the Federated Averaging (FedAvg) algorithm, which remains widely used. However, traditional FL systems rely on centralized aggregation, leading to challenges such as lack of transparency, single points of failure, and vulnerability to malicious updates. Recent studies further analyze scalability and communication challenges in FL systems (Kairouz et al., 2021; Bonawitz et al., 2019). To address these limitations, blockchain technology has been integrated with federated learning to provide decentralization, transparency, and tamper-proof record keeping. Blockchain-based FL systems eliminate the need for a central authority by recording model updates on a distributed ledger. Kim et al. (2020) proposed a blockchain-enabled FL framework using smart contracts for managing updates, while Li et al. (2021) explored secure aggregation through decentralized architectures. However, these approaches face challenges such as high computational overhead and limited scalability. Further research has focused on improving communication efficiency and robustness in federated learning systems (Chen et al., 2021). Reputation-based mechanisms have also been proposed to evaluate participant reliability, where trust scores are assigned based on historical contributions (Kang et al., 2019). Although these methods improve reliability, they often lack strong incentive and penalty mechanisms to handle malicious participants effectively. To overcome storage limitations of blockchain, decentralized storage solutions such as the InterPlanetary File System (IPFS) have been integrated into FL systems. IPFS enables efficient off-chain storage using content-addressed data, significantly reducing blockchain overhead (Benet, 2014). Despite these advancements, existing approaches still face challenges related to scalability, computational cost, incentive design, and practical implementation. In contrast, the proposed system integrates federated learning, blockchain, IPFS, incentive mechanisms, and reputation systems into a unified and practical framework, addressing key limitations of existing solutions.[2]- [5]

3. System Architecture

The proposed system eliminates centralized aggregation by integrating blockchain and decentralized storage. It consists of four layers: Client Layer, Storage Layer (IPFS), Blockchain Layer, and Application Layer.

3.1.Client Layer

The client layer consists of distributed participants that train machine learning models locally using private datasets. Model parameters are stored as local files (e.g., pth) and prepared for submission.

Key functions:

- Local model training.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

- Model update generation.
- Submission to IPFS and blockchain

3.2.Storage Layer (IPFS)

The storage layer uses IPFS for decentralized storage of model updates. Since blockchain is inefficient for large files, model data is stored off-chain, while only content identifiers (CIDs) are recorded on-chain.

Key functions:

- Off-chain storage of model files.
- Generation of unique CIDs.
- Ensuring data integrity and availability.

3.3.Blockchain Layer

The blockchain layer is implemented using a smart contract on the Ethereum Sepolia testnet. Blockchain-based architectures enhance transparency and eliminate central authority (Lu, 2019; Zhang & Wen, 2017).[6]

Key functions:

- Recording model submissions.
- Managing validation and finalization.
- Handling incentives and reputation.
- Enforcing staking and penalty mechanisms

Each submission is recorded as a transaction, ensuring transparency and immutability. Accepted updates are rewarded, while invalid ones are penalized. Smart contracts enable automated and trustless operations (Buterin, 2014; Wood, 2014).

3.4.Application Layer

The application layer provides a React.js-based dashboard for user interaction. Users can connect wallets and monitor system activity.

Key features:

- Display wallet address, balance, and reputation.
- Track submitted updates.
- Visualize system workflow.

3.5.System Workflow

The system follows this workflow: Client → Training → IPFS Upload → Blockchain Submission → Validation → Finalization → Aggregation

Steps:

1.Client trains local model.
2.Model uploaded to IPFS (CID generated).
3.CID submitted to blockchain.
4.Validator evaluates update.
5.Update accepted or rejected.
6.Rewards/penalties applied.
7.Accepted updates aggregated into global model.

3.6.Architectural Advantages

- Decentralization: Removes central server dependency.
- **Privacy:** No raw data sharing.
- **Scalability:** Off-chain storage reduces load.
- **Transparency:** Immutable blockchain records.
- **Security:** Staking and reputation prevent malicious behavior. As Shown in Figure 1.

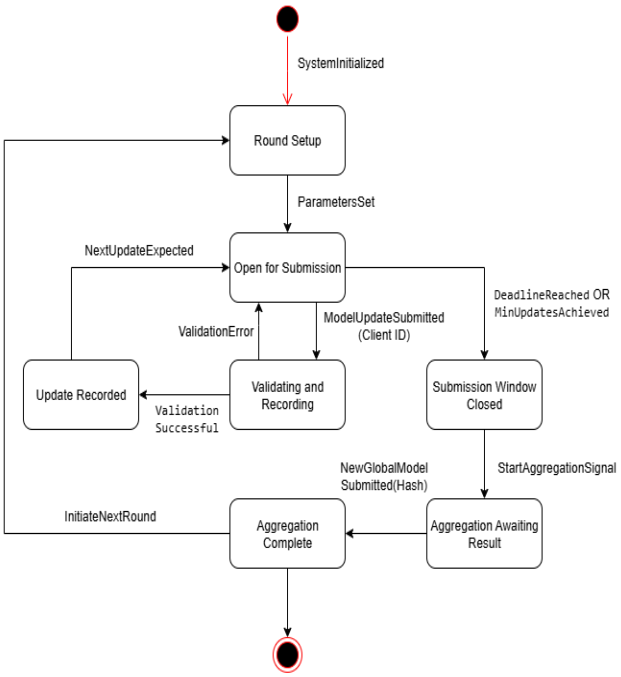

Figure 1 UML Diagram for Decentralized Federated Learning

4. Proposed Methodology

The proposed system introduces a decentralized federated learning framework that integrates blockchain technology and IPFS to ensure secure, transparent, and incentive-driven collaboration among distributed clients. The methodology is designed to address the limitations of traditional federated learning systems by eliminating central authority, incorporating trust mechanisms, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

enabling efficient model aggregation. The overall methodology consists of multiple sequential phases, including local training, decentralized storage, blockchain-based submission, validation, incentive distribution, and aggregation. [6] Each phase is described in detail below.

4.1.Local Model Training

In the proposed system, each client independently trains a machine learning model using its local dataset. This ensures that sensitive data remains private and is never shared with other participants or any central entity. The model training process is implemented using the PyTorch framework. Each client initializes a model and performs training over its dataset using stochastic gradient descent (SGD) or similar optimization techniques. [7] After training, the model parameters are saved locally in a serialized format (e.g., pth file).

This phase ensures:

- Data privacy preservation
- Distributed computation
- Reduced communication overhead

4.2.Model Upload to IPFS

After local training, the generated model file is uploaded to the Interplanetary File System (IPFS) using a pinning service such as Pinata. IPFS is a decentralized storage system that stores files using content-based addressing. Upon uploading the model, IPFS generates a unique Content Identifier (CID), which acts as a cryptographic hash of the file. This CID ensures that any modification in the file will result in a different hash, thereby guaranteeing data integrity. Only the CID is used for further processing, while the actual model file remains stored off-chain. This approach significantly reduces blockchain storage costs.[8]- [12]

4.3.Blockchain-based Model Submission

The client submits the IPFS hash to the blockchain through a smart contract. To ensure commitment and discourage malicious behavior, each submission requires a predefined stake in the form of tokens.

The submission process involves:

- Creating a transaction containing the IPFS hash.
- Sending the transaction to the smart contract.
- Recording the submission on the blockchain.

Each submission is assigned a unique identifier and stored in the smart contract along with the sender's address and stake amount.

4.4.Validation Mechanism

Once a model update is submitted, it enters the validation phase. In this phase, a validator evaluates the quality of the submitted model update.

The validation process can be based on:

- Accuracy improvement on a test dataset.
- Consistency with previous updates.
- Threshold-based evaluation

For the purpose of implementation, a simplified validation mechanism is used, where updates are either accepted or rejected based on predefined criteria.[13]

- If the update is **valid**, it is marked as accepted.
- If the update is **invalid or malicious**, it is rejected.

This phase ensures the integrity and quality of contributions.

4.5.Incentive and Penalty Mechanism

To encourage honest participation, the system incorporates a token-based incentive mechanism. Participants are rewarded for valid contributions and penalized for malicious behavior.

- **Accepted Updates:**
  - Stake is returned.
  - Additional reward tokens are granted.
  - Reputation score is increased
- **Rejected Updates:**
  - Stake is partially or fully slashed.
  - Reputation score is decreased

This mechanism ensures that participants are economically motivated to contribute high-quality updates.

4.6.Reputation System

A reputation system is maintained for each participant to evaluate their historical performance. The reputation score is updated dynamically based on the outcomes of submitted updates.

- Positive contributions → Increase reputation.
- Negative contributions → Decrease reputation

The reputation system helps in:

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

- Identifying reliable participants.
- Reducing the impact of malicious users.
- Enhancing trust within the network.

4.7.Finalization Process

After validation, accepted updates undergo a finalization process. During this phase:

- Rewards are distributed to the contributor.
- Reputation is updated.
- The update is marked as finalized.

Finalization ensures that each update is processed only once and prevents duplication or repeated rewards.[14]

4.8.Model Aggregation

The final phase of the methodology involves aggregating multiple accepted model updates to generate a global model. The aggregation process follows the Federated Averaging (FedAvg) algorithm, which computes a weighted average of client updates (McMahan et al., 2017).

In this process:

- Model parameters from multiple clients are collected.
- Parameters are averaged to produce a global model.
- The global model represents collective knowledge.
- The global model is computed as: $W = \Sigma (ni * wi) / \Sigma ni$

The aggregation process ensures:

- Improved model performance.
- Generalization across multiple datasets.
- Efficient collaboration without data sharing

4.9.Overall Algorithmic Flow

The complete workflow of the proposed system can be summarized as follows:

1. Initialize client models.
2. Train models locally.
3. Upload trained model to IPFS.
4. Obtain IPFS hash (CID).
5. Submit hash to blockchain with stake.
6. Validate submitted update.
7. Accept or reject update.
8. Apply reward or penalty.
9. Finalize accepted updates.
10. Aggregate models to form global model

The proposed methodology effectively integrates federated learning with blockchain and decentralized storage, ensuring privacy, transparency, and incentivized participation. By combining these technologies, the system addresses key challenges in traditional federated learning and provides a scalable and trustworthy solution for distributed machine learning.

5. Implementation Details

The proposed system is implemented as a functional prototype integrating machine learning, blockchain, decentralized storage, and a web-based interface. The backend is developed using Python, while the frontend uses JavaScript. PyTorch is used for model training, and Solidity is used for smart contract development. The smart contract is deployed on the Ethereum Sepolia testnet using Hardhat. Blockchain interactions are handled using Web3.py in the backend and Ethers.js in the frontend. IPFS is used for decentralized storage via the Pinata API, and the frontend dashboard is developed using React.js with MetaMask integration. The smart contract serves as the core component, managing model submissions, validation, incentive distribution, and reputation tracking. Each submission stores the IPFS hash, contributor address, stake, and validation status. A staking mechanism ensures commitment, while accepted updates are rewarded and rejected updates are penalized. The backend consists of Python scripts simulating different roles in the system. Clients perform local model training using PyTorch and upload trained models to IPFS, which returns a unique CID. This CID is submitted to the blockchain via signed transactions. Validator scripts evaluate updates and record results, while finalization scripts distribute rewards and update reputation. An aggregation script combines accepted updates using the Federated Averaging (FedAvg) algorithm to generate a global model. The frontend dashboard provides an interactive interface for users to connect their MetaMask wallet and view information such as account address, token balance, reputation, and system activity. It also displays the status of model submissions and the federated learning pipeline. The system is deployed in a controlled environment, with the smart contract running on the Sepolia testnet and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

backend scripts executed via the command line. During implementation, challenges such as asynchronous transaction handling, nonce conflicts, and frontend-backend integration were addressed through proper debugging and configuration. Overall, the implementation demonstrates the practical feasibility of integrating federated learning, blockchain, and IPFS into a unified system for secure, transparent, and privacy-preserving collaborative machine learning. As Shown in Figure 2 & 3.[15]

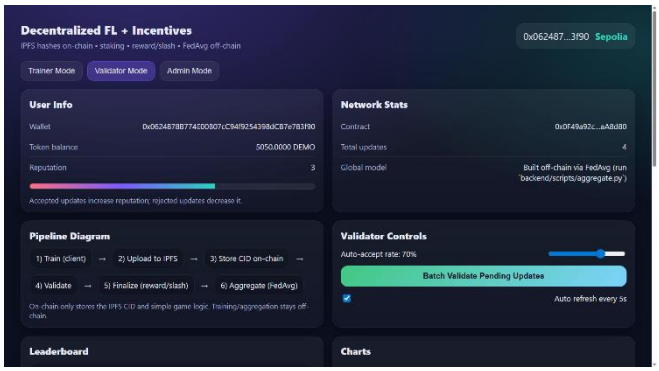

Figure 2 Validator Node Dashboard

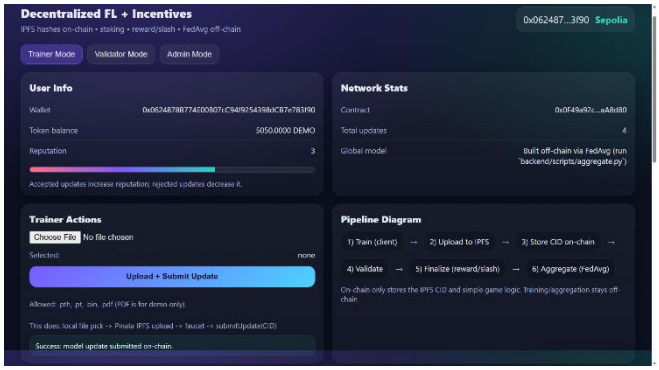

Figure 3 Trainer Node Dashboard

6. Results and Analysis

The proposed decentralized federated learning system was implemented and evaluated to assess its functionality, performance, and reliability. The evaluation verifies the integration of machine learning, blockchain, and decentralized storage, along with the effectiveness of incentive and reputation mechanisms. Blockchain improves security and trust but introduces scalability challenges (Khan & Salah, 2018).

6.1. Experimental Setup

The system was tested in a simulated multi-client environment. Each client trained a local model using PyTorch, uploaded it to IPFS, and submitted the corresponding hash to the Ethereum Sepolia blockchain. Backend scripts simulated submission, validation, and aggregation, while the frontend dashboard was used for monitoring system activity.

6.2. Model Training Performance

Local training was successfully performed without sharing raw data. Model accuracy improved consistently across iterations, demonstrating the feasibility of decentralized training.

6.3. IPFS Storage Evaluation

IPFS integration enabled efficient storage of model files. Each upload generated a unique CID, ensuring data integrity and reducing blockchain storage overhead.

Key observations:

- Successful model uploads to IPFS.
- Generation of immutable content hashes.
- Reduced on-chain storage requirements

6.4. Blockchain Transaction Analysis

All operations, including submission, validation, and finalization, were successfully executed on the Sepolia testnet.

Key observations:

- Immutable transaction records.
- Correct smart contract execution.
- Minimal gas costs (testnet).
- Proper nonce handling

6.5. Incentive and Reputation Evaluation

The incentive mechanism rewarded valid contributions and penalized malicious updates.

- **Accepted updates** → increased tokens and reputation.
- **Rejected updates** → reduced stake and reputation

The reputation system effectively identified reliable participants.[16]

6.6. Multi-Client Simulation

The system handled multiple client submissions efficiently without conflicts.

Key observations:

- Correct recording of multiple updates.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

- Successful validation and finalization.
- No data conflicts due to proper nonce handling

6.7.Aggregation Results

Model aggregation using the Federated Averaging (FedAvg) algorithm produced a global model with improved generalization compared to individual models.

6.8.System Performance

- **Scalability:** Improved via IPFS-based off-chain storage.
- **Security:** Ensured through blockchain immutability and staking.
- **Transparency:** Achieved through verifiable transactions.
- **Efficiency:** Maintained via lightweight validation

6.9.Discussion

The results demonstrate successful integration of federated learning, blockchain, and decentralized storage. The system ensures privacy, transparency, and robustness against malicious behavior. Although tested on a simplified setup, the architecture can be extended to real-world applications requiring secure and decentralized collaborative learning.

Conclusion and Future Work

In this paper, a decentralized federated learning framework integrated with blockchain and IPFS has been proposed and implemented. The system addresses key limitations of traditional federated learning, such as reliance on centralized aggregation servers, lack of transparency, and vulnerability to malicious participants. By leveraging blockchain technology, the proposed solution ensures a trustless and tamper-proof environment where all operations are recorded immutably. The use of IPFS for off-chain storage significantly reduces the computational and storage overhead associated with blockchain systems, making the architecture scalable and efficient. The incorporation of a staking and slashing mechanism, along with a reputation system, promotes honest participation and discourages malicious behavior. The implementation demonstrates that it is feasible to combine federated learning, decentralized storage, and blockchain into a unified system that ensures privacy, security, and transparency. Experimental results validate that the system successfully supports multiple client submissions, secure model storage, validation processes, and aggregation of updates into a global model. The developed prototype provides a practical demonstration of how decentralized technologies can enhance the reliability and robustness of collaborative machine learning systems. Despite its advantages, the proposed system has certain limitations. The validation process is currently simplified and can be further enhanced using more sophisticated evaluation techniques. Additionally, blockchain latency and transaction costs may affect scalability in large-scale deployments. Future work can focus on several enhancements, including the implementation of fully decentralized validation mechanisms using consensus protocols, integration with advanced deep learning models, and deployment on Layer-2 or high-performance blockchain networks to improve scalability. Furthermore, the system can be extended to real-world applications such as healthcare, finance, and IoT environments, where privacy-preserving collaborative learning is critical.

In conclusion, the proposed decentralized federated learning system presents a promising approach for building secure, scalable, and trustworthy machine learning frameworks by combining the strengths of federated learning, blockchain, and decentralized storage technologies.

References

[1]. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017.

[2]. P. Kairouz et al., "Advances and Open Problems in Federated Learning," Foundations and Trends in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021.

[3]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[4]. V. Buterin, "Ethereum Whitepaper: A Next-

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3328-3435
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0443

Generation Smart Contract and Decentralized Application Platform," 2014.

[5]. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014.

[6]. H. Kim, J. Park, M. Bennis, and S. Kim, "Blockchained On-Device Federated Learning," IEEE Communications Letters, vol. 24, no. 6, pp. 1279–1283, 2020.

[7]. J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Incentive Mechanism for Reliable Federated Learning: A Joint Optimization Approach to Combining Reputation and Contract Theory," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10700–10714, 2019.

[8]. Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, and B. He, "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," IEEE Transactions on Knowledge and Data Engineering, 2021.

[9]. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.

[10]. K. Bonawitz et al., "Towards Federated Learning at Scale: System Design," Proceedings of Machine Learning and Systems (MLSys), 2019.

[11]. M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A Joint Learning and Communications Framework for Federated Learning Over Wireless Networks," IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 269–283, 2021.

[12]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375.

[13]. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications. Telematics and Informatics, 36, 55–81.

[14]. Lu, Y. (2019). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 6(2), 231–255.

[15]. Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology. Peer-to-Peer Networking and Applications, 10(4), 983–994.

[16]. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.