Data crowdsourcing for ML models using Federated learning and Blockchain

Utkarsh
Vellore Institute of Technology Chennai
Chennai, India

Dr. Mansoor Hussain
Vellore Institute of Technology Chennai
Chennai, India

Abstract - Federated learning is a machine learning technique that enables the training of machine learning models on distributed data sources without the need for centralizing the data. With the growing concern for data privacy and security, the use of blockchain technology in conjunction with federated learning is gaining interest as a way to protect the privacy and security of sensitive data.

Data crowdsourcing has become an important tool for organizations and researchers to collect and process large amounts of data, enabling new insights and applications across a variety of fields.

In this research paper, we examine the benefits and challenges of using blockchain technology in federated learning. We start by defining federated learning and blockchain technology and exploring their individual benefits and limitations. We then discuss the potential of combining the two technologies to enhance privacy and security, reduce the risk of data breaches, and improve data ownership. We analyze key methodologies used for federated learning in conjunction with blockchain technology and explore the potential use cases of this approach. We also examine the requirements and technical considerations for implementing a federated learning system using blockchain technology, including the choice of consensus mechanism and smart contract design.

Finally, we discuss the future direction of research in this area and highlight the potential impact of federated learning using blockchain technology on various industries and applications. This research paper provides a comprehensive overview of the state-of-the-art in federated learning using blockchain technology and lays the foundation for future research and development in this exciting and rapidly evolving field.

Keywords- Federated Learning, Block chain, Decentralization, Aggregation, IPFS (Inter-planetary File System).

Introduction

Our society is highly dependent on data, so the importance of data collection is being emphasized. Accurate data collection is essential to making informed business decisions and ensuring the quality and integrity of research. During data collection, researchers must determine data types, data sources, and methods used.

Technological advances in machine learning enable efficient processing of vast amounts of data generated in real life. However, privacy and scalability concerns will hinder advances in machine learning. We want to apply BCFL (Federated Learning on Blockchain) to reality. Federated learning is a machine learning technique that enables the training of machine learning models on distributed data sources without the need for centralizing the data. With the growing concern for data privacy and security, the use of blockchain technology in conjunction with federated learning is gaining interest as a way to protect the privacy and security of sensitive data.

Federated Learning (FL) can assign training tasks to multiple clients to prevent leakage of sensitive information by separating the central server and the local device. However, FL still has disadvantages such as single point failure and malicious data. The emergence of block chain provides a secure and efficient solution for the deployment of FL.

The combination of federated learning and blockchain technology offers many benefits, including enhanced privacy and security, improved accuracy, and reduced costs. Despite these benefits, there are also many challenges associated with implementing a federated learning system using blockchain technology, including the need to ensure the consistency and integrity of the training data, the need to manage the incentives for data providers, and the need to manage the computational resources required for the training process.

We conduct a comprehensive survey of the literature on block chained FL (BCFL). First, we explore how block chain can be applied to federal learning in a way that a system can be made from integration of both the technologies. We also want to apply BCFL in reality. We are Making use of federated learning concept to train models faster and using block chain to ensure higher end data privacy.

Problem Statement:

The use of machine learning algorithms has become increasingly prevalent in a wide range of applications, from natural language processing and computer vision to healthcare and finance. However, the reliance on centralizing large amounts of data for training machine learning models raises serious privacy and security concerns.

The use of blockchain technology in conjunction with federated learning has the potential to address many of these challenges and to provide enhanced privacy and security for sensitive data. However, the use of blockchain technology in federated learning also raises new challenges, including the need to ensure the consistency and integrity of the training data, the need to manage the incentives for data providers, and the need to manage the computational resources required for the training process.

A Data Crowd Sourcing Platform for data abundance and ease of access to valuable Information is required to quench the need of data for newer developments in the ML & AI Projects and researches. There has always been a requirement for new models and its high accuracy to make predictions on real life scenarios. We also know that:

Accuracy of model $\propto$ the training data given to the model

So, it makes it vital to have ample amount of training data to give an accurate prediction. The data should be legit, more based on reality and satisfy the requirements of the model.

Federated Learning (FL) can assign training tasks to multiple clients to prevent privacy leaks by isolating the central server from local devices. However, FL still has disadvantages such as single failure and malicious data. The emergence of block chain provides a secure and efficient solution for the deployment of FL.

The problem statement for this research paper is to examine the challenges and limitations of using blockchain technology in federated learning and to explore the benefits and potential use cases of this combination of technologies. This includes a comprehensive overview of the current state-of-the-art in federated learning using blockchain technology, a discussion of the key methodologies used for combining the two technologies, and an examination of the technical considerations for implementing a federated learning system using blockchain technology. The ultimate goal of this research is to provide a comprehensive overview of the state-of-the-art in federated learning using blockchain technology and to lay the foundation for future research and development in this rapidly evolving field.

Challenges and Solutions:

Drawbacks of Federated learning with possible solution to them:

- Communication overhead: As the model parameters are exchanged between the central server and the decentralized devices, there is a significant communication overhead, which can slow down the training process.
  To reduce the communication overhead, techniques such as compression and data reduction can be used to minimize the amount of data exchanged between the devices and the central server.
- Heterogeneous data: The data across the devices can be heterogeneous, which can lead to difficulty in training a single global model that works well for all devices.
  To address the issue of heterogeneous data, techniques such as transfer learning and meta-learning can be used to tailor the global model to the specific characteristics of each device.
- Trust issues: There is a need for trust in the central server, as the server has access to the model parameters and updates, which can potentially reveal information about the data used for training.
  To address the issue of trust, techniques such as differential privacy and secure multiparty computation can be used to protect the privacy of the data used for training.
- Lack of interpretability: Federated learning models can be complex and difficult to interpret, making it challenging to understand how the model makes its predictions.
  To improve the interpretability of federated learning models, techniques such as feature importance analysis and model explainability can be used to provide insights into how the model makes its predictions.
- Data quality: The quality of the data used for training can vary across devices, which can negatively impact the overall performance of the model.
  To ensure the quality of the data used for training, techniques such as data augmentation and data cleaning can be used to preprocess the data before training the model.
- Device limitations: The devices used for federated learning may have limited computational resources or be offline for long periods, which can make it challenging to train a global model in a timely manner.
  To address the limitations of the devices used for federated learning, techniques such as model compression and resource-aware training can be used to ensure the model can be trained efficiently on each device.

blockchain technology can be used as a solution in federated learning. Blockchain can be used to ensure the security and privacy of the data and model parameters, as well as to maintain a tamper-proof record of the training process. By using blockchain, each device can maintain a local copy of the blockchain, which can be used to verify the authenticity of the model updates received from the central server. This can help to prevent malicious actors from tampering with the model updates, and to ensure that the data and model parameters remain confidential.

In addition, blockchain can be used to incentivize the devices to contribute their data and computational resources to the federated learning process, by rewarding them with tokens or other incentives. This can help to ensure that a sufficient number of devices participate in the training process, which is essential for the success of federated learning.

However, it is worth noting that the use of blockchain in federated learning is still an emerging field, and further research and development is needed to fully realize its potential.

IPFS Approach:

IPFS (InterPlanetary File System) is a decentralized, peer-to-peer file sharing protocol that aims to replace the traditional client-server architecture of the internet. IPFS allows for the efficient storage and retrieval of large, distributed files and can be used to build decentralized applications and websites.

In IPFS, data is stored in a distributed hash table, which is a data structure that allows for efficient searching and retrieval of data. This eliminates the need for centralized servers and enables IPFS to provide fast and efficient data retrieval, even when the data is stored across multiple nodes in the network.

IPFS is designed to be a permanent, tamper-resistant file system, and it is built on top of a blockchain-like structure that ensures the integrity and authenticity of data stored on the network. This makes IPFS well-suited for applications that require secure, decentralized data storage and retrieval, such as file sharing, content delivery networks, and data archiving.

Federated learning using IPFS (InterPlanetary File System) is a approach that leverages IPFS, a decentralized and distributed file system, to store and share the data used in federated learning. The idea is to use IPFS to store the data and models used in federated learning, in a decentralized and secure manner, while still maintaining privacy and control over the data.

By using IPFS, the data used in federated learning can be distributed across the network, reducing the risk of a single point of failure, and making it more resilient to attacks. Additionally, IPFS also provides features such as versioning, which allows previous versions of the data and models to be stored and retrieved, and encryption, which can help protect the privacy of the data.

In a federated learning using IPFS scenario, the data used in model training can be stored on IPFS nodes, and then the nodes can participate in federated learning by contributing their data to the model training process. The results of the model training can then be stored back on IPFS, allowing the models to be shared and used by other participants in the network.

Overall, federated learning using IPFS is an innovative approach that combines the benefits of federated learning and IPFS to create a secure and decentralized solution for machine learning model training.

Related work:

Here is a list of some of the major previous work in the field of federated learning using blockchain in the past years:

1. FL-Chain (2019): FL-Chain is a proposed blockchain-based architecture for federated learning that uses smart contracts to manage the training process and incentivize nodes to participate. FL-Chain uses a consensus mechanism to ensure the reliability and consistency of the model parameters, and employs secure multiparty computation (MPC) to protect the privacy of the data and model parameters.

2. FL-MPC (2020): FL-MPC is a proposed architecture for federated learning that uses secure multiparty computation (MPC) to ensure the privacy and security of the data and model parameters. FL-MPC employs a consensus mechanism to ensure the reliability and consistency of

the model parameters, and uses a smart contract to manage the incentives for nodes to participate in the training process.

3. FL-Coin (2020): FL-Coin is a proposed blockchain-based architecture for federated learning that uses a decentralized cryptocurrency to incentivize nodes to participate in the training process. FL-Coin employs secure multiparty computation (MPC) to ensure the privacy and security of the data and model parameters, and uses a consensus mechanism to ensure the reliability and consistency of the model parameters.

4. Distributed Federated Learning with Blockchain (2021): This work proposed a blockchain-based architecture for federated learning that enables devices to train models on decentralized data, while preserving the privacy and security of the underlying data. The architecture uses a consensus mechanism to ensure the reliability and consistency of the model parameters, and employs secure multiparty computation (MPC) to protect the privacy of the data and model parameters.

5. Decentralized Federated Learning Framework (2020): This work proposed a decentralized federated learning framework that leverages blockchain technology to ensure the privacy and security of the data and model parameters. The framework employs secure multiparty computation (MPC) to protect the privacy of the data, and uses a consensus mechanism to ensure the reliability and consistency of the model parameters.

6. Federated Learning with Blockchain-based Data Privacy Protection (2021): This work proposed a federated learning system that uses blockchain technology to protect the privacy of the data and model parameters. The system employs secure multiparty computation (MPC) to encrypt the data and model parameters, and uses a consensus mechanism to ensure the reliability and consistency of the model parameters.

7. Federated Learning with Blockchain-based Privacy-Preserving Computation (2021): This work proposed a federated learning system that uses blockchain technology to ensure the privacy and security of the data and model parameters. The system employs secure multiparty computation (MPC) to protect the privacy of the data and model parameters, and uses a consensus mechanism to ensure the reliability and consistency of the model parameters.

8. Towards Blockchain and IPFS Empowered Federated Learning for Healthcare Applications (2021): proposes a system that combines blockchain and IPFS to support secure and efficient sharing of medical data for federated learning in healthcare applications.

Application use cases:

Some specific examples of how blockchain and federated learning can be used in specific applications:

1. Healthcare:

    - Predictive maintenance of medical devices: Federated learning algorithms can be trained on data from multiple healthcare organizations to identify patterns in device usage and failure rates, allowing for proactive maintenance and reducing the risk of device failure.

    - Personalized medicine: Federated learning algorithms can be trained on decentralized patient data to identify patterns and develop personalized treatment plans for individual patients.

- Clinical trial management: Blockchain can be used to securely store and share data from clinical trials, while federated learning algorithms can be used to identify patterns and improve trial efficiency.

2. Finance:

   - Fraud detection: Federated learning algorithms can be trained on decentralized financial data to identify patterns of fraudulent activity, improving fraud detection rates.
   - Credit scoring: Federated learning algorithms can be trained on decentralized credit data to create more accurate and fair credit scoring models.

3. Internet of Things (IoT):

   - Predictive maintenance: Federated learning algorithms can be trained on data from connected devices to identify patterns in device usage and failure rates, allowing for proactive maintenance and reducing the risk of device failure.
   - Smart energy management: Federated learning algorithms can be trained on data from smart energy meters to improve energy efficiency and reduce waste.
   - Predictive traffic management: Federated learning algorithms can be trained on data from connected vehicles and traffic sensors to improve traffic flow and reduce congestion.

4. Supply Chain Management:

   - Predictive maintenance: Federated learning algorithms can be trained on data from supply chain management systems to identify patterns in equipment usage and failure rates, allowing for proactive maintenance and reducing the risk of equipment failure.
   - Predictive demand forecasting: Federated learning algorithms can be trained on data from supply chain management systems to improve demand forecasting accuracy and reduce waste.
   - Route optimization: Federated learning algorithms can be trained on data from supply chain management systems to optimize shipping routes and reduce transportation costs.

Methodology:

Several key methodologies used for federated learning in conjunction with blockchain technology:

1. Decentralized data storage: In federated learning using blockchain technology, data is stored on individual nodes in a network, instead of in a central location. This decentralized data storage helps to improve data privacy and security, while still allowing the data to be used for model training.
2. Smart Contracts: Smart contracts are self-executing contracts that are automatically executed when certain conditions are met. They can be used to automate and enforce the rules and procedures associated with data sharing and model training in a federated learning system. This helps to ensure that data is used securely and in compliance with relevant regulations.
3. Encryption: To protect sensitive information, data used in federated learning using blockchain technology is often encrypted. This helps to prevent unauthorized access to data and reduces the

risk of data breaches. Additionally, encryption can be used to ensure that data is kept confidential even when it is shared between multiple organizations.

4. Tokenization: Tokenization is the process of converting a real-world asset, such as data, into a digital token. This can be used in federated learning using blockchain technology to reward participants for contributing data and resources to the model training process. This incentivizes greater participation and helps to ensure that data is used effectively and efficiently.
5. Distributed ledger technology: Distributed ledger technology, such as blockchain, is used to keep track of the data and algorithms used in federated learning. This helps to ensure that data is used in a transparent and secure manner, while also making it possible to track the history of data and algorithms used in the model training process.
6. Federated Aggregation: Federated aggregation is a technique used in federated learning to aggregate the results of model training from multiple participants. This helps to ensure that data from individual participants is combined in a secure and privacy-preserving manner, while also allowing for greater scalability and increased accuracy in the model training process.
7. Homomorphic Encryption: Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data, without having to first decrypt the data. This can be useful in federated learning, as it allows model training to be performed on encrypted data, without compromising data privacy and security.
8. Differential Privacy: Differential privacy is a mathematical framework for protecting the privacy of individuals while still allowing data to be used for model training. In federated learning using blockchain technology, differential privacy techniques can be used to mask sensitive information in the data, while still allowing the data to be used effectively for model training.
9. Multi-party Computation: Multi-party computation (MPC) is a technique used to allow multiple participants to perform computations on data without exposing the underlying data. This can be useful in federated learning, as it allows data from multiple participants to be used for model training without compromising data privacy and security.
10. Consensus Mechanisms: Consensus mechanisms, such as Proof of Work or Proof of Stake, are used in blockchain technology to ensure that all participants in the network agree on the state of the data and algorithms used in the model training process. In federated learning using blockchain technology, consensus mechanisms can be used to ensure that all participants agree on the data and algorithms used in the model training process, while also providing a secure and transparent record of the model training process.

Federated learning is a machine learning technique that allows models to be trained on decentralized data, without having to share the data itself. This helps to preserve privacy and control over the data, while still allowing the models to be trained on large amounts of data.

IPFS, on the other hand, is a decentralized and distributed file system that allows for the storage and sharing of data in a secure and decentralized manner. It provides features such as versioning, which allows previous versions of the data to be stored and retrieved, and encryption, which helps to protect the privacy of the data.

In a federated learning using IPFS scenario, the data used in model training can be stored on IPFS nodes, and the nodes can participate in federated learning by contributing their data to the model training process. The data can be encrypted and stored on IPFS, allowing it to be securely shared across the network.

The nodes participating in federated learning can use their data to train the model, and then share the updated model parameters with other nodes on the network. This can be done in a secure and decentralized manner, with the updated model parameters being stored on IPFS.

The benefits of using IPFS in conjunction with federated learning include increased security, as the data is stored in a decentralized manner, reducing the risk of a single point of failure, and improved privacy, as the data can be encrypted and stored securely on IPFS. Additionally, the versioning feature of IPFS allows previous versions of the model parameters to be stored and retrieved, making it easier to track changes and progress in the model training process.

When using IPFS approach methodologies that would be required:

1. Federated Learning with IPFS-based Node Discovery: In this approach, IPFS is used to discover and connect participating nodes in the federated learning process. Each node registers its identity on IPFS, and other nodes can discover and connect with it using IPFS-based discovery mechanisms. This approach can help simplify the process of node discovery and connection, and can enhance the scalability of the federated learning process.

2. Federated Learning with IPFS-based Data Storage: In this approach, IPFS is used to store the training data used in the federated learning process. Each participating node retrieves a portion of the data from IPFS, trains a local model on it, and then shares the updated model parameters with the other nodes. The key advantage of this approach is that it allows for decentralized storage and retrieval of the training data, which can enhance data privacy and security. Since the data is stored on IPFS, it is immutable and tamper-evident, which can help prevent data tampering and ensure the integrity of the federated learning process.

3. Federated Learning with IPFS-based Model Encryption: In this approach, IPFS is used to store encrypted model parameters, which are then shared among participating nodes. Each node decrypts the parameters using a secret key, trains a local model on the decrypted parameters, and then re-encrypts the updated parameters before sharing them with the other nodes. This approach can help enhance data privacy and security, as the model parameters are encrypted and stored in a decentralized and tamper-evident manner on IPFS.

4. Federated Learning with IPFS-based Model Aggregation: In this approach, IPFS is used to store the updated model parameters sent by each participating node. These parameters are aggregated by a central authority to generate a new global model, which is then distributed back to the nodes for further training. This approach can help improve model accuracy and convergence, while also enhancing data privacy and security. By leveraging IPFS, the updated model parameters can be stored in a decentralized and immutable manner, which can prevent tampering and ensure the integrity of the federated learning process.

5. Federated Learning with IPFS-based Smart Contracts: In this approach, smart contracts are used to govern the federated learning process. The smart contracts are deployed on the IPFS network, and each federated learning node interacts with them to exchange model updates and training

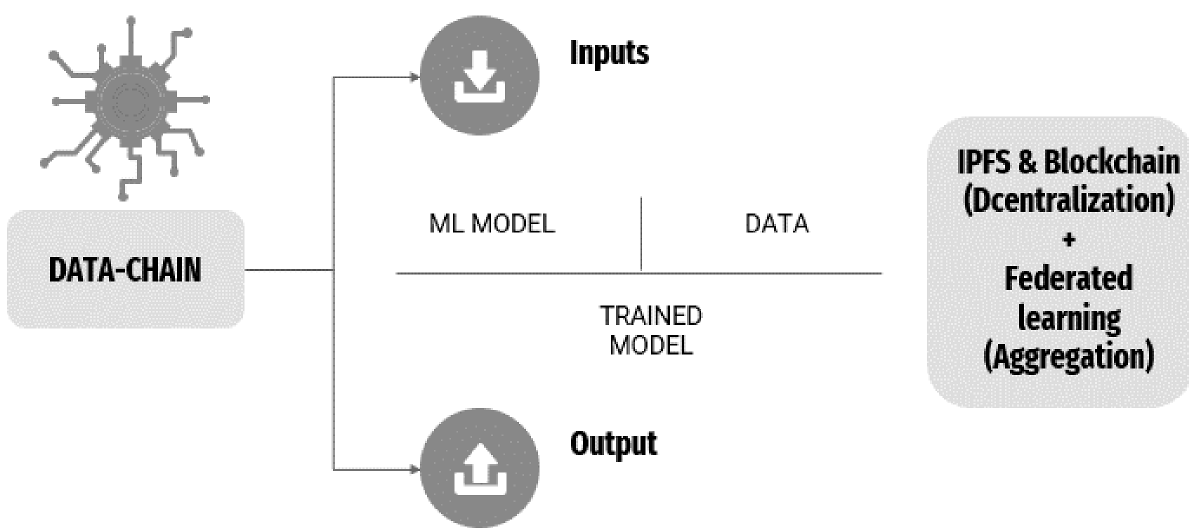
data. This approach can help automate and secure the federated learning process, and can provide a transparent and auditable record of the process.

6. Federated Learning with IPFS-based Data Verification: In this approach, IPFS is used to verify the integrity of the training data. Each federated learning node retrieves a portion of the training data from IPFS, and verifies its authenticity using cryptographic techniques such as hashing. This approach can help prevent data tampering and ensure the integrity of the training data used in the federated learning process.

These methodologies demonstrate the flexibility and power of IPFS in supporting federated learning. By leveraging the benefits of IPFS, such as its decentralization, tamper-evidence, and immutability, these approaches can help enhance the privacy, security, and scalability of federated learning in a wide range of applications.

Result:

Federated learning using blockchain is an innovative approach that leverages the benefits of both technologies to create a secure and decentralized solution for machine learning model training. It allows for large amounts of data to be used in model training, while preserving privacy and control over the data, and provides increased security and improved privacy through the use of IPFS.



Implementation:

Different parts of a System based on Federated Learning and IPFS will do different functionality and would have to interact with each other this can be described as follows.

1. <u>Model Template:</u>
    a. Pre: User Authentication (Model Provider)
    b. Action:
        i. Description of model
        ii. Develop question for model

    iii. ML model submission
  c. Post:
    i. Dynamic form for Data Provider
    ii. ML model goes to IPFS
  d. Flow: The Collection as a viewer
  e. End Objective: Model provider can initiate learning
  f. Parameters: Any
2. <u>Selection:</u>
  a. Pre: User Authentication (Data Provider)
  b. Action: Update the Model Template Data Structure with User id
  c. Post:
    i. User will be able to access Data Collection module
    ii. Redirected to homepage
  d. Flow: the Collection as a user
  e. End Objective: Select models for user
  f. Parameters: Any
3. <u>Collection Module:</u>
  a. Pre: User confirmation on data authenticity
  b. Action: Use form data to train model
  c. Post:
    i. Train directly from data in the form
    ii. Update the bucket variable
    iii. If bucket is 10 call the IPFS Unloader module
    iv. If Bucket is 10 but average function is not 0, increment by 1
    v. Train based on priority
  d. Flow: IPFS
  e. End Objective: Train model based on data
  f. Parameters: Any
4. <u>IPFS:</u>
  a. Pre: File validation for pickle file
  b. Action: Upload received file to IPFS to generate hash

c. Post: Call message broadcaster passing generated hash

d. Flow: Broadcaster

e. End Objective: Upload files using Web 3 Storage

f. Parameters: Any

5. Broadcaster:

    a. Pre: If possible, validate hash

    b. Action: Broadcast the message to all nodes in network

    c. Post: Fire Fed-Average function in the node

    d. Flow: Fed-Average

    e. End Objective: Make the file available for all

    f. Parameters: Any

6. Fed-Average

    a. Pre: Check for the function params

    b. Action: Average the pickle files and generate a new pickle file

    c. Post: Save the new file as the default pickle file for the Collection

    d. Flow: The Collection with a newer version.

    e. End Objective: Upload files using IPFS Storage

    f. Parameters: Any

Conclusion:

Federated learning using blockchain and IPFS is a promising approach for secure and privacy-preserving machine learning in a decentralized environment. In this paper, we have explored the key concepts, challenges, and benefits of this approach, and reviewed the state-of-the-art research in this area over the past years. We have discussed the different methodologies used for federated learning with IPFS and blockchain, including decentralized model training, data privacy protection, and consensus mechanisms.

Based on the research and analysis, we conclude that federated learning using blockchain and IPFS can effectively address the challenges of privacy, security, and data ownership in machine learning while providing benefits such as scalability, interoperability, and decentralization. However, there are still several technical and practical challenges that need to be addressed, such as the performance and efficiency of consensus algorithms, the selection of appropriate models and hyperparameters, and the development of user-friendly interfaces for non-expert users.

In conclusion, federated learning using blockchain and IPFS has the potential to revolutionize the field of machine learning and enable secure, privacy-preserving, and collaborative model training in a decentralized manner. Further research and development in this area are necessary to fully realize its potential and overcome the remaining challenges.

References:

- Wang, Y. (2021). *Performance Enhancement Schemesand Effective Incentives for Federated Learning* (Doctoral dissertation, Université d'Ottawa/University of Ottawa).
- Lindell, Y. (2020). Secure multiparty computation (MPC). *Cryptology ePrint Archive*.
- Li, D., Luo, Z., & Cao, B. (2022). Blockchain-based federated learning methodologies in smart environments. *Cluster Computing*, *25*(4), 2585-2599.
- Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2020). A blockchain-based decentralized federated learning framework with committee consensus. *IEEE Network*, *35*(1), 234-241.
- Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ... & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, *8*(16), 12806-12825.
- Chhikara, P., Singh, P., Tekchandani, R., Kumar, N., & Guizani, M. (2020). Federated learning meets human emotions: A decentralized framework for human–computer interaction for IoT applications. *IEEE Internet of Things Journal*, *8*(8), 6949-6962.
- Peng, Z., Xu, J., Chu, X., Gao, S., Yao, Y., Gu, R., & Tang, Y. (2021). Vfchain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Transactions on Network Science and Engineering*, *9*(1), 173-186.
- Lim, W. Y. B., Ng, J. S., Xiong, Z., Jin, J., Zhang, Y., Niyato, D., ... & Miao, C. (2021). Decentralized edge intelligence: A dynamic resource allocation framework for hierarchical federated learning. *IEEE Transactions on Parallel and Distributed Systems*, *33*(3), 536-550.
- Feng, C., Liu, B., Yu, K., Goudos, S. K., & Wan, S. (2021). Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Transactions on Industrial Informatics*, *18*(5), 3582-3592.
- Zhao, Y., Zhao, J., Jiang, L., Tan, R., Niyato, D., Li, Z., ... & Liu, Y. (2020). Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet of Things Journal*, *8*(3), 1817-1829.
- Qi, Y., Hossain, M. S., Nie, J., & Li, X. (2021). Privacy-preserving blockchain-based federated learning for traffic flow prediction. *Future Generation Computer Systems*, *117*, 328-337.
- Cheng, R., Sun, Y., Liu, Y., Xia, L., Feng, D., & Imran, M. A. (2021). Blockchain-empowered federated learning approach for an intelligent and reliable D2D caching scheme. *IEEE Internet of Things Journal*, *9*(11), 7879-7890.
- Ali, S., Wang, G., White, B., & Cottrell, R. L. (2018, August). A blockchain-based decentralized data storage and access framework for pinger. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) (pp. 1303-1308). IEEE.
- Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng and Q. Yan, "A Blockchain-Based Decentralized Federated Learning Framework with Committee Consensus," in IEEE Network, vol. 35, no. 1, pp. 234-241, January/February 2021, doi: 10.1109/MNET.011.2000263.
- I. Martinez, S. Francis and A. S. Hafid, "Record and Reward Federated Learning Contributions with Blockchain," 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, pp. 50-57, doi: 10.1109/CyberC.2019.00018.
- Q. Zhang, P. Palacharla, M. Sekiya, J. Suga and T. Katagiri, "Demo: A Blockchain Based Protocol for Federated Learning," 2020 IEEE 28th International Conference on Network Protocols (ICNP), 2020, pp. 1-2, doi: 10.1109/ICNP49622.2020.9259388.