Blockchain and Cryptocurrencies: Federated Learning
Federated Proximal

Lorenzo Cassano and **Jacopo D'Abramo**
Master's Degree in Artificial Intelligence, University of Bologna
{ lorenzo.cassano2, jacopo.dabramo }@studio.unibo.it

Abstract

This project builds upon blockchain and cryptocurrency foundations, extending a pre-existing system with Federated Learning. Enhancements include the implementation of Federated Proximal optimization [1], simulation of out-of-battery devices, and expansion to more than three simulated devices. A new dataset is introduced, and diverse experiments are conducted on both datasets, showcasing the system's adaptability and scalability in a decentralized context. The integration of these features contributes to the project's goal of advancing the understanding and applicability of Federated Learning within blockchain environments.

1 Introduction

In a landscape dominated by data-driven technologies, our project addresses the critical challenge of reconciling privacy and decentralized solutions. Building upon blockchain foundations, we integrate Federated Learning into an existing system to tackle the inherent tension between the demand for data-driven insights and the need to protect individual privacy. By implementing Federated Proximal optimization [1], simulating out-of-battery devices, and expanding the device network, our project enhances the system's adaptability and scalability in a decentralized context. Through these advancements, we strive to contribute to a deeper understanding and increased applicability of Federated Learning within blockchain environments

Various integration approaches exist for combining blockchain with Federated Learning systems:

- Fully Coupled Blockchain Federated Learning: In this configuration, the clients of Federated Learning also serve as nodes on the blockchain. Essentially, clients not only train local models but also verify updates and generate new blocks [2].
- Flexibly Coupled Blockchain Federated Learning: Here, the blockchain and Federated Learning systems operate in separate networks. Clients of Federated Learning are distinct from blockchain nodes (miners). Clients are responsible for local data collection and training, while miners on the blockchain handle verification of local model updates [2].
- Loosely Coupled Blockchain Federated Learning (LoC-BCFL): the framework is used to verify model updates and manage the reputation of participates, and only the reputation related data can remain on distributed ledger. Verification of the updates and reputation management are a part of incentive mechanisms to ensure the participates can behave honestly [2].

Originating from the foundation set by this work [3], which employs a Loosely Coupled Blockchain Federated Learning architecture, our mission was to enhance the project through the incorporation of novel features for system simulation and the execution of supplementary experiments. The primary aim of these experiments was to scrutinize variations in weight aggregation methods, specifically FedAvg and FedProx. Our investigation extended to understanding the impact of the hyperparameter μ on the FedProx method, applying this approach to diverse datasets, and simulating the intentional disconnection of some devices during the global training process

2 Background

The task at hand involves image classification on Alzheimer and Brain Tumor datasets, aiming to distinguish various types of images. The solution employs a straightforward convolutional neural network [4], which consistently achieves high performance.

To address the collaborative learning aspect, a loosely coupled Blockchain Federated Learning approach is adopted to simulate the entire system. A random split is applied to collaborators, ensuring a diverse number of samples across different devices. Notably, the InterPlanetary File System (IPFS) is utilized for the distribution ledger [5], while Ganache is employed for simulating the Ethereum blockchain [6]. This setup facilitates the secure and decentralized coordination of the federated learning process.

3 System description

The extended features implemented in the project include the ability to create additional devices for testing federated learning on a larger scale, addressing the limitation of only three devices in the original project. However, for practical experimentation, we restricted our tests to a maximum of 20 devices due to dataset size considerations. Working with more than 20 devices would potentially lead to situations where a single device possesses very few samples, introducing variations in data distribution that could impact the efficacy of federated learning.

The original Convolutional Neural Network has beeen changed, in order to implement the Federated Proximal techniques, so the training has been changed in order to have the following loss function:

$$\min_{w} h_k(w; w_t) = F_k(w) + \frac{\mu}{2}\|w - w_t\|_2^2$$

Where $F_k(w)$ represents the local loss function, w denotes the local weights, and w_t signifies the global weights, the purpose of incorporating this loss function is to introduce a term influenced by the disparity between local and global weights.

In particular, for varying heterogeneous settings, at each round, we assign a number of epochs (chosen uniformly at random between 1 and the assigned epochs for the device) [2].

Additionally, the paper [2] employs this strategy for a subset of devices; however, due to a limited number of devices and constraints on data and computational power, we adopt this strategy for all devices in our case.

The devices that ran out of battery were treated as if in a real-world scenario by establishing a designated time during which the Blockchain awaits the local weights. After this specified duration, the Blockchain disregards the weights from the inactive device and proceeds with the round procedure. For simulation purposes, the waiting time is determined based on the conducted experiments.

4 Data

The datasets used to conduct the experiments are as follows:

- Alzheimer dataset: the original dataset utilized by the repository [3].
- Brain Tumor dataset: an additional dataset introduced for supplementary experiments.

Both datasets consist of images and encompass four classes, exhibiting a slight imbalance among these classes. The decision to incorporate the Brain Tumor dataset is driven by the intention to perform experiments on a new dataset with features similar to the original one. This approach aims to prevent divergent results caused by the neural network initially designed for the Alzheimer dataset (Fig.1).

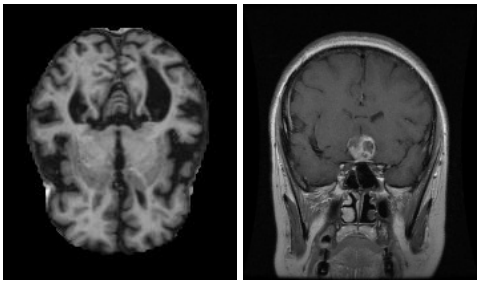

Figure 1: Alzheimer and Brain Tumor images share similar visual features, as evident from the observed images

To emulate a realistic scenario, a random split is implemented to partition the dataset across various devices. This random division is introduced to mimic the authentic conditions where datasets on individual devices exhibit diverse distributions. In real-world scenarios, the distribution of data across devices is not uniform, and this randomized split aims to capture such heterogeneity.

5 Experimental setup and results

The general pipeline conducted for the experiments is as follows:

- Tested FedAvg on a dataset with specified rounds and epochs.

- Subsequently, retested the same configuration with one or more devices out of battery.
- Conducted experiments with the FedProx techniques.
- Explored different hyperparameters, such as μ.
- Retested FedProx with one or more devices out of battery.

This pipeline is employed to facilitate a comprehensive comparison of various configurations that can be obtained.

Furthermore, to gain a better understanding of how the two tested techniques work, the loss plots for each device in the conducted experiments have also been analyzed. This allows for an examination of the behavior of each device and how the loss pattern may vary based on the type of strategy and experiments.

The following displays the training loss for both FedProx and FedAvg in the most significant experiments.

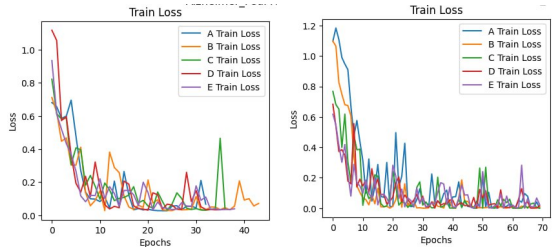

Figure 2: Train loss for FedProx with μ 0.0001 and for FedAvg, Alzheimer Dataset

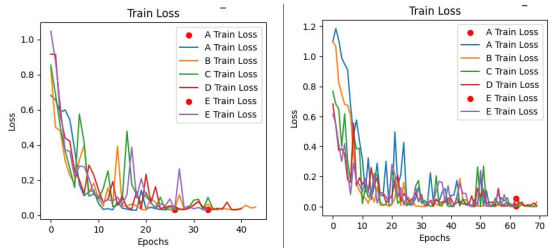

Figure 3: Train loss for FedProx with μ 0.0001 and for FedAvg with devices out of battery, Alzheimer Dataset

As it is possible to observe, the loss of Federated Proximal for the Alzheimer dataset remains more stable. This trend is guaranteed thanks to the heterogeneity introduced by FedProx. In this case, the graph seems to exhibit the same trend as explained by [1].

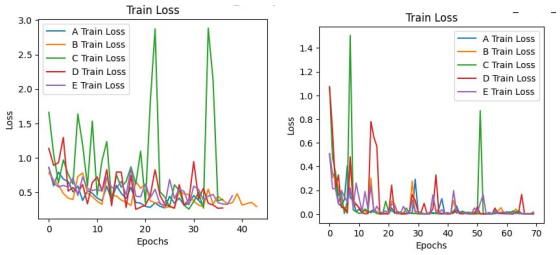

Figure 4: Train loss for FedProx with μ 0.001 and for FedAvg, Brain Tumor Dataset

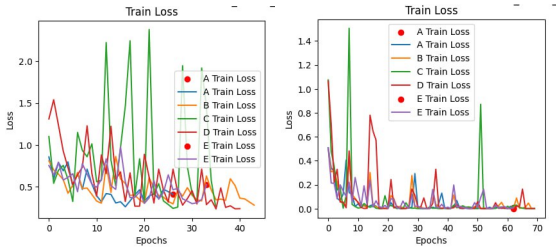

Figure 5: Train loss for FedProx with μ 0.001 and for FedAvg with devices out of battery, Brain Tumor Dataset

On the other hand, the training loss of the two methods in the Brain Tumor dataset appears to follow a different trend. In this scenario, FedAvg demonstrates a more stable loss. The reason behind this behavior is that the training of a single device does not consistently lead to model improvement, resulting in a more unstable loss.

In the following, the table presents the results of the experimented configurations.

Alzheimer dataset					
N.dev.	Meth.	Round	Ep.	Out	Acc.
5	FedProx	10	7	0	96%
5	FedProx	10	7	2	96%
5	FedAvg	10	7	0	95%
5	FedAvg	10	7	2	95%
3	FedProx	10	5	0	95%
3	FedProx	10	5	2	95%
3	FedAvg	10	5	0	95%
3	FedAvg	10	5	0	94%
10	FedAvg	10	7	0	92%
10	FedProx	10	7	0	88%
20	FedAvg	20	10	0	92%
20	FedProx	20	20	0	94%

Table 1: Experiments results on Alzheimer Dataset

Brain Tumor dataset					
N.dev.	Meth.	Round	Ep.	Out	Acc.
5	FedAvg	10	7	0	92%
5	FedAvg	10	7	2	92%
3	FedProx	10	5	0	91%
3	FedAvg	10	5	0	91%
3	FedProx	10	5	0	95%
5	FedProx	10	5	0	90%
5	FedProx	10	7	2	88%
5	FedProx	10	5	2	88%
5	FedProx	10	5	2	82%
6	FedAvg	10	7	0	90%
6	FedProx	10	7	0	91%

Table 2: Experiments results on Brain Tumor Dataset

6 Discussion

The majority of experiments were conducted on the Alzheimer dataset, while some experiments on the Brain Tumor dataset were omitted due to computational constraints. Overall, the observation is that with the appropriate configuration, FedProx outperforms FedAvg.

Notably, with 20 devices (the experiments involving the highest number of devices), FedProx demonstrates superior performance compared to FedAvg.

Another noteworthy observation is that, in many instances, the presence of devices out of battery does not significantly impact the overall model performance. This could be attributed to the data being split across various devices, and when two devices are out of battery, only a negligible portion of the dataset is lost.

Lastly, the chosen metric for evaluation is accuracy. While it may have limitations, in this context, it aligns with the model's performance as it exhibits a consistent trend with macro-F1.

7 Conclusion

In conclusion, this project has yielded intriguing results through the implementation of federated learning with Blockchain technology. The promising outcomes suggest avenues for future exploration. Subsequent work could involve experimenting with new models, even within the same task, while incorporating diverse dataset formats. Expanding the simulation to involve a larger number of devices, perhaps exceeding 100, presents an unexplored yet computationally challenging direction.

Regarding the Blockchain component, there exists potential for extension by incorporating reputation mechanisms. This enhancement could play a crucial role in selecting weights for aggregation, thereby refining the efficiency and reliability of the federated learning process. These proposed directions open up exciting possibilities for advancing the field and addressing challenges associated with scalability and robustness.

8 Links to external resources

- Alzheimer dataset
- Brain Tumor dataset

References

[1] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. Federated optimization in heterogeneous networks. *Proceedings of Machine learning and systems*, 2:429–450, 2020.

[2] Zhilin Wang and Qin Hu. Blockchain-based federated learning: A comprehensive survey. *arXiv preprint arXiv:2110.02182*, 2021.

[3] Ferretti Cialone, Imboccioli. Federated Learning on Blockchain with Hospital Peers for Alzheimer's MRI Image Classification. 2023.

[4] Keiron O'Shea and Ryan Nash. An introduction to convolutional neural networks. *arXiv preprint arXiv:1511.08458*, 2015.

[5] Interplanetary file system (ipfs): A peer-to-peer hypermedia protocol. `https://ipfs.io/`, Year.

[6] Ganache: A personal blockchain for ethereum development. `https://www.trufflesuite.com/ganache`, Year. Truffle Suite.