Blockchain in Federated Learning

Team Member 1:

First Name: Arjun Ramesh

Last Name: Kaushik

Email: kaushik3@buffalo.edu

Person Number: 50413327

Team Member 2:

First Name: Hari Preetham Reddy

Last Name: Nandyala

Email: haripree@buffalo.edu

Person Number: 50468240

Approved by: Prof. Bina Ramamurthy and Chen Xu

Reference Papers:

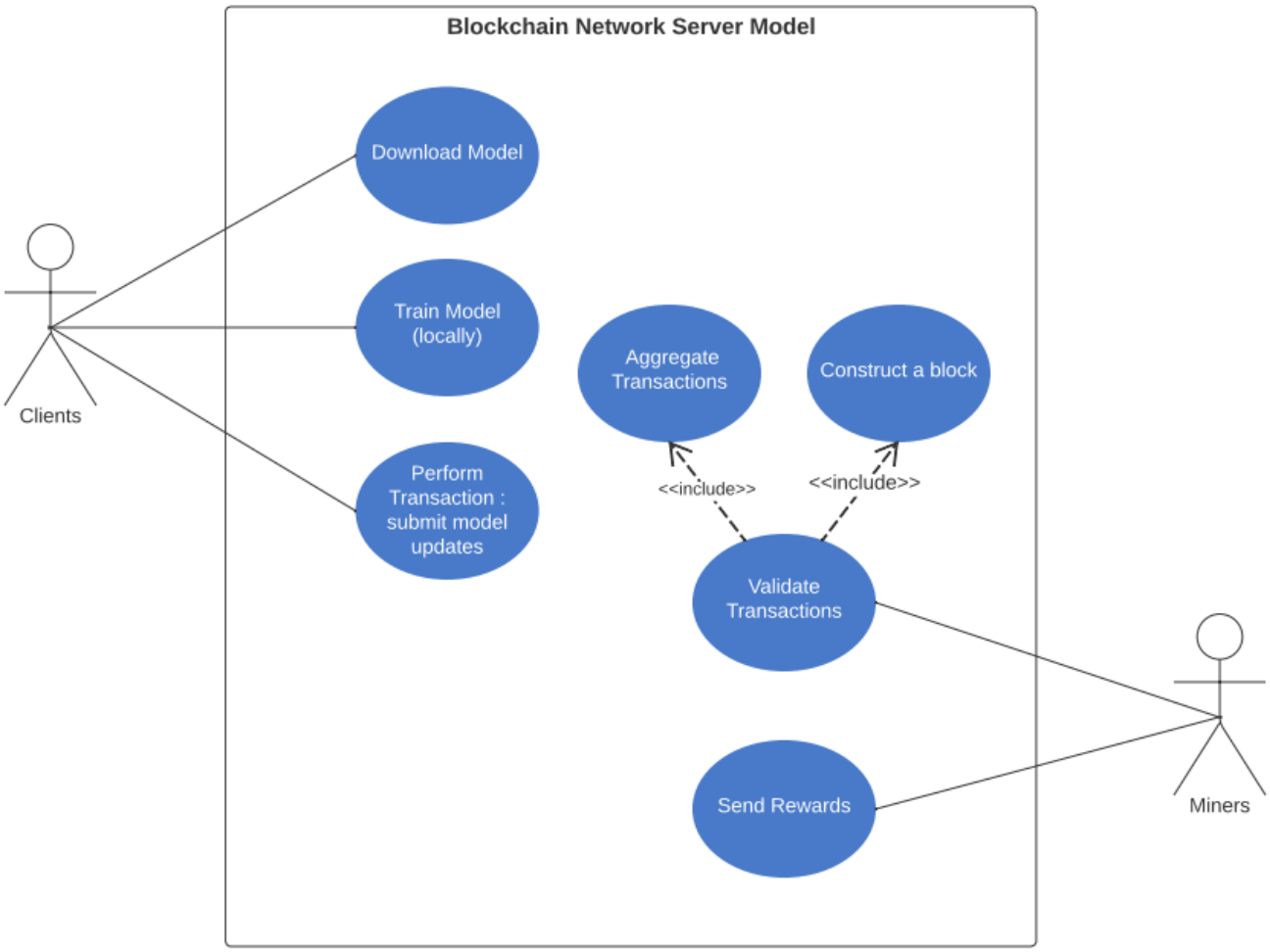
1. https://drive.google.com/file/d/1tbIfXJRVTmbeQYT6QmckV_Yq_u1rkow4/view?usp=sharing
2. https://drive.google.com/file/d/1BuzRDZioCtsEgFR9L0FLIYoCveJlaYY6/view?usp=sharing

Issue(s) addressed: Improving privacy in a world driven by increasing needs for privacy

Abstract:

Federated learning is a type of Machine Learning which works like a decentralised system. Here, learning happens locally in the devices of clients; the gradients from client devices are aggregated in a server and then each client is updated with a new ML model from the server called “global model”. The idea of Federated learning is to preserve privacy of client data. But it doesn’t prevent the clients from using malicious data to train, which might degrade the performance of the global model. This is where we bring in Blockchain Technology. Before updating the server model, we validate, using smart contracts, that the global model is performing better with the aggregation of locally trained gradients. And then, add the global model (aggregated gradients) to the blockchain network.

Use Case Diagram:



Working Model: