FUJITSU

shaping tomorrow with you

Demo:
A Blockchain Based Protocol for Federated Learning

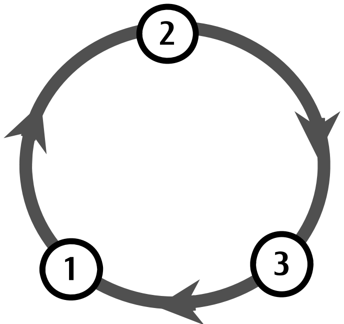
Qiong Zhang, Paparao Palacharla
Fujitsu Network Communications, Richardson, Texas, USA

Motoyoshi Sekiya, Junichi Suga, Toru Katagiri
Fujitsu Laboratories Limited, Kawasaki, Japan

Federated Learning (FL)

- FL is a distributed Machine Learning (ML) approach which enables ML models training on decentralized private data
- FL usually involves a central server and a group of clients
- FL can have hundreds of training rounds when converged
- FL server aggregates received local models from clients, e.g., weighted avg.

Clients get the global model and train it with local data, then provide local model to the server



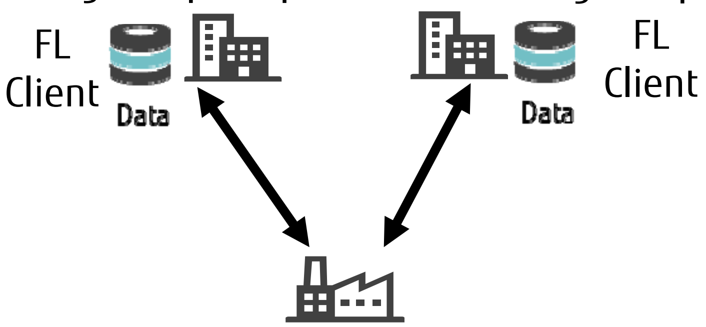
A FL server sends a global ML model to a group of clients

The server gets local models and aggregates them to a global model

Three steps in a single training round

local model: x1
#training samples: p1

local model: x2
#training samples: p2



FL Server

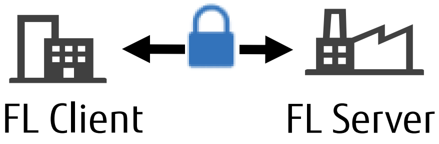
Aggregated global model: x0

$x0 = (x1 \cdot p1 + x2 \cdot p2)/(p1+p2)$

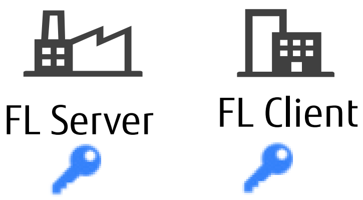
FL sever aggregation

Challenges in Federated Learning

- Focus on cross-silo FL
  - Organizations act as FL server/clients and share a common incentive to train a model based on all of their data
  - FL server and clients are physically distributed at different organizations



Secure network communications



Authentication

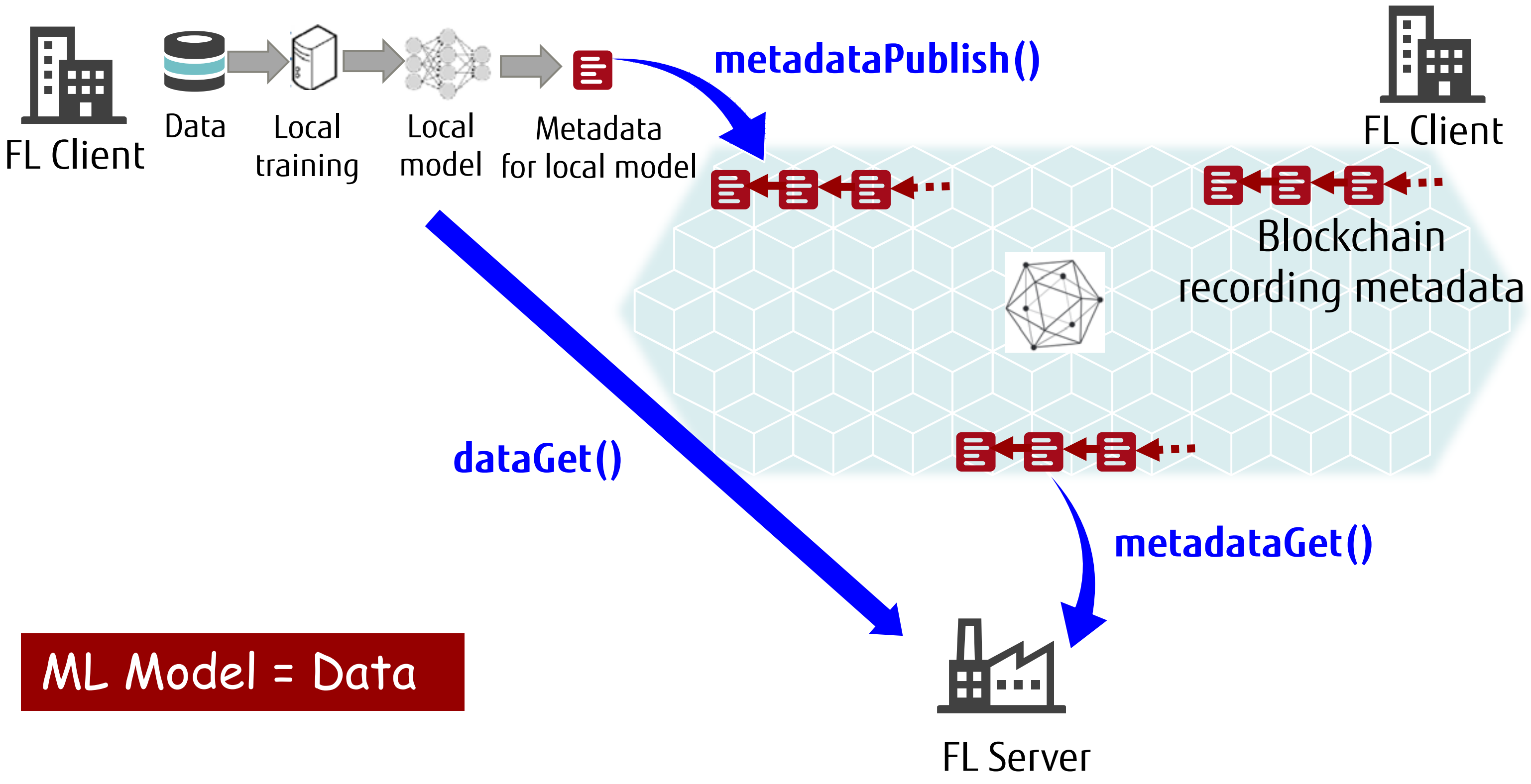
Tracking

P. Kairouz, et. al., “Advances and Open Problems in Federated Learning,” https://arxiv.org/abs/1912.04977

Blockchain for Data Exchange

Fujitsu's technology applying blockchain to enable secure data exchange

VPX: Virtual Private digital eXchage



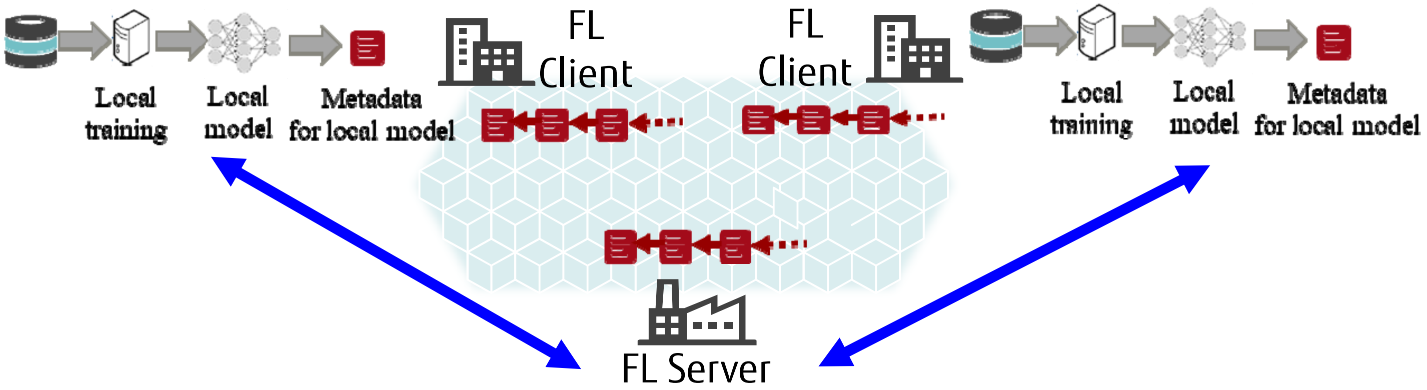
ML Model = Data

J. Suga and Q. Zhang, "Cross-Organizational Secure Data Exchange with Access Control using Blockchain," presented at Hyperledger Global Forum https://www.youtube.com/watch?v=YyKEQqxzBJI, March 2020.

Proposed Blockchain-based Protocol for FL

At FL Clients:

2. metadataGet()- read metadata from the blockchain
3. Check if a new global model is available. If no, go to step 2. If yes:
    4. dataGet() – get the global model from the server
    5. Local training on the local data set
    6. metadataPublish() – write metadata for the local model update to the blockchain; go to Step 2



At the FL aggregation server:

1. metadataPublish() – write initial global model metadata to the blockchain
7. metadataGet() – read metadata from the blockchain
8. Check if # available local models meets a threshold. If no, go to Step 7. If yes:
    9. dataGet() – get local model updates from the selected clients
    10. Aggregate local model updates to a new global model
    11. metadataPublish() – write the global model metadata to the blockchain; go to Step 7

Only the metadata of ML models are written to the blockchain, the actual models are directly transferred between FL server and clients

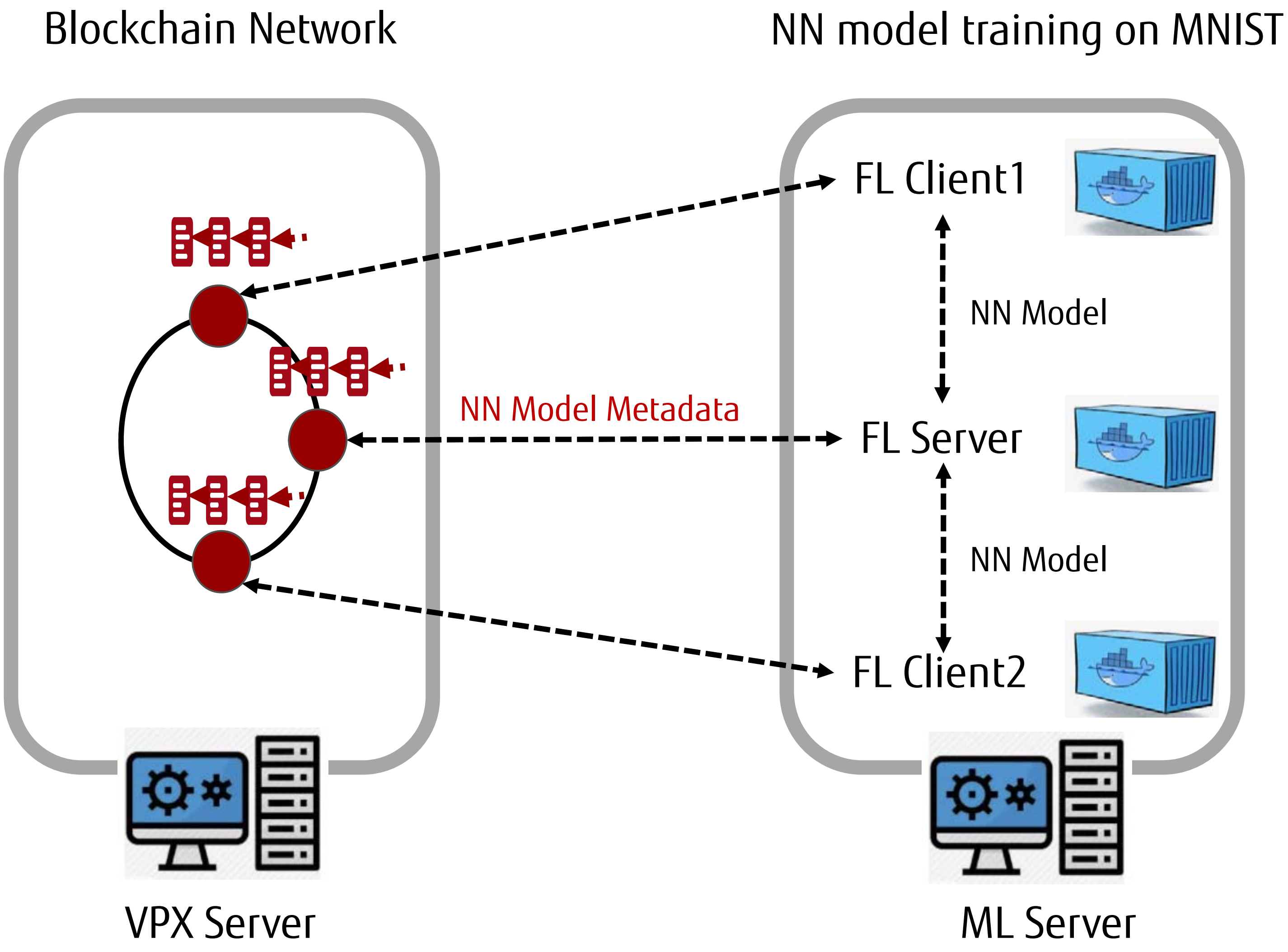
Advantages

- Track FL training steps with immutable records on the blockchain

- Transfer only selected ML models between FL server and clients
  - Consensus (metadata) on blockchain indicate the availability and quality of ML models
  - Enable client selection without transferring unnecessary local models to the server

- Simplify the underlying network configurations for FL
  - Take advantage of security features provided on the blockchain platform

Demo Configuration



FUJITSU

THE POSSIBILITIES ARE INFINITE