NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

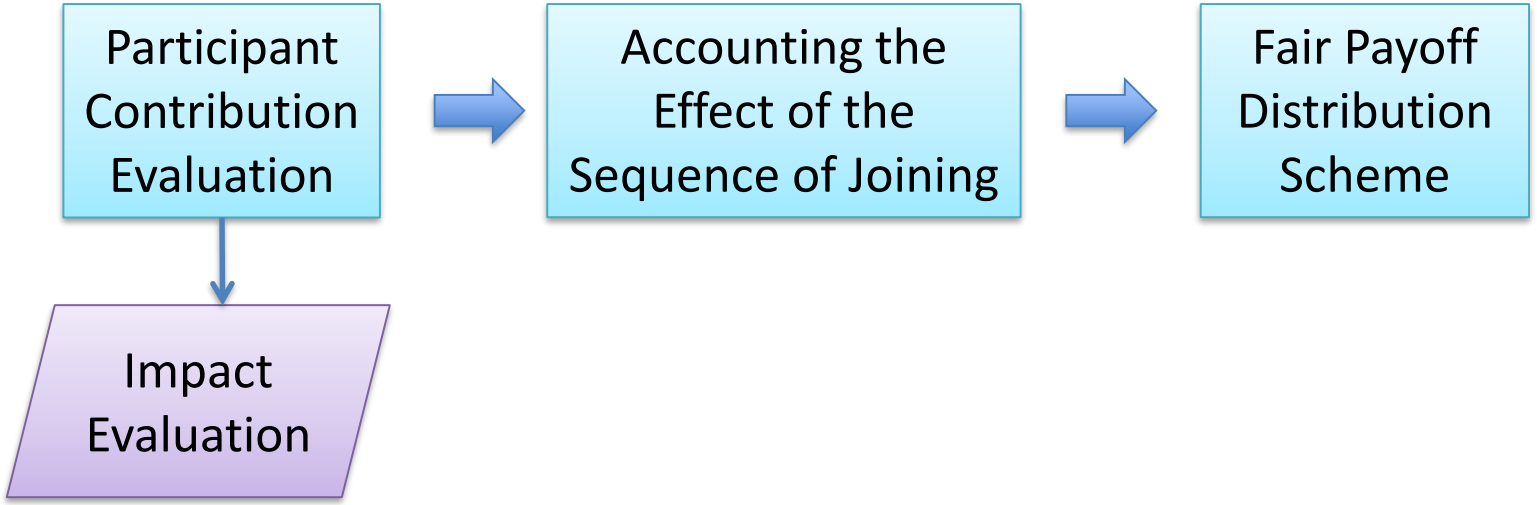
Federated Learning (Enrichment)

Han Yu

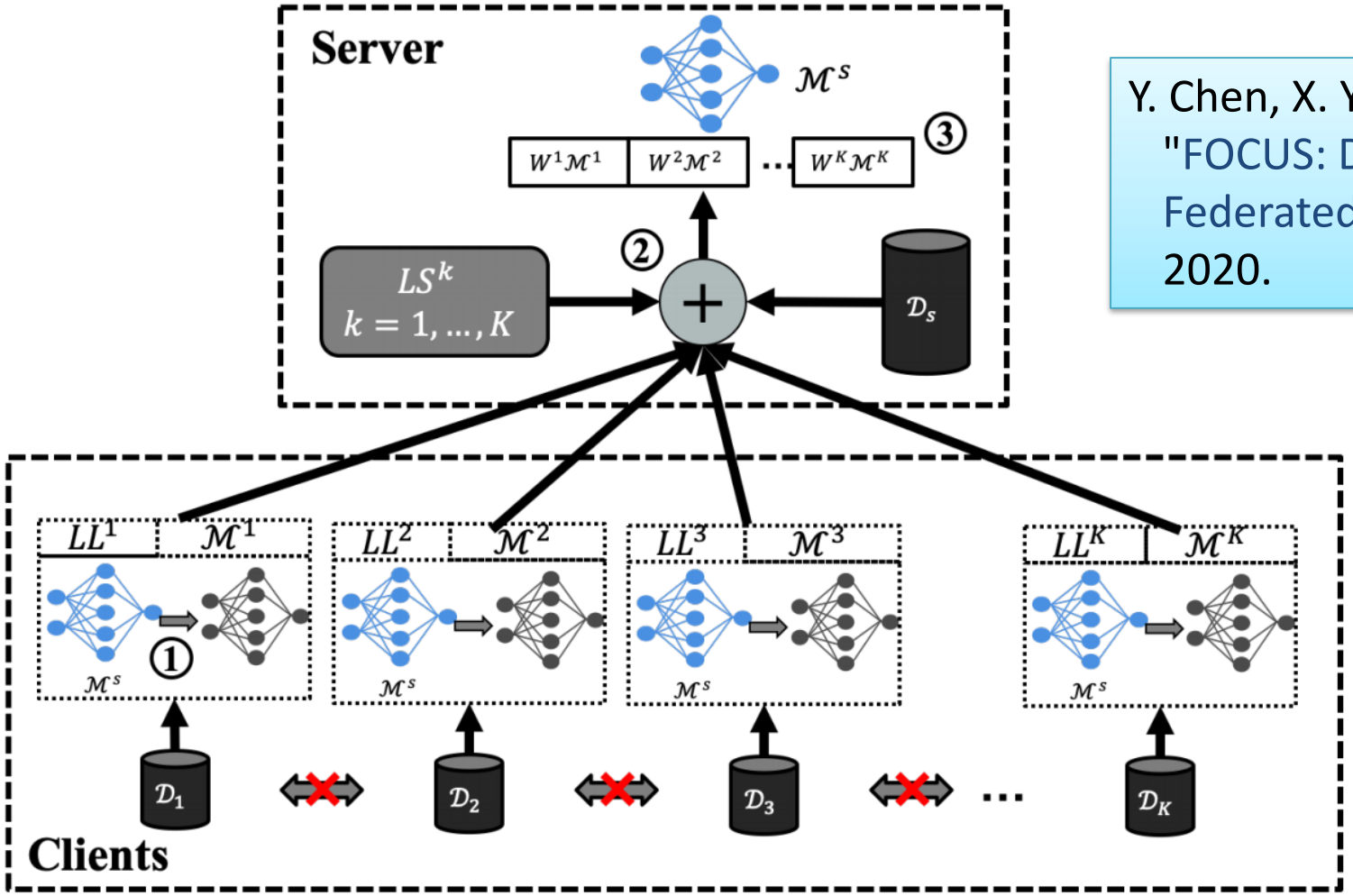
Nanyang Assistant Professor

School of Computer Science and Engineering
Nanyang Technological University
Singapore

Overview

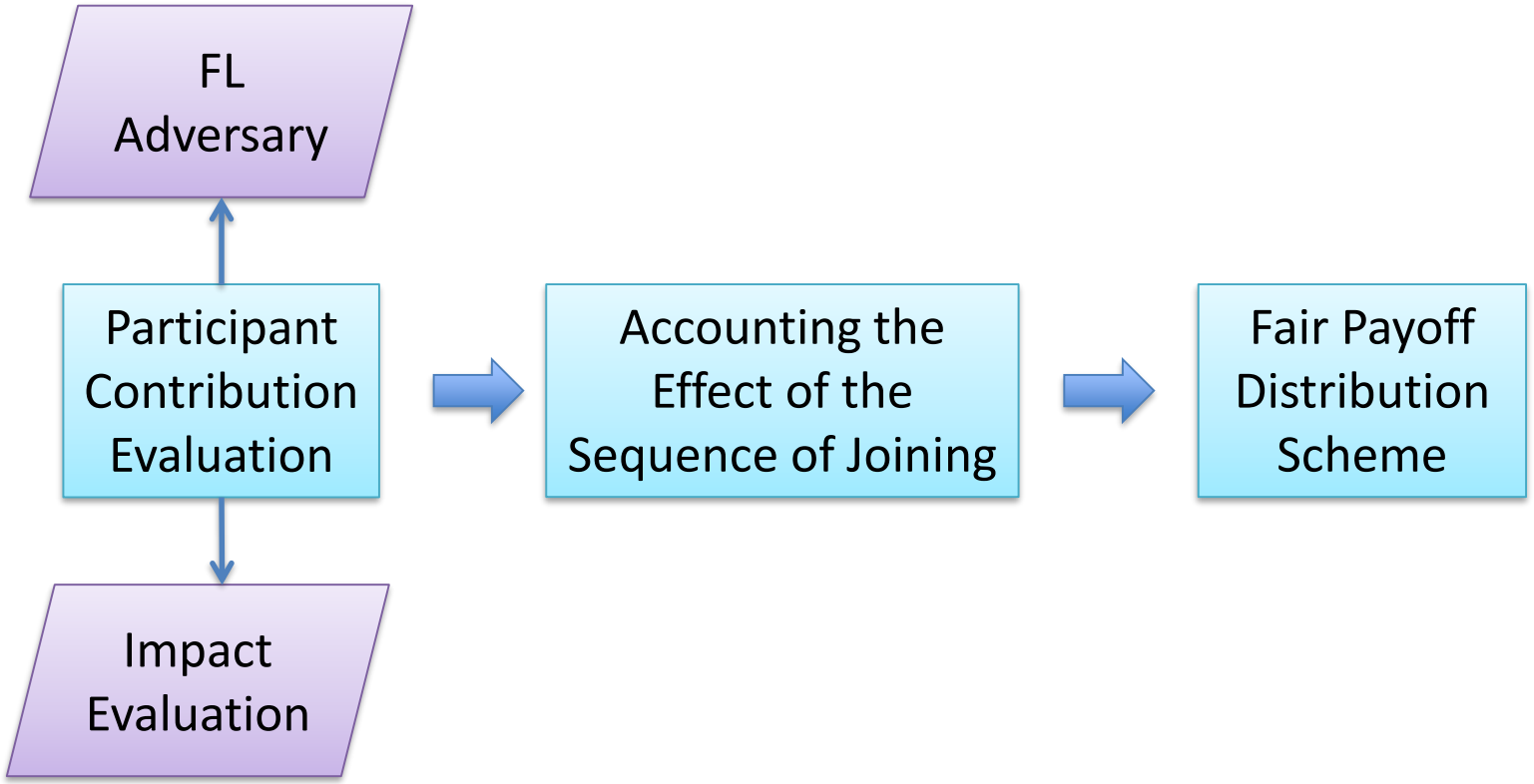

Participant Contribution Evaluation
Accounting the Effect of the Sequence of Joining
Fair Payoff Distribution Scheme
Impact Evaluation

Dealing with Label Quality Disparity in Federated Learning



Y. Chen, X. Yang, X. Qin, H. Yu, B. Chen & Z. Shen, "FOCUS: Dealing with Label Quality Disparity in Federated Learning," *CoRR*, arXiv:2001.11359, 2020.

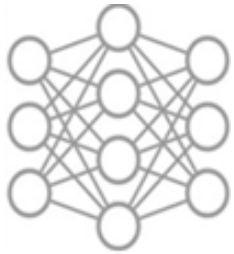
Overview


FL Adversary
Participant Contribution Evaluation
Impact Evaluation
Accounting the Effect of the Sequence of Joining
Fair Payoff Distribution Scheme

Game Theoretic Research for Adversarial FL Participants

Data Owner
(attacker)

1. **Attack** (e.g., inject biased data, artificially enlarging its dataset, etc.)
2. **Do not Attack**



Data Federation
(defender)

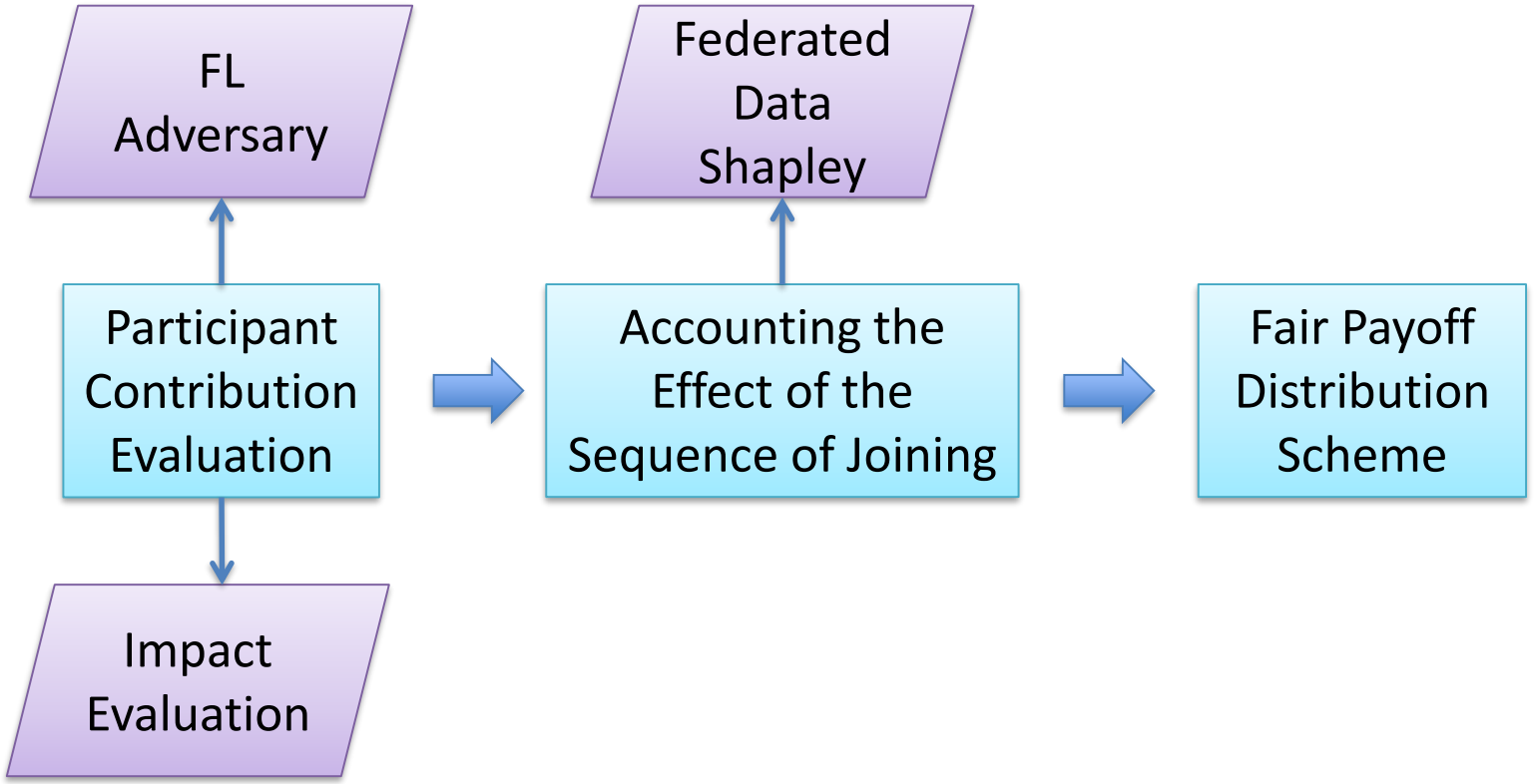
1. **Detect in Sandbox and Reject Dataset** (no payment)
2. **Retrain Model** (detected late, costly, serious reputation sanctioning affecting FLI payoff)
3. **Do nothing**
4. **… …**

- Can we find a dynamic and cost-effective best response function for the defender that maximizes the attacker's probability of selection "Do not Attack"?
- Defenders:
  - Faces many types of threats
  - Has a limited budget for screening submitted model parameters (different screening methods incur different costs)
  - Can announce punitive measures before-hand

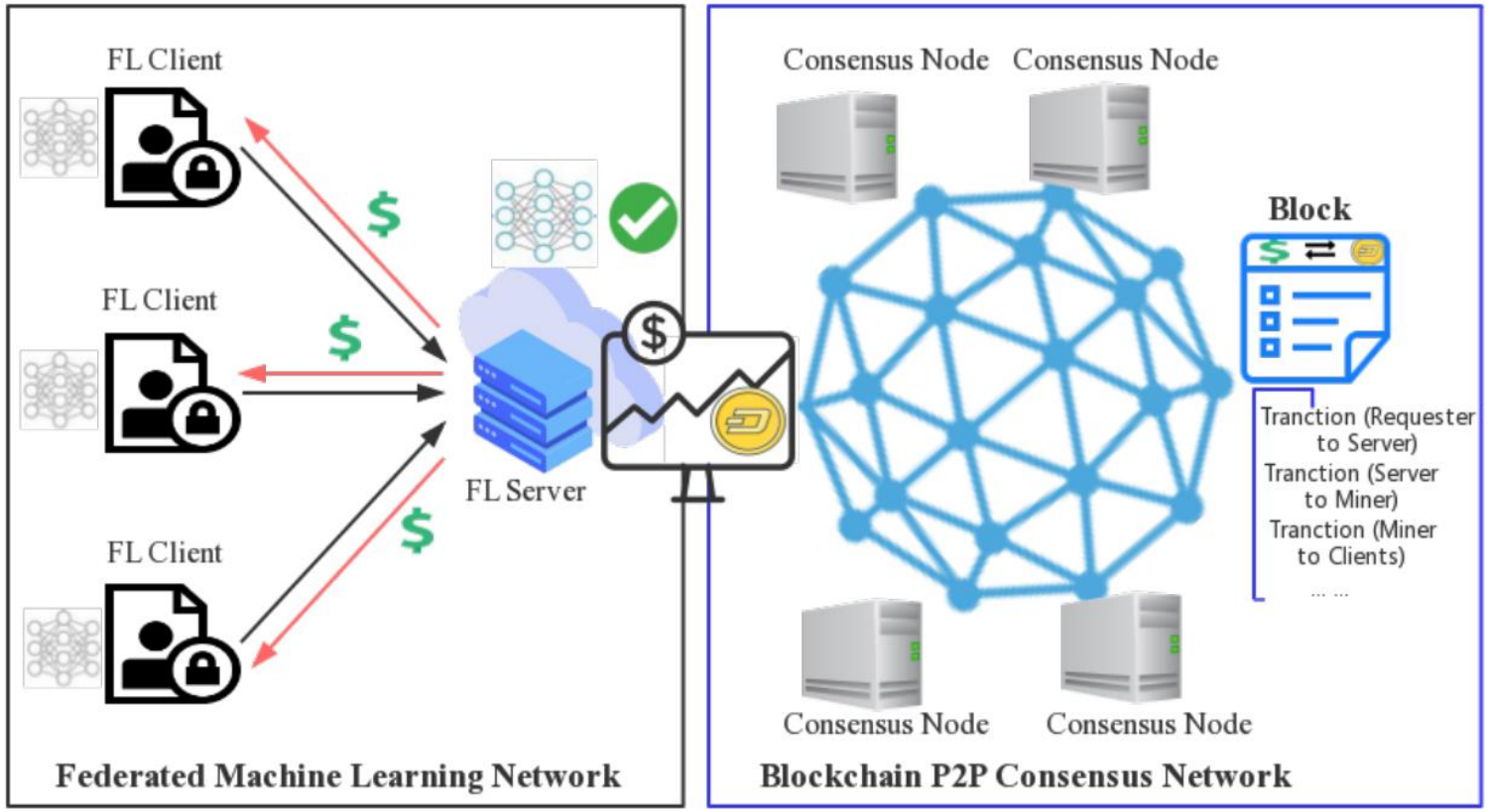
L. Lyu, H. Yu & Q. Yang, "Threats to Federated Learning: A Survey," *CoRR*, arXiv:2003.02133, 2020.

Following the Stackelberg Game formulation, *since the leader (attacker) will make the first move, she knows that a rational follower (the data federation) will react by maximizing the follower's payoff. The attacker takes this into account before making the first move.*

Overview


FL Adversary
Federated Data Shapley
Participant Contribution Evaluation
Accounting the Effect of the Sequence of Joining
Fair Payoff Distribution Scheme
Impact Evaluation

FedCoin: A Peer-to-Peer Payment System for Federated Learning

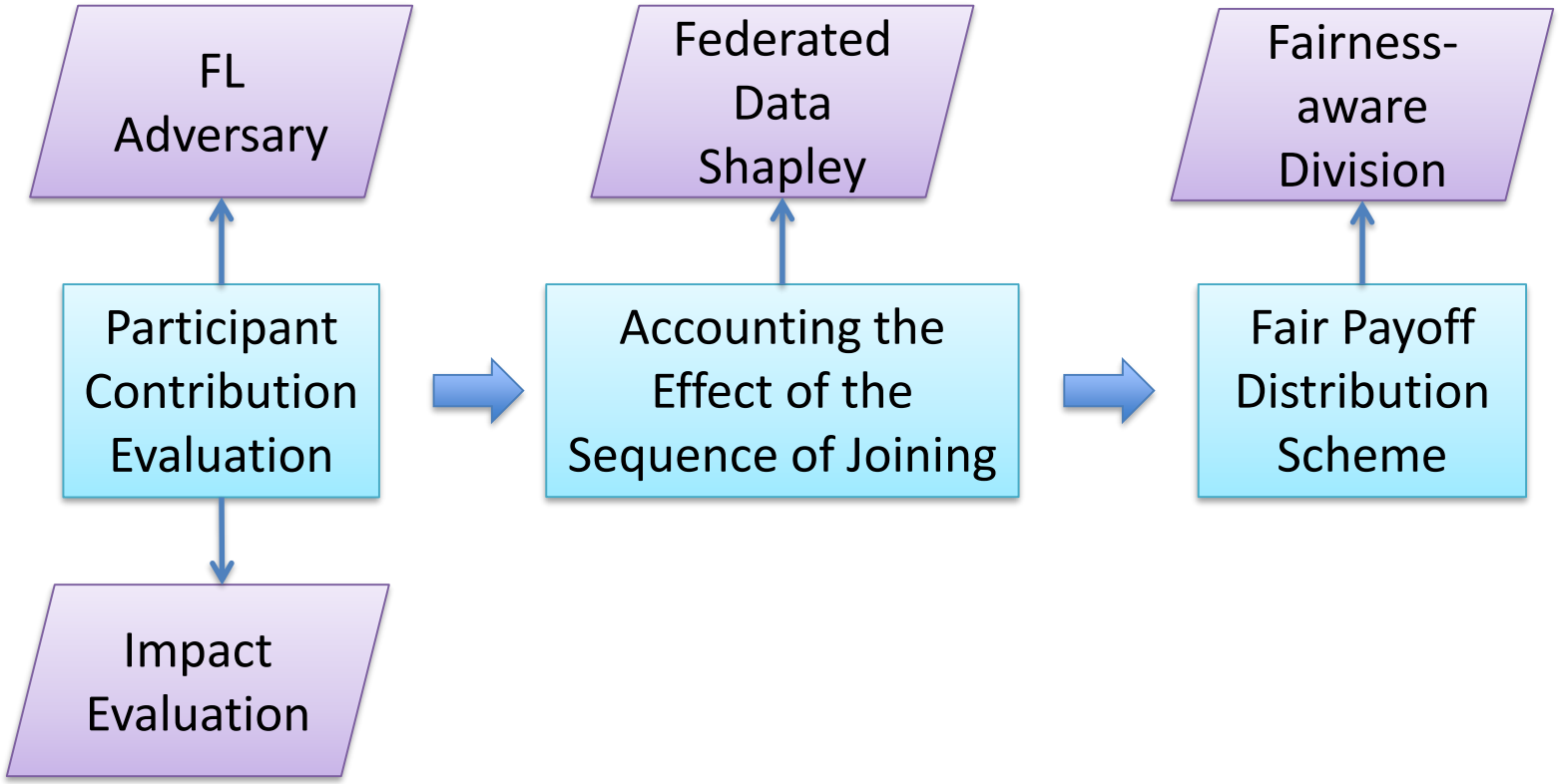


Demo Video: https://youtu.be/u5LPLdZvd0g

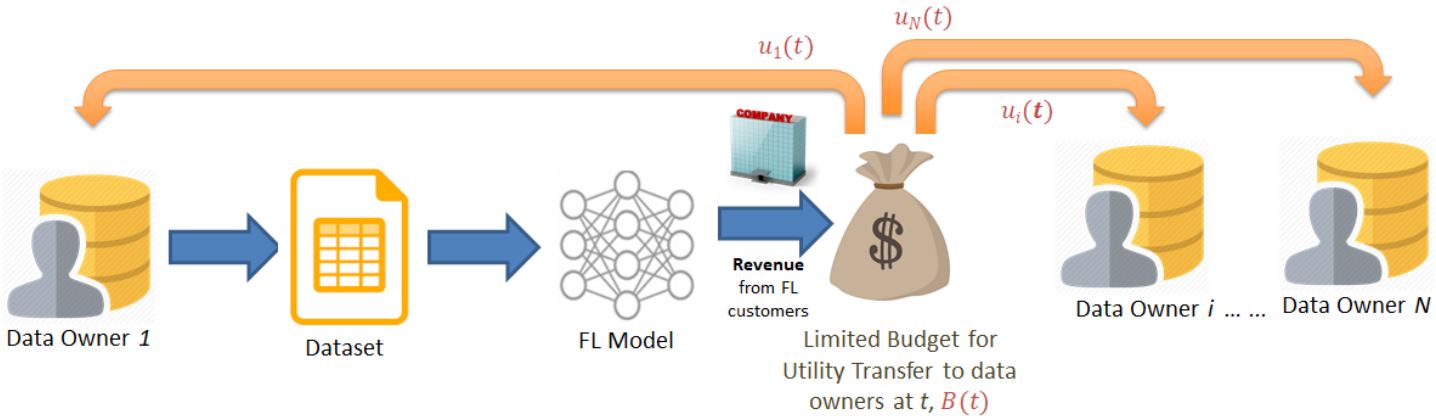
Y. Liu, S. Sun, Z. Ai, S. Zhang, Z. Liu & H. Yu, "FedCoin: A Peer-to-Peer Payment System for Federated Learning," *CoRR*, arXiv:2002.11711, 2020.

Under FedCoin, blockchain consensus entities calculate SVs and a new block is created based on the proof of Shapley (PoSap) protocol. The winning node divides the payoff among FL clients, and receives a fee.

Overview


FL Adversary
Federated Data Shapley
Fairness-aware Division
Participant Contribution Evaluation
Accounting the Effect of the Sequence of Joining
Fair Payoff Distribution Scheme
Impact Evaluation

A Fairness-aware Incentive Scheme for Federated Learning



H. Yu, Z. Liu, Y. Liu, T. Chen, M. Cong, X. Weng, D. Niyato & Q. Yang, "A Fairness-aware Incentive Scheme for Federated Learning," in *Proceedings of the 3rd AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society (AIES-20)*, pp. 393–399, 2020.

Individual

Contribution

- $q_i(t)$: Contribution of the dataset towards improving the FL model at t

Data Owner i

Cost

- $c_i(t)$: Cost of contributing a dataset at t
- $Y_i(t)$: A "regret queue" to track payoff due for data owner i at t
- $Q_i(t)$: A "temporal queue" to track how long data owner i has been waiting to receive full payoff from the federation at t

The Data Federation

Collective Utility

$U = \frac{1}{T}\sum_{t=0}^{T-1}\sum_{i=1}^{N} u_i(t)q_i(t)$:
Data owners who contribute high quality datasets should receive high payoff

Distribution of "Regret"

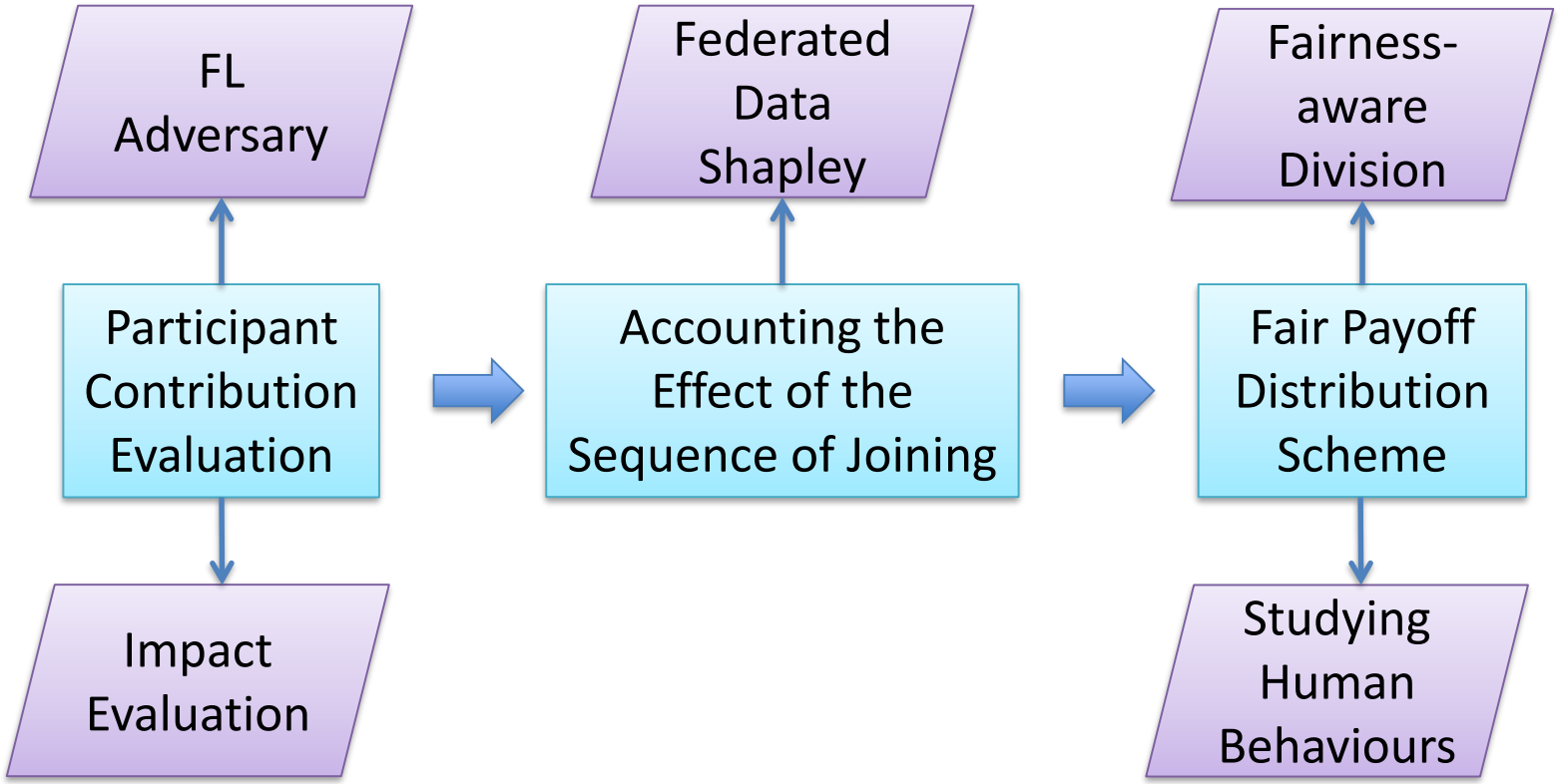
$$L(t) = \frac{1}{2}\sum_{i=1}^{N}[Y_i^2(t) + Q_i^2(t)]$$

$$\Delta = \frac{1}{T}\sum_{t=0}^{T-1}[L(t+1) - L(t)]$$

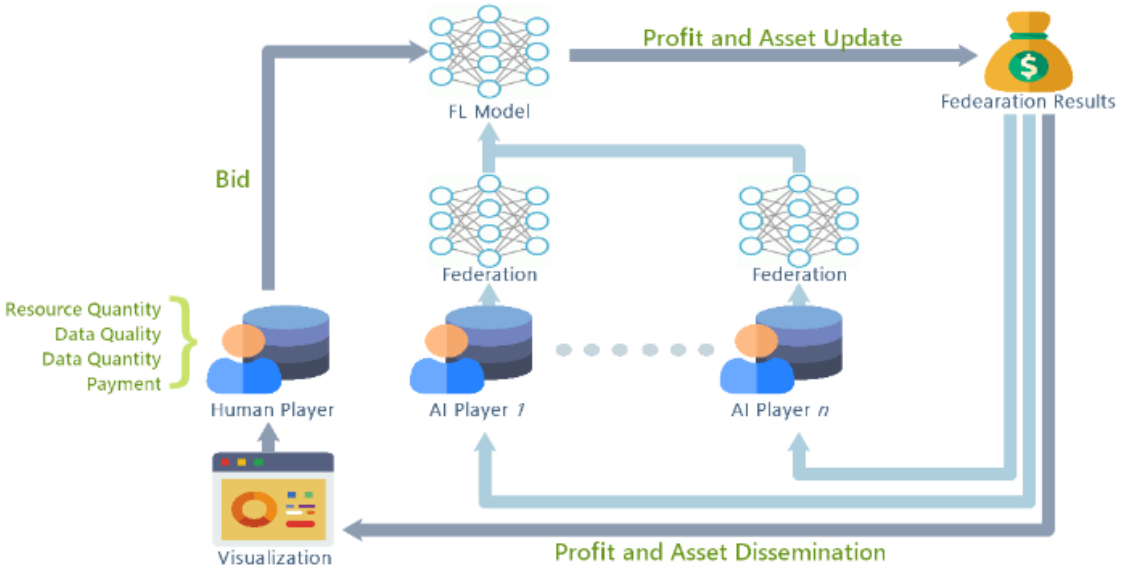
Distribution of regret and waiting time among data owners + the change of such distributions over time

- **Contribution Fairness:** a data owner i's payoff shall be positively related to his contribution qi(t);
- **Regret Distribution Fairness:** the difference of the regret and the temporal regret among data owners shall be minimized; and
- **Expectation Fairness:** the fluctuation of data owners' regret and temporal regret values shall be minimized

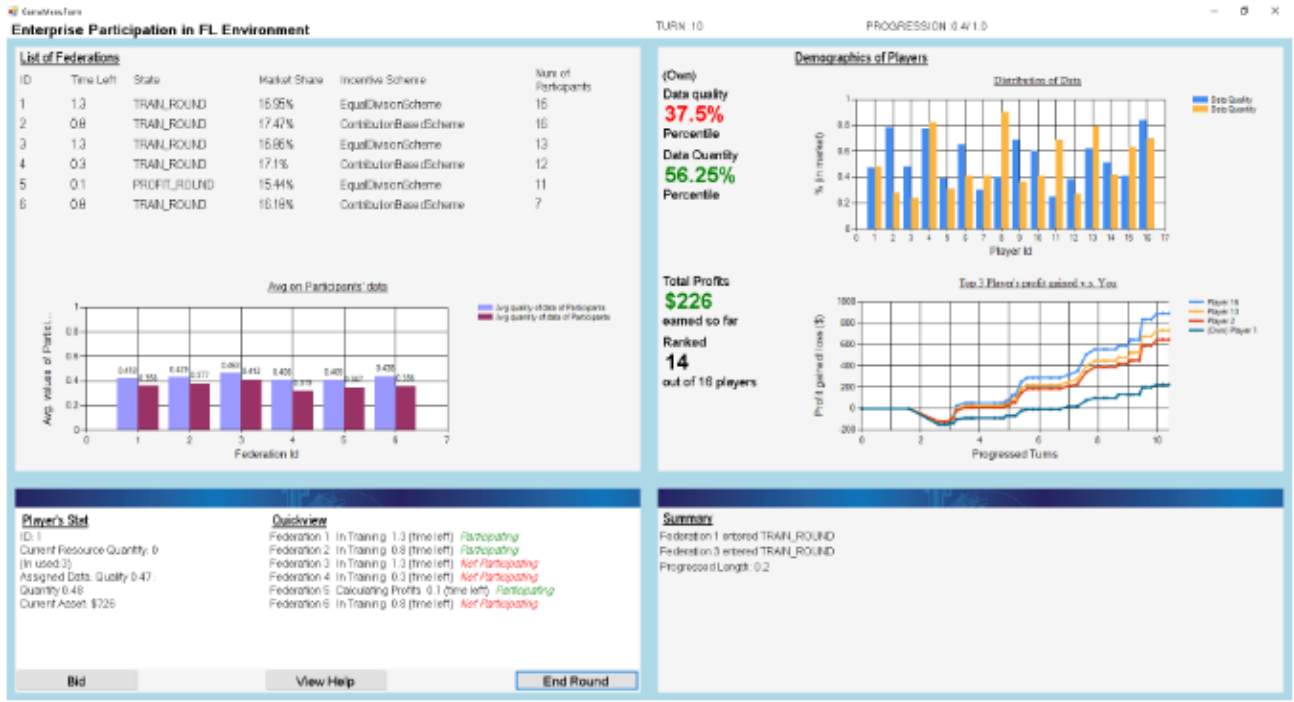
Overview


FL Adversary
Federated Data Shapley
Fairness-aware Division
Participant Contribution Evaluation
Accounting the Effect of the Sequence of Joining
Fair Payoff Distribution Scheme
Impact Evaluation
Studying Human Behaviours

A Multi-player Game for Studying FL Incentive Schemes



- To design an effective incentive scheme, it is important to understand how FL participants respond under such schemes.
- We propose a multi-player game to study how FL participants make action selection decisions under different incentive schemes.
- It allows human players to role-play under various conditions to guide FL incentive research.



Demo Video: https://youtu.be/4qd48QfcsXI

Thank you!