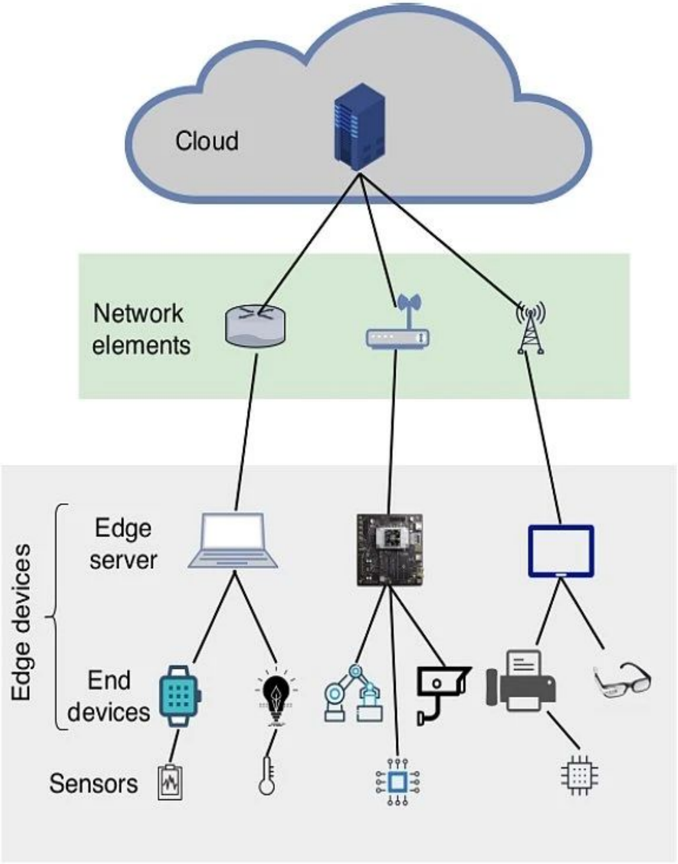
IPAFLB

Incentive-Based Privacy Preserving Asynchronous Federated Learning over Blockchain

Atharva Haldankar, Thomas Nguyen, Arman Riasi

Introduction

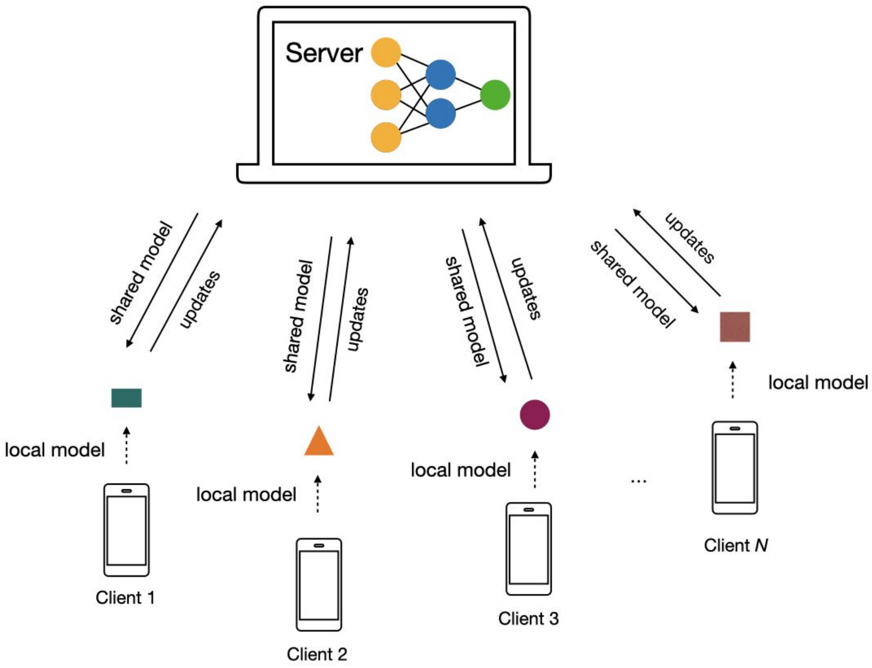
- Edge devices gather a large amount of data
  - Conducive to ML
- Privacy & scalability concerns
  –> Federated Learning (FL)
- FL Challenges:
  - Data and Device Heterogeneity
  - Privacy & Security Concerns
  - Incentive for Good Behavior



https://viso.ai/wp-content/uploads/2021/04/general-overview-of-the-edge-computing-architecture.jpg

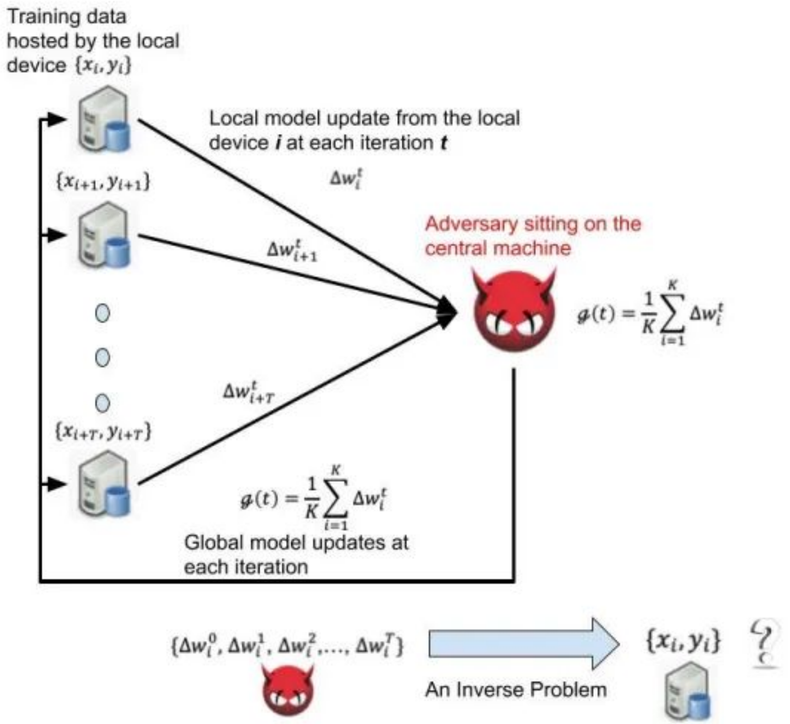
Federated Learning

- Data never leaves edge devices
- Organized into rounds
    a. Clients download global model
    b. Clients perform local updates
    c. Clients upload model weights
    d. Server aggregates client updates



FL Challenges

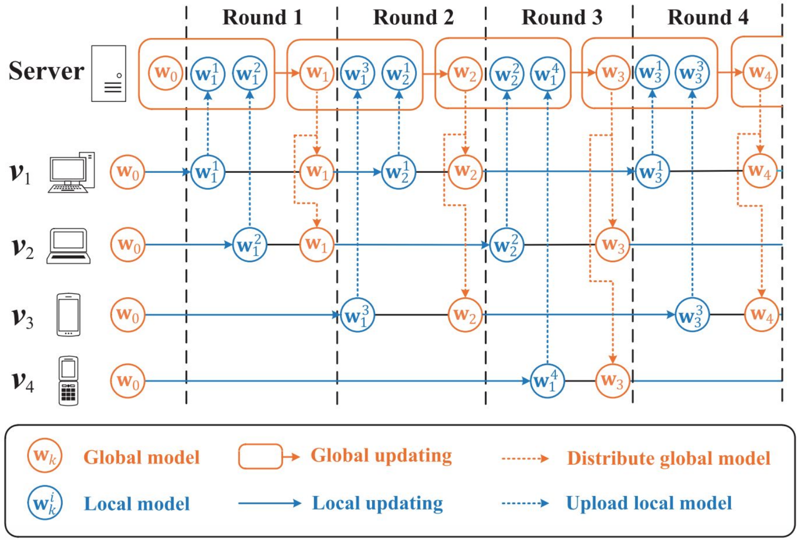
- Straggler problem
  - Server has to wait for slowest client
  - Caused by device/data heterogeneity
- Privacy/Security
  - Membership Inference Attacks
  - Model Poisoning Attacks
- Incentive Mechanism
  - Encourage honest and active nodes



https://www.nortonlifelock.com/sites/default/files/styles/blogs_inline_small/public/2020-01/Model%20Inversion.jpg.webp?itok=1TPfMGVH

Asynchronous FL

- Clients can join training process at any time
  - Different notion of rounds
- Fully asynchronous:
  - One client update –> Global update
- Semi-asynchronous:
  - K client updates –> Global update
- Challenge: Staleness



https://ieeexplore-ieee-org.ezproxy.lib.vt.edu/stamp/stamp.jsp?tp=&arnumber=9533794&tag=1

Incentive Mechanism

- The incentive should encourage all nodes to actively collaborate on the training process
- We are interested in non-monetary incentives
  - Fairness: “better models” for nodes with major contributions
  - Personalize: meet client interest/objective (due to data heterogeneity)
- The ability to track/acknowledge major contributions for future rewards
- Challenge: require an applicable privacy-preserving method

State-of-the-Art Limitations

- Straggler effect due to data heterogeneity, limited bandwidth, network disruption
  - Causing the overall system to perform slower
- The gap between the current asynchronous approach and an applicable privacy-preserving mechanism
- For current incentive mechanisms:
  - Game-based monetary reward
  - Less contribution —> less effective model (by reweighting global model)

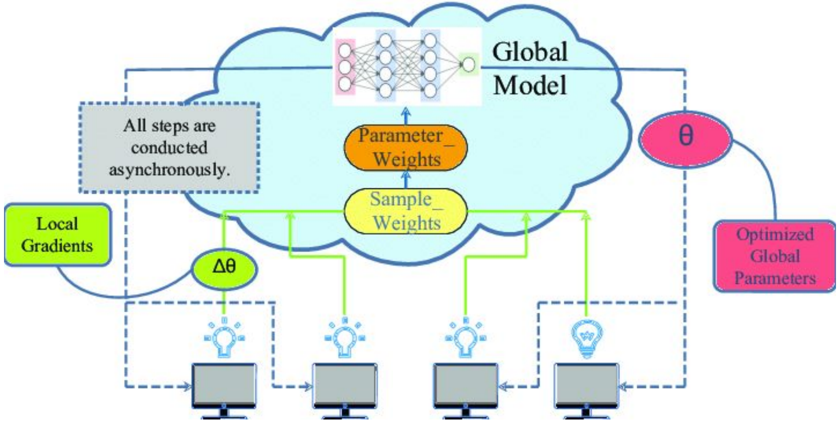
Our Contributions

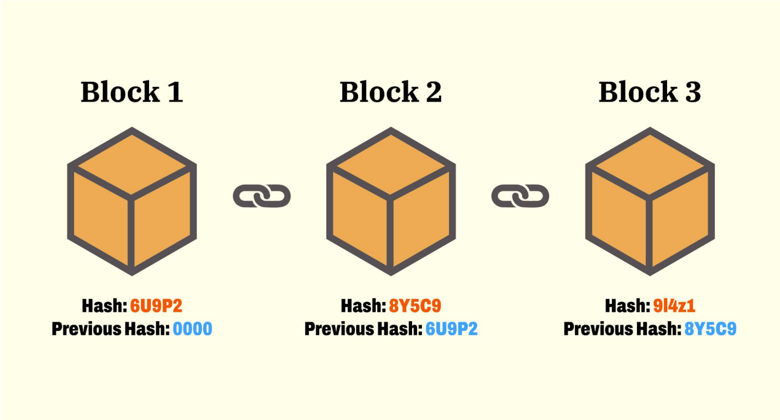
- We proposed a method for FL that works in a semi-asynchronous setting
- We applied a privacy-preserving mechanism to the proposed FL method
- We employed the blockchain as an immutable distributed ledger
- We studied existing incentive mechanisms for FL and their practicality

System Model

System Model

- N clients; 1 aggregation server
- Semi-Asynchronous FL setting
  - Server aggregation after k client updates
  - Staleness bound
  - Urgent notifications
- Blockchain
  - Immutable distributed ledger
  - Smart contracts
    - Record encrypted weights



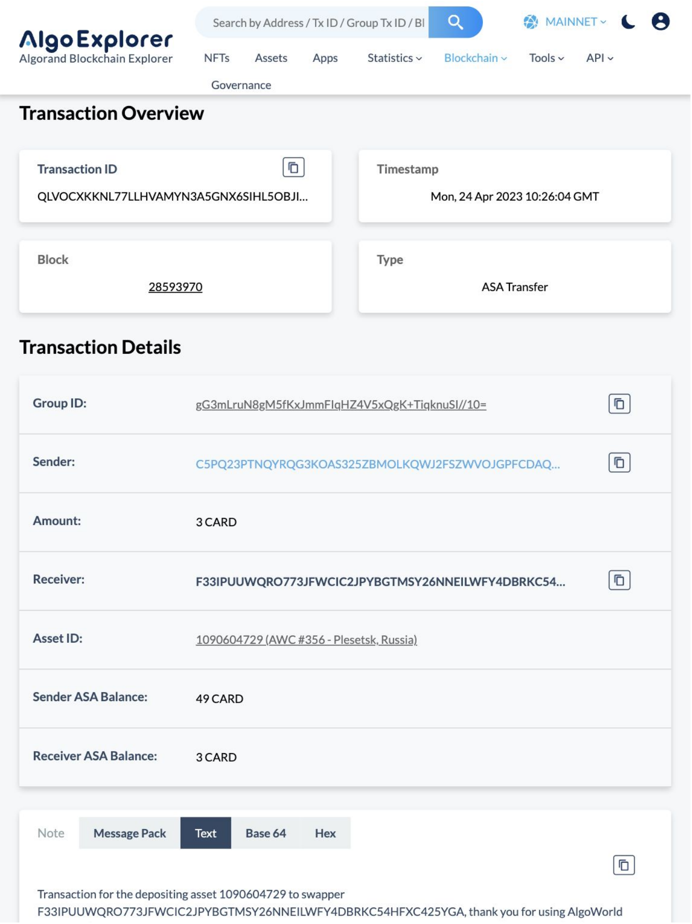


https://www.researchgate.net/publication/339669150/figure/fig3/AS:865167944450049@1583283520259/Detail-of-asynchronous-federated-learning-in-PAFLM.png
https://img.money.com/2022/06/What-Is-Blockchain-Infographic.jpg

Network Model

Network Model

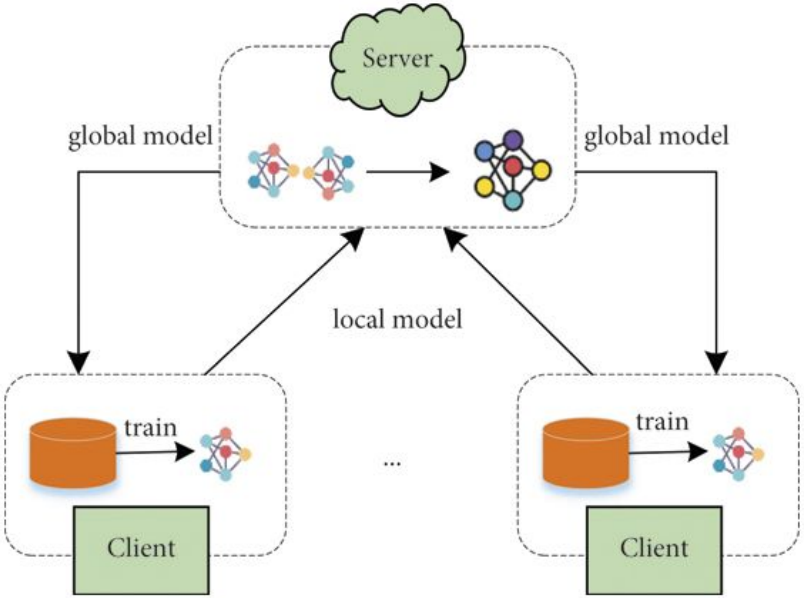
- The interaction between clients and the aggregation server occurs through blockchain smart contracts:
  - The Smart Contract ID:
    - The identification number for smart contracts.
  - The Transaction Note Field:
    - The area for noting transaction information.



Threat Model

Threat Model

- Adversary: server
- Goal
    - Break confidentiality
    - Infer client data from model uploads
- Semi-Honest (Honest-but-curious)
    - Server will follow the protocol
    - However, will try to infer sensitive client data

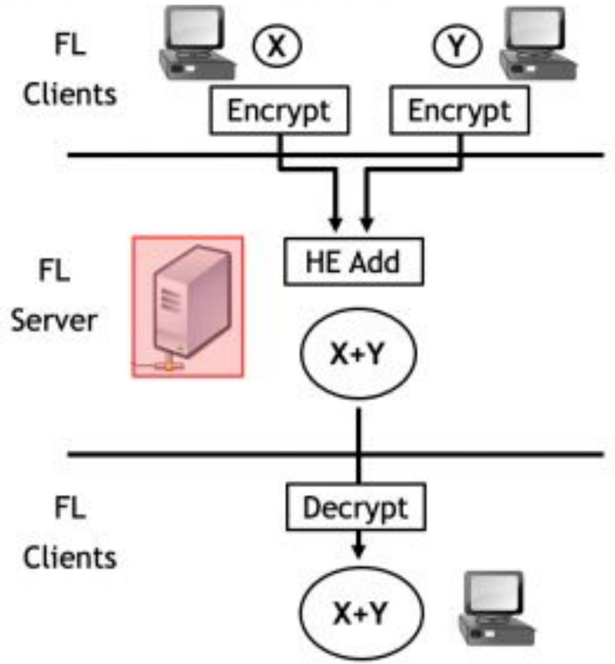


https://static.hindawi.com/articles/scn/volume-2022/7268347/figures/7268347.fig.001.jpg, https://cdn1.vectorstock.com/i/1000x1000/91/10/icon-of-red-devil-vector-18879110.jpg

Security Model

Security Model

- Homomorphic Encryption
  - Allow aggregation on encrypted local models
  - Achieve confidentiality
- Blockchain as a distributed ledger
  - Allow clients to commit their local models in an asynchronous manner
  - Acknowledge client contribution in FL process
  - Achieve immutability



https://developer-blogs.nvidia.com/wp-content/uploads/2021/06/Why-homomorphic-encryption-1.png

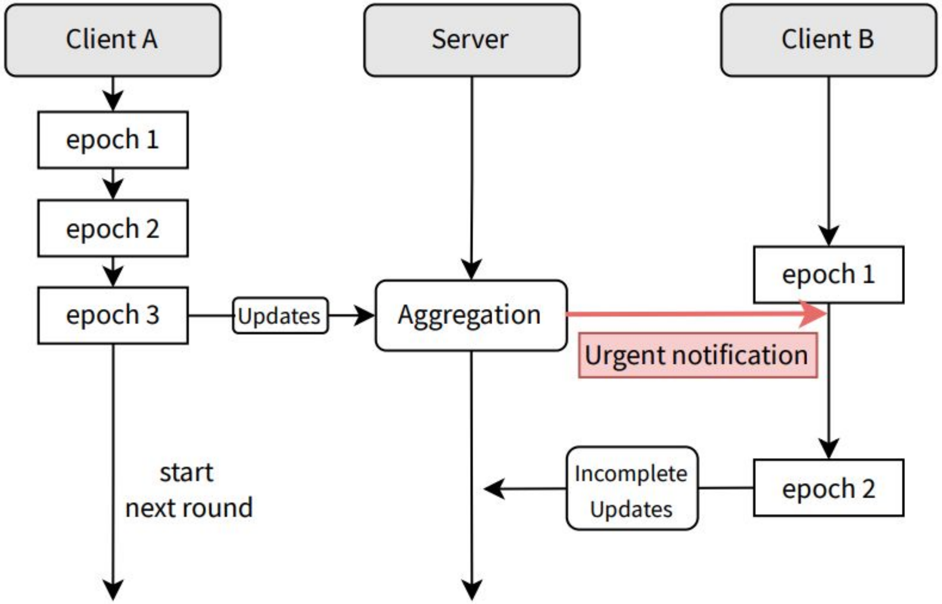
Research Methodology: Terminology

$t - \tau$	Staleness Value
$s(t - \tau)$	Staleness function
Ω	Staleness bound
Π	Threshold weight difference
w_t	Global model on epoch t
w_t^i	Client i's uploaded weights on global epoch t

Research Methodology: AFL

- Server aggregates weights after k client updates, unless:
  - One or more clients reach the staleness bound (Case #1)
    - $t - \tau = \Omega$
    - Those clients are sent an urgent notification from the server
  - A client upload significantly changes the global model (Case #2)
    - $w_t^i - w_{t-1} >= \Pi$
    - All clients training on w_{t-1} or an earlier model get an urgent notification
- Upon receiving the urgent notification:
  - Clients finish current local epoch then upload weights to server
  - Server doesn't aggregate until receiving all stale client updates

Research Methodology: AFL

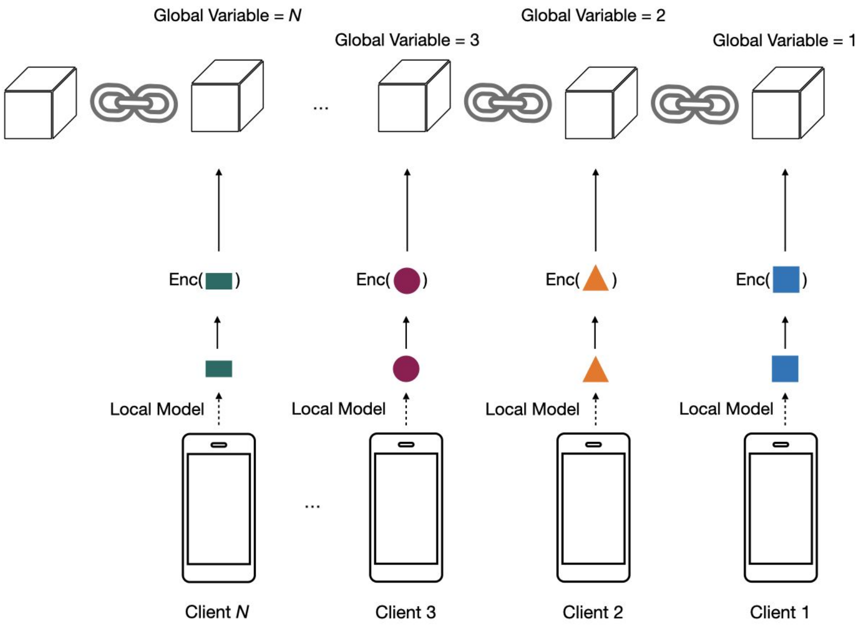


push-pull mechanism

https://iqua.ece.toronto.edu/papers/ningxinsu-iwqos22.pdf

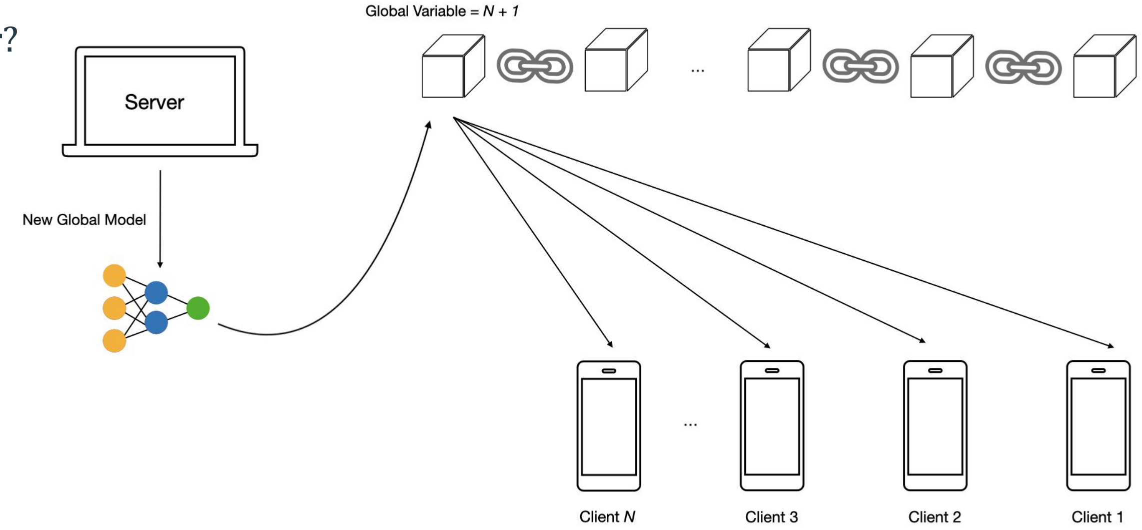
Research Methodology: Privacy Preserving

- What is the role of each Client?
  - What to upload?
    - Encrypted weights
  - Where to upload?
    - Smart Contracts



Research Methodology: Privacy Preserving

- What is the role of the Server?



Conclusion & Future Work

- We proposed a semi-asynchronous approach for FL:
  - Achieve confidentiality for the FL process under semi-honest server
  - Use blockchain to acknowledge contribution and achieve immutability
- Future work:
  - Analyze convergence rate for FL on the proposed semi-asynchronous method
  - Research security mechanisms for preventing poisoning attack
  - Research metric to quantify major contributions from the clients
  - Adjust global model to incentivize clients based on their interest

Thank You