Blockchain-based Federated Learning: privacy and incentive

ECE6903J - Distributed Machine Learning Systems (Research project)

Hugo Vanhille, Pedro Hernández Rubio

Department of Automation

2022 年 12 月

目录

第 1 节

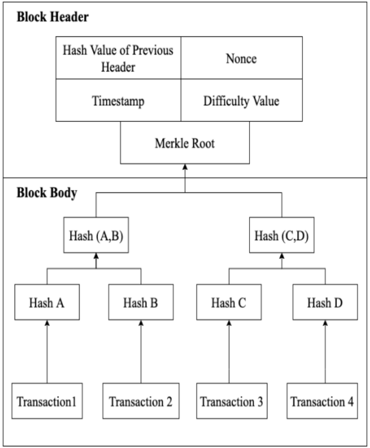
Background

Motivation

- Research interest mainly targeted to blockchain technology (its application to distributed Machine Learning systems)
- Specifically, applied to data-aggregation systems (e.g. crowdsensing in the Internet of Things (IoT) field)
- Could similar approach be applied for Federated Learning?

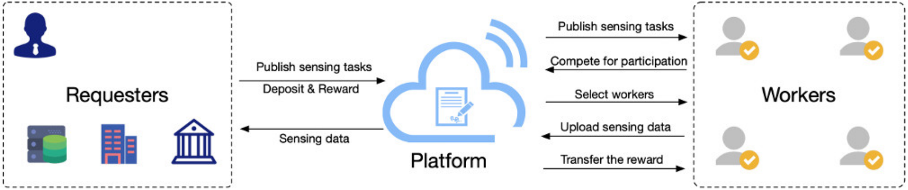
Blockchain technology

Distributed ledger containing a time-stamped series of immutable blockchains, trustless, decentralized, proof-tampering and full traceability



Crowdsensing: definition

- **Crowdsensing:** emerging paradigm of data aggregation, having a key role in data-driven applications. Specially used for getting large ammounts of IoT sensing data, by using the individual intelligent sensing devices.
- **Benefit:** improved data collection efficiency and reduced costs effectively



Crowdsensing issues: security

1. Managed and maintained centralized platforms suffer from the single point of failure

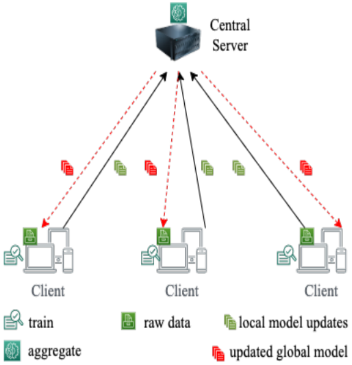


图: Topology of traditional FL

Crowdsensing issues: incentive

1. Encouraging workers by offering appropiate incentive mechanisms (monetary usually) →auction theory guarantees benefits for both requesters and workers but only provide short-term incentives

图: Monetary reward

图: Worker reputation

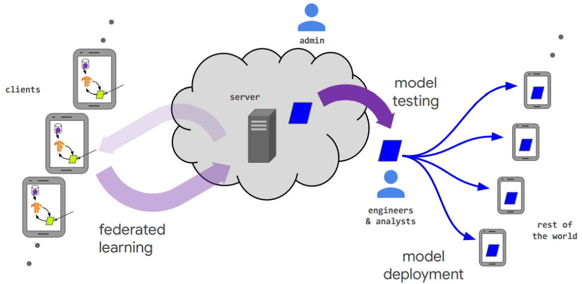
图: Data quality

第 2 节

Research

The privacy-preserving of Federated Learning

- FL provides an attractive structure for decomposing the overall machine learning workflow into the approachable modular units we desire.
- FL provides a level of privacy to participating users through data minimization.



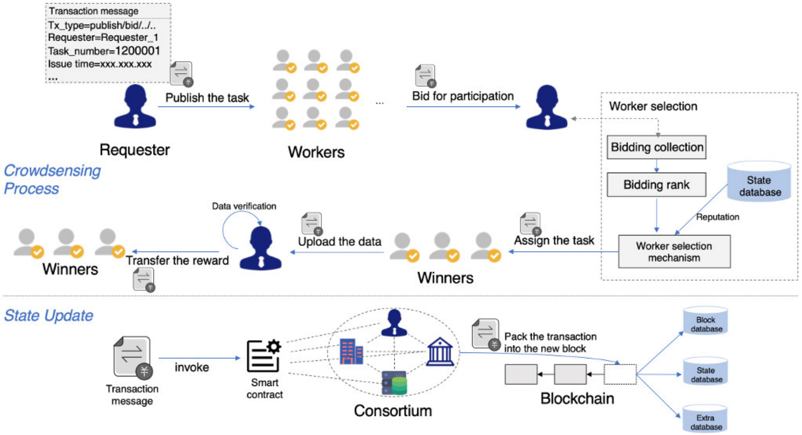
The incentive mechanism of Federated Learning

- Main types of incentive mechanisms:
  1. Monetary-based: distributing rewards.
  2. Reputation-based: reputation framework for worker selection (algorithms)
- **Limitations**
  1. Relies on a central platform, vulnerable to target attacks
  2. Single-attribute incentive mechanisms (multifactor incentive needed)

第 3 节

System architecture

System architecture



第 4 节

Security issues: privacy

Provenance of data

Model updates

A blockchain-based privacy-preserving federated learning framework leverages the immutability and decentralized trust properties of blockchain to provide the provenance of model updates **(smart contracts)**

Data privacy

Improving data privacy in FL scenario:

- Storing evidence: by using hashing and fingerprint mechanisms, references can be stored proving both local data and models are correct
- Limiting access: by making the ledger network only accessible via private network of participants
- Zero Knowledge Proofs: advanced (and computationally expensive) cryptographical techniques for granular information disclosure (both for mutual verification and partial data disclosure)

第 5 节

Quality management: incentive

Incentive mechanism

Federated Learning scenario

An effective incentive mechanism combining reputation with contract theory motivates high-reputation mobile devices with high-quality data to participate in model learning

Mechanism design: multifactor

- Based on three parameters:
  1. Workers' bidding
  2. Reputation
  3. Recent data quality estimation
- Analytic Hierarchy Process (AHP) framework →(top-down)
  1. Objective level: winning workers
  2. Criteria level: parameters criteria
  3. Alternative level: workers available

Multifactor worker evaluation approach

$$\theta_i = \omega_1 B_i + \omega_2 R_i + \omega_3 Q_i \qquad \text{where } \omega_i \geq 0 \text{ and } \sum_{\omega_i=1}^{3} \omega_i = 1$$

Mechanism design: issues

1. **How to select appropriate workers?**
   - **Proposal:** decentralized architecture (blockchain technology) that lacks a single point of failure, and enhances privacy with asymmetric encryption and digital signature technology
2. **How to distribute the rewards to the workers?**

With the help of mechanism design theory two important properties for the incentive mechanism are guaranteed:

- **Incentive quality (IC):** the truthful submission of training cost is the worker's optimal bidding strategy
- **Individual rationality (IR):** the reward must compensate for the worker's cost (non-negative)

第 6 节

Conclusions

Results

- **Benefits of consortium blockchain technology:**
  - resistant to the single point of failure (system security)
  - more transparency (trusting data provenance)
  - privacy-preserving (e.g. ZKP)
  - cooperative management (by requesters) reduces cost and enhances the flexibility of the system (selection criteria)
- **Benefits of hybrid incentive mechanism:**
  - encourages workers to contribute valuable data (and penalizes malicious ones)
  - ensures favorables short-term and long-term incentives for workers

Limitations

Further research:

1. Dynamic situation where evaluations attributes are changing
2. Optimization of consensus protocol (better performance)
3. Further protection of worker privacy

谢谢