



# 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

## ① Background

Motivation  
Crowdsensing

## ② Research

Problems  
The privacy-preserving of crowdsensing  
The incentive mechanism of  
crowdsensing

## ③ System architecture

Software application

## ④ Security issues: privacy

Single point of failure

## ⑤ Quality management: incentive

Mechanism design: multifactor  
Mechanism design: issues

## ⑥ Conclusions

Application  
Limitations  
Further research



## 第 1 节

# Background



## 第 1 节

## Background

## 第 1 小节

## Motivation



# Motivation

## Goal

Applying ML to systems (blockchain-based models)

- Research line mainly targeted to **blockchain technology** (its application to systems)
- Research group in Department of Automation (PhD supervisors) has been recently working in blockchain-based models applied to **trust management systems**
- Specifically, applied to data-aggregation systems in the Internet of Things (IoT) field **crowdsensing**
- Could similar approach be applied for **Federated Learning**?



## 第 1 节

## Background

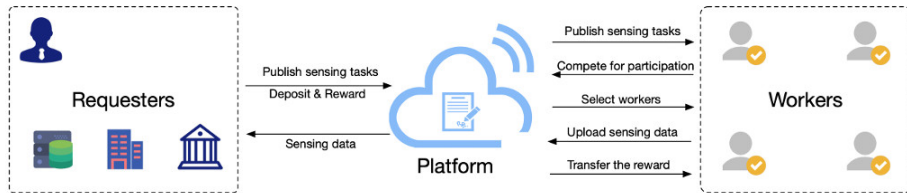
## 第 2 小节

## Crowdsensing



# Crowdsensing: definition

- **Crowdsensing:** emerging paradigm of data aggregation<sup>paper1</sup>, having a key role in data-driven applications. Specially used for getting large amounts of IoT sensing data, by using the individual intelligent sensing devices.
- **Benefit:** improved data collection efficiency and reduced costs effectively<sup>paper2</sup>



# Crowdsensing: issues

- ① Managed and maintained **centralized platforms** suffer from the single point of failure
  - **Proposal:** decentralized architecture (blockchain technology) that lacks a single point of failure, and enhances privacy with asymmetric encryption and digital signature technology
- ② Encouraging workers by offering appropriate **incentive mechanisms** (monetary usually)  
→ auction theory guarantees benefits for both requesters and workers<sup>paper15</sup> but only provide short-term incentives
  - **Proposal:** hybrid incentive mechanism, adopting mechanism design theory, considering three factors:
    - Monetary reward
    - Reputation evaluation
    - Data quality





## 第 2 节

## Research



## 第 2 节

# Research

## 第 1 小节

# Problems



# Blockchain background

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

- Research approaches on blockchain-based crowdsensing:
  - Evaluating time consumption and task cost of applying a blockchain-based system<sup>paper33</sup>
  - Blockchain-based crowdsensing quality control model<sup>paper34</sup>
  - Considering privacy issues<sup>paper35</sup>
  - Handling location privacy protection<sup>paper37</sup> (confusion mechanism)



## 第 2 节

## Research

## 第 2 小节

## The privacy-preserving of crowdsensing



## 第 2 节

## Research

## 第 3 小节

## The incentive mechanism of crowdsensing



# The incentive mechanism of crowdsensing

- Main types of incentive mechanisms:
  - ① **Monetary-based**: distributing rewards. And two subtypes can be considered<sup>paper16</sup>:
    - **price-decision-first** (auction theory) design optimal mechanism benefiting both requesters and workers
    - **upload-decision-first**: distributing rewards based on the uploaded data (quality)
  - 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)

Some previous hybrid incentive mechanisms<sup>paper52</sup> suffer of usability problems because the difficulty of hybrid data management



## 第 3 节

# System architecture



## 第 3 节

## System architecture

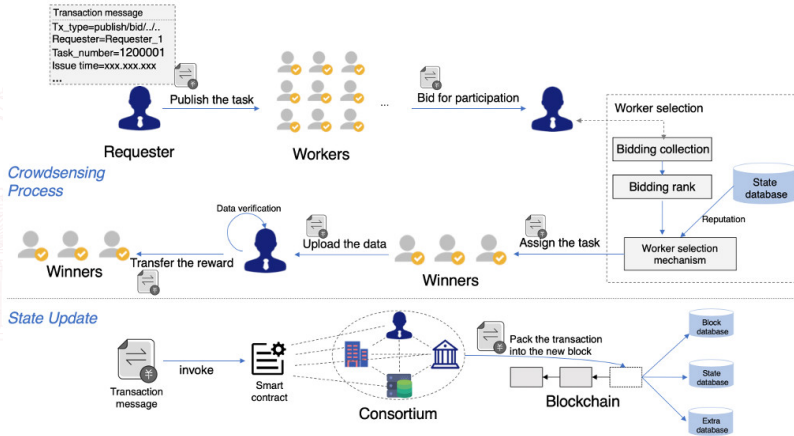
## 第 1 小节

## Software application





# System architecture



# System flow

- **System initialization:** configuration and identity authentication mechanisms
- **Task process:** Specific steps of crowdsensing
  - Step 1: **Task publishing** (invoking the smart contract to update the task state)
  - Step 2: **Worker selection** (workers submit the bidding price and workers select appropriate workers)
  - Step 3: **Data uploading** (selected workers perform the task and upload data)
  - Step 4: **Reward assignment and data evaluation** (requester distribute rewards and evaluate data quality)
- **System synchronization:** state update about tasks and workers (validating transactions into new blocks)



## 第 4 节

# Security issues: privacy



## 第 4 节

# Security issues: privacy

## 第 1 小节

# Single point of failure



## 第 5 节

# Quality management: incentive



## 第 5 节

# Quality management: incentive

## 第 1 小节

# Mechanism design: multifactor



# 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

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



## 第 5 节

## Quality management: incentive

## 第 2 小节

## Mechanism design: issues





# 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**<sup>article56</sup> two important properties for the incentive mechanism are guaranteed:

- **Incentive quality (IC):** the truthful submission of sensing 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



## 第 6 节

## Conclusions

## 第 1 小节

## Application



# Results

A consortium blockchain-based incentive model for crowdsensing system is proposed

- **Benefits of consortium blockchain technology:**
  - resistant to the single point of failure (system security)
  - 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



## 第 6 节

## Conclusions

## 第 2 小节

## Limitations



# Limitations

Further research:

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

## Possible solutions

Application of ML techniques to blockchain-based system



## 第 6 节

## Conclusions

## 第 3 小节

## Further research



## 第 I 部分

# 附录

## 参考文献



# 参考文献 I

- [1] JIANG X, WANG H, CHEN Y, et al. MNN: A Universal and Efficient Inference Engine[EB/OL]. arXiv. 2020. <https://arxiv.org/abs/2002.12418>.





谢谢