Federated Learning & Blockchain

Decentralized & Collaborative

AI on Blockchain

Yi Liu

Background

Problems

- The large datasets required are generally proprietary
- Predictions are often sold on a per-query basis
- Publishing models can quickly become out of date without effort to acquire more data and re-train them
- Lack of large collaborative AI platform

Background

Goal

The goal of our system is not for the creators to profit: the goal is to create valuable shared resources. It is possible for the data contributors to profit financially (depending on the incentive mechanism) but this is mainly a result of mechanisms designed to penalize the contributors who submit bad data.

Decentralized & Collaborative AI on Blockchain framework [1]

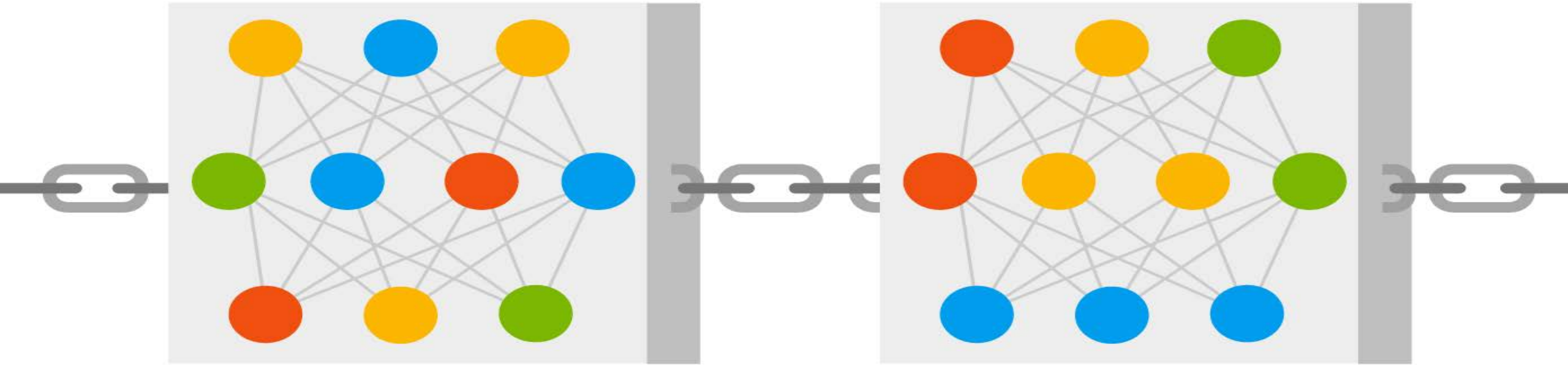
Smart Contracts: Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.

Incentive Mechanisms: IM is design element of framework that influences the behavior of system participants by changing the relative costs and benefits of choices those participants may make.

[1] Decentralized & Collaborative AI on Blockchain

Smart Contracts

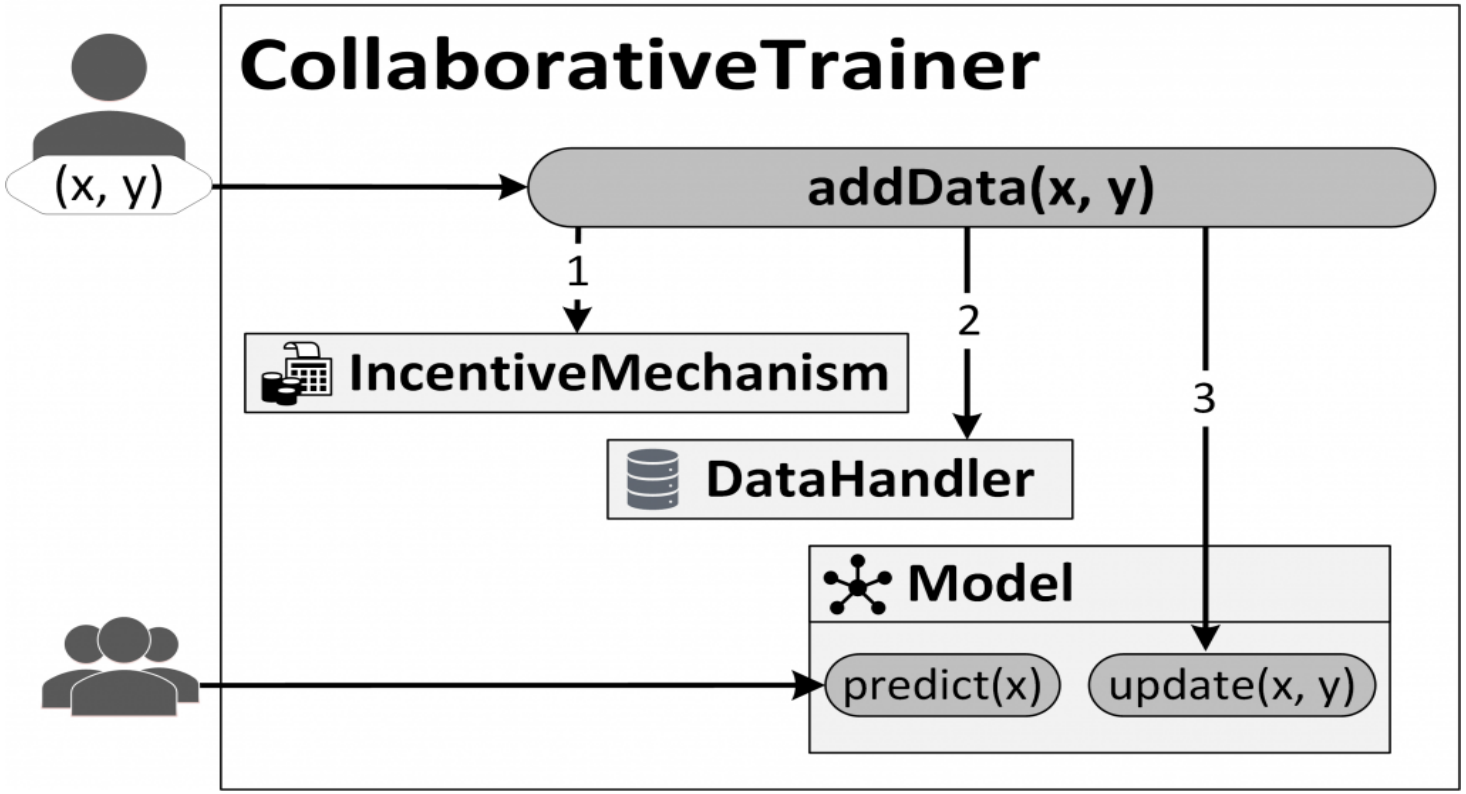
A smart contract is an object (in the sense of object-oriented programming) in this shared code.



A computation **on-chain** means the computation is done inside of a smart contract. The input and result of the computation are usually stored on the blockchain. In contrast, **off-chain**[1] means the computation can be done locally on the client's machine.

[1]Weng, Jia-Si et al. "DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive." IACR Cryptology ePrint Archive 2018 (2018): 679.

Deploying and updating models



① The **IncentiveMechanism** validates the transaction.
② The **DataHandler** stores data and meta-data onto the blockchain. This ensures that it is accessible for all future uses, not limited to this smart contract.
③ The **machine learning model** is updated according to predefined training algorithms.

Incentive Mechanisms

The proposed **incentive mechanisms (IM)** encourage contributors to submit data that will **improve the model's accuracy**.

IM

➢ Gamification

- a specified number of data samples has been contributed
- submitting diverse data samples
- submitting data with different labels
- submitting data routinely (e.g. weekly)

➢ Based on Prediction Markets

- ✓ A commitment phase in which a provider stakes a bounty to be awarded to contributors and shares enough of the test set to prove the test set is valid
- ✓ A participation phase in which participants submit training data samples with a small deposit of funds to cover the possibility their data is incorrect
- ✓ A reward phase in which the provider reveals the rest of the test set and a smart contract validates it matches the proof provided in the commitment phase

➢ Self-Assessment

- ■ Participants effectively validate and pay each other for good data contributions

Potential Issues

Data contributors and smart contract creators should consider several vulnerabilities when using our framework. We analyze issues specific to systems where models can be trained.

Submitting Bad Data (Bad Behavior)

A wealthy and determined agent can corrupt a model deployed by submitting incorrect or nonsensical training data.

Solution

- **Incentive mechanism (this paper)**

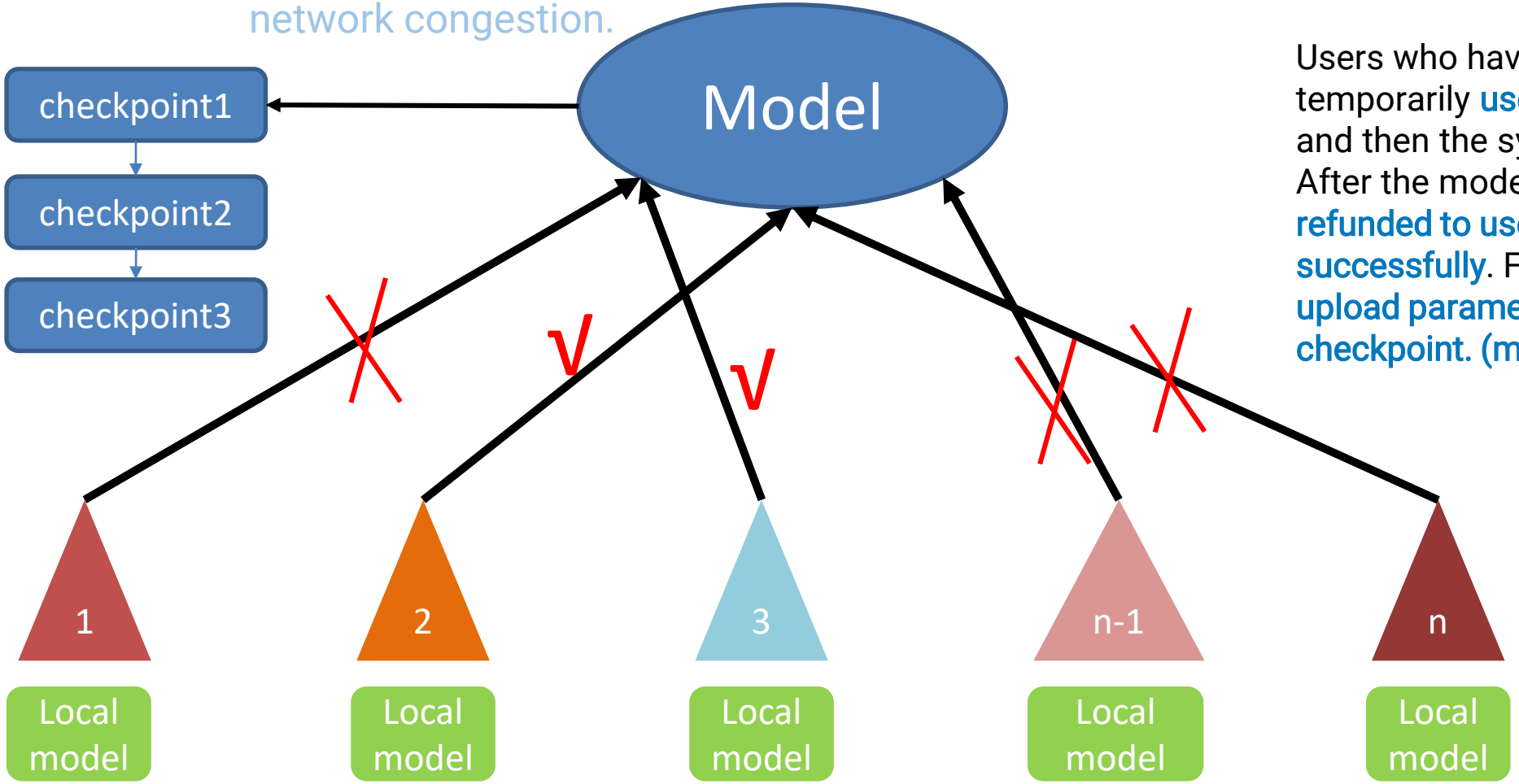
  The incentive mechanism should make it costly and unbeneficial to submit bad data.

  These transactions are auditable as well, and computation results are guaranteed to be correct only if 2/3 workers are honest. After parameters are updated, participants download and collaboratively decrypt the parameters by providing their decryption shares and corresponding proofs for correctness verification.

- **Audit system (my idea)**

Overwhelming the Network

Some applications relying on public blockchains have had reliability issues due to network congestion.



Users who have not uploaded parameters temporarily use the local model for inference, and then the system records the user ID. After the model is stable, the cost will be refunded to users who have not uploaded successfully. Finally, the user can continue to upload parameters using the last trained checkpoint. (my idea)

C

Federated Learning System[1]

Federated computation: where a server coordinates a fleet of participating devices to compute aggregations of devices' private data.

Federated learning: where a shared global model is trained via federated computation.

Blockchain: Smart Contracts and Incentive Mechanism

[1] Bonawitz K, Eichner H, Grieskamp W, et al. Towards federated learning at scale: System design[J]. arXiv preprint arXiv:1902.01046, 2019.

System Design——Protocol [1]

There are currently **two security risks** in the system. In other words, we have to add security mechanisms.

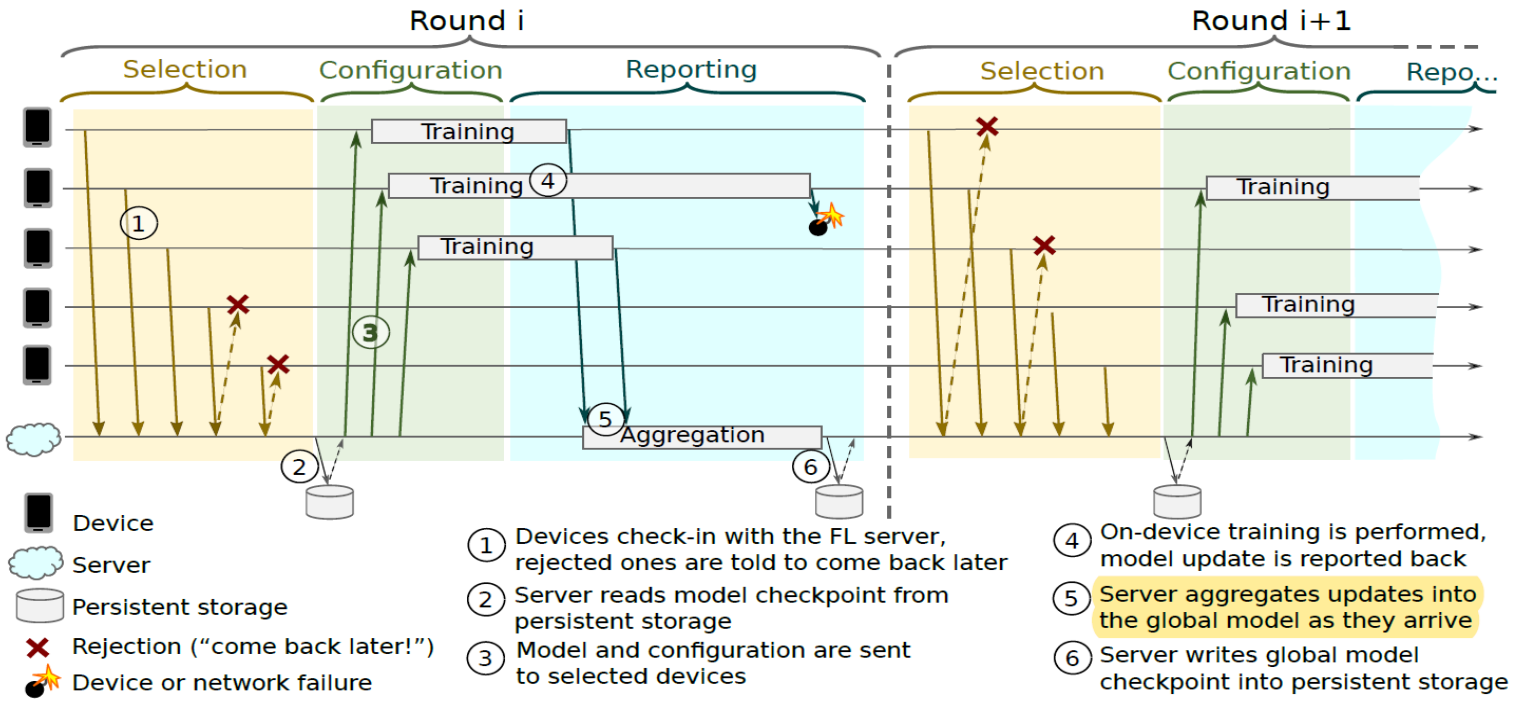


Figure 1: Federated Learning Protocol

Threat 1: Disclosure of local data and model

Threat 2: Participants with inappropriate behaviors.

[1] Bonawitz K, Eichner H, Grieskamp W, et al. Towards federated learning at scale: System design[J]. arXiv preprint arXiv:1902.01046, 2019.

Contract Theory [1][2]

The system needs to design an **effective incentive mechanism**. By adding the accuracy of local data to the model as a relevant parameter, participants with higher precision and more data resources can get more rewards.

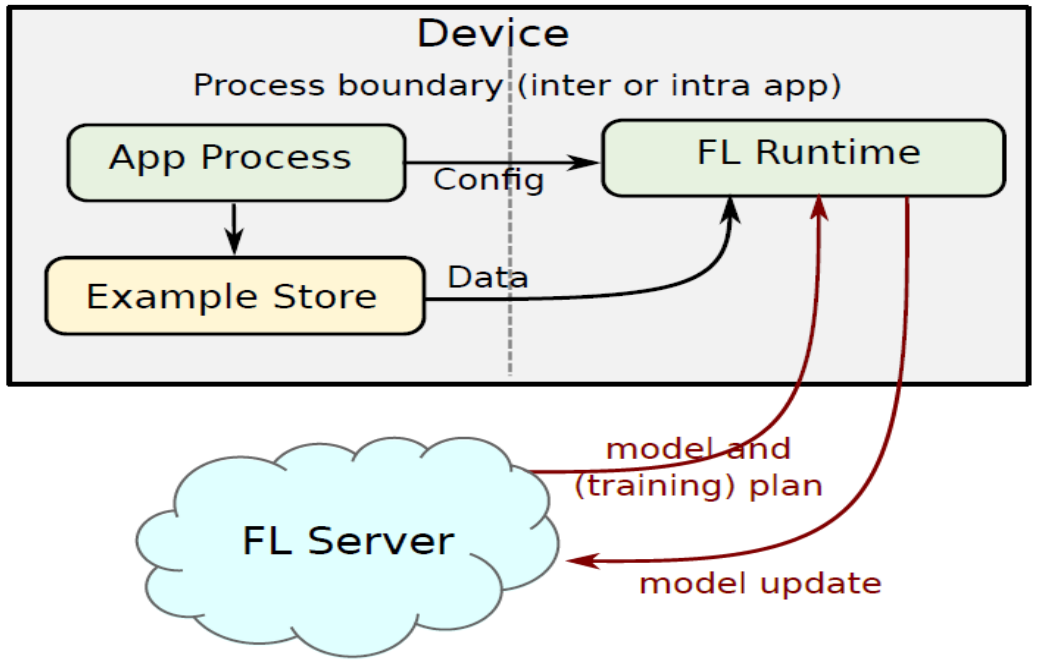


Figure 2: Device Architecture

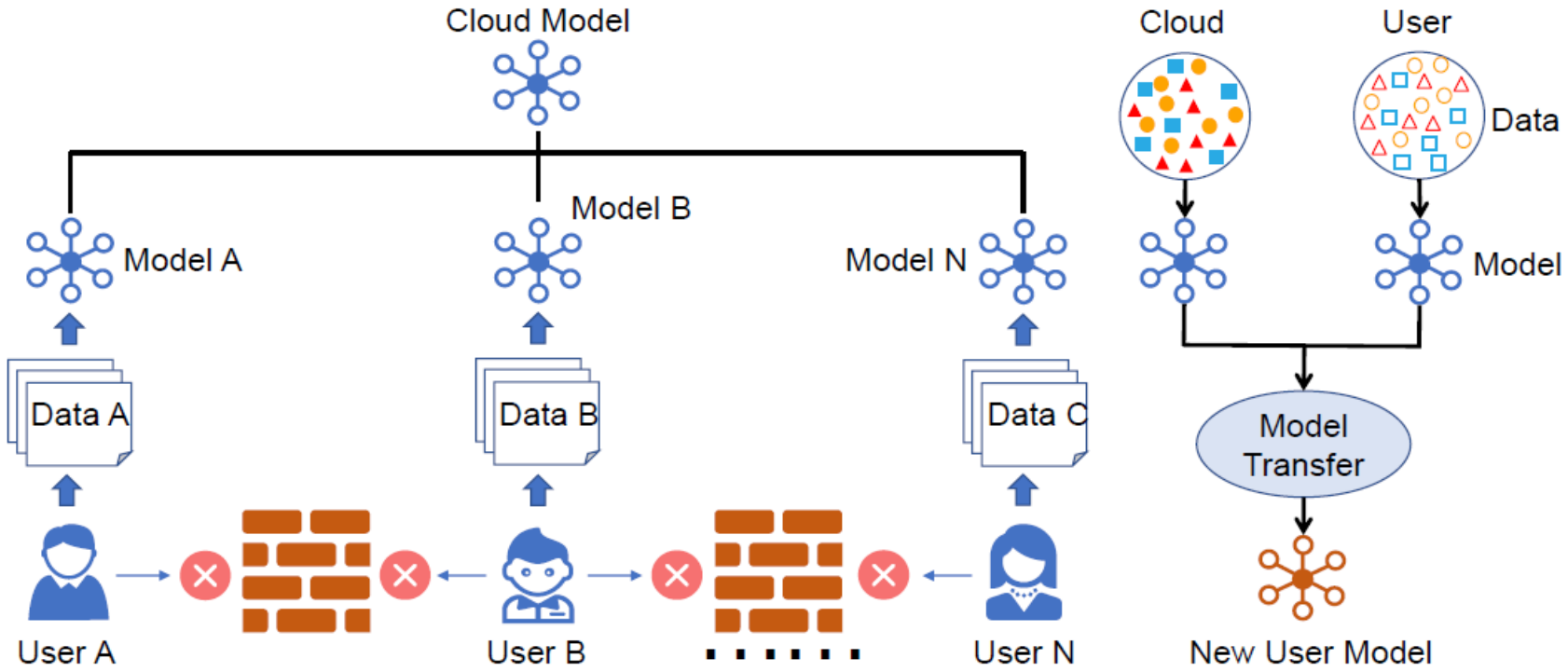
The contract mechanism needs to be added to the model as shown.
The model shown in the picture is for illustrative purposes only.

[1] Kang J, Xiong Z, Niyato D, et al. Incentive Design for Efficient Federated Learning in Mobile Networks: A Contract Theory Approach[J]. arXiv preprint arXiv:1905.07479, 2019.

[2] In cooperation, from NTU.

Federated Transfer Learning For Healthcare [1]

Firstly, user data often exists in the form of isolated islands, making it difficult to perform aggregation without compromising privacy security. Secondly, the models trained on the cloud fail on personalization.



The framework shown in the figure does not use blockchain, we can consider adding blockchain related technology.

[1] Chen Y, Wang J, Yu C, et al. FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare[J]. arXiv preprint arXiv:1907.09173, 2019 .