Decentralized Artificial Intelligence with Data Privacy Protection

Xiaoyan "Sherry" Sun

Department of Computer Science

Redefine the Possible™

Motivation

AI solutions require model training. The data provided for the model training are usually deployed on centralized servers. However, there are some issues that originate with centralized systems such as

- ➢Data Centralization
- ➢Lack of privacy (data can be publicly revealed)
- ➢Lack of control over data (illegal or third-party data sharing)
- ➢Users do not benefit from the data usage (they are not paid for their data)

Background

- Model Training in AI:

  Training is the stage of machine learning when the model is gradually optimized, or the model learns the dataset. We calculate the training loss each time during this process to measure the performance of model. User data is stored on centralized servers to train AI model for predictions.

- Blockchain

  A blockchain is a shared, distributed ledger that cannot be changed once a transaction has been recorded and verified.

Background

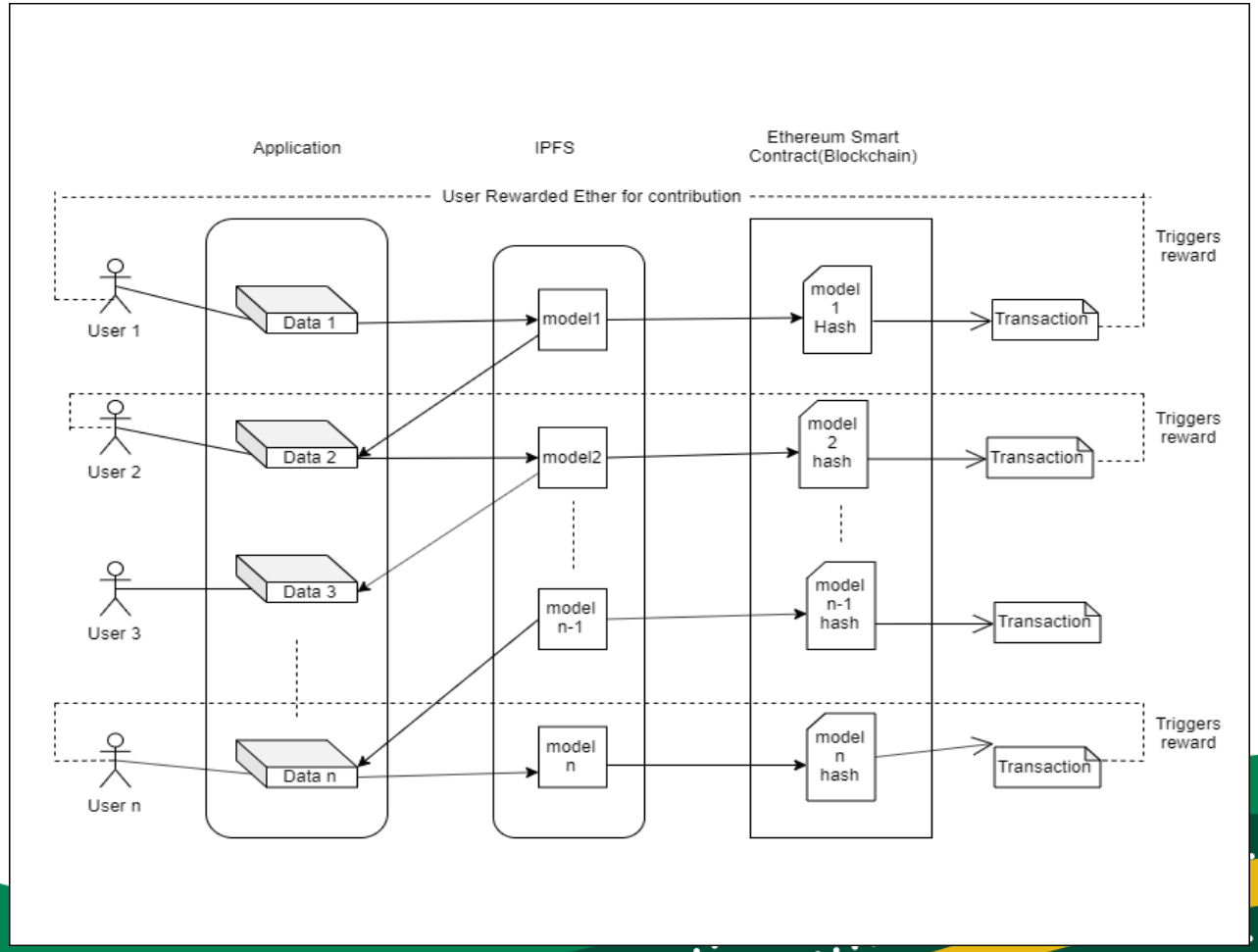
- Ethereum Blockchain

  Ethereum is a blockchain-based distributed computing platform and operating system featuring smart contract functionality.

- Smart Contract

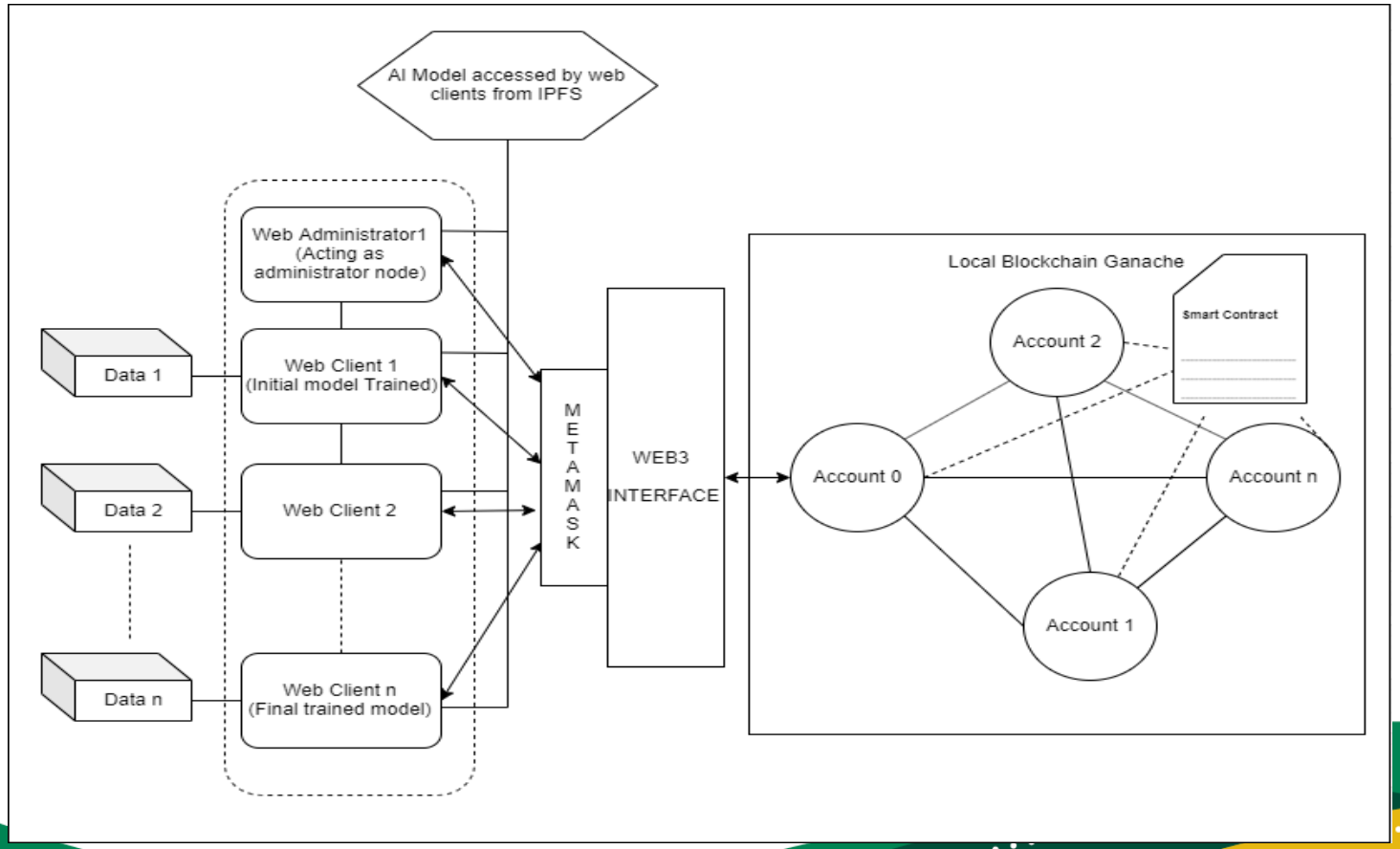
  Code inside the blockchain resides in smart contract. Smart contract is where all the business logic of the application resides. They are executed when predetermined conditions are met.

Our Approach



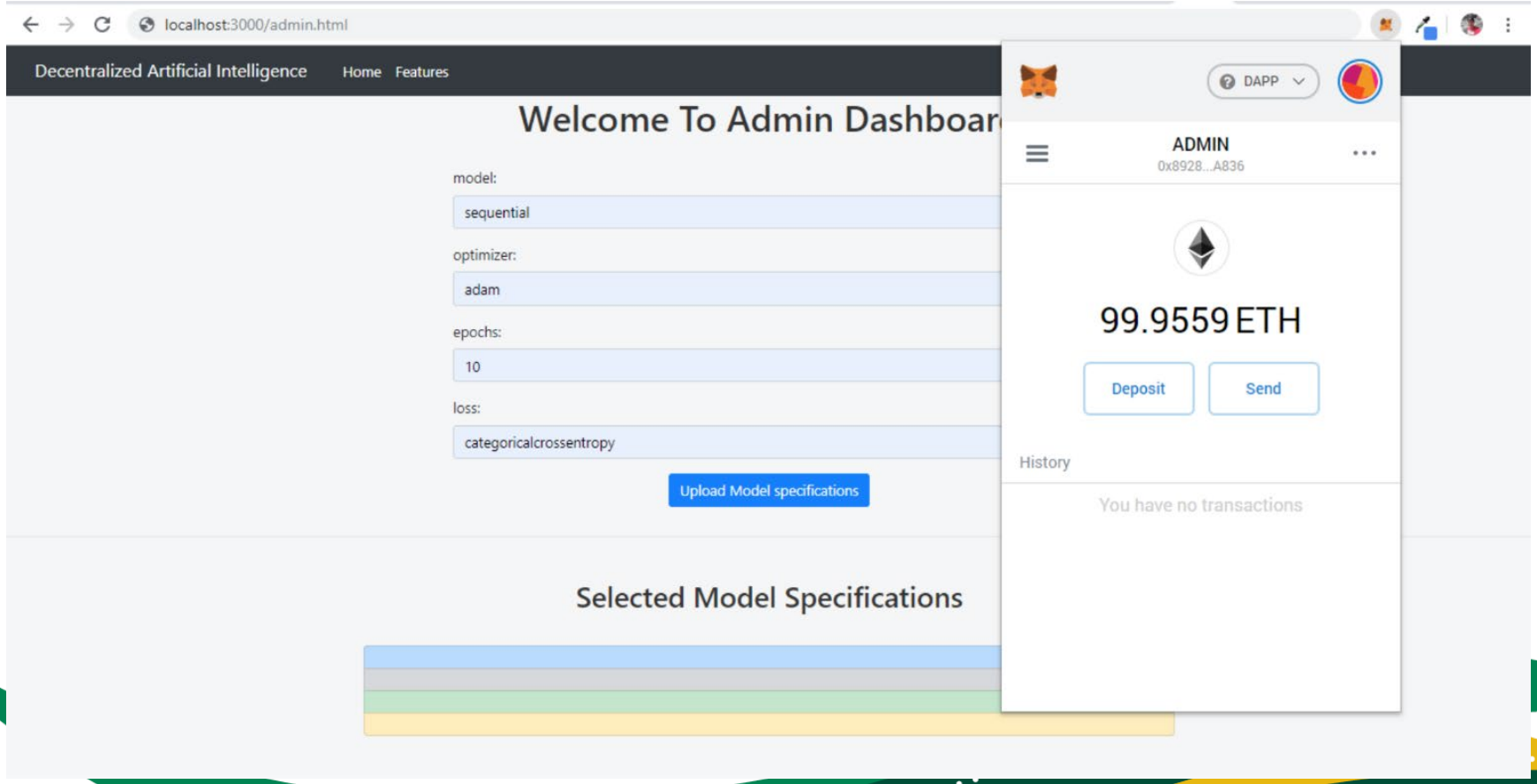
SACRAMENTO STATE

Architecture



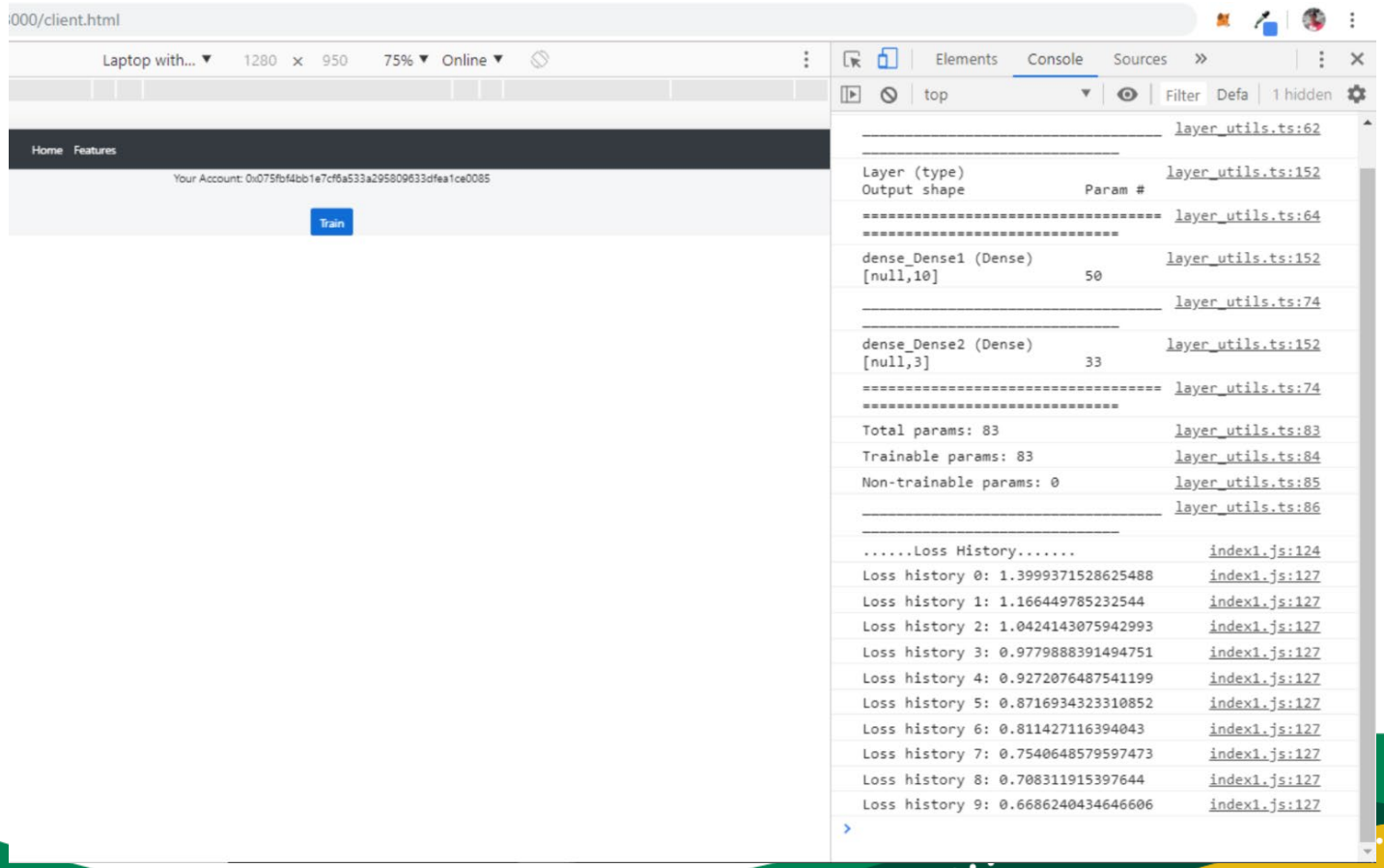
SACRAMENTO STATE

Admin Provides Model Specifications



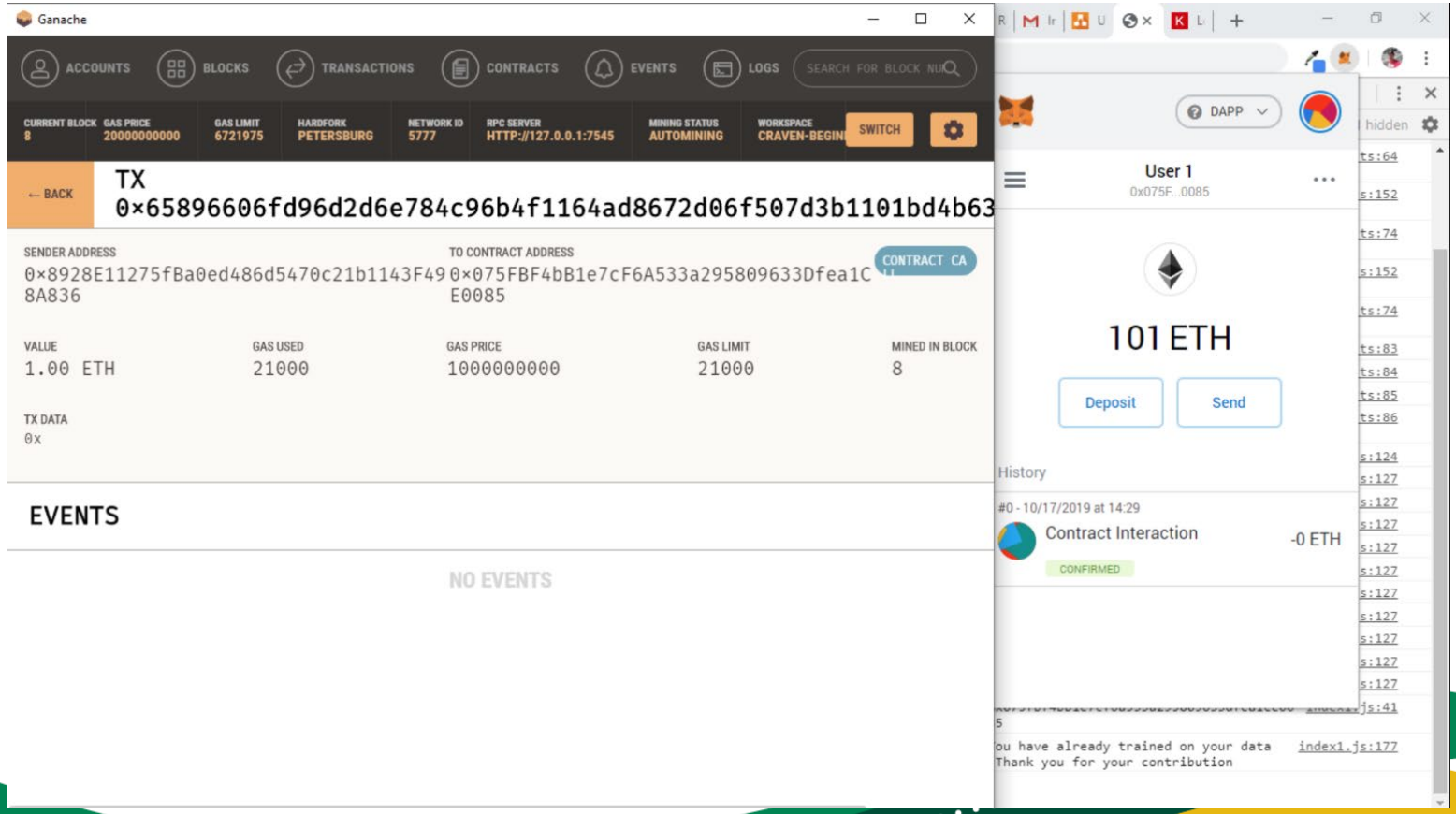
SACRAMENTO STATE

User Training



SACRAMENTO STATE

User Getting Rewards



SACRAMENTO STATE