

* 본 연구는 2022년도 정부의 재원으로 한국과학기술인재진흥원의 지원을 받아 "디지털 헬스케어를 위한 블록체인 융합 원격임상시험 서비스 개발" 과제로서 수행된 연구임

블록체인 기반 연합학습을 위한 레퍼런스 아키텍처

이노피아테크 고은수, 이광기

Contact kwangkeelee@gmail.com for any questions/suggestions



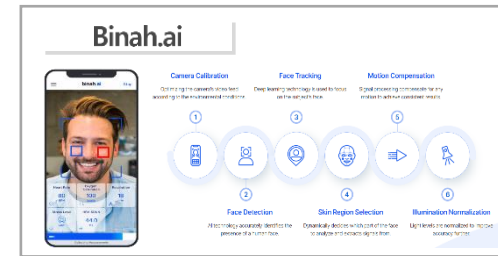
디지털 헬스케어의 3가지 기술적 단절

- 디지털 헬스케어 서비스 각 단계에서 극복해야 할 3가지 단절 (데이터 단절, 사용성 단절, 생태계 단절)을 정의/분석하고, 핵심기술 및 융합 솔루션 개발 계획 도출
- **개인정보보호와 데이터 무결성/추적성은 원격임상시험을 위한 핵심 기본조건.** 블록체인 기술과 연합학습 기술의 융합을 통한 원격임상시험 기술은 세계 최초 시도

■ 사용성 단절 극복 사례

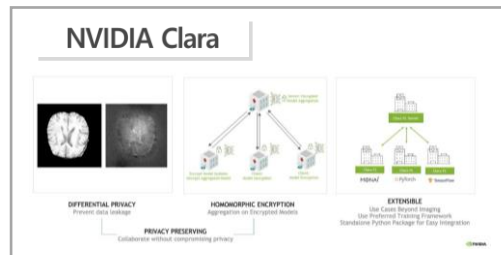


스마트폰 카메라만으로 심박수(98%) 및 호흡수 (1회 이내 오차) 측정 (2021)



안면영상을 통한 비접촉 생체신호/스트레스 인식기술 상용화, SDK 출시 (2022 CES Award)

■ 데이터 단절 극복 사례

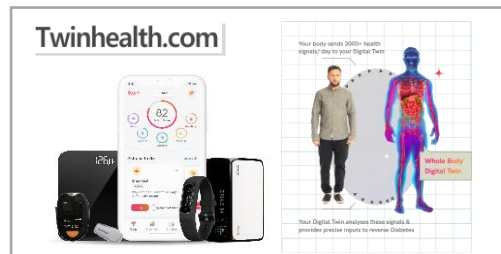


연합 학습을 통한 의료기관 데이터 수집 및 분석, 프라이버시 문제 없는 데이터 학습 (2021)

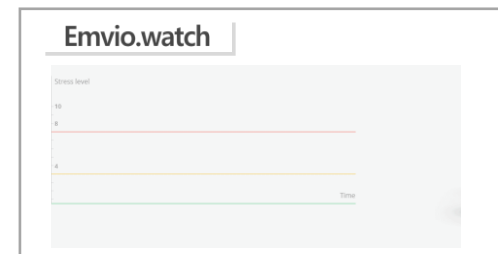


연합학습 활용 임상시험. 의료기관 및 연구자들과 협력
- 더 많은 사람들이 프라이버시 침해 없이 데이터 기여, 연구에 참여 (2021)

■ 생태계 단절 극복 사례



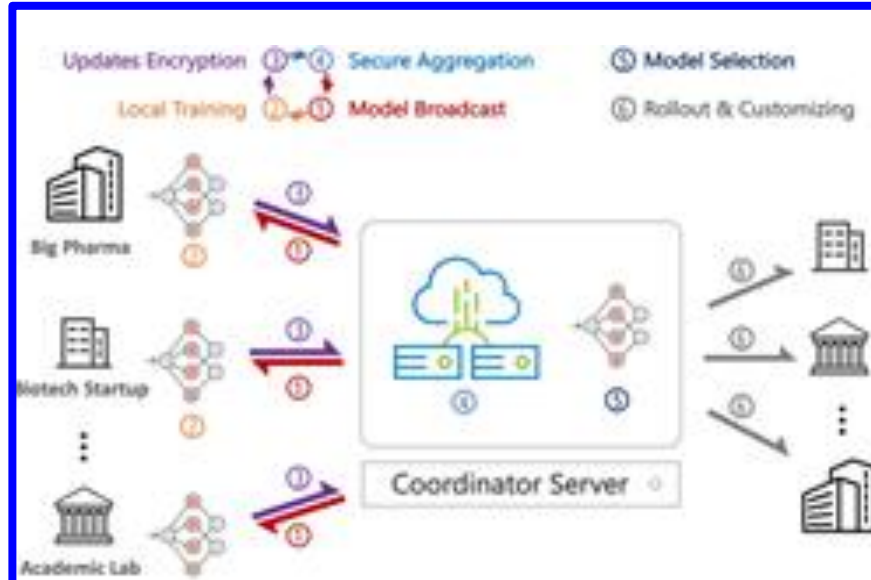
디지털트윈 시뮬레이션을 이용해 당뇨병 환자들의 치료를 돕고 영양학적 조언을 제공하는 서비스 운영 중



웨어러블 기기를 통해 실시간으로 스트레스 모니터링 및 관리하는 제품 최초 출시

연합학습 개요 : Cross-silo vs. Cross-device

- 연합학습은, 로컬 데이터 샘플을 보유하는 다수의 분산 에지 장치 또는 서버들이 원시 데이터를 교환/공유하지 않고 기계학습 문제를 해결하기 위해 협력하는 기술
- 각 로컬노드(클라이언트/디바이스)는 생산한/보유한 원시 데이터를 로컬모델 학습에만 사용함으로써, **데이터 생산자/제공자의 프라이버시를 보호하고, 데이터 소유/활용의 파편화 문제를 해결**
- 모든 로컬 데이터 세트가 하나의 서버에 업로드/공유 되는 전통적인 중앙집중식 기계학습 방식 혹은 로컬 데이터 샘플이 동일하게 분포 (identically distributed) 된다고 가정하는 전통적인 분산 접근 방식과는 대비됨
- 연합학습은 데이터 소유/관리/활용의 파편화 문제를 해결하기 위한 **사일로-교차(Cross-silo) 연합학습**, 디바이스/서비스 사용자 데이터를 활용하기 위한 **디바이스-교차(Cross-device) 연합학습**으로 특징과 이슈를 구분



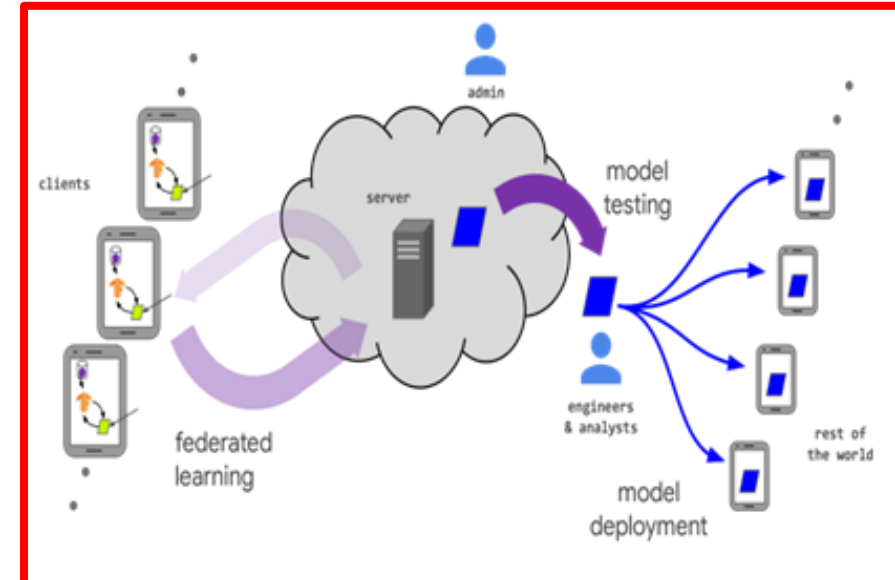
사일로-교차 연합학습 (Cross-silo FL) :

- 서로 다른 기관 (의료 혹은 금융) 혹은 지리적으로 분산되어 있는 데이터센터들이, 각자의 사일로 데이터를 학습 : 2 - 100 clients
- 데이터/통계적 이질성, 디바이스/시스템적 이질성 문제 小
- 모든 클라이언트가 항상 가용

* **통계적 이질성**: 다수의 다양한 사용자/디바이스, 동적 환경 및 시공간으로부터 수집된 데이터는 독립동일분포(iid: independent identically distributed) 조건을 만족하지 못하고 비균일/불균형의 특성을 지님

** **시스템적 이질성**: 연합학습에 참여/기여하는 디바이스의 성능과 기능 및 네트워크 환경이 다양하고, 디바이스의 추가, 변동이 지속적으로 발생

- 인공지능 기술청사진 2030 2차년도 보고서, <https://www.iitp.kr/kr/1/knowledge/openReference/view.it?ArticleIdx=5248&count=true>
- 동적인 디바이스 환경에서 적응적 연합학습 기술, <https://itfind.or.kr/publication/regular/weeklytrend/pastList/read.do?selectedId=1237>



디바이스-교차 연합학습 (Cross-device FL) :

- 사용자의 개인 디바이스 (휴대폰, IoT) 가 개인 데이터를 학습 : Massive # of clients
- 데이터/통계적 이질성, 디바이스/시스템적 이질성 문제 大
- 일정 시간에 일부 클라이언트만 가용하고, straggler effect 대응 필요

- 디지털 헬스케어 3가지 단절 (데이터 단절, 사용성 단절, 생태계 단절)을 극복하기 위한 핵심기술 개발
- 대표적인 디지털 헬스케어 서비스 시나리오에 대한 탐색임상/확증임상 실증
- 분산형 원격임상시험 플랫폼 구축/고도화
- 의료기관 및 CRO 협업, B2B, B2B2C 및 사용자데이터 활용/자산화 사업모델 검증

	주관연구개발기관 (이노피아테크)	공동연구개발기관 (헬스커넥트)	공동연구개발기관 (광운대학교)	공동연구개발기관 (가천대학교)
A. 블록체인 융합 연 합학습 핵심기술	- A-1. 적응적 연합학습 - A-2. 블록체인 융합 연합학 습 (BCFL)	-	-	- A-3. 연합학습 수명주기 관리 (FedMLOps)
B. 원격-PPG 다중 생 체신호 인식 핵심기술	- B-1. 원격-PPG 최적화	-	- B-2. 원격-PPG 다중 생체신 호 인식 딥러닝 기술 - B-3. 멀티모달 (카메라+웨어 러블) 융합 인식기술 - B-4. Multitask, On-Device DNN 최적화	-
C. 유효성/적합성 검 증/평가 핵심기술	- C-1. 모바일/재택/허브 디 바이스 플랫폼	- C-2. 원격임상시험 플랫폼 고도화, 본 과제 핵심기술 적용	- C-3. 인식/진단 기술의 신뢰 성과 설명가능성 (eXplainable AI)	- C-4. 헬스케어 디지털트윈 모델링/시뮬레이션 기술
D. 실증	D-0. 실증 지원 - 핵심기술의 유효성과 우수 성 (기능·성능·사용성) 검증 /평가	D-1. 실증 - DTx - CRO 및 임상시험 실시 기 관(병원)과 협업	D-2. 실증 - RPM - 원격-PPG 다중 생체신호 인 식	D-3. 실증 - SaMD - 다중생체신호 기반 스크 리닝, 중증도 분류

- 디지털 헬스케어를 위한 블록체인 융합 원격임상시험 서비스 개발, <https://drive.google.com/drive/u/0/folders/1qV5jN-KspZWYuUZEzx0mzLEYPsomzhko>

블록체인 융합 연합학습 (BCFL) 구조 설계

실증 요구사항에 따른 BCFL 구조설계

- D-1. 실증 - DTx : BCFL Cross-Device 모델: 대규모 임상시험 참여자 모델
- D-2. 실증 - RPM : BCFL Cross-Device 모델: 대규모 임상시험 참여자 모델
- D-3. 실증 - SaMD : BCFL Cross-Silo 모델: 多 의료기관/병원 간 협력 모델

	Cross-device FL	Cross-Silo FL
실증 적용	D-1. 실증 - DTx , D-2. 실증 - RPM	D-3. 실증 - SaMD
FL scenario	Cross-device FL scenario (≥ 1000 lightweight Clients)	Cross-Silo FL scenario (≤ 10 Server- level Clients)
In 2CP settings	Crowdsourcing Setting	Consortium Setting
Stake Holders Role	<ul style="list-style-type: none"> - SC Publisher - Aggregator - Evaluator/Validator - Trainer (≥ 1000 lightweight Clients) 	<ul style="list-style-type: none"> - SC Publisher - (Optional) Aggregator - Trainer (& Evaluator/Validator) (≤ 10 Server- level Clients)
Evaluation/ Validation	<ul style="list-style-type: none"> - Trainers 와 evaluator/validator 는 서로 다른, 별도로 구분된 역할을 가짐 - Evaluator evaluate the contributions from each Trainers 	<ul style="list-style-type: none"> - 각 Client가 Training 과 Validation 모두 수행 - Each client is responsible for both training and evaluation - Evaluation based on each client's Voting
Validation Dataset	<ul style="list-style-type: none"> - 검증용/평가용 Validation Dataset 필요 - Evaluator has the validation dataset which is not shared/exposed to the Trainers. 	<ul style="list-style-type: none"> - 별도의 Validation Dataset 없는 구조 가능 - No validation dataset is defined/required - Each Trainer evaluates (other Trainers' contribution) using its own data
Etc.	With Evaluation/Validation, BCFL can support: <ul style="list-style-type: none"> - Dynamic client/Trainer selection for the next FL round, kicking out bad/lazy guys - Weighted Averaging during Model Parameters aggregation 	

연합학습과 Blockchain 기술 융합 필요성

Blockchain-based Federated Learning: A Comprehensive Survey, <https://arxiv.org/abs/2110.02182>

일반적 연합학습 문제점	극복 방안	기대효과
Single point of failure	중앙서버 의존형 연합학습의 문제점 (single point of failure problem) 극복	정보보호, 데이터 무결성, 추적성 (integrity, traceability) 개선
Malicious clients and false data	악의적 참여자 및 가짜 데이터 (Malicious clients and false data) 걸러내기	학습/인식 정확도, 수렴 성능 향상
The lack of incentives	데이터 생산자/제공자 (원격임상시험 대상자)에게 블록체인 융합 보상/인센티브 제공	더 많은/성실한 참여를 위한 동기부여. 보상을 통한 자기주도적 학습환경 제공

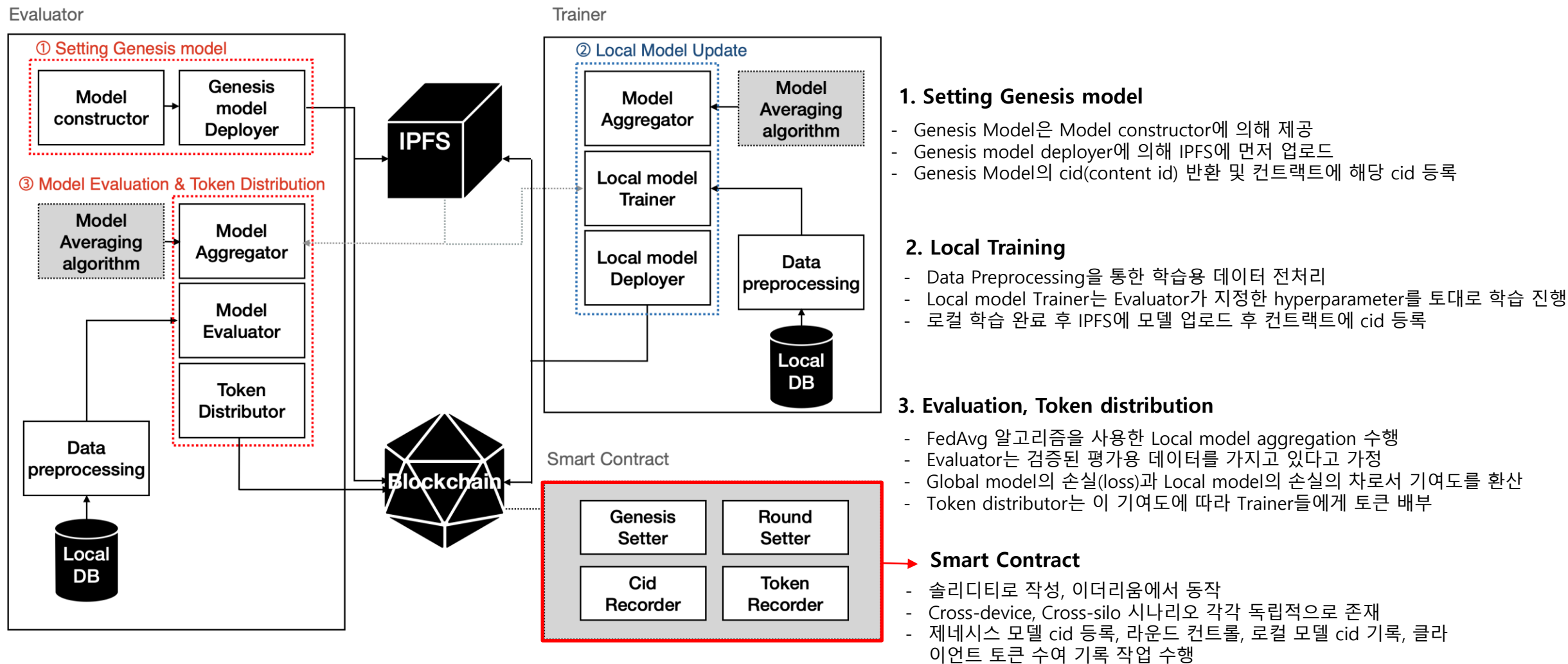
개요 : 블록체인 기반 연합학습 레퍼런스 아키텍처 구현 및 검증

- 이더리움 기반 블록체인 인프라와 호환되는 연합학습 레퍼런스 아키텍처를 정의/구현하고, 해당 아키텍처의 실용성과 확장성을 검증하기 위하여 대표적인 연합학습 알고리즘과 데이터셋에 대한 실험을 수행
- BCFL의 구성 요소로, 스마트 컨트랙트와 모델 평가자(Evaluator) 및 학습 참여자(Trainer)를 정의 하였으며, 연합학습 참여자 간의 학습모델 공유를 위하여 IPFS를 활용. 기존 중앙집중형 연합학습에서는, 중앙 서버의 제어 하에 로컬 노드의 선정과 각 라운드 (round) 마다의 학습결과가 취합되었지만, BCFL에서는 스마트 컨트랙트를 통해 연합학습 진행/평가
- 디바이스-교차(Cross-device) 연합학습 시나리오 및 사일로-교차(Cross-silo) 연합학습 시나리오 지원

향후 지원 기능

- 로컬 학습 참여자(Trainer)들의 학습 기여도 (데이터, 연산통신 능력, etc) 평가 및 보상 (Reward/Incentive) 메커니즘
- 연합학습 수명주기관리 MLOps 연계

레퍼런스 아키텍처



레퍼런스 아키텍처 - 동작

Training Info

- Shakespeare + Lstm
- 2 global rounds, 2 trainers

Setting Genesis model

- Evaluator: Deploying contract...
- Evaluator: Connected to contract at address 0xbfDfAb65243798c23095ba7Ce14E691b2Bd5abAb
- Evaluator: Setting genesis...
- Evaluator: Genesis model cid : QmWSsLP149bVa43drKg1RVmwK1S1sH7qzhTfreMwQUUQEj

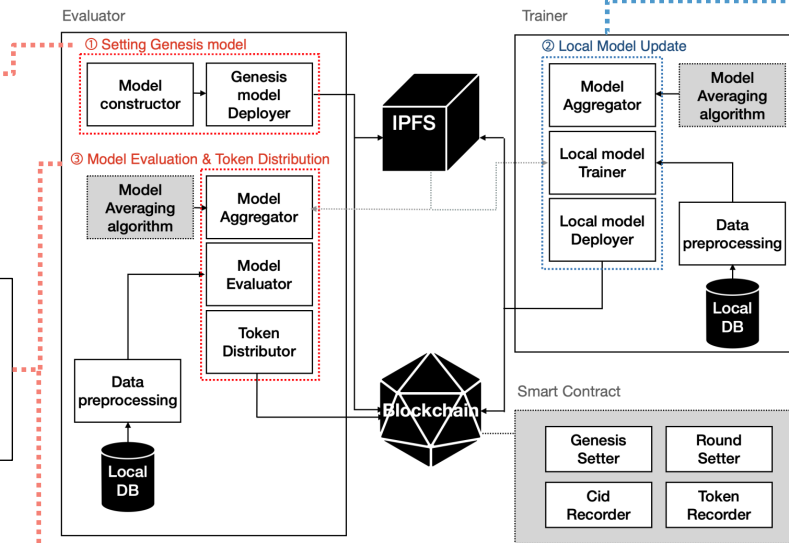
Model Evaluation

- Evaluator: Evaluating updates in round 1...
- Evaluator: Scores in round :1 are :[2.825691750452693, 2.851672221573775]: and cids : ['QmYdwoKpWGjDp7tJtNfcYEaRWxaga7zHkF53VP1uXYwu8j', 'QmY9rtbSbWo5YRgYhNhXyn4f7DJqBesUqfoZVko4xHtYwn']

Token Distribution

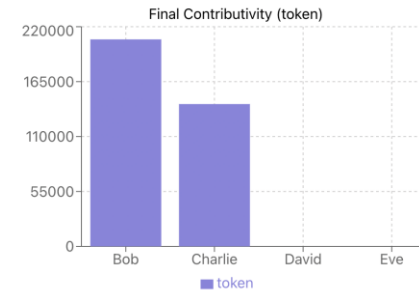
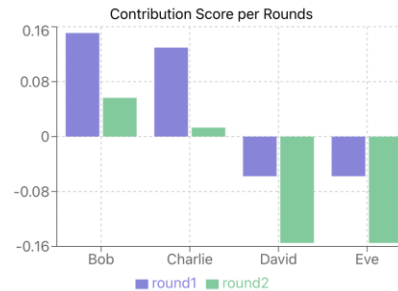
Evaluator: cid :QmYdwoKpWGjDp7tJtNfcYEaRWxaga7zHkF53VP1uXYwu8j
score :2.825691750452693: and tokens :2825691750452692992

Evaluator: cid :QmY9rtbSbWo5YRgYhNhXyn4f7DJqBesUqfoZVko4xHtYwn
score :2.851672221573775: and tokens :2851672221573774848



Local Model Update

- trainer1: Round 1 started
- trainer1: Training model, round 1...
- trainer1: Adding model update..., local model cid : QmY9rtbSbWo5YRgYhNhXyn4f7DJqBesUqfoZVko4xHtYwn, round : 1
- trainer2: Round 1 started
- trainer2: Training model, round 1...
- trainer2: Adding model update..., local model cid : QmYdwoKpWGjDp7tJtNfcYEaRWxaga7zHkF53VP1uXYwu8j, round : 1

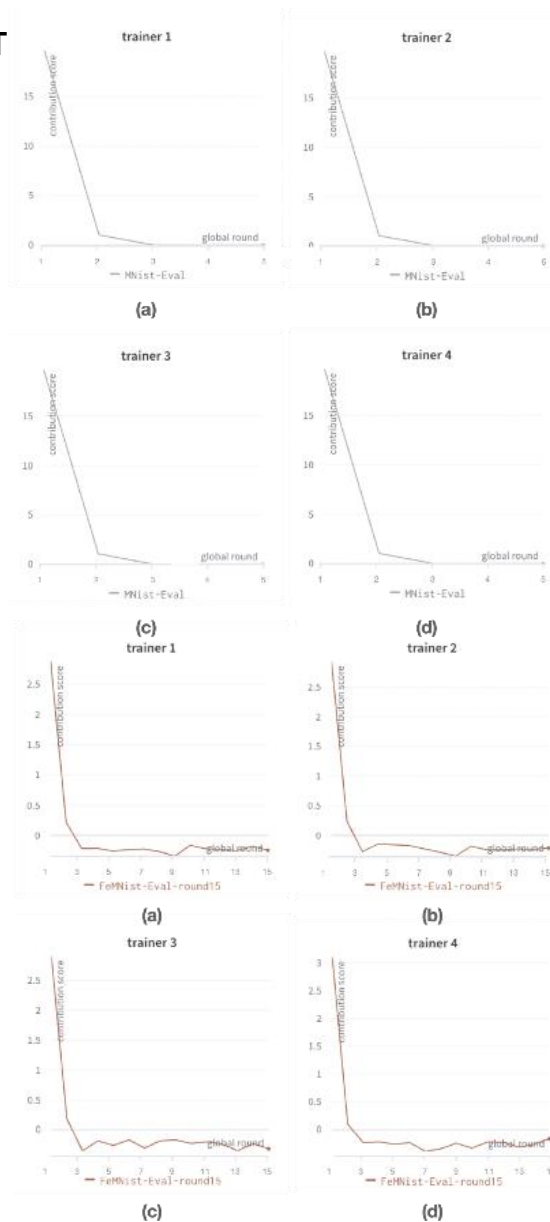
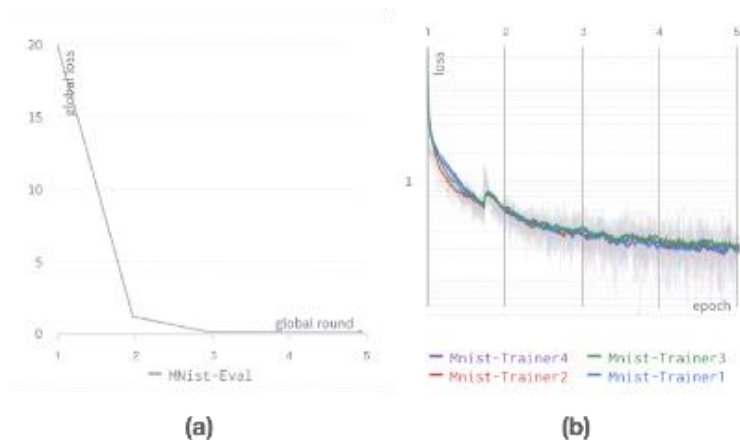


데이터셋 사이즈에 따른 토큰 배부 결과

- Evaluator : Alice
- Large Data Trainers : Bob
- Medium Data Trainers : Charlie
- Small Data Trainers : David, Eve

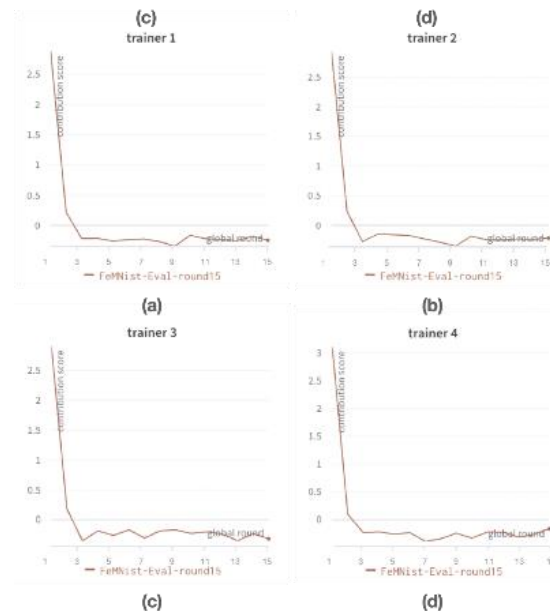
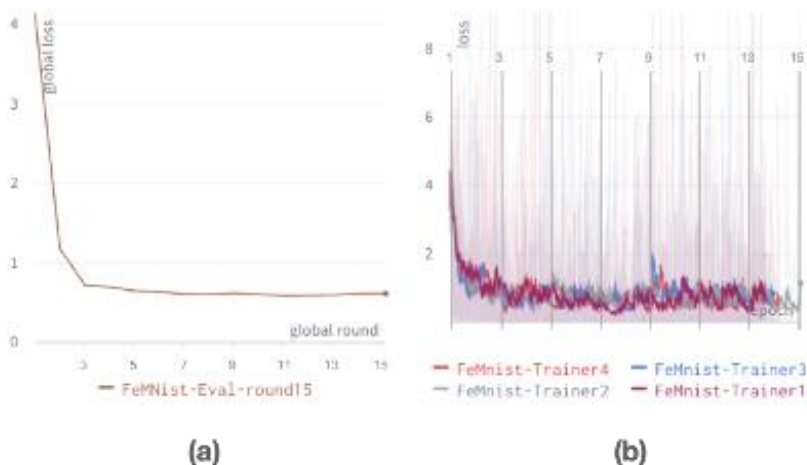
실험 결과 – iid MNIST vs non-iid FeMnist

독립동일분포 (iid : independent identically distributed) 데이터셋 : MNIST



- **MNIST** : 기초 딥 러닝 태스크 수행 결과 측정
 - CNN 분류 네트워크
 - global round 5, local epoch 2, trainer 4
 - 초반 라운드에서 빠르게 수렴하는 양상을 보임
 - global model이 수렴함에 따라 Trainer의 기여도도 함께 감소
 - 네 Trainer들 모두 20.0 이상의 loss로부터 5개의 global round 이후 local loss가 대략 0.2로 수렴
 - global loss : **20.1 -> 0.1**

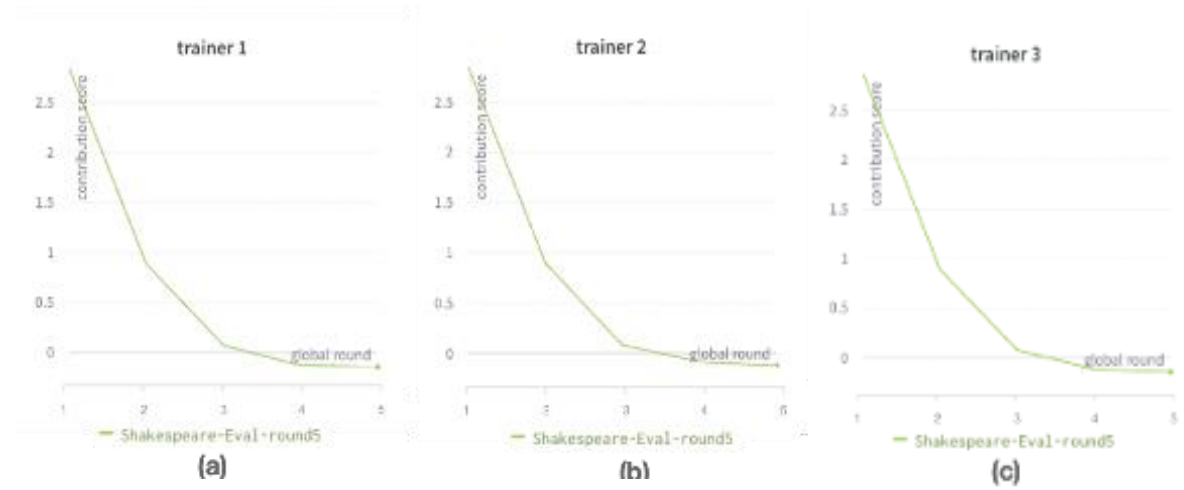
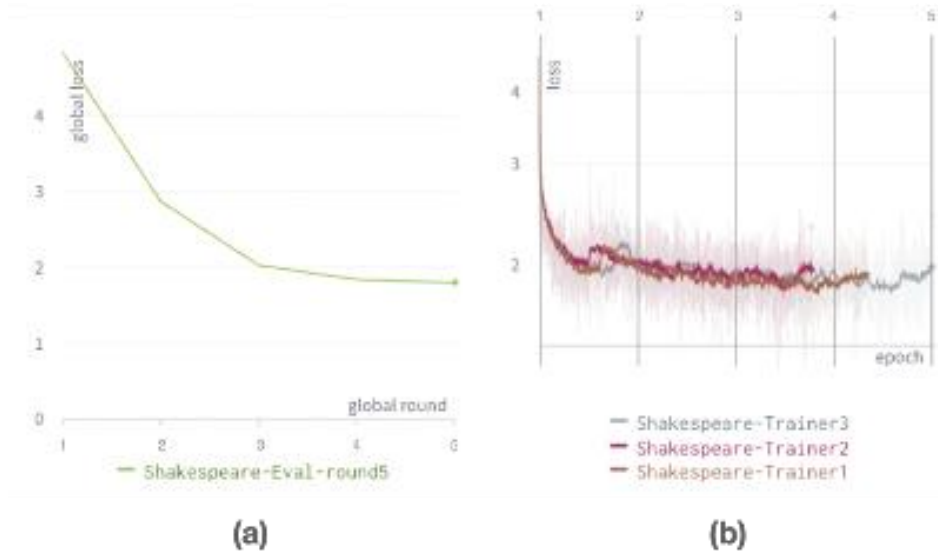
Non-iid 데이터셋 : FeMnist



- **FEMNIST** : MNIST 데이터를 실제 환경과 가까운 non-iid 분포로 변경한 데이터셋
 - 네트워크는 MNIST와 동일
 - global round 15, local epoch 2, trainer 4
 - global model이 수렴함에 따라 Trainer의 기여도도 함께 감소
 - 네 Trainer들 모두 4.0 이상의 loss로부터 15개의 global round 이후 local loss가 대략 0.7로 수렴
 - global loss : **4.15 -> 0.61**

실험 결과 – Non-iid Shakespeare

Non-iid 데이터셋 : Shakespeare



- **Shakespeare** 데이터셋
 - LSTM(Long Short-Term Memory) 모델
 - Global round 5, local epoch 5, trainer 3
 - global model이 수렴함에 따라 Trainer의 기여도도 함께 감소
 - 세 Trainer들 모두 3.4 이상의 loss로부터 5개의 global round 이후 local loss 대략 1.9로 수렴
 - global loss : **4.83 -> 1.79**