한국빅데이터학회지
제5권 제1호, 2020, pp. 89-96 https://doi.org/10.36498/kbigdt.2020.5.1.89

블록체인 기반의 연합학습 구현

An Implementation of Federated Learning based on Blockchain

박준범 · 박종서†

한국항공대학교 컴퓨터 공학과

요 약

인공신경망(artficial neural networks)를 활용한 딥러닝은 최근 이미지인식, 빅데이터 및 데이터분석 등 다양한 분야에서 연구되고 개발이 진행되고 있다. 하지만 데이터 프라이버시 침해 이슈와 학습을 많이 할수록 소모 비용과 시간이 증가하는 문제점이 있어서 이를 해결하기 위해 연합학습(Federated Learning)이 연구되었다. 연합학습에서는 프라이버시 문제를 완화하면서, 분산 처리 시스템의 이점을 가져오는 학습기법을 제시하였다. 하지만 여전히 연합학습에서도 프라이버시 및 보안 문제가 존재한다. 그래서 우리는 연합학습의 서버에 해당하는 부분을 블록체인으로 대체하여 연합학습의 문제점인 프라이버시 문제 와 보안 문제를 해결하였다. 또한 사용자가 제출하는 데이터에 대한 보상을 지급하여서 동기를 부여하고, 기존 성능은 유지하면서도 더 적은 비용의 유지비를 필요로 하는 시스템을 연구하였다. 본 논문에서는 우리가 개발한 시스템의의 타당성을 보이기 위해 실험결과를 제시하면서 기존 연합학습과 연구한 블록체인 기반의 연합학습 결과를 비교한다. 또한 향후 연구로 보안문제에 대한 해법과 와 적용 가능한 비즈니스 분야를 제시를 보여주면서 논문을 마무리 하였다.

■ 중심어 : 블록체인, 인공지능, 연합학습, 스마트 컨트랙트, 디앱

Abstract

Deep learning using an artificial neural network has been recently researched and developed in various fields such as image recognition, big data and data analysis.

However, federated learning has emerged to solve issues of data privacy invasion and problems that increase the cost and time required to learn. Federated learning presented learning techniques that would bring the benefits of distributed processing system while solving the problems of existing deep learning, but there were still problems with server-client system and motivations for providing learning data.

So, we replaced the role of the server with a blockchain system in federated learning, and conducted research to solve the privacy and security problems that are associated with federated learning. In addition, we have implemented a block-chain-based system that motivates users by paying compensation for data provided by users, and requires less maintenance costs while maintaining the same accuracy as existing learning.

In this paper, we present the experimental results to show the validity of the blockchain-based system, and compare the results of the existing federated learning with the blockchain-based federated learning. In addition, as a future study, we ended the thesis by presenting solutions to security problems and applicable business fields.

■ Keyword : Blockchain, Artificial intelligence, Fedrated Learning, Smart Contract, dApp

2020년 08월 03일 접수; 2020년 08월 18일 수정본 접수; 2020년 08월 25일 게재 확정.

† 교신저자 (jspark@kau.ac.kr)

Ⅰ. 서 론

인공신경망(artficial neural networks)를 활용한 딥러닝[1]은 최근 음성인식 과 이미지인식, 빅데이터, 데이터분석 등 다양한 분야에서 연구되고 개발이 진행되고 있다. 딥러닝의 더 높은 정확도를 위해서는 엄청난 양의 데이터가 필요하지만, 모든 데이터를 직접 얻을 수 는 없어서 사용자들의 데이터를 취득하여 학습을 진행하여야 한다. 사용자들은 자신들의 데이터를 기업, 연구소, 등에 제출해야 하는데 이 과정에서 프라이버시 문제가 대두된다. 또한 서버에서 모든 과정을 진행하기 때문에 보안 공격이 발생 시 모든 데이터가 공격받을 수 있다. 이를 해결하기 위해서 연합학습(federated learning)[2]이 등장하였다.

연합학습이란 사용자들이 데이터를 바로 서버에 보내는 것이 아니라 각 사용자들의 기기에서 학습을 하고 결과값인 가중치만 보내기 때문에 데이터에 대한 프라이버시 문제를 완화할 수 있다.

그리고 서버에서는 전달받은 데이터를 모아서 알고리즘을 통해 합산하고, 이를 바탕으로 기존 모델을 개선한다. 이 개선된 모델을 다시 사용자들에게 배포되어 기존 모델과 교체된다. 이 과정을 반복하여 모델의 정확도를 높이는 것이 연합학습의 시나리오 이다.

하지만 연합학습에서도 데이터에 대한 정보보호혜택은 제공하지만 사용자에 대한 프라이버시는 보호되지 않는다. 그리고 사용자들이 자신들의 컴퓨팅 자원을 소모하여 얻은 학습결과를 서버에 제출해야 할 이유가 없으며, 여러 환경, 다양한 기기에서 비동기적으로 사용자들이 접속 및 데이터를 전송하므로 이를 관리할 통합 플랫폼이 필요하다. 또한 가중치를 합산하고 모델을 개선하기 위해 필요한 서버 운용비용은 여전히 존재한다.

본 연구에서는 이러한 문제점을 해결하기 위하고자 연합학습에서 서버에 해당하는 역할을 블록체인[3][4][5]으로 대체하여 사용자들의 정보 및 데이터에 익명성을 부여하여서 프라이버시 문제를 개선하였다. 사용자들이 데이터를 보내기 위해서는 암호화[6]된 주소값으로 보내야 하기 때문에 이럴 해결 할 수 있다. 그리고 사용자들이 자신들의 자원을 소모하여 학습시키고, 이를 통해 얻은 결과값 을 제출함에 있어서 차등적으로 보상을 지급하여서 데이터 제출에 동기를 부여하였다. 그리고 사용자들이 비동기적인 제출과 각각 다른 환경에서 서비스를 활용하기 때문에 통합된 블록체인 시스템을 구축하여서 이를 보다 관리하기 편하게 만들었다. 그리고 기본적으로는 블록체인을 활용한 연합학습이 기존 연합학습 보다는 상대적으로 적은 비용으로 운용이 가능한 것을 실험 결과를 통해 보여줄 것이다

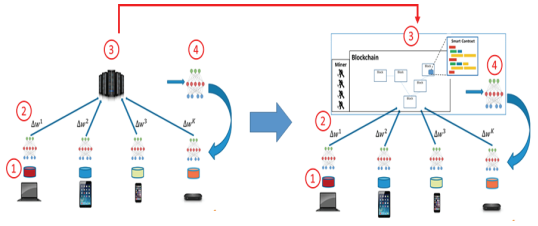
본 논문의 구성은 다음과 같다. 2장에서는 블록체인 기반의 연합학습 구현 내용을 설명하고, 3장에서는 기존의 연합학습과 블록체인 기반의 연합학습을 비교하는 실험을 하고 이를 설명한다. 4장에서는 연구에 대한 결론과 향후 연구 진행 방향을 소개하면서 마무리 한다.

Ⅱ. 제안 방법

2.1 기존 연합학습 제안 방법의 비교

기존 연합학습에서는 (1)과 같이 각각의 디바이스 가 다양한 환경에서 자신들의 데이터를 바탕으로 학습을 시킨다. 이 학습에서는 구글에서 제공하는 Federated learning api를 활용하였으며, 데이터는 mnist세트를 활용하여 진행하였다. 이렇게 각각의 기기에서 학습을 시켜서 얻은 결과들 중에서 가중치(weight) 값들만 (2)과 같이 서버로 전송한다. 이렇게 보내진 데이터는 (3)에서처럼 서버에서 데이터를 합산하는데 여기서

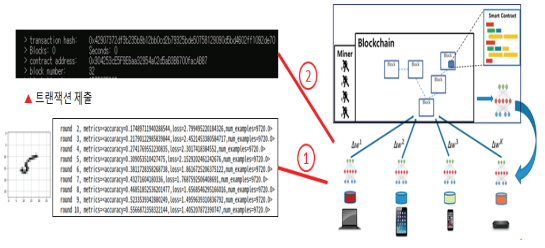
FedAVG[7][8] 알고리즘을 통해서 합산하여 기존에 제공했던 모델을 새롭게 더 나은 모델로 개선한다. 이렇게 개선된 모델은 사용자들의 디바이스로 다시 배포가 되고 이렇게 배포된 모델로 다시 데이터를 학습시켜서 향상된 정확도를 가진 모델을 도출해낸다.



〈그림 1〉 기존학습과 제안방법 비교

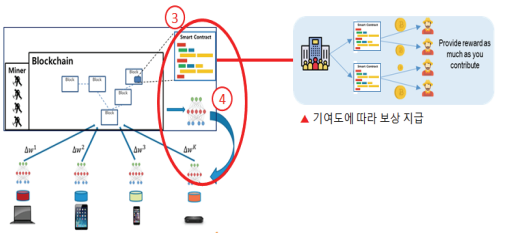
2.2 블록체인 기반의 연합학습 비교

기존 연합학습 시스템과는 다르게 이번 연구에서 새롭게 제안하는 블록체인 기반의 연합학습 시나리오에서는 우선 (1)과 같이 학습시키는 내용은 동일하게 진행된다. 이렇게 학습시킨 이후에 이 결과에 대해서 (2)과 같이 제출할 때에는 먼저 구성해놓은 dApp 환경에서 연동된 사용자의 주소와 계좌를 통해서 트랜잭션의 형태로 값을 보내게 된다. 여기서 보내는 데이터는 학습시킨 결과중 가중치만 보내게 되는데 이 가중치 값이 74 * 10 * 10 행렬로 구성되어있어서 우선 dApp 단에서 간단한 합산을 통해서 결과값만 스마트 컨트랙트로 제출하게 된다.



〈그림 2〉 블록체인 기반 연합학습 시나리오1

이렇게 보내진 데이터는 스마트 컨트랙트에서 전달받아서 작성해놓은 알고리즘을 통해서 가중치들을 합산하고, 기존 모델을 새롭게 개선한다. 그리고 사용자들이 보낸 값들에 대해서 가중치를 판단하여 해당하는 사용자들에게 보상을 차등으로 지급한다. [11][12]



〈그림 3〉 블록체인 기반 연합학습 시나리오1

사용자들에게 보내는 보상 차등 지급 알고리즘은 <그림 4>와 같다. 스마트 컨트랙트에서는 사용자들이 보낸 가중치를 받아서 기존 모델의 가중치와 비교 한다. 그래서 기존 모델의 가중치에서 사용자의 가중치를 뺀 값의 절대값에 대해서 그 절대값이 일정 범위 안에 들어오면 더 많은 보상을 주고, 이전 범위보다 조금 더 큰값이라면 적은 보상을 주는 알고리즘으로 스마트 컨트랙트를 구성하였다. 사용자들이 가중치 값을 보낼 때 위의 알고리즘을 통하여 값을 받음과 동시에 기존 모델과 비교하고,그에 따라서 바로 보상을 받게되는 스마트 컨트랙트를 구현하였다. 이렇게 작성된 스마트 컨트랙트는 이더

Algorithm 1 Give Incentive to User

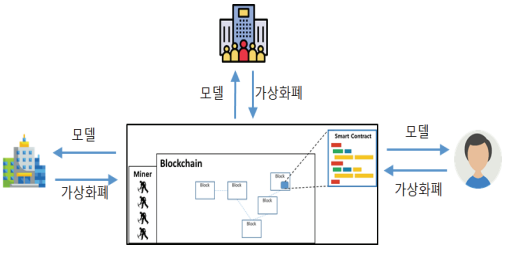
```
Procedure FL_Token(Weight_Retrainded_model, Weight_user_model, Address_user)
        Let rWeight ← average of Weight_Retrainded_model
        Let uWeight ← average of Weight_user_model

        Let dif_weight ← absolute_value(rWeight − uWeight)

        if dif_weight < 0.1 then
          Send five tokens to Address_user
        else if dif_weight < 0.2 then
          Send three tokens to Address_user
        else
          Send a token to Address_user
        end if
end procedure
```

〈그림 4〉 보상 차등 지급 알고리즘 수도코드

리움 네트워크에서 참가하고 있는 마이너들에 의해서 처리가 되는데 마이너들은 사용자들이 값을 제출할 때 같이 제출하는 가스 비용으로 수수료를 받게 된다.

이제 제출이 다 처리되고 새로운 모델로 개선되게 되면 (4)과 같이 개선된 모델을 사용자들이 내려받게 된다. 내려받는 경우에는 블록체인상에 새롭게 기록된 모델 값을 web3[9] 라이브러리를 통해서 값을 읽기만 하기 때문에 추가로 비용을 지불 하지는 않는다. 바뀌어진 모델에 대한 값을 읽어서 자신이 가지고 있는 모델과 교체 후, 새롭게 학습을 진행하면 된다. 그래서 기존 연구와의 비교에서는 (1), (4)과 같이 학습을 시키고 새로운 모델을 내려받는 과정을 같게 진행되고, (2), (3)에서는 본 연구에서 새롭게 구현하여서 진행하는 차이점을 보여주었다.

이렇게 구현된 블록체인 기반의 연합학습 구현을 통해서 <그림 5>와 같이 인공지능을 위한 블록체인 생태계[10]를 구축 할 수 있었다. 기존에 기업 또는 사용자, 즉 모든 서버에서 데이터를 가져가서 사용 하는 것이 아닌 블록체인상에 데이터 또는 모델이 올라가서 이를 필요로 하는 기업,사용자 연구소 등등은 일정한 비용을 지불하고 이를 이용하여야한다. 이렇게 지불한 비용은 앞서서의 학습과정처럼 본인이 자원을 소모하여 학습시킨 사용자들에게 보상으로 지급된다. 또는 허가를 받았다는 가정 하에 자신들의 데이터를 제공한 사용자에게도 보상이 지급된다. 이는 모두 암호화되고 공개되지 않도록 구현되어 있기 때문에 프라이버시 문제[13][14] 또한 개선 할 수 있다.

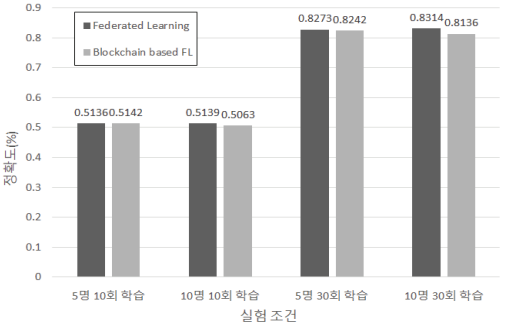


〈그림 5〉 인공지능을 위한 블록체인 생태계 구축

Ⅲ. 실험 결과

3.1 연합학습과 블록체인 기반 연합학습 성능 비교

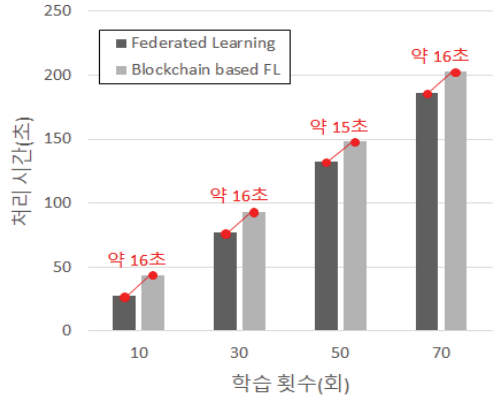
<그림 6>에서는 기존 연합학습의 정확도와 블록체인 기반연합학습의 정확도를 비교를 보여준다. 각 환경은 5명의 사용자가 10회 학습 하는 것과 10명의 사용자아 10회의 학습을 하는 것, 5명의 사용자가 30회 학습을 하는 것, 10명의 사용자가 30회 학습하는 것을 표시하였다. 각각의 환경 구성은 연합학습 api를 활용하여 구성하였고, 연합학습 환경은 api에서의 client 수를 5명과 10명으로 구성하였다. 블록체인에서는 각 사용자수를 5명과 10명의 계좌를 만들어서 각각 트랜잭션을 보내서 값을 처리하였다. 값을 합산하는 알고리즘은 FedAVG 알고리즘을 사용하지는 않았고, 평균값 합산을 통해서 처리하였다. 이렇게 나온 결과값에서는 연합학습과 블록체인 기반의 연합학습이 정확도 차이, 성능 차이에서 차이가 없음을 보여준다. 조금의 차이는 각 라운드별, 학습별, 유저별로 발생하는 차이 이므로 무시 가능한 값이다.



〈그림 6〉 연합학습과 블록체인 기반 연합학습의 실험 조건에 따른 학습 정확도

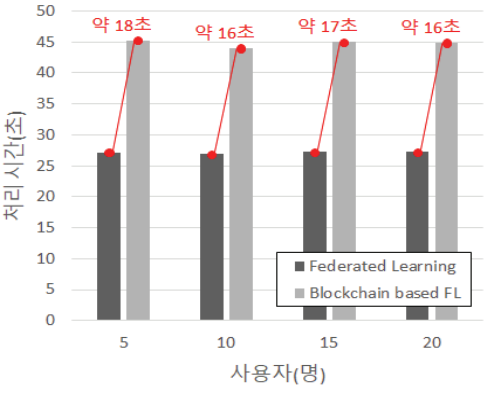
3.2 연합학습과 블록체인 기반 연합학습 처리 시간 비교

<그림 7>에서는 사용자를 5명으로 고정시키고 각각의 기기에서 학습시키는 라운드 수를 증가 시켰을 때의 연합학습과 블록체인 기반의 연합학습 처리 시간을 비교하는 그림이다. 비교하였을 때 각각의 시간이 약 15~16초 차이가 나는데 이는 서버를 대체하는 블록체인 스마트 컨트랙트에서 값을 받아서 처리 할 때에 블록의 생성시간에 의존하게 되는데 이더리움에서 일반적으로 블록 생성시간이 12~18초 사이를 오가면서 진행되기 때문에 그림 [7]과 같은 결과가 나오게 되었다. 이는 학습이 많아지거나 사용자가 많아져도 이더리움의 블록생성시간에 따라 값이 변동하게 된다.



〈그림 7〉 연합학습과 블록체인 기반 연합학습의 사용자 수에 따른 처리시간 비교

<그림 8>에서는 학습 횟수는 10회로 고정하고 사용자 수를 증가시키면서 실험한 결과 값이다.[15] 그래서 마찬가지로 학습은 사용자들의 기기에서 각자 학습시키기 때문에 학습시간은 고정이고, 이 데이터를 서버에 전송하고 다시 새로운 모델을 내려받기까지의 시간을 표시하였다. 블록체인 기반의 연합학습에서도 학습시간은 동일하지만 블록체인 스마트 컨트랙트에서 처리되는 시간이 약 16~18초로 측정되어 추가하였기 때문에 그림과 같은 시간의 차이를 보여준다. <그림 7>과 마찬가지로 두 그림에서 보여주는 약 15~18초 시간 차이는 블록 생성시간에 따라가게 된다. 사용자가 보내는 트랜잭션이 처리되기 위해서는 마이너들이 일을 처리하고 블록을 생성하여야 하는데 이 블록 생성시간이 위와 같기 때문에 그림과 같은 결과가 나오게 되었다.

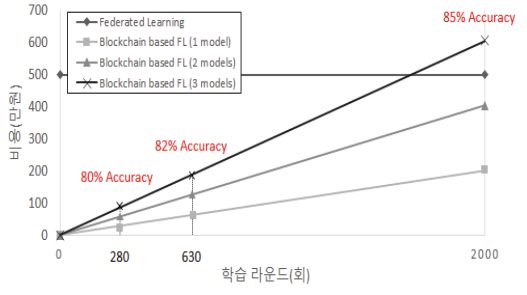


〈그림 8〉 연합학습과 블록체인 기반 연합학습의 학습 횟수에 따른 처리시간 비교

3.3 연합학습과 블록체인 기반 연합학습 처리 시간 비교

<그림 9>는 연합학습과 블록체인 기반의 연합학습의 학습 라운드 수를 많이 할수록 드는 비용에 대한 그림이다. 이 실험에서는 우선 가정으로 연합학습에 드는 서버의 비용 과 운용비용을 500만원으로 책정하였고, 이 서버는 약 100명의 데이터를 처리 가능하다고 가정하였다. 그리고 블록체인 기반의 연합학습에서는 학습한 이후에 값을 제출하는 트랜잭션 비용을 10원, 스마트 컨트랙트 연산 비용은 10원으로 책정하였다. 그리고 학습을 위해서 필요한 데이터는 CIFAR-10 dataset을 활용한 연합학습 결과를 활용하여 진행하였다. 사용한 dataset 은 50000개

의 학습예제와 10000개의 테스트 예제로 구성되어 있고, 이번 실험에서는 사용자 100명이 dataset을 바탕으로 학습하도록 진행하였다. 그래서 참조한 논문에서는 100명이서 dataset을 가지고 280 회 학습할 경우 80%의 정확도를 나타낸다고 하였다. 마찬가지로 630회 의 경우 82%의 정확도, 2000 회 의 경우는 85%의 정확도 결과를 보여주었다. 그래서 하나의 85% 정확도를 가지는 모델을 학습시켰을 경우에는 최종적으로 약 200만원의 비용이 들었다. 학습 횟수에 따라서 값이 선형적으로 증가한다. 그래서 한번 모델을 학습시키는 경우는 연합학습에 비해서 더 적은 비용으로 학습이 가능하다. 하지만 한번 서버를 구축해 놓았을 때 1개의 모델만 학습시키지는 않기 때문에 실험에서는 이어서 2개의 모델, 3개의 모델을 학습시키는 것으로 가정하였다. 그럴 경우 3개의 모델을 학습시킬 때는 85%의 정확도를 얻기위해 오히려 연합학습의 비용이 더 적게드는 것을 확인하였다. 하지만 실험에서는 서버 한 대를 사용해서 연산이 더 많거나 더 많은 사용자가 참가하는 것은 가정에서 제외시켰기 때문에 500만원 고정 값이여서 이러한 결과가 나오게 되었다. 그리고 단순히 값을 소모하는 것 뿐만 아니라 사용자들은 보상을 받기 때문에 더 비용이 많이든다고 표현하기는 어렵다.



〈그림 9〉 연합학습과 블록체인 기반 연합학습의 학습 라운드에 따른 비용 비교

Ⅳ. 결론 및 향후 연구

딥러닝의 문제점을 해결하고자 등장한 연합학습에서도 문제점이 발생하였는데, 이를 해결하고자 블록체인 기반의 연합학습 연구를 제안하였다. 연합학습의 프라이버시 문제와 동기부재 문제점을 해결하기 위해서 서버역할에 해당하는 부분을 블록체인으로 대체하여 시스템을 구축하였다. 블록체인 기반의 연합학습 연구를 통해서 기존 연합학습의 성능을 유지하면서도 서버의 구축 및 운용 비용 없이도 시스템을 운용 할 수 있음을 보여주었다. 그리고 사용자들이 제출한 데이터에 대해서도 기여도에 따라 각각의 사용자들에게 보상을 지급하는 스마트 컨트랙트를 만들어서 사용자들의 동기를 부여할 수 있었다. 또한 블록체인에서 값을 전송하는 과정에 있어서 암호화된 사용자의 주소로 보내기 때문에 사용자 정보에 대한 프라이버시 문제를 해결할 수 있었다.

향후 연구로는 악의적인 사용자가 다른 사용자의 데이터를 탈취하거나 이용하여 학습을 하지 않더라도 그 데이터를 보내서 자신이 또한 보상을 받을 수 있으므로 사용자들이 학습한 데이터는 동형암호화(Homomorphic Encryption)을 통해서 암호화하여 보낼 수 있도록 연구해야 할 것이다.

그리고 사용자가 실제로 학습을 하여 보낸 데이터인지 판단하기 위해서 블록체인에서 쓰는 방법중 하나로, 실제로 마이닝 했는지 검증하기 위한 PoW 변수와 같은 방법을 사용하여 판단하도록 연구해야 할 것이다. 이를 통해서 사용자가 실제로 성실하게 학습을 했는지 판단을 하여서 악의적인 사용자가 데이터를 위변조 하여 전송하고, 부당한 보상을 획득하지 못하도록 구현해야할 것이다.

그리고 이렇게 구축한 시스템은 데이터의 프라이버시가 중요한 의료분야에 적용하여서 사

용자, 환자들의 데이터 제공에 대해서도 적절한 보상을 지급하고, 사용자들의 프라이버시도 지킬 수 있도록 하는 비즈니스 생태계에 접목 가능 할 것이다.

참 고 문 헌

[1] Yann LeCun, Yoshua Bengio & Geoffrey Hinton, “Deep Learning”, nature, 27 May 2015.

[2] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, Dave Bacon, “Federated Learning: Strategies for Improving Communication Efficiency”, arXiv:1610.05492v2 [cs.LG] 30 Oct 2017.

[3] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Oct. 2008.

[4] Vitalik Buterin, “A next-generation smart contract and decentralized application platform”, cryptorating.eu,2014.

[5] W.Gavin, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, 2014.

[6] D Hankerson, A Menezes, *Elliptic curve cryptography*, Boston, Springer, 2011.

[7] H.Bredan McMahan, “Communication-Efficient Learning of Deep Networks from Decentralized Data”, AISTATS 2017.

[8] H.Bredan McMahan, “Communication-Efficient Learning of Deep Networks from Decentralized Data”, AISTATS 2017.

[9] Lightweight Java library for integration with Ethereum clients Available : https://web3j.io/

[10] E. Gawehn, J. A. Hiss, and G. Schneider, “Deep learning in drug discovery,” Molecular informatics, vol. 35, no. 1, pp. 3-14, 2016.

[11] A. B. Kurtulmus and K. Daniel, “Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain,” arXiv preprint arXiv:1802.10185, 2018.

[12] J.-S. Weng, J. Weng, M. Li, Y. Zhang, and W. Luo, “Deepchain: Auditable and privacy-preserving deep learning with blockchainbased incentive,” Cryptology ePrint Archive, Report 2018/679, 2018, https://eprint.iacr.org/2018/679.

[13] A. Bansal, T. Chen, and S. Zhong, “Privacy preserving backpropagation neural network learning over arbitrarily partitioned data,” Neural Computing Applications, vol. 20, no. 1, pp. 143-150, 2011.

[14] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016, pp. 839-858.

[15] Hyesung Kim, Jihong Park, Mehdi Bennis “On-Device Federated Learning via Blockchain and its Latency Analysis”, IEE Communications letters 2019.

저 자 소 개

박 준 범(Park June Beom)

·2018년 : 한국항공대학교 컴퓨터공학과 학사
·2020년 : 한국항공대학교 컴퓨터공학과 석사
·현재 : 한국항공대학교 컴퓨터공학과 박사과정
·관심분야 : 블록체인, 블록체인 융합, 빅데이터, 정보보안

박 종 서(Park Jong Sou)

·1983년 : 한국항공대학교 항공통신공학과 학사
·1986년 : North Carolina State University 전기컴퓨터공학 석사
·1994년 : Pennsylvania State University 컴퓨터공학 박사
·관심분야 : 정보보안, 블록체인, 인공지능, 헬스케어