블록체인을 활용한 딥러닝 형상관리 시스템에 대한 연구

배수환*, 이홍재**, 신용태***
*숭실대학교 컴퓨터학과
**프리랜서
***숭실대학교 컴퓨터학부
shbae0213@soongsil.ac.kr, jace@ssu.ac.kr, shin@ssu.ac.kr

A Study on Deep learning Configuration Management System using Block chain

Su-Hwan Baeg*, Jace Lee**, Young-Tae Shin***
*Dept. of Computer, Soongsil University
**Freelancer
***Dept. of Computer Science and Engineering, Soongsil University

요 약

최근 인공지능에대한 관심과 COVID-19의 영향으로 인공지능을 적용하려는 연구가 계속되고 있다. 인공지능 학습 방식 중 딥러닝에서는 학습 결과에 따라 가중치를 두며 지속적인 학습을 수행한다. 이때 사용하는 가중치에 따라 학습 능력이 향상되게 되지만, 과다 학습으로 인한 퇴화 현상과 잘못된 결과 도출이 되는 경우가 발생한다. 이를 해결하기 위해 본 논문에서는 문제를 해결하기 위해 비연속적 PoW 합의방식을 사용한 블록체인에 가중치와 학습 결과를 지속적으로 보관하여 형상관리를 할 수 있는 시스템을 설계하였다.

1. 서론

최근 많은 산업 분야에서 인공지능을 적용하여 새로운 서비스를 제공하려는 관심이 높아지고 있다. 이 트렌드는 전세계적으로 확산되고 있는 COVID-19의 영향으로 사회적거리두기가 확산되며 더욱 빠르게 적용할 수 있도록 연구가 계속되고 있다[1]. (그림 1)과 같이 2020년 9월 가트너에서 발표한 하이프 사이클에 따르면 AI에 대한 기술 성숙도가 빠르게 발전되어 가는 것을 확인할 수 있다.

(그림 1) Gartner Hype Cycle for AI 2020

딥러닝의 경우에는 2019년에 발표한 자료에서는 “The Peak of Inflated Expectations”단계에 가까웠지만, 2020년에는 “Trough of Disillustionment”에 가까워지고 있다[2].

이와 같은 기술의 발전이 있지만 딥러닝을 통해 학습 결과를 도출해내는 과정에서는 가중치에 따른 잘못된 결과를 표현해주거나, 잦은 학습의 반복으로 인해 퇴화하는 경우가 발생하고 있다. 이를 해결하기 위해서 정상적인 상태로 복원해주는 방안이 필요하며 이를 함수형태로 제공하고 있다. 하지만, 최대 5회 이내의 학습 결과로의 복원 기능만을 제공하고 있으며, 학습 모델별로 상이한 과정을 거쳐 복원을 진행해야하는 번거로움이 존재한다. 또한, 딥러닝을 통해 학습하는 환경이 대규모 환경이 되거나 잦은 학습을 수행하는 경우에는 딥러닝 학습 작업이 충돌하거나 악의적인 설정 변경 등으로 인한 가중치 변화로 인해 정상적인 학습 결과를 도출해 내지 못하는 경우가 발생하기도 한다. 이를 해결하기 위해 본 논문에서는 블록체인을 활용하여 딥러닝 형상관리 시스템을 설계하는 연구를 수행하였다. 제안하는 기술에서는 비연속적 PoW 합의 방식을 사용한 블록체인에 학습 당시의 가중치와 학습 정확도, 손실률

등을 기록하고 학습 결과에 문제가 발생하였을 때 기존의 상태로 복원하는 기능을 설계하였다.

2장에서는 본 연구에 필요한 관련연구, 3장에서는 제안하는 기술의 설계 항목, 4장에서는 결과와 향후 연구내용에대해서 기술하였다.

2. 관련연구

2.1 블록체인

기존의 보안 방식은 암호화, 난독화, 분리형과 같은 기존의 폐쇄적인 방법을 사용하였다. 반면, 블록체인은 데이터를 분산 원장의 형태로 공유하여 네트워크의 모든 참여자가 동일한 내용을 알게하는 방식을 사용한다. 이를 통해 데이터 변조를 원하는 공격자가 특정 데이터를 수정하더라도 인정받지 못하도록 설계되어 있다.

블록체인은 네트워크 방식에 따라서는 크게 퍼블릭 블록체인과 프라이빗 블록체인으로 구분되어진다. 이는 아래의 [표 1]과 같은 특징을 가진다.

	Public	Private
읽기 권한	제한없음	허가된 참여자
거래 검증, 승인	제한 없음	허가된 참여자
트랙잭션 생성	제한 없음	허가된 참여자
권한관리	사용 안함	읽기, 쓰기

[표 1] 퍼블릭 블록체인과 프라이빗 블록체인의 비교

퍼블릭 블록체인의 경우는 네트워크 참여와 블록체인 시스템 이용에 제한을 가지고 있지 않아, 암호화폐 시스템에서 주로 사용된다. 대표적인 예로는 비트코인[3], 이더리움[4]이 있다. 프라이빗 블록체인의 경우에는 특수한 목적에 의한 특정집단이 주로 사용한다. 이를 위하여 허가된 사용자만 블록체인에 참여가능하며 권한이 제한되어 있다. 대표적인 예로는 하이퍼레저 페브릭[5]이 있다.

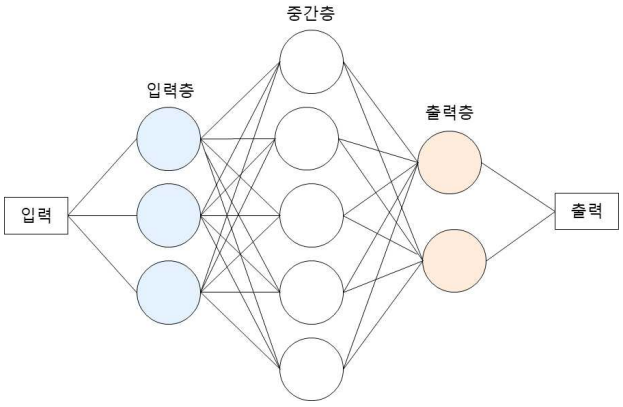
블록체인의 합의 방식은 크게 PoW(Proof-of-Work), PBFT(Practical Byzantine Fault Tolerance)[6][7]로 동작한다.

PoW는 비트코인과 이더리움에서 사용하는 합의 방식으로, 블록체인이 제시하는 문제의 해답을 네트워크 참여자들이 SHA-256 알고리즘을 사용하여 찾아내는 방식이다. 네트워크 참여자중 가장 먼저 문제에 대한 해답을 찾아내면 이를 51% 이상의 참여자가 동의하였을 때 이를 블록으로 등록한다.

PBFT는 블록에 등록할 내용이 있을 때 리더 노드가 참여자 노드에게 내용을 전파한다. 이를 2차로 참여자 노드들끼리 주고받는 절차를 통해 이중 확인을 거친다. 이후 참여자들이 동일한 내용을 전달받았음을 확인하면 블록을 생성하여 블록체인에 등록한다.

2.2 딥러닝

딥러닝은 머신러닝의 한 종류로 여러 층의 신경망(Neural Network)을 사용하여 학습하는 기법이다. 기존의 머신러닝과의 가장 큰 차이점은 특징량을 추출하는 방법의 차이가 있다. 기존 방식에서는 사람이 내부의 특징을 지정해주어야 하는 번거로움이 있었지만, 딥러닝에서는 이를 기계가 자동으로 추출하여 학습할 수 있다. 이를 위해 사용되는 것이 신경망이다.



(그림 2) 신경망 구조

신경망의 구조는 위의 (그림 2)과 같이 나타낼 수 있다. 신경망에서 입력층에 학습하고자하는 데이터들을 입력한다. 데이터가 입력되면 입력층, 중간층, 출력층을 거쳐가면서 처리가 이루어진 후 출력물이 생성된다. 이러한 신경망 형태를 3개 이상 중첩 시키는 경우를 깊은 신경망이라 하며 이를 활용하여 기계학습을 하는 것이 딥러닝이다[8].

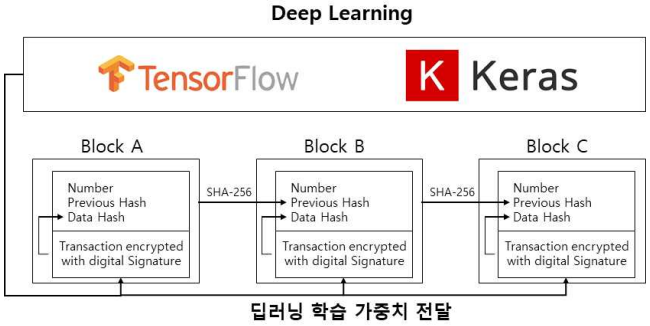
이때 각 입력에서는 입력한 값에 대하여 최정적인 출력을 도출할 때 각 입력에 대해 가중치라는 매개변수를 사용한다. 가중치는 올바른 의사결정을 하기 위한 방향으로 변경되어지지만 과잉 학습이 되면 학습 퇴화가 이루어지거나 가중치의 변화로 인해 전혀 다른 결과값을 나타내게 될 수 있다.

3. 제안 설계

3.1 제안하는 기법의 구조

제안 하는 기법에서는 딥러닝에서 학습을 수행할

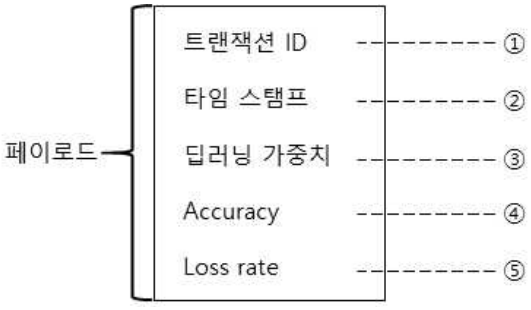
때 변경되는 가중치와 학습 결과를 블록체인의 트랜잭션으로 저장하는 방식을 사용한다. 블록체인에 보관되어 있는 가중치는 딥러닝 학습의 형상관리에 사용된다. 딥러닝 수행 결과가 퇴화 학습 결과로 나타나거나 잘못된 값을 출력해 주는 경우, 블록체인에 보관된 학습 기록을 참조하여 가장 최근 혹은 최고의 효율일 때의 상태로 전환할 수 있도록 한다. 제안하는 구조를 도식화하면 다음의 (그림 3)과 같다.



(그림 3) 제안하는 기법의 구조도

3.2 블록 구조

제안하는 기법에서 블록의 헤더에는 기존의 블록체인에서 사용하는 내용과 비슷한 형태를 가진다. 블록 헤더는 블록체인 버전, 이전 블록 해시 값, 페이로드 해시 값, 타임스탬프, Nonce 값이 포함된다. 페이로드에는 딥러닝에 수행 결과를 반영할 수 있는 데이터가 포함되어야 하므로 아래의 (그림 4)과 같은 형태의 데이터로 구성되어야 한다.



(그림 3) 블록체인 페이로드 내용

① 딥러닝이 수행되었을 때의 순서 또는 딥러닝이 수행된 것을 확인하기 위한 고유한 식별자
② 딥러닝이 수행되서 블록체인의 페이로드에 기록된 시간을 기록
③ 딥러닝 수행 시 사용된 가중치 값
④ 딥러닝 수행 결과의 정확도
⑤ 딥러닝 수행 결과의 손실율

3.3 블록체인 네트워크와 합의 방안

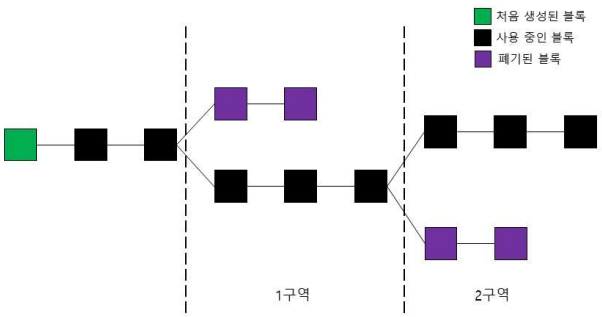
제안하는 기법에서 블록체인 네트워크는 퍼블릭, 프라이빗의 제한 없이 모든 방식에서 사용 가능한 것으로 설계하였다. 이는 딥러닝 형상관리 기능의 사용 대상이 대규모 집단 뿐만아니라 소규모 구성에서도 사용할 수 있어야 하기 때문이다. 프라이빗 블록체인 네트워크를 구성하기 위해 필요한 권한 설정의 경우, Smart Contract를 이용하여 사용자의 권한과 딥러닝 수행의 가능 여부 등을 결정할 수 있도록 제공하는 것을 목표로 한다.

기존의 블록체인에서 합의를 진행할 때 24/7의 연속적인 동기식 방식의 PoW 혹은 PBFT와 같은 합의 방식을 사용한다. 하지만, 딥러닝 학습의 경우에는 24/7으로 동작하지 않는 경우가 많다. 이 때문에 연속적 방식을 사용하였을 때 불필요한 컴퓨팅 파워와 자원이 소모되기 때문에 적합하지 않아 비연속적 방식을 사용하는 것이 적합하다.

PoW와 PBFT의 두 가지 합의 방식 중에서는 PoW 방식을 사용하는 것으로 설계하였다. PBFT의 경우에는 Chain-Code라는 정교한 형태의 동작을 구현해주는 기능이 존재하지만, 블록 생성 시 실제 데이터보다 헤더에 포함되는 내용이 너무 많다. 이에 블록을 하나 생성할 때 블록 사이즈가 200Mbyte를 가지게 되기 때문에 부적합하다[9]. PoW의 경우에는 Chain-Code와 같은 정교한 작업 수행은 어렵지만, Smart Contract를 사용하여 기능을 수행하고 권한을 부여하는 역할을 수행할 수 있다.

3.4 딥러닝 학습 결과 롤백 기능

답러닝 학습을 수행한 결과가 잘못되었을 경우 기존의 학습을 수행했을때의 가중치를 가진 상태로의 복원이 필요하다. 이를 위해 사용자는 블록체인 네트워크에 접근하여 이전 상태의 블록에 등록되어있는 가중치를 가져온다. 이때 블록체인의 상태를 그림으로 도식화하면 (그림 4)와 같이 생성된다.



(그림 4) 서비스 진행중인 블록체인의 형태

그림에서 검정색으로 표현된 부분은 계속하여 최상의 결과를 도출해낸 가중치 값이 가지고 있는 블록이다. 보라색으로 표기된 블록의 경우 기존에는 최상의 결과를 가지고 있었으나, 가중치의 변경 혹은 초과 학습으로 인한 이상 결과가 나타났을 때 폐기된 블록이 있는 것을 표현하였다.

4. 향후 연구 계획 및 결과

제안하는 기법을 설계하며 딥러닝을 활용한 학습을 수행할 때, 가중치의 중간값을 하나씩 관리하지 못하여 처음부터 학습해야하는 상황을 해결하도록 설계하였다. 현재 연구에서의 한계점은 블록체인에 블록이 계속해서 생성되고 중간에 분기가 발생하였을 때, 기존의 블록을 어떻게 처리할 것인지에 문제가 존재한다. 또한 비연속적 방식으로 블록을 생성할 때 한 개의 블록에 최대 몇 개의 학습 결과를 포함시켜 블록을 생성할 것인지에 대한 연구가 필요하다. 이 때문에 향후에는 딥러닝 학습 환경과 블록체인 네트워크를 구성하여 테스트를 진행하고 이 결과값을 바탕으로 시스템을 보완하고자 한다.

ACKNOWLEDGE

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음" (IITP-2020-2020-0-01602)

참고문헌

[1] Gartner "2Megatrends Dominate the Gartner Hype Cycle for Artificial Interlligence, 2020" 2020
[2] 우지환 "인공지능 기술 최신 동향" 2020
[3] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009
[4] Vitalik Buterin "Ethereum White Paper: A Next Gerneration Smart Contract & Decentralized Application Platform", 2014
[5] IBM "An Introduction to Hyperledger", 2018
[6] Kevin Driscoll et al. "Byzantine Falut Tolerance, from Theory to Reality", "Computer safy, Realiability, and Security. pp235-248, 2003
[7] Miguel Castro, Barbara Likov. "Practical Byzantine Fault Tolerance". Third Symposium on Operating System Design and Implementation. 1999.
[8] 쿠지라 히코우즈쿠에 "파이썬을 이용한 머신러닝, 딥러닝 실전 개발 입문" 위키북스
[9] 봉진숙 "하이퍼레저 패브릭 블록체인 기반의 개인건강정보 공유플랫폼" 국내박사학위논문 숭실대학교 대학원, 2019