사물인터넷을 위한 경량 합의 알고리즘 동향

강예준*, 김현지*, 김원웅*, 임세진*, 서화정*†

*한성대학교 (대학원생)

*†한성대학교 (교수)

Trends in Lightweight Consensus Algorithms for the Internet of Things

Yea-Jun Kang*, Hyun-Ji Kim*, Won-Woong Kim*, Se-jin Lim*, Hwa-Jeong Seo*†

*Hansung University(Graduate student)

*Hansung University(Professor)

요 약

강력한 보안 성능을 지니고 있는 블록체인은 비교적 보안 성능이 약한 사물인터넷의 문제점을 보완해줄 수 있다. 하지만 사물인터넷의 경우 저장 공간 부족, 낮은 컴퓨팅 성능 등과 같은 문제점 때문에, 블록체인을 적용하기에는 많은 문제점이 있다. 본 논문에서는 이러한 문제점을 해결해줄 수 있는 경량 합의 알고리즘에 대해 살펴본다. 보안을 유지한 채로 합의가 이루어지는 알고리즘, 클러스터 헤드 노드를 통해 에너지 효율을 높이는 등의 다양한 합의 알고리즘이 연구되었으며, 이를 통해 블록체인을 사물인터넷에 적용할 수 있음을 보였다.

I. 서론

강력한 보안 성능을 지니고 있는 블록체인은 비교적 보안 성능이 약한 사물인터넷의 (Internet of Things : IoT) 문제점을 보완해줄 수 있다. 하지만 사물인터넷의 경우 저장 공간 부족, 낮은 컴퓨팅 성능 등과 같은 문제점이 존재하므로, 블록체인을 사물인터넷에 적용시키기 위해서는 블록체인을 경량화 시킬 필요가 있다. 이러한 이유로 최근 사물인터넷 상에 블록체인을 적용하려는 연구가 다수 이루어지고 있다. 본 논문에서는 블록체인을 경량화 시키기 위한 경량 합의 알고리즘 동향에 대해 살펴본다.

II. 관련 연구

2.1 합의 알고리즘

블록체인은 중앙 기관이 없고, 모든 네트워크 참여자들이 peer To peer(P2P) 네트워크 방식으로 동일한 원장을 공유하고 있는 분산 원장 네트워크이다[1]. 합의 알고리즘은 이러한 분산 네트워크 상의 서로 신뢰할 수 없는 참여자들이 특정한 절차를 거쳐 시스템의 무결성을 보장하고 같은 의사결정을 하기 위해 사용되는 알고리즘을 말한다. 따라서 블록체인 네트워크 내에서 합의 알고리즘은 매우 중요한 기술이며, 많은 종류의 합의알고리즘이 있다. 대표적으로 비트코인에서 사용하는 합의 알고리즘인 작업증명(PoW)과 이더리움에서 사용되는 지분증명(PoS) 합의 알고리즘이 있다. 이 외에도 DPoS, 경과시간증명(PoET), 그리고 중요도증명(PoI) 등이 있다.

2.2 경량 블록체인

대부분의 기존 블록체인은 많은 양의 컴퓨팅 성능을 요구하는 합의 알고리즘을 사용하여, 처리 속도가 느리고 트랜잭션 지연이 높다. 따라서 이와 같은 블록체인을 사물인터넷 상에서 활용하기에는 사물인터넷의 부족한 자원으로 인해 매우 제한적이다. 하지만 최근 사물인터넷 상에서 블

록체인을 활용하기 위해, 합의 알고리즘을 경량화 시키려는 다양한 연구가 진행되고 있다.

III.본론

본 논문에서는 IoT를 위한 경량 합의 알고리즘 동향에 대해 살펴본다.

[2]에서는 거래 검증 및 블록 생성 단계에서 보안을 유지한 채로 합의에 도달할 수 있는 PoBT(Proof of Block & Trade) 합의 알고리즘을 제안하였다. PoBT는 크게 거래 검증 과정과 합의 형성 과정으로 나뉜다. 거래 검증 단계는 트랜잭션과 직접적으로 관련된 노드만 연결되도록 제한된다. 이로써 보안을 유지한 채로 정보를 교환할 수 있으며 요구되는 시간과 오버헤드를 감소시킬 수 있다. 블록 생성 과정에서는 주문자가 주어진 시간 동안 수집한 여러 검증된 거래를 포함하는 후보 블록에 대해 합의를 수행한다. PoBT를 Hyperleger fabric과 비교하여 성능을 평가한 결과 소요 시간과 메모리 측면에서 성능이 크게 향상되었음을 확인할 수 있었다.

[3]에서는 에너지 소비가 적어 사물인터넷에 적합한 PoEWAL 합의 알고리즘을 제안하였다. PoEWAL 합의 알고리즘은 클러스터로 분할된 계층적 네트워크 상에서 합의가 이루어진다. 클러스터는 여러 IoT 장치와 클러스터 헤드 노드로 구성된다. 해당 시스템에서 트랜잭션은 서로 다른 IoT 장치 간의 데이터 전송을 말한다. IoT 장치는 즉각적인 환경을 모니터링하기 위해 배포된 리소스가 제한되어있는 노드이다. 각각의 IoT 장치는 데이터를 감지하여 클러스터 헤드 노드로 데이터를 보내고, 클러스터 헤드 노드는 기지국으로 데이터를 보낸다. 클러스터 헤드 노드들은 각각 180개의 노드를 관리하고 감지 정보를 수신 및 전달하며, 블록체인 네트워크를 유지하기에 충분한 연산과 저장 그리고 배터리 용량을 갖춘 IoT 장치이다. 일반 IoT 장치는 저장할 용량을 갖추고 있지 않기 때문에, 원장은 클러스터 헤드 노드들이 저장하고 있다. PoEWAL을 contiki-Cooja 시뮬레이터를 통해 구현하여 사물인터넷 상에서의 실행 가능성을 확인하였다. 또한 PoW, PoA, PoS 그리고 PoAu 합의 알고리즘과 비교하였을 때, 낮은 에너지를 소비한다는 점에 있어서 사물인터넷에 더욱 적합한 합의 알고리즘임을 증명하였다.

[4]에서는 검증 측면에서 확장성을 향상시킨 합의 알고리즘 CBCIoT을 제안하였다. 해당 알고리즘에서는 투표를 통해 마스터 노드를 선출한다. 그 후 모든 노드는 마스터 노드에게 데이터를 보낸다. 마스터 노드는 30초 동안 데이터를 수신하고, 30초가 지나면 유효성 검사를 위해 무작위로 선택된 5개의 노드에 데이터를 보낸다. 5개의 노드는 블록을 생성하고, 1개의 노드만 먼저 블록을 다른 4개의 노드에 블록을 보낸다. 만약 동시에 블록을 생성할 경우에는 검증 횟수가 많은 블록이 승리한다. 검증이 완료되면, 블록은 마스터 노드에 의해 모든 블록체인 노드로 브로드캐스트 되어 원장에 저장된다. 블록이 생성된 후에는 동일한 절차가 반복된다. 해당 합의 알고리즘은 시간 지연이 필요한 합의 알고리즘이므로 지연을 허용할 수 있는 사물인터넷에 적합하다.

IV.결론

본 논문에서는 사물인터넷을 위한 경량 합의 알고리즘 동향에 대해 살펴보았다. 사물인터넷의 경우 저장공간 부족, 낮은 컴퓨팅 성능 등과 같은 문제가 존재함으로 이러한 문제를 해결하기위해 다양한 합의 알고리즘이 연구되고 있다. 일반적으로 합의에 참여하는 노드들을 제한하는 방법이 다수 연구되고 있었다. 이러한 경량 합의 알고리즘을 통해 사물인터넷에도 블록체인이 적용될 수 있음을 확인할 수 있었다.

V. Acknowledgement

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 100%).

[참고문헌]

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[2] Biswas, Sujit, et al. "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain." IEEE Internet of Things Journal 7.3 (2019): 2343-2355.

[3] Andola, Nitish, Sharannya Venkatesan, and Shekhar Verma. "PoEWAL: A lightweight consensus mechanism for blockchain in IoT." Pervasive and Mobile Computing 69 (2020): 101291.

[4] Uddin, Moin, et al. "CBCIoT: A Consensus Algorithm for Blockchain-Based IoT Applications." Applied Sciences 11.22 (2021): 11011.