경량 IoT 디바이스를 위한 블록체인 경량화 기법 동향

김원웅[1], 강예준[1], 서화정[2]
[1]한성대학교 IT융합공학과 석사과정
[2]한성대학교 융합보안학과 교수
dnjsdndeee@gmail.com, etus1211@gmail.com, hwajeong84@gmail.com

A Study on Lightweight Blockchain technique for Lightweight IoT Device

Won-Woong Kim[1], Yea-Jun Kang[1], Hwa-Jeong Seo[2]
[1]Dept. of IT Convergence Engineering Han-Sung University
[2]Dept. of Convergence Security, Han-sung University

요 약

최근 스마트 시티 등과 같은 이유로 IoT에 대한 관심이 증가하며 이에 대한 보안 솔루션 또한 주목받게 되었다. 이때 블록체인이 보안 솔루션으로써 많은 관심을 받고있지만 확장성에 한계에 의하여 IoT와의 융합에 제한을 받고있는 상황이다. 따라서 이러한 확장성 문제를 해결하기 위한 다양한 기법들이 존재한다. 본 논문에서는 확장성의 한계를 해결하기 위해 블록체인 경량화 기법의 연구 사례에 대하여 알아본다.

1. 서론

최근 IoT의 증가에 의해 IoT 디바이스에 대한 보안 솔루션에 대한 필요성이 대두되고 있다. 이때 블록체인이 보안을 향상시키기 위한 훌륭한 솔루션으로 주목받고 있지만, 확장성에 한계에 의하여 IoT와의 통합에 문제점이 존재한다. 대표적으로 블록체인은 플러딩 기술을 사용하여 블록을 공유하므로 중복되고 비효율적인 대역폭 사용이 발생한다. 또한 무작위 이웃 선택 기술(Random Neighbor Selection, RNS)을 사용하여 처리량에 제한이 존재한다.[1] 더불어 블록이 증가함에 따라 필연적으로 스토리지 요구사항이 증가함으로써, 상대적으로 금융 시스템과 같이 빠른 속도로 많은 양의 데이터가 생성되는 산업용 IoT (Industrial IoT)와의 통합에 문제가 존재한다.[2] 따라서 이를 해결하기 위한 많은 연구들이 진행되고 있으며 본 논문에서는 이러한 연구 사례들에 대하여 알아본다.

2. 배경 지식

2.1 블록체인

블록체인이란 신뢰할 수 있는 중앙 기관의 존재 없이 사용자들끼리의 Peer-to-Peer 형태의 거래를 가능하도록 한 네트워크 구조이다. 중앙 기관이 존재하지 않으므로 합의 알고리즘이라고 부르는 고유한 알고리즘을 통하여 거래에 대해 사용자들끼리의 합의를 이루게 된다. 블록체인에는 거래를 담고있는 블록이 존재하며, 시간이 지남에 따라 지속적으로 추가된다. 또한 이러한 블록이 이전 블록과 암호학적으로 연결되어 있으며 이러한 모양이 체인과 비슷하다고 하여 블록체인이라는 이름이 붙게 되었다. 대표적으로 비트코인과 이더리움이 있다. 이러한 네트워크의 사용자들은 모든 거래에 대한 블록을 지니고 있는데 이로 인하여 매우 높은 저장 공간이 요구된다.

2.2 PBFT (Practical Byzantine Fault Tolerance)

PBFT란 네트워크 내의 악의적인 노드가 존재하였을 경우에 발생할 수 있는 비잔틴 장군 문제를 해결하기 위한 알고리즘이다. REQUEST, PRE-PREPARE, PREPARE, COMMIT, REPLY의 단계로 구성되며 해당 과정에서 수차례의 브로드캐스팅을 통해 악의적인 노드가 전체 노드의 1/3이하로 존재하게 될 경우 무시할 수 있도록 해주는 알고리즘이다. 이때 수차례의 브로드캐스팅이 발생하기 때문에 확장성의 한계가 존재한다.

3. 연구 사례

3.1 Storage Compression Consensus (SCC) [3]

SCC는 기존의 PBFT에 블록 압축 기술을 적용함으로써 IoT상에서의 블록체인 저장에 대한 부담을 줄여 합의를 원활히 이룰 수 있도록 한 알고리즘이다. 초기화, 리더 선출, 압축, 저장의 네 단계로 구성되어 있다. 초기화 과정은 새롭게 연결된 IoT 디바이스의 정보를 네트워크에 등록하기 위한 과정이다. SCC를 통한 정상적인 합의를 위해서는 합의를 제안하는 노드의 실제 저장 용량을 확인해야 한다. 따라서 네트워크에 합류하게 되는 새로운 IoT는 저장 용량 S와 저장 용량의 한계값인 임계값 T를 네트워크에 알리게 된다. 일정 라운드 이후 디바이스에 저장되어 있는 블록체인의 크기가 B일 때 디바이스의 저장 용량 한계를 초과하였는지에 대해 다음과 같은 식을 통해 확인할 수 있다.

$$\frac{B_i}{S_i} \geq T_i \, (i = 1, 2, \cdots, n) \qquad (1)$$

이때 I는 디바이스의 인덱스이며 n개의 노드가 있다고 가정한다.

리더 선출 과정은 새로운 라운드가 시작되었을 때 합의를 이루고자 하는 리더를 선출하는 과정이다. SCC에서는 PBFT의 라운드가 종료되고 초기화 과정을 기반으로 저장 용량이 부족함을 인지하였을 때 리더 선출 과정을 수행한다. 즉, 블록체인을 저장할 수 있는 남은 용량이 가장 적은 노드가 리더로 선출된다. 선출된 리더는 압축 과정을 통해 새로운 블록을 생성한 후 브로드캐스팅함으로써 다른 노드들에게 블록을 제안한다. 다른 노드들은 해당 블록을 수신하였을 때 초기화 과정에 근거하여 해당 노드가 리더가 되는 것이 합리적인지에 대해 검증할 수 있다.

압축 과정은 선출된 리더가 블록체인을 압축하기 위한 과정이다. 기존의 PBFT는 라운드 당 하나의 블록을 처리하는 반면, SCC는 한 라운드에 두 개의 블록을 처리하게 된다. 리더는 압축 블록(BLOCc)와 체인에 추가하고자 하는 넥스트 블록(BLOCn)의 두 블록을 생성한 후 브로드캐스팅 한다. 압축 블록은 머클 트리의 형태로 블록체인에 존재하던 모든 블록들을 통해 생성된 블록이다. 해당 과정을 통해 이전 블록들을 단일 블록으로 만듦으로써 IoT 디바이스의 여유 공간을 확보할 수 있다. 넥스트 블록은 기존의 PBFT와 마찬가지로 해당 라운드에서 생성되고 합의에 의해 블록체인에 추가되는 블록이다. 블록체인의 기본적인 프로토콜을 따르기 위하여 압축 블록은 가장 최근 블록의 해시값을 저장하고 있으며, 넥스트 블록은 압축 블록의 해시값을 저장하고 있다. 두 개의 블록을 생성한 후 다른 노드들에게 브로드캐스팅하게 되면 PBFT에서의 합의 과정을 거치게 된다. 이때, 압축 블록이 저장되어 있던 블록체인을 압축함으로써 생성되었는지, 넥스트 블록이 이번 라운드에 생성된 블록이 맞는지, 각 블록들이 올바른 해시값을 저장하고 있는지 등에 대하여 검증한다.

저장 과정은 노드들이 검증 과정을 마친 블록을 자신의 블록체인에 추가하는 과정이다. 경량 IoT 디바이스는 저장 용량이 비교적 작기 때문에 두 개의 블록을 저장한 후에는 이전에 저장되어 있던 모든 블록들을 삭제한다. 비경량 IoT 디바이스의 경우 추가적인 저장 공간을 확보할 필요가 없기 때문에 단순히 두 개의 블록을 블록체인에 추가하는 것으로 저장 과정을 마치게 된다. 이때 장치 간 저장 방법의 차이로 인하여 각 노드들이 서로 다른 길이의 블록체인을 가지게 된다. 이는 블록체인에서 데이터의 무결성을 검증하는 것에 문제를 야기할 수 있으므로 비경량 IoT 디바이스는 경량 IoT 디바이스에 저장된 블록체인의 길이를 알기 위하여 SCC를 통해 처리된 블록의 인덱스를 저장한다. 만약 비경량 IoT 디바이스의 용량이 부족하게 되더라도 인덱스 이전의 블록을 삭제함으로써 시스템을 일관적으로 유지할 수 있다. 또한 이를 통해 모든 노드가 서로에 대한 검증을 가능토록 할 수 있다.

해당 논문은 초당 1개의 블록을 생성하였으며 블록 당 250개의 트랜잭션을 포함시켜 성능 측정을 진행하였다. 또한 PBFT의 확장성의 한계에 의해 최소 4개의 노드부터 최대 20개의 노드까지 포함하여 성능을 측정하였다. 성능 측정 결과로 SCC 과정에 의해 기존 PBFT에 비해 평균 1.98%의 딜레이가 발생하였지만 평균 63%의 저장 공간을 줄이는 것에 성공하였다.

3.2 Block Summarization [4]

해당 논문은 트랜잭션이 있는 시스템에서의 블록체인 스토리지 오버헤드를 줄이기 위한 블록 요약이라는 기법을 제안하였다. 블록 요약은 노드가 네트워크 내의 모든 블록을 저장하는 것 대신, 일련의 블록을 하나의 블록으로 요약함으로써 네트워크 내에 저장되는 블록의 개수를 줄이는 기법을 의미한다.

요약 블록은 요약된 일련의 블록 내에 존재하던 트랜잭션들에 대한 입력과 트랜잭션에서 사용되지 않은 값인 출력으로 이루어져 있으며 이는 트랜잭션들로 인한 네트워크의 총 변경 사항을 나타낸다. 이러

한 변경 사항들에 대하여 저장함으로써 일련의 블록이 요약 블록으로 대체된 후에도 블록체인의 상태를 동일하게 유지할 수 있다. 또한 출력에 트랜잭션 ID 및 추력의 인덱스가 포함되어 있어 추후 이를 참조하여 트랜잭션에 대한 확인 및 검증이 가능하다. 더불어 요약 블록에 포함된 블록들의 해시나 경우에 따라 블록의 높이 등이 포함될 수 있다.

네트워크의 빈번한 포크에 대하여 모든 체인을 요약하게 될 경우 막대한 네트워크 오버헤드가 발생하게 된다. 따라서 이러한 경우의 오버헤드를 최소화하고 요약 블록을 쉽게 확인할 수 있도록 하기 위하여 체인의 끝에 길이 o만큼의 블록을 제외하고 고정된 길이 l만큼의 블록들을 요약한다. 즉, 블록체인이 $o+l$만큼의 요약되지 않은 블록이 존재하는지에 대해 확인 후 길이 l만큼의 블록을 요약하게 된다. 이때, 요약 체인의 크기 또한 커지게 될 경우 요약 블록들에 대한 요약을 취함으로써 이를 해결할 수 있고 이 경우 트리의 형태가 구성된다. 요약 블록 내에 있는 일련의 블록들은 기존에 이미 검증된 것으로 가정하므로 요약 블록 또한 검증된 블록으로 취급된다.

해당 논문은 높이 200,000부터 250,000까지의 비트코인 블록을 사용하여 성능을 측정하였다. 최적의 l값을 찾기 위하여 l값을 변경해가며 성능을 측정하였으며 $l=75$에서 최적의 압축이 가능하였으며 54%의 압축률을 달성하였다. 결과적으로 블록체인의 크기를 줄임으로써 메모리 용량이나 연산 능력이 낮은 노드에서의 채굴 활동이 가능하게 하였다. 또한 라이트 노드가 블록체인의 일부를 저장함으로써 독립적으로 트랜잭션의 유효성을 검증할 수 있도록 하여 풀 노드에 대한 의존도를 낮추었다.

3.2 Block Summarization + Compression [5]

해당 논문은 [4]의 후속 연구로써, 기존 연구에 deflate 압축 기법을 추가적으로 적용한 알고리즘이다. deflate 압축 기법은 중요한 정보의 손실없이 블록의 크기 자체를 압축할 수 있는 기법으로써, [4]에서 요약 블록의 크기가 기존의 블록보다 크거나 같을 경우를 방지하기 위하여 사용된다.

deflate 압축 기법은 LZ77과 Huffman 압축 알고리즘의 복합 알고리즘이다. 압축은 LZ77로 중복되는 문자열을 제거하는 것으로부터 시작된다. 이때 문자열에 대한 식별은 처리되는 각 블록에 대하여 수행된다. 만일 문자열내의 중복되는 비트가 발견될 경우, 해당 시퀀스의 길이와 블록의 시작으로부터 거리를 포함하는 값이 기록된다. 그 후 Huffman 트리를 사용하는 압축을 통해 자주 나타나는 비트 시퀀스나 데이터를 더욱 짧은 특정 기호로 대체하게 된다.

해당 논문에서의 성능 측정 또한 [4]와 마찬가지로 비트코인의 높이 200,000부터 250,000의 블록을 데이터로 사용하였으며, 실험 결과로써 요약 블록의 압축율이 22.318%에 달할 때 압축 블록의 압축율은 78.104%를 달성하였다. 이를 통해 요약 블록의 크기가 기존 블록의 크기와 동일하다는 문제가 발생하지 않으며, 요약 블록의 공간 절약율을 높일 수 있음을 보여주었다.

4. 결론

본 논문에서는 IoT와 블록체인의 융합을 위해 블록체인의 확장성의 한계를 해결할 수 있는 기법들의 연구 사례에 대해 알아보았다. 해당 기법들의 경우 기존의 블록을 제거함으로써 스토리지 오버헤드를 감소시켰다.

5. Acknowledgements

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] Antwi, Robert, et al. "A survey on network optimization techniques for blockchain systems." *Algorithms* 15.6 (2022): 193.

[2] Akrasi-Mensah, Nana Kwadwo, et al. "An Overview of Technologies for Improving Storage Efficiency in Blockchain-Based IIoT Applications." *Electronics* 11.16 (2022): 2513.

[3] Kim, Teasung, Jaewon Noh, and Sunghyun Cho. "SCC: Storage compression consensus for blockchain in lightweight IoT network." *2019 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2019.

[4] Palai, Asutosh, Meet Vora, and Aashaka Shah. "Empowering light nodes in blockchains with block summarization." *2018 9th IFIP international*

conference on new technologies, mobility and security (NTMS). IEEE, 2018.

[5] Nadiya, Ulfah, Kusprasapta Mutijarsa, and Cahyo Y. Rizqi. "Block summarization and compression in bitcoin blockchain." *2018 International Symposium on Electronics and Smart Devices (ISESD)*. IEEE, 2018.