경량 IoT 디바이스를 위한 블록체인 경량화 기법 동향

한성대학교 김원웅

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

서론

배경 지식

연구 동향

결론

서론

- IoT에 대한 관심이 증가함에 따라 IoT 디바이스에 대한 보안 솔루션의 필요성 필요

  → 보안 솔루션으로써 **블록체인**이 관심을 받고 있음

  → 그러나, 블록체인의 **확장성의 한계**에 의해 IoT와의 통합에 있어 문제점이 존재

  → IoT상에서의 블록체인 저장에 대한 부담을 감소시켜 원활히 합의

배경 지식

- 블록체인
  - 신뢰할 수 있는 중앙 기관의 존재 없이 사용자들끼리의 Peer-to-Peer 형태의 **"거래"**를 가능하도록 한 네트워크 구조
  - **"합의 알고리즘"**을 통해 거래에 대해 사용자들끼리의 합의를 이룸
  - 다수의 거래가 담겨있는 **"블록"** 을 **"체인"**의 형태로 묶음으로써 데이터를 저장

배경지식

- PBFT (Practical Byzantine Fault Tolerance)
  - 네트워크 내의 악의적인 노드가 존재하였을 경우 **비잔틴 장군 문제** 발생

    →PBFT는 이를 해결하기 위한 알고리즘
  - REQUEST, PRE-PREPARE, PREPARE, COMMIT, REPLY의 5단계로 구성
  - 결론적으로, 네트워크 내 악의적인 노드가 **전체 노드의 1/3 이하**로 존재하게 될 경우 무시할 수 있음

Storage Compression Consensus (SCC)

- 기존의 PBFT에 블록 압축 기술을 적용한 알고리즘
- 초기화, 리더 선출, 압축, 저장의 4단계로 구성

1) 초기화

- 네트워크에 새롭게 연결된 디바이스의 정보를 네트워크에 등록하는 과정
- 노드의 실제 저장 용량을 알기 위함
- 저장 용량 S, 저장 용량 한계 T
- $\frac{B_i}{S_i} \geq T_i \, (i = 1, 2, \cdots, n)$

Storage Compression Consensus (SCC)

2) 리더 선출

- PBFT가 종료되었을 때 블록체인을 저장할 수 있는 남은 용량이 가장 적은 노드가 리더로 선출
- 선출된 리더는 압축 과정을 통해 새로운 블록을 생성한 후 브로드캐스팅
- 다른 노드들은 해당 블록을 생성한 리더가 적법한지에 대해 검증

Storage Compression Consensus (SCC)

3) 압축

- 압축 블록(BLOCc)와 체인에 추가하고자 하는 다음 블록 (BLOCn) 생성

  → 압축 블록은 머클 트리의 형태로 블록체인에 존재하던 모든 블록들을 통해 생성된 블록

  → 다음 블록은 합의에 의해 블록체인에 추가되는 블록

- 압축 블록은 가장 최근 블록의 해시값 저장
- 다음 블록은 압축 블록의 해시값 저장
- 블록 생성 후 PBFT을 통해 합의
- 이때, 압축 블록이 블록체인을 압축함으로써 생성되었는지,
- 다음 블록이 이번 라운드에 생성한 블록이 맞는지에 대해 검증

Storage Compression Consensus (SCC)

4) 저장

- 블록을 자신의 블록체인에 추가하는 과정
- 경량 IoT 디바이스의 경우, 두 개의 블록을 저장한 후 이전 블록들을 삭제하여 저장공간 유지
- 비경량 IoT 디바이스의 경우, 추가적인 저장공간을 확보할 필요가 없기 때문에 단순히 두 개의 블록을 추가함으로써 저장

  → 이 때, 디바이스 간 저장 방법의 차이로 인해 각 노드들의 서로 다른 길이의 블록체인을 가질 수 있음

  → 이를 해결하기 위해, 비경량 IoT 디바이스는 경량 IoT 디바이스에 저장된 블록체인의 길이를 알기 위하여 SCC를 통해 처리된 블록의 인덱스를 저장

Block Summarization

- 네트워크 내의 일련의 블록을 하나의 블록으로 요약함으로써 네트워크 내의 저장되는 블록의 개수를 줄이는 기법
- 요약 블록을 요약된 일련의 블록 내에 존재하던 트랜잭션들에 대한 입력과 트랜잭션에서 사용되지 않은 값인 출력으로 구성
- 출력에 트랜잭션 ID 및 출력의 인덱스를 통해 트랜잭션에 대해 검증
- 그러나, 빈번한 포크에 의해 모든 체인을 요약하게 될 경우 막대한 네트워크 오버헤드 발생

  → 이를 위해, 체인 끝의 길이 o 만큼의 블록을 제외하고 고정된 길이 l 만큼의 블록을 요약

Block Summarization + Compression

- 앞전 연구 사례의 후속 연구로써, 기존 연구에 deflate 압축 기법을 추가한 알고리즘
- 중요한 정보의 손실없이 블록의 크기 자체를 압축할 수 있는 기법
- 기존 연구 사례의 요약 블록의 크기가 기존의 블록보다 크거나 같은 경우를 방지하기 위해 사용

- Deflate 알고리즘
  - LZ77과 Huffman 압축 알고리즘으로 구성
  - LZ77 알고리즘을 통해 중복 문자열 제거
  - Huffman 압축 알고리즘을 통해 자주 나타나는 비트 시퀀스나 데이터를 더욱 짧은 특정 기호로 대체

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.

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.

Q & A