블록체인에서 샤딩을 지원하는 P2P 멀티캐스트 통신 방안

김정연, 박세진, 주홍택
계명대학교 컴퓨터공학과
jungyeonkim@stu.kmu.ac.kr, baksejin@kmu.ac.kr juht@kmu.ac.kr

P2P multicast Communication Method Supporting Shading on Blockchain

Jungyeon Kim, Sejin Park, Hongtaek Ju
Department of Computer Engineering, Keimyung Univ.

요 약

최근 블록체인의 주요 관심사 중 하나는 사용자 유입을 고려하여 높은 트랙잭션 처리량과 미래 성장을 지원하는 확장성 개선에 있다. 네트워크 크기 증가와 수평 스케일링(Horizontal Scaling)을 달성하기 위해 샤딩 기술이 확장성 해결 방안으로 주목받고 있다. 샤드 메커니즘에 대한 연구는 샤드 간 교차 샤드 원자성 검증 프로토콜 단계에서 이루어지고 있으며 실용화를 위한 세부적인 기술 연구는 부족하다. 따라서 본 논문에서는 샤드 리더 간 통신 방안에 대한 제안을 담고 있다.

Ⅰ. 서 론

P2P(Peer-to-Peer) 네트워크를 통한 분산 데이터 저장기술인 블록체인은 금융, 물류·유통 등 다양한 분야에서 적용되고 있다. 블록체인은 참여 노드와 사용자가 증가함에 따라 트랜잭션 처리량이 충분하지 않은 확장성(Scalability) 문제가 대두되었다. 확장성 문제는 블록체인 사용을 제한하기 때문에 블록체인이 해결해야 할 중요한 문제이다. 확장성 증가를 위한 대표적인 해결책은 네트워크에 참여하는 노드를 여러 개의 그룹으로 분할하는 샤딩(Sharding)이다. 현재 샤딩은 주로 샤드 간 검증을 위한 교차 샤드 통신(Cross Shard Communication) 프로토콜에 대한 연구가 활발히 진행되고 있으나 세부적인 기술 연구는 부족하다. 따라서 본 논문에서는 블록체인 샤드에서 샤드 리더 간 통신 방식에 대한 제안을 담고 있다.

Ⅱ. 배경 지식

1) Sharding

블록체인에서 사용되는 샤딩은 블록체인 네트워크를 여러 개의 작은 네트워크들로 분할하여 각 샤드에서 독립적으로 트랜잭션을 처리하고 자체 원장을 관리하는 병렬처리 방법이다 [1]. 샤딩 기술을 활용하여 블록체인의 노드 수가 증가함에 따라 초당 트랜잭션 처리량(TPS: Transaction Per Second)을 선형적으로 증가시킬 수 있다.

샤드는 리더(Leader)와 노드(Node)로 그림 1과 같이 이루어진다. 샤드 리더는 블록체인의 합의 알고리즘에 따라 선정되고 위원회(Committee)에 포함된다. 리더는 네트워크를 샤드하고 해당 샤드에 노드를 할당한다. 리더는 교차 검증(Cross Verification)을 지원하여 교차 샤드 원자성(Cross Shard Atomicity)을 보장해야 한다. 샤딩 메커니즘은 서로 다른 샤드 간 트랜잭션(Transaction)과 스마트 컨트랙트(Smart Contract)를 지원할 수 있는 것이 중요하다. 개별 샤드가 서로 통신할 수 없다면 여러 개의 독립적인 블록체인과 같기 때문이다.

교차 샤드 통신(Cross Shard Communication) 프로토콜에 대한 연구는 OmniLedger의 Atomix Protocol[2], Ethereum 2.0의 Receipts[3] 등으로 활발하게 연구되고 있다. 그러나 샤드 리더 간의 효율적인 통신 방식에 대한 연구 진행은 부족하다.

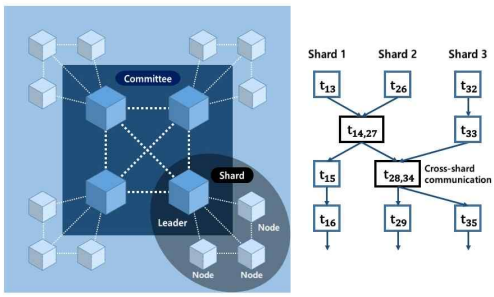

그림 1. 샤드 구조 및 교차 샤드 트랜잭션

2) Kademlia

Kademlia는 분산 P2P 컴퓨터 네트워크를 위한 분산 해시 테이블(Distributed Hash Table)을 구축하는 프로토콜이다 [4]. UDP를 이용한 노드 탐색으로 네트워크에 참여하는 노드의 정보를 교환하고 정보를 이용하여 노드와 통신할 수 있다. 모든 정보는 <key, value> 쌍의 형태로 저장된다.

네트워크에 참여하는 노드들은 서로를 식별하기 위해 자체적으로 랜덤한 160bit의 노드 ID를 생성한다. Kademlia는 두 임의 노드 ID인 x와 y 사이의 거리를 $d(x,y) = x \oplus y$로 정의한다. 각 노드는 노드 탐색을 위해 인접 노드로 노드 정보 요청 메시지를 전송한다. 응답으로 노드 ID, IP 주소, UDP 포트 정보를 수신하고, 이를 k-bucket에 저장한다. k-bucket은 $0 \le i < 160$개의 버킷으로 분할되며, 각 버킷은 노드 거리가 2^i에서 2^{i+1}사이인 노드 목록이다. k-bucket은 일반적으로 노드를 통과하는 요청 트래픽으로 인해 최신 상태로 유지된다. 트래픽이 없는 경우, 비활성 노드로 인지하고 해당 노드 ID에 대한 노드 검색을 수행한다.

Kademlia는 노드 간의 거리를 XOR metric을 사용하여, 모든 노드가 동일한 시스템 로드 확률을 가지고 있기 때문에 모든 노드들이 동등하게 연결되어 부하 분산시킬 수 있다. 또한, 시스템 전체에 n개의 노드가 존재할 때, $O(\log_2 n)$ 검색만으로 특정 노드를 찾을 수 있다.

Ⅲ. 교차 샤드 통신 메커니즘 설계

본 논문에서는 샤드 리더 간 효율적인 통신을 위한 Kademlia 기반의 P2P 멀티캐스트 메커니즘을 제안한다. 위원회에 포함되는 샤드 리더들은 개별적으로 노드 ID를 생성하고 리더 노드의 정보를 버킷에 저장한다. P2P 멀티캐스트에서 그룹은 고유 그룹 ID를 가지고 있다. 멀티캐스트 그룹의 루트 노드(Root Node)는 멀티캐스트 그룹 트리의 루트에 위치한 노드다. 노드 ID와 그룹 ID의 거리가 0 이거나 가장 가까운 노드가 루트 노드의 역할을 수행한다.

1) P2P 멀티캐스트 그룹 생성

멀티캐스트 그룹을 생성하기 위해 P2P 멀티캐스트 참여 노드들은 랜덤한 그룹 ID를 포함한 메시지를 생성한다. 생성 메시지는 위원회에 참여하는 모든 노드에게 브로드캐스팅(Broadcasting) 방식으로 전송된다. 생성 메시지가 가장 많은 ID가 그룹 ID로 선정된다. 참여 노드들은 브로드캐스팅 받은 생성 메시지를 집계하여 그룹 ID를 인정한다. 루트 노드를 교대하기 위해서 주기적으로 그룹 ID를 새로 생성해야 한다.

2) P2P 멀티캐스트 그룹 가입

멀티캐스트 그룹에 가입하기 위해 노드는 그룹 ID에 가장 가까운 노드로 그룹 가입 메시지를 보낸다. 가입 요청을 멀티캐스트 그룹에 가입 완료된 노드가 응답할 경우에는 해당 노드를 부모 노드(Parent Node)로 지정하고 자식 노드(Child Node)로 연결된다. 결합된 부모 노드는 루트 노드에 대한 위치 정보를 알려준다. 멀티캐스트 그룹 트리에 연결되면 그룹 가입 요청을 중지한다. 그룹에 연결된 노드를 찾지 못했을 경우에는 Kademlia 알고리즘으로 계속해서 가입 요청을 전송한다.

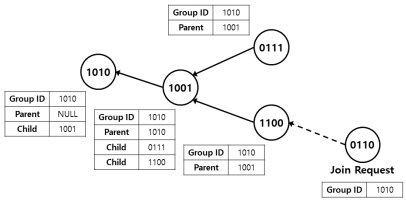

그림 2. P2P 멀티캐스트 그룹 가입

3) P2P 멀티캐스트 그룹 탈퇴 및 유지

멀티캐스트 그룹의 가입된 멤버 노드(Member Node)는 자식 노드의 유무에 따라 탈퇴 메시지를 전송한다. 탈퇴할 노드가 리프 노드(Leaf Node)라면 부모 노드에게 탈퇴 메시지를 전송하여 부모 노드의 그룹 버킷에서 삭제되면 탈퇴 완료된다. 그림 3과 같이 탈퇴할 노드가 자식 노드가 있다면 부모 노드 ID와 자식 노드 ID를 포함한 탈퇴 메시지를 부모 노드와 그룹 ID에 거리가 가까운 자식 노드로 전송한다. 노드 ID가 포함된 탈퇴 메시지를 받은 부모 노드와 자식 노드는 그룹 버킷에서 메시지를 송신한 노드 ID를 삭제하고 서로의 노드 ID를 저장한다.

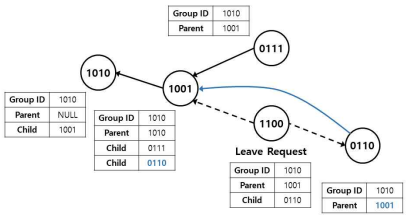

그림 3. P2P 멀티캐스트 그룹 탈퇴

멀티캐스트 그룹 멤버 노드들은 다양한 이유로 탈퇴 공지 없이 그룹에서 탈퇴할 수 있다. 그림 4에서 볼 수 있듯이, 노드 1001의 연결이 실패할 때 자식 노드 0111과 1100은 그룹 가입 요청을 재전송한다. 재요청을 통해 멤버 노드를 찾아 멀티캐스트 재연결할 수 있다.

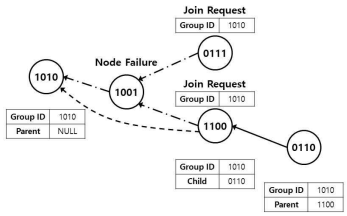

그림 4. P2P 멀티캐스트 그룹 유지

4) P2P 멀티캐스트 그룹 메시지 전달

멀티캐스트 그룹의 가입 후에 루트 노드에 대한 정보를 수신받고 저장하므로, 멤버 노드가 교차 검증을 위한 메시지를 직접적으로 루트 노드로 보낸다. 그림 5는 메시지 전달 과정을 보여준다. 루트 노드는 검증 메시지를 하위 노드로 전송하고, 전달받은 노드들도 하위 노드로 전송한다. 최종적으로 리프 노드까지 중복 없이 메시지가 전달된다.

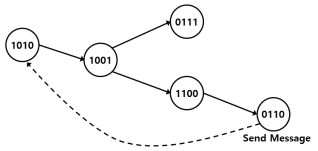

그림 5. P2P 멀티캐스트 메시지 전달

Ⅳ. 결 론

본 논문에서는 Kademlia를 이용한 참여 노드 간에 가상 또는 오버레이 네트워크 형성과 샤드 리더 노드 간 P2P 멀티캐스트 방안을 제안하였다. 기존에 존재하는 대부분의 교차 샤드 통신 관련 연구들은 시스템 요구사항이나 프로토콜을 제안하는 것에 그치고 있다. 이와 달리, 본 논문은 구체적인 교차 샤드 통신 개발을 위한 기술적 방법을 제안하였다. P2P 멀티캐스트 방식은 기존에 사용하는 브로드캐스팅보다 중복 전송이 적어 메시지 전달 효율성이 높일 수 있다. 향후 연구에서는 Libp2p를 이용하여 제안한 P2P 멀티캐스트를 구현할 예정이다.

ACKNOWLEDGMENT

이 논문은 2021년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2018R1D1A1B07050380) 및 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2019R1G1A1100305).

참 고 문 헌

[1] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14155-14181, 2020.

[2] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta and B. Ford, "OmniLedger: A secure scale-out decentralized ledger via sharding," *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 583-598, May 2018.

[3] V. Buterin. (2020, Jun.). Ethereum Sharding FAQ [Online]. Available: https://eth.wiki/sharding/Sharding-FAQs

[4] P. Maymounkov and D. Mazières, "Kademlia: A peer-to-peer information system based on the XOR metric," *International Workshop on Peer-to-Peer Systems*, pp. 53-65, Mar. 2002.