Gossip 기반 P2P 라우팅을 통한 블록체인 성능 개선 연구

최원석, 강창훈, 홍원기
포항공과대학교 컴퓨터공학과

{ws4583, chkang, jwkhong}@postech.ac.kr

A Study on Improvement of Blockchain Performance through Gossip-based P2P Routing

Wonseok Choi, Changhoon Kang, James Won-Ki Hong
Department of Computer Science and Engineering, POSTECH

요 약

Peer-to-Peer(P2P) 네트워크는 기존의 클라이언트-서버 모델과 달리 모든 노드들이 자원을 공유하며 서비스 요청자와 서비스 제공자의 역할을 수행한다. 다양한 P2P 서비스들의 등장과 더불어 현재 혁신적인 기술로 큰 주목을 받고 있는 블록체인 기술 역시 P2P 네트워크를 기반으로 하고 있다. 현재 블록체인의 주요 관심사 중 하나는 실용화를 위한 성능 개선에 있다. 이러한 성능개선에 관한 연구는 대부분 합의 알고리즘 단계에서 이루어지고 있으며 여러 블록체인들이 독자적인 합의 알고리즘을 적용하여 성능을 개선하고 있다. 하지만 블록체인에서의 P2P 라우팅의 경우 메시지 전파를 위해 여러 P2P 서비스에서 사용하고 있는 Gossip 기반의 라우팅을 적용하고 있다. 합의 알고리즘뿐만 아니라 P2P 라우팅 방식 역시 블록체인에서 노드 간의 메시지 전달에 주요한 역할을 하기 때문에 P2P 라우팅의 개선 또한 블록체인의 성능 개선으로 이어질 수 있다. 본 논문에서는 기존의 Gossip 기반 P2P 라우팅 방식들에 대해 분석하여 블록체인에 적합한 형태의 Gossip 기반 P2P 라우팅을 어떻게 구성해야 할지에 대해 제안함으로써 블록체인의 성능 개선에 기여하고자 한다.

Ⅰ. 서 론

Peer-to-Peer(P2P)[1] 네트워크는 별도의 중앙 서버가 존재하지 않는 분산된 시스템으로 모든 노드들이 동등한 권한을 가진다. 기존의 클라이언트-서버 모델과 달리 P2P 네트워크에서는 노드들이 서비스 요청자와 서비스 제공자의 역할을 동시에 수행하기 때문에 모든 노드들이 자원을 공유 해야 하는 시스템에서 주로 사용된다. 사토시 나카모토라는 익명의 개발자로부터 처음 제안된 비트코인[2]에서부터 비롯되어 현재 많은 연구가 진행되고 있는 분산 컴퓨팅 기술인 블록체인 기술 역시 P2P 네트워크를 기반으로 하고 있다.

블록체인은 탈중앙성이나 익명성 등의 장점으로 많은 주목을 받고 있으나 실용화를 위해서는 여전히 성능적인 부분에서 문제가 존재한다. 대표적인 블록체인인 비트코인에서는 대략 10 정도의 초당 거래량(TPS), 이더리움에서는 15~20 정도의 TPS 를 보이고 있다. 대부분의 블록체인들은 이러한 TPS 문제를 개선하기 위해 기존의 합의 알고리즘을 개선하는 것에서 방법을 있다. 대표적으로 Cosmos[3] 에서는 DPoS(Delegated Proof of Stake)[3]와 PBFT(Practical Byzantine Fault Tolerance)[4]를 결합한 텐더민트 합의 알고리즘[3]을 사용하고 있으며 Algorand[5] 역시 DPoS 를 이용해 TPS 를 개선하였다.

하지만 P2P 라우팅 단계에서는 별다른 개선 없이 대부분 기존 Gossip 기반의 라우팅을 사용하고 있다. P2P 네트워크에서는 하나의 노드로부터 빠르게, 많은 노드들에게 메시지를 전송하는 것이 중요하다. 이를 위해 효율적인 멀티캐스팅[6]이 요구되며 현재 P2P 네트워크에서 대표적으로 사용되는 것이 Gossip 기반의 멀티캐스팅[7] 방식이다. Gossip 프로토콜에서 노드들은 주기적으로 이웃 노드들에게 메시지를 전송하며 메시지를 받은 노드들 역시 동일하게 이를 이웃 노드들에게 전송한다. 모든 이웃 노드들에게 메시지를 보내는 대신 메시지를 보낼 이웃 노드를 선정하는 알고리즘을 달리 하여 성능 개선이 가능하고 메시지 전송 방식에도 Eager Push, Lazy Push, Pull 등의 접근 방식[8]이 존재한다.

Gossip 프로토콜에도 여러 접근 방식이 존재하고 이를 통한 성능 개선이 가능하다. 본 논문에서는 Gossip 기반 P2P 라우팅을 분석하고 블록체인에 사용하기 적합한 형태의 Gossip 프로토콜을 찾기 위한 고려 사항들을 분석함으로써 블록체인 성능 개선에 기여하고자 한다.

Ⅱ. 관련 연구

GossipPINE[9] 에서는 Gossip 프로토콜에서 확률적으로 메시지를 보낼 이웃 노드를 선정하는 Probabilistic Neighbor-Aware Gossip 알고리즘인 Probabilistic Inverse Neighbor-degree Edge 알고리즘을 제안하였다. GossipPINE 은 이웃 노드들의 차수(Degree)를 기반으로 하며 이웃 노드의 차수가 낮을수록 해당 노드에게 메시지를 전송할 확률이 높아지게 된다. 이 접근 방식을 통해 차수가 지나치게 낮은 노드의 경우 장애가 발생했을 것이라 예측할 수 있으며 차수가 높은 노드에게는 중복된 메시지를 보낼 확률이 낮아지게 된다. GossipPINE 은 기존의 Probabilistic Neighbor-Aware Gossip 알고리즘들보다 낮은 Latency 와 높은 Reliability 를 보였다.

Plumtree[8] 에서는 Push-Lazy-Push Multicast Tree 프로토콜을 제안하여 멀티캐스트를 개선하였다. Plumtree 는 랜덤하게 선정된 노드에서 받은 메시지를 바로 전송하는 Eager Push 방식과 처음에는 메시지의 식별자를 전송한 후 이를 받은 노드가 해당 메시지의 페이로드를 요청하는 Lazy Push 방식을 혼합해서 사용하였다. 처음 메시지를 전송한 노드들과는 Eager Push 방식으로 통신하고 중복된 메시지를 전송한 노드들과는 Lazy Push 방식으로 통신함으로써 전체 노드들의 신장 트리를 구성하였다. Plumtree 또한 기존의 Gossip 프로토콜보다 overhead 가 적고 높은 reliability 를 보였다.

Ⅲ. 블록체인에서의 Gossip 기반 라우팅

1. 기존 블록체인에서의 Gossip 기반 라우팅

비트코인에서는 Lazy Push 방식의 Gossip 기반 브로드캐스트를 사용한다. 메시지 발신자는 연결된 노드들에게 Inventory 메시지를 전송 하고 메시지를 수신한 노드들은 GetData 메시지로 응답한다. 그리고 메시지 발신자는 GetData 메시지로 응답한 노드들에 데이터를 전송함으로써 메시지 전달 과정이 마무리 된다. 비트코인은 여기서 Lazy Push 방식을 좀 더 개선하기 위해 Compact Block Relay 를 도입하였다. 노드들 간에 블록 정보를 교환할 때 노드들은 새 블록이 발견되면 블록 헤더와 트랜잭션 해시 정보들만을 전송하며 이를 전달받은 노드들은 트랜잭션 해시 정보들만으로 블록을 구성할 수 없을 경우에만 추가적으로 트랜잭션 정보를 요청한다. Compact Block Relay 방식은 전체 bandwidth 와 블록 전파 시간을 크게 단축할 수 있지만 최악의 경우 메시지 교환 과정이 늘어나 latency 면에서 더 나빠질 수 있다는 문제점이 존재한다.

비트코인과 같이 가장 유명한 블록체인 중 하나인 이더리움에서는 노드들이 새로운 블록 정보를 받을 경우 이웃 노드들 중 랜덤하게 일부 노드들을 선정한다. 그리고 선정된 노드들에게는 블록 헤더만을 검증한 이후 모든 블록 데이터를 전송하고 나머지 노드들에게는 전체 블록 정보를 검증한 뒤 블록 해시 값만을 전송한다. 블록 해시 값을 전송받은 노드는 일정시간을 대기한 후 블록 정보를 아는 주변 노드들에게 블록 헤더를 요청한다. 블록 헤더를 전달 받으면 다시 일정 시간을 대기한 뒤 블록 바디 정보를 요청하여 전달받는다. 이러한 방식은 대기 시간으로 인해 노드들이 전체 블록 정보를 얻기 까지 오랜 시간이 걸린다는 문제점이 존재한다.

2. Gossip 기반 라우팅 성능 개선 방안

P2P 라우팅의 성능은 크게 세 가지 관점에서 바라볼 수 있다. 첫 번째는 latency 이다. 당연하게도 노드와 노드간의 메시지 전달 속도는 메시지를 모든 노드에게 전달하는 데 걸리는 시간에 큰 영향을 미친다. 두 번째는 reliability 이다. 노드의 수가 적은 환경이라면 모든 노드를 서로 연결함으로써 안전하게 모든 노드들에게 동일한 메시지를 전송하는 것이 가능하다. 하지만 퍼블릭 블록체인과 같이 노드의 수가 많은 환경이라면 모든 노드를 연결하는 것은 불가능하고 하나의 노드에 연결되는 노드의 수가 제한된다. 하나의 노드에서 메시지를 보낼 때 해당 노드는 자신과 연결된 모든 노드, 혹은 일부 노드에게 메시지를 보내게 되는데 이때 네트워크 연결이 불안정 할 경우 메시지를 전달 받지 못하는 노드가 발생할 수 있다. 네트워크의 reliability 를 높이기 위해서는 노드와 연결되는 노드의 수를 적절히 선정하는 것이 필요하다. 마지막으로 redundancy 이다. 노드와 연결되는 노드의 수가 많아질 경우 메시지를 전송하는 과정에서 동일한 메시지를 중복해서 수신할 가능성이 높아진다. 이러한 불필요한 메시지는 네트워크의 트래픽을 높여 결과적으로 전체 네트워크의 메시지 전달 속도를 낮추게 된다. 따라서 불필요하게 중복되는 메시지를 줄여 redundancy 를 낮춤으로써 Gossip 프로토콜의 성능을 개선할 수 있다.

Latency, reliability, redundancy 와 같은 특성들은 네트워크 토폴로지에 따라서도 다르게 나타날 수 있다. 따라서 주어진 토폴로지 환경에 적합한 라우팅 방식을 선정하는 것 역시 중요하다. 또한, reliability 를 높이기 위해 노드와 연결되는 노드 수를 늘릴 경우 redundancy 가 낮아지는 문제가 존재한다. 따라서 단순히 노드와 연결되는 노드의 수를 조정하는 것이 아닌, 연결된 노드 중 메시지를 전달할 노드를 적절하게 선정할 필요가 있다. 이러한 방법으로 메시지를 전송하는 노드의 수를 제한하거나 랜덤하게 선정된 노드들에게만 메시지를 전송하는 등의 방안들이 존재한다.

Gossip 프로토콜을 구성하기 위해서는 먼저 네트워크에서 메시지를 전송하는 주체가 되는 메시지 발신자에 대한 정의가 필요하다. 일반적인 퍼블릭 블록체인에서는 모든 노드들이 트랜잭션을 생성하거나 블록을 생성할 수 있기 때문에 모든 노드들이 최초 메시지 발신자가 될 수 있다.

그리고 최초 메시지 발신자로부터 메시지를 수신한 이웃 노드들 역시 이후에 메시지 발신자가 되어 해당 메시지를 주변 노드에게 메시지를 전송하게 된다. 이때, 노드들이 메시지를 전송할 때 메시지에 자신의 서명을 추가함으로써 메시지 수신자로 하여금 동일한 노드로부터 받은 중복된 메시지를 확인할 수 있게 하는 것이 가능하다. 메시지 전송 방식은 기본적으로 모든 정보를 보내는 Eager Push 나 간략한 정보만을 보낸 뒤 응답을 받은 뒤에 모든 정보를 보내는 Lazy Push 방식으로 정할 수 있다.

신장 트리(spanning tree) 기반의 라우팅 역시 하나의 가능성이 될 수 있다. 신장 트리 기반의 라우팅은 P2P 네트워크 상의 모든 노드를 포함하는 최소 신장 트리를 구성하여 메시지를 전파함으로써 메시지 전송 과정에서 중복된 메시지의 전달을 없앨 수 있다. 따라서 신장 트리 기반의 라우팅은 redundancy 가 적고 reliability 가 높다는 장점이 있다. 하지만 신장 트리 구조로 노드를 구성할 경우 노드에 장애가 발생했을 때 메시지를 전달할 수 없게 되기 때문에 신장 트리를 빠르게 재구성할 수 있어야 한다. 그림 1 은 신장 트리 예시를 보여준다.

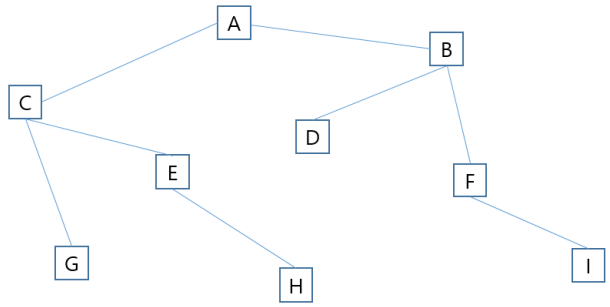

그림 1. 신장 트리 예시

신장 트리 기반의 라우팅을 개발하기 위해서는 우선 트리를 구성할 때 메시지 발신자 마다 개별적인 트리를 구성할 것인지, 혹은 모든 노드들이 공유하는 하나의 트리를 구성할 것인지에 대한 고려가 필요하다. 메시지 발신자 마다 개별적인 트리를 구성할 경우 블록체인에서는 모든 노드들이 메시지 발신자가 될 수 있기 때문에 노드 수만큼의 트리가 필요하다. 따라서 이를 유지하는 데 큰 비용이 발생할 수 있다. 모든 노드들이 공유하는 하나의 트리를 구성할 경우 메시지를 전송하는 경로가 기존 Gossip 기반의 라우팅보다 길어질 수 있다. 따라서 어떠한 방식을 적용할 것인지, 어떻게 해당 문제들을 극복할 것인지에 대해 고려하여야 한다.

신장 트리가 올바르게 작동하기 위해서는 트리를 생성할 때 노드와 연결할 노드들을 선정해야 하며 각 노드들이 최소 하나의 정상적인 다른 노드와 연결되어야 한다. 또한, 노드가 네트워크에 참여하거나 네트워크에서 나갈 때 신장 트리에 바로 반영이 되어야 한다. 노드가 네트워크에 참여하면 트리에 해당 노드가 추가되어야 하며 연결된 노드를 주기적으로 확인하여 해당 노드가 네트워크에서 나갈 경우 트리에서 제거되어야 한다. 트리 구조에서 하나의 노드에 장애가 발생 할 경우 해당 노드가 속해있는 가지에 문제가 발생한다. 따라서 연결된 노드가 일정 시간 동안 응답이 없다면 기존의 다른 노드와 연결하여 메시지를 전달 받아야 한다. 이 경우 어떤 노드와 새롭게 연결할 지를 고려해야하며 기존 연결을 끊고 새로운 노드와 연결되었을 때 신장 트리에 루프가 발생하지 않도록 해야한다.

Ⅳ. 결 론

본 논문에서는 블록체인의 성능을 높이기 위한 방안으로 Gossip 기반의 P2P 라우팅에서의 개선을 제안하였다. 그리고 Gossip 기반의 P2P 라우팅을 개선한 연구들을 소개하였다. GossipPINE 에서는 새로운 이웃 노드 선정 방식을 도입하여 성능을 개선하였으며 PlumTree 에서는 신장 트리를 기반으로 한 Gossip 프로토콜을 제안하였다. 대표적인 블록체인인 비트코인과 이더리움에서의 Gossip 프로토콜을 분석하였으며 이를 통해 블록체인에서 사용될 Gossip 프로토콜을 구성하기 위해 고려해야할 사항들을 분석하였다. Gossip 프로토콜을 개선하기 위해서는 크게 Latency, Reliability, Redundancy 세 가지 측면에서 접근할 수 있으며 이웃 노드 선정 알고리즘의 개선, 혹은 신장 트리와 같은 네트워크 토폴로지 도입을 통해 이들을 개선 가능하다.

향후 연구로는 동일한 환경에서 여러 이웃 노드 선정 알고리즘을 분석 및 비교하여 성능을 측정해보고 최적의 이웃 노드 선정 알고리즘을 찾아내고자 한다. 또한 신장 트리에서 학습을 기반으로 한 메타 휴리스틱 기술을 통해 최적의 신장 트리 라우팅 경로를 찾아내고자 한다.

ACKNOWLEDGMENT

본 연구는 2021 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (2018-0-00749, 인공지능 기반 가상 네트워크 관리기술 개발, IITP-2021-2017-0-01633*, 대학 ICT 연구센터육성지원사업)

참 고 문 헌

[1] Lua, Eng Keong, et al. "A survey and comparison of peer-to-peer overlay network schemes." *IEEE Communications Surveys & Tutorials* 7.2 (2005): 72-93.

[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *URL: https://bitcoin.org/bitcoin.pdf (accessed: 01.04. 2010)* (2008).

[3] Cosmos, “Cosmos Whitepaper.” *URL: https://v1.cosmos.network/resources/whitepaper (accessed: 01.04. 2021).*

[4] Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." *OSDI*. Vol. 99. No. 1999. 1999.

[5] Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." Proceedings of the 26th Symposium on Operating Systems Principles. 2017.

[6] Défago, Xavier, André Schiper, and Péter Urbán. "Total order broadcast and multicast algorithms: Taxonomy and survey." *ACM Computing Surveys (CSUR)* 36.4 (2004): 372-421.

[7] Birman, Kenneth P., et al. "Bimodal multicast." *ACM Transactions on Computer Systems (TOCS)* 17.2 (1999): 41-88.

[8] Leitao, Joao, Jose Pereira, and Luis Rodrigues. "Epidemic broadcast trees." *2007 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007)*. IEEE, 2007.

[9] Hu, Ruijing, and Leander Jehl. "Reliable Probabilistic Gossip over Large-Scale Random Topologies." *arXiv preprint arXiv:1704.05808* (2017).