프랙티컬 비잔틴 장애 허용 기반의 합의 알고리즘의 평가 프레임워크

이은영 · 김남령 · 한채림 · 이일구*

성신여자대학교

Evaluation Framework for Practical Byzantine Fault Tolerant based Consensus Algorithms

Eun-young Lee · Nam-ryeong Kim · Chae-rim Han · Il-gu Lee*

Sungshin Women's University

E-mail : o.lee.eunyoung@gmail.com / namyoung0718@gmail.com / hcl7524@gmail.com / iglee@sungshin.ac.kr

요 약

PBFT(Practical Byzantine Fault Tolerant)는 PoW(Proof of Work) 대비 높은 처리 속도를 보장하며 컴퓨팅 파워의 우위로 인한 기록이 번복되지 않는 절대적 최종성을 보장하는 합의 알고리즘이다. 하지만 메시지 복잡도로 인해 참여하는 노드의 수가 증가할수록 네트워크 부하가 지수적으로 증가한다는 한계가 있다. PBFT는 블록체인 네트워크의 성능을 결정짓는 중요한 요소이지만 평가지표와 평가 기술에 관한 연구는 부족한 실정이다. 본 논문에서는 PBFT를 평가할 수 있는 정량적 지표와 개선된 방안을 쉽게 평가할 수 있도록 합의 알고리즘 변경이 편리한 PBFT 평가 프레임워크를 제안한다.

ABSTRACT

PBFT (Practical Byzantine Fault Tolerant) is a consensus algorithm that guarantees higher processing speed compared to PoW (Proof of Work) and absolute finality that records are not overturned due to the superiority of computing power. However, due to the complexity of the message, there is a limit that the network load increases exponentially as the number of participating nodes increases. PBFT is an important factor in determining the performance of a blockchain network, but studies on evaluation metrics and evaluation technologies are lacking. In this paper, we propose a PBFT evaluation framework that is convenient to change the consensus algorithm to easily evaluate quantitative indicators and improved methods for evaluating PBFT.

키워드

Practical Byzantine Fault Tolerant, Consensus Algorithm, Blockchain, Evaluation Framework

Ⅰ. 제안 배경

비트코인으로부터 출발한 블록체인은 이 시대를 이끌 혁신적 기술로서 많은 관심을 끌고 있으며 산업적으로도 영향력을 확대해가고 있다[1].

블록체인은 네트워크 오류, 자체 고장 등의 문제로 비정상적인 동작이 발생할 수 있다. PBFT는 고장 노드뿐 아니라 악의적 노드가 있어도 안정적으로 전체 시스템을 동작하도록 하는 장애 허용(Fault Tolerant) 합의 알고리즘이다. 통신 도중에 메시지가 전달, 지연, 훼손, 소실되거나 악의적인 노드가 생성하는 의도적인 메시지 오류인 비잔틴 폴트(Byzantine fault)를 해결한다.

PBFT는 비동기 네트워크에서 악의적 노드가 f개일 때, 총 노드 수가 3f+1개 이상이면 해당 네트워크의 합의는 신뢰 가능하다는 것을 수학적으로 증

* corresponding author

명하였다[3]. 더하여 PoW(Proof of Work) 대비 높은 TPS(Transactions Per Second)를 보장하고, 절대적 최종성을 보장하기에 그 활용도가 높다. 하지만 전체 노드의 1/3개 이상을 확보하면 교착상태의 합의를 만들 가능성이 있고[4], 합의 과정에서 발생하는 메시지의 양으로 인해 네트워크를 확장하기 어렵다.

최근 PBFT 합의 알고리즘을 개선하기 위한 연구가 활발히 진행되고 있지만 연구마다 평가지표를 다르게 설정하여 정량적 비교가 어려우며, 같은 조건에서 비교할 수 있는 평가 기술이 없다. 본 연구에서는 PBFT의 확장성과 보안성을 평가할 수 있는 PBFT 평가 프레임워크를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 분석하고, 3장에서는 PBFT 평가 프레임워크를 제안하고, 4장에서 결론을 맺으며 향후 연구 방향에 대해 논의한다.

II. 관련 연구

블록체인은 확장성, 탈중앙화, 보안성의 트릴레마로 모든 속성을 만족하는 합의 알고리즘을 설계할 수 없고, 현존하는 알고리즘들은 특정 속성을 희생하여 장점을 부각한다. PBFT는 3f+1의 내결함성을 보장해 일정 수의 악성 노드가 존재하더라도 합의할 수 있다. 그러나 노드 수가 증가함에 따라 $O(n^2)$에서 $O(n^4)$까지 증가하는 통신 복잡도 문제가 발생한다[5]. 이러한 확장성 문제를 해결하고자 하는 다양한 연구가 존재한다. 2014년을 기점으로 PBFT에 DPoS(Delegated Proof of Stake)를 결합한 Tendemint, PBFT에 PoS(Proof of Stake)를 결합한 이더리움 Casper 등 각 알고리즘의 장점을 결합한 하이브리드 알고리즘들이 등장하였다[6]. 또한 소규모의 네트워크 그룹들을 형성하여 병렬적으로 트랜잭션을 처리하는 샤딩, 외부에서 트랜잭션 처리 후 결과만 체인에 기록하는 라이트닝 네트워크 등은 PBFT의 확장성 개선에 힘을 가했다[7].

합의 위원회의 리더 선발방식을 변경하거나, 합의 계층을 분리하는 연구도 존재한다[5, 7, 8]. 먼저 전자의 경우, Yin Yang이 제안한 LinBFT[5]은 에포크(Epoch)마다 무작위로 리더를 선택하여 시간 복잡도를 $O(n)$으로 줄였다. SG-PBFT(Score Grouping-PBFT)[8]는 점수 매김 메커니즘을 적용하여 리더를 선출한다. 특히 SG-PBFT는 다양한 평가지표(합의 지연, 스루풋, 통신 오버헤드)를 평가하였다. 합의 지연은 트랜잭션 요청을 마스터 노드에 보내는 순간부터 응답까지의 시간을, 스루풋은 단위 시간당 시스템에서 완료된 트랜잭션의 수를 측정했다. 통신 오버헤드의 경우 합의를 진행할 때 생성되는 통신량을 측정하며 평가하였다. 결과적으로 PBFT와 비교하여 합의 지연 27% 감소, 2.67배 높은 스루풋, 통신 오버헤드를 75% 감소하는 결과를 보였다. 그러나 이들은 주로 확장성과 보안성 중 하나의 속성 보완에 치우쳐 있고, 노드 수에 따라 처리량이 감소한다. 또한, 리더가 View-change 전 노출될 수 있고 리더 선발 과정에서 보안성이 약화하거나, 리더에게 권한이 집중되는 문제가 발생할 수 있다.

후자는 노드 수가 적을 때 빠른 속도를 보장하는 PBFT 속성을 활용해 리더를 선출하지 않고 소규모의 네트워크를 구성한다. 클러스터 기반의 PBFT 합의 알고리즘[7]은 전체 노드를 복수의 클러스터로 분할하고 역할을 부여함으로써 클러스터 단위별 합의를 진행한다. $T_{delay} = T_{request} - T_{reply}$으로 합의 지연이 감소하고, 시간 복잡도를 $O(n)$으로 줄이는 결과를 도출했다. 그러나 클러스터 단위로 합의를 진행하면 선형 통신 방식으로 인해 보안성이 약화할 수 있으며, 클러스터 속 노드 수에 따라 합의 지연이 증가한다. 또한, 합의 중 충돌과 노드의 지속적인 수신 대기 문제가 발생한다.

이처럼 PBFT 개선 방안은 활발하게 연구되고 있지만 제안된 알고리즘의 평가지표가 각각 달라 정량적인 비교가 불가능하며 통합 평가가 가능한 플랫폼이 존재하지 않는다. 따라서 블록체인 또는 PBFT의 산업 적용 및 효율성 개선을 위한 평가 프레임워크에 대한 연구개발이 요구된다.

III. 평가 프레임워크

본 논문에서 제안하는 PBFT 평가 프레임워크는 다음과 같다. 그림 1은 PBFT 평가 프레임워크의 구조도이다.

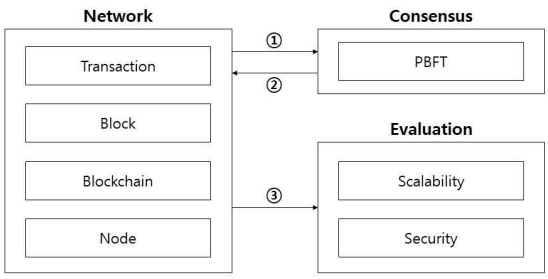

그림 1. PBFT 평가 프레임워크 구조도

네트워크(Network)는 블록체인 네트워크의 구성요소로 이루어져 있다. 네트워크를 구성하는 노드는 트랜잭션(Transaction), 블록(Block)을 생성하고 배포할 수 있으며 합의가 완료된 블록을 블록체인에 연결할 수 있다.

합의(Consensus)는 네트워크 노드가 합의를 호출하여 합의 성공 여부를 확인할 수 있다. PBFT 평가 프레임워크는 합의를 따로 분리하여 개선된 합의 알고리즘 탑재하기 편리하다.

평가(Evaluation)는 평가지표에 맞추어 평가 결과

를 산출한다. 제안하는 PBFT 평가 프레임워크는 두 가지 평가지표를 측정할 수 있다.

첫 번째는 확장성이다. 확장성은 네트워크 규모의 증감에 따라 시스템이 유연하게 대응할 수 있는 정도이다. PBFT는 합의 단계 중 Prepare와 Commit에서 모든 노드가 모든 노드에 브로드캐스팅을 진행하여 메시지 복잡도가 높다. 이로 인해 합의 과정에 참여할 수 있는 노드의 규모가 제한되기 때문에 확장 가능한 노드의 규모를 파악하는 것이 중요하다.

두 번째는 보안성이다. 보안성은 결함 노드로 인해 의도되지 않은 동작을 허용하는 정도이다. 결함 노드에는 네트워크 지연, 시스템 오작동 등으로 인해 합의에 참여하지 않는 노드와 합의를 방해하려는 악의적인 노드가 있다. 다양한 원인으로 결함 노드가 발생할 수 있으므로 사전에 얼마나 결함 노드를 견딜 수 있는지 파악하는 것이 중요하다.

PBFT 평가 프레임워크를 통해 PBFT의 확장성과 보안성을 측정할 수 있으며, 여러 개의 합의 알고리즘을 정량적으로 평가할 수 있다.

Ⅳ. 결 론

PBFT는 절대적 최종성, 처리 속도 등의 장점을 가진 블록체인 합의 알고리즘이지만 대규모 블록체인 네트워크에 적용되기에 한계가 있어 성능 향상 연구가 활발히 진행되고 있다. 하지만 평가 지표와 평가 기술에 관한 연구가 부족하여 연구 결과들을 동일선상에서 비교할 수 없어 연구에 지연이 발생하고, 산업에 도입하기 어렵다.

본 논문에서는 PBFT의 정량적 평가가 가능한 프레임워크를 제안하였다. PBFT 평가 프레임워크를 통해 PBFT와 개선 알고리즘의 정량적 비교가 가능하며 간편하게 평가할 수 있다. 향후 제안한 PBFT 평가 프레임워크를 기반으로 기존 선행 연구의 확장성과 보안성을 정량적으로 비교하고, PBFT 개선 방안에 관한 연구를 진행할 예정이다.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. 2020R1F1A1061107)과 2021년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원(P0008703, 2021년 산업혁신인재성장지원사업)을 받아 수행된 연구임.

References

[1] Don Tapscot, Alex Tapscot, “Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world”, Penguin, 2016.

[3] Miguel Castro, Barbara Liskov, “Practical byzantine fault tolerance”, OSDI, Vol. 99. No. 1999, pp. 173-186, 1999.

[4] H. D. Kim, J. S. Yun, Y. Y. Goh, J. M. Chung, “Adaptive Consensus Bound PBFT Algorithm Design for Eliminating Interface Factors of Blockchain Consensus”, Journal of Internet Computing and Services, Vol. 21, No. 1, pp. 17-31, 2020.

[5] Y. Yang, “Linbft: Linear-communication byzantine fault tolerance for public blockchains”, arXiv, 2018.

[6] A. Harshavardhan, T. Vijayakumar, S. R. Mugunthan, “Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities”, the Second International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Palladam, 2018.

[7] H. S. Heo, D. Y. Seo, “A Study on Scalable PBFT Consensus Algorithm based on Blockchain Cluster”, The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 20, No. 2, pp. 45-53, 2020.

[8] G. Xu, Y. Liu, J. Xing, T. Luo, Y. Gu, S. Liu, X. Zheng, A. V. Vasilakos, “SG-PBFT: a Secure and Highly Efficient Blockchain PBFT Consensus Algorithm for Internet of Vehicles”, arXiv, 2018.