JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 26, No. 2: 271~277, Feb. 2022

프랙티컬 비잔틴 장애 허용 기반 블록체인의 확장성과 내결함성 평가 및 비교분석

이은영[1] · 김남령[2] · 한채림[2] · 이일구[3*]

Evaluation and Comparative Analysis of Scalability and Fault Tolerance for Practical Byzantine Fault Tolerant based Blockchain

Eun-Young Lee[1] · Nam-Ryeong Kim[2] · Chae-Rim Han[2] · Il-Gu Lee[3*]

[1]Graduate Student, Department of Future Convergence Technology Engineering, Sungshin Women's University, Seoul, 02844 Korea
[2]Undergraduate Student, Department of Convergence Security Engineering, Sungshin Women's University, Seoul, 02844 Korea
[3*]Assistant Professor, Department of Future Convergence Technology Engineering, Sungshin Women's University, Seoul, 02844 Korea

요 약

PBFT(Practical Byzantine Fault Tolerant)는 분산 네트워크 환경에서 비의도적·의도적 결함을 해결하여 합의를 달성할 수 있는 합의 알고리즘으로 높은 성능과 절대적 최종성을 보장할 수 있다. 하지만 합의 과정에서 반복적으로 발생하는 메시지 브로드캐스팅으로 인해 네트워크의 규모가 증가할수록 네트워크 부하도 커진다. PBFT 알고리즘의 특성상 소규모·프라이빗 블록체인에는 적합하지만, 대규모·퍼블릭 블록체인에 적용하기엔 한계가 있다. PBFT는 블록체인 네트워크의 성능에 영향을 끼치기 때문에 산업에서는 PBFT가 제품 및 서비스에 적합한지 테스트할 수 있어야 하며, 학계에서는 PBFT 성능 향상 연구를 위한 통일된 평가지표와 평가 기술이 필요하다. 본 논문에서는 PBFT 계열 합의 알고리즘을 평가할 수 있는 정량적 지표와 평가 프레임워크에 대해 연구한다. 또한 제안한 PBFT 평가 프레임워크를 사용하여 PBFT의 처리량, 지연시간, 내결함성을 평가한다.

ABSTRACT

PBFT (Practical Byzantine Fault Tolerant) is a consensus algorithm that can achieve consensus by resolving unintentional and intentional faults in a distributed network environment and can guarantee high performance and absolute finality. However, as the size of the network increases, the network load also increases due to message broadcasting that repeatedly occurs during the consensus process. Due to the characteristics of the PBFT algorithm, it is suitable for small/private blockchain, but there is a limit to its application to large/public blockchain. Because PBFT affects the performance of blockchain networks, the industry should test whether PBFT is suitable for products and services, and academia needs a unified evaluation metric and technology for PBFT performance improvement research. In this paper, quantitative evaluation metrics and evaluation frameworks that can evaluate PBFT family consensus algorithms are studied. In addition, the throughput, latency, and fault tolerance of PBFT are evaluated using the proposed PBFT evaluation framework.

키워드 : 프랙티컬 비잔틴 장애 허용, 합의 알고리즘, 블록체인, 평가 프레임워크

Keywords : Practical byzantine fault tolerant, Consensus algorithm, Blockchain, Evaluation framework

Received 29 November 2021, **Revised** 24 December 2021, **Accepted** 6 January 2022

*** Corresponding Author** Il-Gu Lee(E-mail:iglee@sungshin.ac.kr, Tel:+82-2-920-7145)
Assistant Professor, Department of Future Convergence Technology Engineering, Sungshin Women's University, Seoul, 02844 Korea

Open Access http://doi.org/10.6109/jkiice.2022.26.2.271 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 제안 배경

블록체인은 비트코인으로부터 출발하였으며 4차 산업혁명을 이끄는 혁신적 기술로서 사회적·산업적 영향력을 확대해 나아가고 있다[1].

블록체인은 트랜잭션 정보를 기록한 분산 장부 시스템이다. 중앙집중형 시스템은 신뢰할 수 있는 중앙 기관이 모두가 같은 장부를 공유하고 있음을 보장한다. 하지만 일반적인 분산형 네트워크는 네트워크 장애, 메시지 훼손, 소실 또는 위조 등 비잔틴 폴트(Byzantine Fault)로 인해 상대방의 장부를 신뢰할 수 없다. 블록체인은 이 문제를 해결하기 위해 합의 알고리즘을 사용하여 모두가 신뢰할 수 있는 장부를 합의한다.

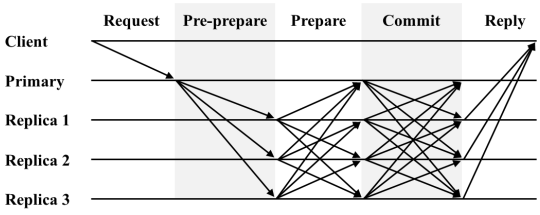


Fig. 1 Practical Byzantine Fault Tolerant Consensus Algorithm

PBFT(Practical Byzantine Fault Tolerant)는 비의도적 의도적 결함을 일으키는 노드가 있어도 네트워크 합의를 이루어 내어 전체 시스템을 안정적으로 동작할 수 있는 장애 허용(Fault Tolerant) 합의 알고리즘이다. PBFT는 그림 1과 같이 동작하며 리퀘스트(Request), 프라-프리페얼(Pre-prepare), 프리페얼(Prepare), 커밋(Commit), 리플라이(Replay) 다섯 단계로 구성된다. 먼저 리퀘스트 단계에서 클라이언트(Client)는 블록을 생성한 뒤에 합의 요청 메시지를 프라이머리(Primary) 노드에 전송한다. 프리-프리페얼 단계에서 프라이머리 노드는 클라이언트의 합의 요청 메시지를 검증한다. 검증 결과가 참이라면 레플리카(Replica) 노드들에게 메시지를 브로드캐스팅한다. 프리페얼과 커밋 단계는 각각의 레플리카 노드들이 전달받은 메시지를 확인하고 브로드캐스팅하는 검증 과정을 두 번 반복 수행한다. 마지막으로 리플라이 단계에서 레플리카 노드들은 일정 수 이상의 메시지를 받으면 클라이언트의 요청을 수용한다. 이후, 클라이언트에게 합의 완료 메시지를 전송하게 되고, 클라이언트는 일정 수 이상의 메시지를 받은 클라이언트는 요청이 수용됐음을 알게 된다. 이와 같은 합의를 통해 클라이언트가 요청한 연산을 수행하고 최종적으로 모든 노드가 동일한 상태를 가진다[2].

PBFT는 비동기 네트워크에서 악의적 노드가 f대일 때, 총 노드 수가 3f+1 이상이면 해당 네트워크의 합의를 신뢰할 수 있음을 증명하였다[3]. 그뿐만 아니라 PBFT는 PoW(Proof of Work)와 비교하였을 때, 높은 TPS(Transactions Per Second)와 절대적 최종성을 보장할 수 있어 그 활용도가 높다. 하지만 전체 노드의 1/3 이상을 확보하면 합의가 교착될 가능성이 크고[4], 합의 과정에서 많은 양의 메시지가 발생하기 때문에 네트워크를 확장하기 어려운 문제가 있다.

확장성 문제를 해결하여 PBFT 합의 알고리즘의 성능을 개선하기 위한 연구는 꾸준히 진행되어왔다. 하지만 선행연구마다 지정한 평가지표가 달라 정량적인 비교가 힘들고, 동일 선상에서 비교할 수 있는 평가 기술에 관한 연구가 부족하다. 문제를 해결하기 위해 본 연구에서는 PBFT 계열 합의 알고리즘을 통합 평가할 수 있는 프레임워크를 연구하여 블록체인 기술의 발전과 산업의 적용을 촉진할 수 있다. 또한 PBFT 평가 프레임워크를 사용하여 PBFT의 처리량, 지연시간 그리고 내결함성을 평가한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 비교 분석하고, 3장에서는 PBFT 평가 프레임워크를 설명한다. 4장에서 제안한 PBFT 평가 프레임워크를 사용해 PBFT를 평가하고, 5장에서 결론을 맺으며 향후 연구 방향에 대해 논의한다.

Ⅱ. 관련 연구

블록체인의 트릴레마는 확장성, 탈중앙화, 보안성 세 가지 속성을 모두 만족하는 합의 알고리즘을 설계하기 어렵다는 문제이다. 현존하는 알고리즘들은 세 가지 속성 중 특정 속성을 희생하여 성능을 개선한다. PBFT는 총 노드의 수가 3f+1대 이상이면 f대의 결함 노드를 견딜 수 있는 수준의 내결함성을 보장하여 결함 노드가 존재하더라도 합의할 수 있다. 그러나 노드 수가 증가함에 따라 통신 복잡도가 $O(n^2)$에서 $O(n^4)$까지 증가하는 문제[5]가 발생하기 때문에 이러한 확장성 문제를 해결하려는 다양한 연구가 제안되었다. 2014년을 기점

으로 여러 합의 알고리즘의 장점을 결합한 하이브리드 합의 알고리즘들이 등장하였다[6]. 텐더민트(Tendermint) 합의 알고리즘은 PBFT와 DPoS(Delegated Proof of Stake)의 장점을 결합하였고, 이더리움 캐스퍼(Casper) 합의 알고리즘은 PBFT와 PoS(Proof of Stake)의 장점을 결합하였다. 여러 합의 알고리즘의 장점을 결합한 선행연구 외에도 PBFT의 성능을 향상시키기 위한 다양한 선행연구가 존재한다.

2.1. 합의 위원회 리더 선발 방식

합의 위원회 리더 선발 방식에 관한 대표적인 선행연구는 LinBFT과 SG-PBFT이다[5,7]. 먼저 LinBFT는 시간 복잡도를 $O(n)$으로 줄이기 위해 에포크(Epoch)가 변경될 때마다 무작위로 리더를 선출하였다[5]. SG-PBFT (Score Grouping-PBFT)는 점수 매김 메커니즘을 통해 리더를 선발하였으며 다양한 평가지표(합의 지연, 처리량, 통신 오버헤드)를 사용해 제안한 합의 알고리즘을 평가하였다[7]. 사용한 평가지표 중 합의 지연은 마스터 노드에 트랜잭션 요청을 보내는 시점부터 응답하는 시점까지의 시간, 처리량은 단위 시간당 완료된 트랜잭션의 개수, 통신 오버헤드는 합의 진행 시 발생한 통신량을 기준으로 하였다. 최종적으로 PBFT 대비 합의 지연이 27% 감소하였고, 처리량은 2.67배 증가하였으며, 통신 오버헤드는 75% 감소하였다.

2.2. 합의 계층 분리

합의 계층 분리는 합의 위원회의 리더를 선출하는 중앙 집중적인 방식을 사용하지 않는 방법이다. 합의 계층 분리하는 방법에 대한 대표적인 선행 연구는 클러스터 방식과 다층 레이어 방식이다[8, 9]. PBFT는 노드의 수가 적을수록 속도가 빠르므로 소규모 네트워크를 구성하여 빠른 속도를 보장한다.

먼저 클러스터 기반의 선행 연구[8]는 전체 네트워크를 복수의 클러스터로 분할하고 역할을 부여하여 클러스터 단위별로 합의한다. 결과적으로 합의 지연은 $T_{delay} = T_{request} - T_{reply}$으로 감소하고 시간 복잡도는 $O(n)$으로 줄어들게 된다.

Wenyu Li는 다층 레이어로 분리하여 노드 수가 증가하더라도 균일한 통신 복잡도을 유지하였다[9]. X를 레이어 수, m을 레플리카라고 할 때, 수식(1)은 네트워크 깊이에 따른 통신 복잡도를 나타낸다.

$$C_X = \sum_{i=1}^{X} m_{i-2} m_{i-1} (m_i + 1)^2 \quad (1)$$

2.3. 선행연구 비교 분석

표 1은 합의 위원회 리더 선발 방식과 합의 계층 분리 선행 연구의 한계점을 분석한 내용이다.

Table. 1 Limitations of the prior research

Prior research	Limitation
Leader selection method	- Consensus algorism trilemma - Reduced throughput due to increased number of nodes - Leader exposure before View-Change - Centralization - Reduced security
Consensus layer separation	- Reduced security due to linear communication method - Increased consensus delay due to increased number of cluster nodes - Conflicts and listening issues during consensus

먼저 합의 위원회의 리더 선발 방식을 변경하는 방법을 사용한 선행 연구의 한계점이다. 합의 위원회 리더 선발 방식은 블록체인 트릴레마의 확장성과 보안성 중 하나의 속성을 향상하는 데 그친다. 또한, 리더가 View-change 전에 노출되어 공격의 표적이 될 수 있으므로 리더 선발 과정에서 보안성이 약화하는 문제가 발생할 수 있다. 더불어, 리더에게 권한이 집중되는 중앙 집중화 문제가 발생할 수 있다.

다음은 합의 계층 분리 선행 연구의 한계점이다. 합의 계측 분리 방식은 클러스터 단위로 합의를 진행하여 선형 통신 방식으로 인한 보안성 약화가 발생할 수 있고, 개별 클러스터의 노드 규모에 따라 합의 지연이 증가할 수 있다. 또한, 합의 중 충돌이 발생할 수 있으며 노드의 지속적인 수신 대기 문제가 생길 수 있다.

각 선행연구에서 사용한 평가지표는 표 2에서 확인할 수 있다.

Table. 2 Limitations of the prior research

Prior research	Evaluation metrics
LinBFT[5]	- Time complexity
SG-PBFT[7]	- Consensus latency - Throughput - Overhead
CBS-PBFT[9]	- Time complexity - Consensus latency

리더 선발방식을 변경한 LinBFT는 시간 복잡도를 평가지표로 사용하였다. 마찬가지로 리더 선발방식을 변경한 SG-PBFT에서는 합의 지연, 처리량 그리고 통신 오버헤드를 사용하였다. 합의 계층을 분리한 CBS-PBFT는 시간 복잡도와 합의 지연을 평가지표로 사용하였다.

블록체인 합의 알고리즘의 성능을 측정할 수 있는 시뮬레이터에 관한 선행연구도 존재한다[10 ,11]. 두 선행연구는 블록 생성 간격, 블록 사이즈, 노드의 수 등 다양한 파라미터를 조정하여 성능을 측정할 수 있는 블록체인 시뮬레이터에 대해 연구하였다. 블록체인 합의 알고리즘은 PoW를 기본적으로 제공하며 PoS는 별도로 모듈을 제작하여 확장할 수 있으므로 평가에 소모되는 시간과 비용을 절약할 수 있다. 하지만 하나의 시뮬레이터에서 합의 알고리즘을 변경하며 테스트할 수 없기 때문에 테스트하고자 하는 합의 알고리즘의 개수만큼 시뮬레이터를 제작해야 하는 한계가 있다. 또한, 논문에서 PBFT는 지원하지 않거나, 적합하지 않다고 설명되어있어 PBFT 계열의 합의 알고리즘을 평가할 수 없는 문제가 있다.

이처럼 PBFT 개선 방안은 활발하게 연구되고 있다. 하지만 선행연구마다 확장성, 보안성 등 연구에서 개선하려는 목표가 다르며, 제안한 알고리즘을 평가하는 지표가 다르다. 또한, 평가할 수 있는 시뮬레이터에 관한 연구가 부족하여 연구자와 실무자는 직접 합의 알고리즘을 구현하지 않는 이상 정량적인 비교가 불가능하다. 직접 구현하더라도 많은 시간과 비용이 소모되고, 근본적으로는 다양한 합의 알고리즘을 통합 평가할 수 있는 플랫폼이 존재하지 않는다. 따라서 블록체인 또는 PBFT의 산업 적용과 효율성 개선을 위한 평가 프레임워크의 연구·개발이 요구된다.

Ⅲ. 평가 프레임워크

3.1. 구조

본 논문에서는 PBFT 평가 프레임워크에 대해 제안한다. 그림 2는 PBFT 평가 프레임워크의 구조도이다.

PBFT 평가 프레임워크는 네트워크(Network), 합의(Consensus), 평가(Evaluation)로 구성된다.

네트워크(Network)는 블록체인 네트워크의 구성요소이다. 노드(Node)는 네트워크의 행위 주체이며 네트워크에서 트랜잭션(Transaction), 블록(Block)을 생성하고 배포하는 역할을 한다. 또한, 블록 검증 결과, 합의에 실패했다면 생성한 블록을 삭제하고, 합의에 성공했다면 생성한 블록을 블록체인에 연결한다.

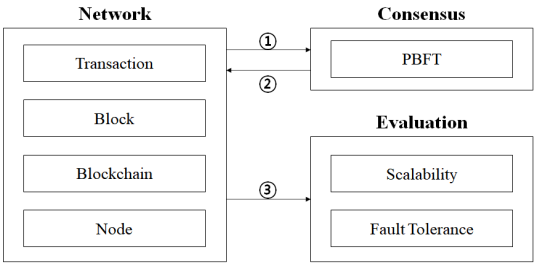


Fig. 2 Evaluation Framework for Practical Byzantine Fault Tolerant

합의(Consensus)는 블록체인의 합의 알고리즘의 역할을 담당한다. 네트워크의 노드가 합의를 호출하고, 합의 결과를 받는다. 호출 결과에 따라 노드는 블록체인의 블록 추가 여부를 결정한다. PBFT 평가 프레임워크는 합의를 따로 분리하여 평가의 편의성을 높였다. 만약 개선된 합의 알고리즘을 평가하고 싶다면 합의에 개선된 합의 알고리즘을 탑재하면 되기 때문에 다양한 알고리즘을 평가하기 쉽다.

평가(Evaluation)는 최종적으로 합의 알고리즘의 평가 결과를 산출한다. 제안하는 프레임워크에서는 확장성과 내결함성을 측정한다.

3.2. 평가지표

PBFT 평가 프레임워크는 확장성과 내결함성을 측정할 수 있다.

첫 번째, 확장성은 네트워크 규모에 따라 얼마나 시스템이 유연하게 대응할 수 있는가에 대해 측정한다. PBFT는 합의 단계 중 프리페얼와 커밋에서 모든 노드가 모든 노드에게 메시지 브로드캐스팅을 진행하여 복잡도가 높아진다. 이로 인해 네트워크에 부하가 발생하거나 네트워크의 규모를 제한적으로 운영해야 하므로 확장 가능한 네트워크의 규모를 파악하는 것은 중요하다. 본 연구에서는 확장성을 평가하기 위해 처리량과 지연시간을 측정한다.

두 번째는 내결함성이다. 내결함성은 결함 노드로 인해 의도되지 않은 동작을 허용하는 정도이다. 결함 노드는 네트워크 지연, 시스템 오작동 등의 비의도적 결함으

로 인해 합의에 참여하지 않는 노드와 의도적인 결함을 발생시켜 합의를 방해하려는 악의적인 노드로 구분할 수 있따. 결함은 다양한 원인으로 발생할 수 있으므로 사전에 합의 알고리즘이 결함 노드를 견딜 수 있는 수준을 파악하는 것은 중요하다.

PBFT 평가 프레임워크를 통해 처리량과 지연시간을 측정하여 확장성을 평가하고 견딜 수 있는 노드의 수를 측정하여 내결함성을 평가할 수 있다. 또한, 다양한 합의 알고리즘을 간편하게 평가할 수 있다.

Ⅳ. 평가 결과

4장에서는 제안한 PBFT 평가 프레임워크를 사용하여 PBFT를 평가하였다. 처리량과 지연시간은 노드의 규모, 내결함성은 결함 노드의 비율에 따른 시뮬레이션을 수행하였다. PBFT 평가 프레임워크는 Python을 사용해 구현하였다. PBFT 평가 프레임워크의 구성요소인 네트워크, 합의, 평가는 클래스로 구현하였다. 각 구성요소의 세부적인 기능들은 클래스의 메서드로 구현하였고, 클래스에서 요구하는 데이터는 클래스 변수를 생성하여 저장하였다. 최종 평가 결과는 엑셀 파일로 내려받을 수 있도록 제작하였다. 실험은 Windows 10 운영체제, RAM 32GB, CPU Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz PC 환경에서 수행하였다.

4.1. 처리량과 지연시간 분석

PBFT의 확장성을 평가하기 위하여 처리량과 지연시간을 측정하였다.

처리량은 합의 시간 내에 처리된 유효한 정보량을 의미한다. 지연시간은 합의가 지연된 시간을 의미한다. PBFT는 네트워크의 규모가 확장됨에 따라 합의 지연시간이 증가한다. PBFT는 메시지의 복잡도가 높아 합의에 참여할 수 있는 노드 규모가 제한적이기 때문에 확장 가능한 노드의 규모를 파악해야 한다.

그림 3은 노드 수 증가에 따른 처리량과 지연시간을 평가한 그래프이다.

이때, 노드 수는 100부터 1000대까지 100대 단위로 증가시키며 시뮬레이션을 진행하였으며, 노드는 정상 노드로만 구성하였다. 블록의 크기는 평균 크기와 최대 크기로 설정하여 평가를 진행하였다. 현재 블록체인의

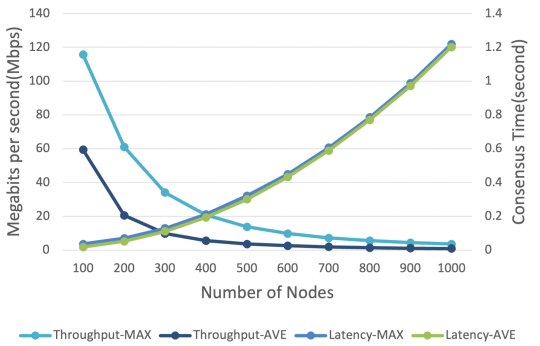


Fig. 3 Throughput and Latency of Practical Byzantine Fault Tolerant

블록당 평균 크기는 1MB로 측정되며[12], 선행 연구인 [13]를 참고하여 블록의 최대 크기는 4MB로 설정해 평가를 진행하였다.

처리량은 처리된 블록 크기를 한 라운드에 소요되는 시간으로 나눈 값으로 정의하였다. 지연시간은 블록체인을 초기화하여 블록을 생성하는 순간부터 블록이 체인에 추가되거나 삭제되는 순간까지 한 라운드에 걸리는 시간(초)으로 정의하였으며, 노드별 측정 결과치를 합산해 전체 노드 수로 나눈 값을 지연시간 측정 결과로써 나타내었다.

처리량은 왼쪽 y축에서 확인할 수 있다. Throughput-MAX는 블록 최대 크기인 4MB, Throughput-AVE는 블록 평균 크기인 1MB로 설정한 시뮬레이션 결과를 그래프로 나타내었다. x축을 노드의 수, y축을 초 단위로 처리되는 비트의 양으로 기록하였을 때, 노드 수가 증가할수록 처리량은 점차 감소하는 반비례 그래프가 도출되었다. 비율 또한 점차 넓은 격차로 늘어나는 결과가 도출되었다. 특히, 데이터의 크기가 작을수록 노드 수에 따른 처리량의 차이가 큰 것을 확인할 수 있다. 노드의 규모가 100대인 경우에 블록 크기가 1MB, 4MB일 때 처리량은 각각 59,336,246bps, 115,697,880bps로 약 2배의 차이가 발생하지만, 노드의 규모가 1000대인 경우에는 3,560,817bps, 910,228bps로 약 4배 차이가 나는 것을 확인할 수 있다.

블록별 메시지 생성부터 도착할 때까지의 평균 지연시간은 오른쪽 y축에서 확인할 수 있다. Latency-MAX는 블록 최대 크기인 4MB, Latency-AVE는 블록 평균 크기인 1MB로 설정한 시뮬레이션 결과를 그래프로 나타내었다. x축은 노드의 수, y축은 합의 완료 시간을 초

단위로 기록하였을 때, 노드 수에 따라 합의 지연이 점진적으로 증가하며 증가 비율 또한 점차 넓은 격차로 늘어나는 결과가 도출되었다. 특히, 노드 규모가 100이고, 블록 크기가 1MB, 4MB일 때 지연시간은 각각 0.036초, 0.017초로 2배가량의 차이가 발생한다. 노드 규모가 증가할수록 이 차이는 줄어들지만, 0.014~0.02초의 일정한 범위 안에서 발생한다. 즉, 같은 비율로 노드 수가 증가할 때 전체 노드 수에 따라 합의 지연 정도는 더 높아지지만, 블록 크기에 따른 합의 지연의 차이는 같은 범위의 차를 보인다.

4.2. 내결함성 분석

내결함성은 PBFT 합의 과정에서 결함 노드를 감내할 수 있는 수준을 의미한다. PBFT는 3f+1의 내결함성을 보장하는데, 이는 최대 보장을 나타낸다. 즉, PBFT 합의 수행 시 결함 노드 비율이 전체 노드의 1/3 이하로 존재할 때, 합의 성공을 보장할 수 있는 것이다. 이에 대해 블록은 평균 블록 크기인 1MB, 전체 노드 규모를 300으로 설정한 뒤, 결함 노드 비율에 따른 합의 성공률을 그림 4로 나타내었다.

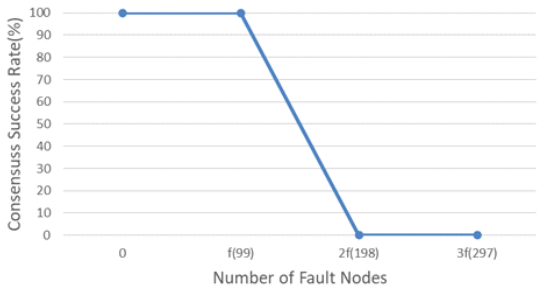


Fig. 4 Fault Tolerance of Practical Byzantine Fault Tolerant

x축을 결함 노드의 비율, y축을 합의 성공률(%)로 나타내어 그래프를 그린 결과, 전체 노드 300대 중 f(약 1/3)에 해당하는 99대의 노드까지는 100%의 합의 성공을 보장한다. 그러나 결함 노드의 수가 f 이상으로 증가할수록 합의에 성공할 확률은 급격하게 줄어들어 결국 결함 노드 비율이 2f(약 2/3)를 차지하는 순간부터 합의는 모두 실패하는 결과를 보인다.

평가 결과, 처리량과 지연시간은 노드의 수가 증가함에 따라 지수적으로 성능이 감소하는 것을 확인하였다. 또한, 지연시간은 블록의 크기 차이가 성능에 큰 영향을 끼치지 않지만, 처리량은 노드의 규모가 증가할수록 블록 크기에 따른 성능 차이가 큰 것으로 확인되었다. 내결함성은 총 노드의 수가 3f+1대일 때, f대의 악성 노드를 견딜 수 있음[3]을 시뮬레이션으로 확인하였다.

Ⅴ. 결 론

PBFT는 성능과 절대적 최종성 측면에서 장점이 있는 블록체인 합의 알고리즘이다. 하지만 알고리즘의 특성상 대규모·퍼블릭 블록체인에 사용하기에는 한계가 있다. 블록체인 산업이 발전하기 위해서는 산업에서 관련 기술을 테스트할 수 있어야 하고, 학계에서 기술의 성능 향상 연구를 위한 통일된 평가지표와 평가 기술이 필요하다. 하지만 이와 관련 연구가 부족한 실정이다.

본 논문에서는 PBFT 평가 프레임워크를 연구하였으며 프레임워크를 사용해 PBFT와 개선 알고리즘을 간편하게 정량적인 평가를 진행할 수 있다. 또한, 제안한 PBFT 평가 프레임워크를 사용하여 PBFT 합의 알고리즘의 처리량, 지연시간, 내결함성에 대해 평가하였다. 처리량과 지연시간은 네트워크 규모가 증가할수록 지수적으로 성능이 감소하는 것을 확인하였으며, 내결함성은 PBFT의 수식적 증명과 같은 결과를 도출하는 것을 확인하였다. 향후 본 논문에서 연구한 PBFT 평가 프레임워크를 기반으로 PBFT 성능 개선 연구들의 확장성과 내결함성을 정량적으로 비교할 예정이다. 또한, PBFT의 성능과 보안성을 개선할 방법에 관한 연구를 진행할 예정이다.

ACKNOWLEDGEMENT

This work was partly supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F 1A1061107) and Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist).

REFERENCES

[1] D. Tapscot and A. Tapscot, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*, Penguin, 2016.

[2] J. C. Yim, H. K. Yoo, J. K. Kwak, and S. M. Kim, "Blockchain and Consensus Algorithm," *Electronics and Telecommunications Trends*, vol. 33, no. 1, pp. 45-56, Feb. 2018.

[3] M. Castro and B. Liskov, "Practical byzantine fault tolerance," *OSDI*, vol. 99, no. 1999, pp. 173-186, Feb. 1999.

[4] H. Kim, J. Yun, Y. Goh, and 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, Feb. 2020.

[5] Y. Yang, "Linbft: Linear-communication byzantine fault tolerance for public blockchains," *arXiv preprint arXiv: 1807.01829*, Jul. 2018.

[6] A. Harshavardhan, T. Vijayakumar, and 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, pp. 1279-1286, Aug. 2018.

[7] G. Xu, Y. Liu, J. Xing, T. Luo, Y. Gu, S. Liu, X. Zheng, and A. V. Vasilakos, "SG-PBFT: a Secure and Highly Efficient Blockchain PBFT Consensus Algorithm for Internet of Vehicles," *arXiv preprint arXiv:2101.01306*, Jan. 2018.

[8] H. S. Heo and 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, Apr. 2020.

[9] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable mult-layer PBFT consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146-1160, Dec. 2020.

[10] M. Alharby and A. V. Moorsel, "Blocksim: a simulation framework for blockchain systems," *ACM SIGMETRICS Performance Evaluation Review*, vol. 46, no. 3, pp. 135-138, 2019.

[11] M. Alharby and A. V. Moorsel, "Blocksim: An extensible simulation tool for blockchain systems," Frontiers in Blockchain, vol. 3, pp. 28, Jun. 2020.

[12] Github. bip-0141.mediawiki [Internet]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki#cite_note-3.

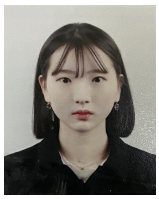
[13] Blockchain.com. Average Block Size(MB) [Internet]. Available: https://www.blockchain.com/charts/avg-block-size.

이은영(Eun-Young Lee)

성신여자대학교 미래융합기술공학과 석사
성신여자대학교 융합보안공학과
※관심분야 : 블록체인, 융합보안, 정보보안

김남령(Nam-Ryeong Kim)

성신여자대학교 융합보안공학과
※관심분야 : 블록체인, 개인정보, 인공지능, 정보보안



한채림(Chae-Rim Han)

성신여자대학교 융합보안공학과
※관심분야 : 블록체인, 정보보안

이일구(Il-Gu Lee)

성신여자대학교 미래융합기술공학과/
융합보안공학과 조교수
한국전자통신연구원 5G기가통신시스템연구본부
선임연구원
KAIST 전산학부 박사
※관심분야 : 융합보안, 미래융합기술, 정보통신