J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

블록체인 합의 방해요인 제거를 위한 Adaptive Consensus Bound PBFT 알고리즘 설계☆

Adaptive Consensus Bound PBFT Algorithm Design for Eliminating Interface Factors of Blockchain Consensus

김 형 대[1] 윤 주 식[1] 고 윤 영[1] 정 종 문[1*]
Hyoungdae Kim Jusik Yun Yunyeong Goh Jong-Moon Chung

요 약

블록체인 기술이 급속도로 발전하고 있음에 따라 금융·물류 등 다양한 분야에서 블록체인 기술을 실용화하려는 시도들이 진행되고 있으며, 데이터 무결성이 매우 중요한 공공분야 또한 마찬가지이다. 국방분야 또한 네트워크 중심 작전환경(NCOE) 하에 작전운영을 위해서는 지휘통신 네트워크의 보안성 강화 및 완전무결성 확보가 매우 중요하다. 이를 위해 블록체인 네트워크를 적용한 지휘통신네트워크 구축이 필요하나, 현재까지의 블록체인 기술은 51% 공격 등의 보안 이슈들을 해결하지 못하고 있어, 국방에 접목하기 어려운 것이 현실이다. 특히, 현재 블록체인에서 많이 사용되고 있는 Practical Byzantine fault tolerance (PBFT)알고리즘은, 악의적인 행동을 하는 노드들에게 penalty 요소가 없고, 합의를 방해하는 노드가 전체 노드의 33%이상만 차지해도 합의 실패를 만드는 문제점이 있다. 본 논문에서는 블록체인의 주요 합의 알고리즘인 PBFT의 보안성 향상을 위해, Trust 모델을 접목하여 비정상 행위에 대한 penalty 메커니즘이 적용된 Adaptive Consensus Bound PBFT (ACB-PBFT) 합의 알고리즘을 제안한다.

☞ 주제어 : 블록체인, 합의 알고리즘, 실용적 비잔티움 장애 허용, 적응 합의 경계 실용적 비잔티움 장애 허용

ABSTRACT

With the rapid development of block chain technology, attempts have been made to put the block chain technology into practical use in various fields such as finance and logistics, and also in the public sector where data integrity is very important. Defense Operations In addition, strengthening security and ensuring complete integrity of the command communication network is crucial for operational operation under the network-centered operational environment (NCOE). For this purpose, it is necessary to construct a command communication network applying the block chain network. However, the block chain technology up to now can not solve the security issues such as the 51% attack. In particular, the Practical Byzantine fault tolerance (PBFT) algorithm which is now widely used in blockchain, does not have a penalty factor for nodes that behave maliciously, and there is a problem of failure to make a consensus even if malicious nodes are more than 33% of all nodes. In this paper, we propose a Adaptive Consensus Bound PBFT (ACB-PBFT) algorithm that incorporates a penalty mechanism for anomalous behavior by combining the Trust model to improve the security of the PBFT, which is the main agreement algorithm of the blockchain.

☞ keyword : Blockchain, Consensus Algorithm, PBFT (Practical Byzantine Fault Tolerance), Adaptive Consensus Bound PBFT (ACB-PBFT)

1. 서 론

최초 분산 디지털 통화 개념은 1982년에 David Chaum에 의해 고안되었으며, 1995년 실현되어 US bank에 의해 1998년까지 micropayment 시스템으로 사용되었다[1]. 그러나 중앙집권적 중개인에 의존한 거래방식을 가짐으로써 지금의 블록체인 암호화폐와 큰 차이를 가진다. 1998년, Wei Dai는 분산합의와 퍼즐 해결 방식을 통해 디지털 화폐를 발행하는 'B-money'를 제안하였으나, 실제로 구현 방법을 제시하지 못하였다[2]. 2008년 10월 Satoshi Nakamoto라는 익명의 인물(또는 단체)은 Wei Dai의 아이디어를 기반으로 탈중앙화 P2P (Peer-to-Peer) 디지털화폐인 비트코인(Bitcoin)을 제안하였고[3], 2009년 3월 실제 구현하여 현재의 비트코인 시스템을 만들었다. 비트코인은 단순한 P2P 디지털화폐 구현뿐만 아니라, 기존에 제안

[1] Electrical & Electronic Engineering, Yonsei University, Seoul, 03722, Korea.
* Corresponding author (jmc@yonsei.ac.kr)
[Received 23 April 2019, Reviewed 10 May 2019(R2 23 August 2019, R3 17 October 2019), Accepted 7 November 2019]
☆ 본 논문은 행정안전부의 시뮬레이션 기반 조직단위 비상대비 훈련기술 개발(2018-MOIS33-001-01010000-2019)의 지원으로 수행되었습니다.

된 모델들의 문제점들을 블록체인 및 암호기술 등을 통해 해결했다. 기존 P2P 기반 디지털화폐는 악의적 참가자에 의한 변조, 정보 전달 지연에 따른 이중 지불 가능성 등 여러 문제점이 있었는데, 비트코인은 이를 금융기관 부재에 따른 변조 가능성을 블록체인이라는 분산원장으로 신뢰도를 향상시키고, 작업증명(PoW : Proof of Work)이라는 합의 알고리즘을 통해 블록을 임의대로 만들어 조작하는 것을 방지하였다. 비트코인은 최초로 블록체인 기술이 적용된 서비스로서, 이후 나오고 있는 다수의 블록체인 기술 연구 및 프로젝트의 기초 모델이 됐다. 여러 프로젝트들이 비트코인의 기술적 한계를 보완 및 기능 확장을 위해 다양한 모델을 제안하였다[4].

블록체인 기술은 '4차 산업혁명'의 대두될 시점에는 핵심기술로 분류되지 못했지만, 세계적 정보기술 연구 및 자문 회사인 가트너社가 발표한 '2018년 10대 전략 기술 트렌드'에 선정되며 그 혁신성을 인정받았다. 보고서는 블록체인이 디지털 통화 인프라 뿐 아니라 디지털 혁신 플랫폼으로서 혁신적 디지털 비즈니스의 토대를 제공할 것이며, 금융·유통·제조·신원확인·소유권 등뿐만 아니라 정부·의료 등 공공 분야까지도 혁신을 가져올 것으로 전망했다[5]. 또한 세계경제포럼은 'Trade Tech – A New Age for Trade and Supply Chain Finance'라는 보고서를 통해, 블록체인이 향후 10년 간 세계 무역에서 1조 달러 이상의 가치를 창출할 것이라 전망했다[6]. 국내외 여러 분야에서 블록체인을 전 산업영역에서 활용하기 위해 ICT 기술과 접목을 통한 기술개발에 박차를 가하고 있으며, 세계 각국 정부 또한 블록체인 경쟁력 강화를 위한 제도 개선 및 기술 육성을 추진하고 있다. 우리 정부도 블록체인이 제4차 산업혁명의 국가 핵심 인프라 기술로서, 블록체인 진화 패러다임과 환경변화에 신속히 대응할 수 있는 생태계 조성을 위해 '블록체인 기술 발전전략'을 수립 및 추진 중에 있다[7]. 또한, 작전운영을 위해 지휘통신 네트워크의 보안성 강화 및 완전무결성 확보가 매우 중요한 국방 분야도 블록체인 네트워크를 적용한 지휘 통신 네트워크 구축을 필요로 한다.

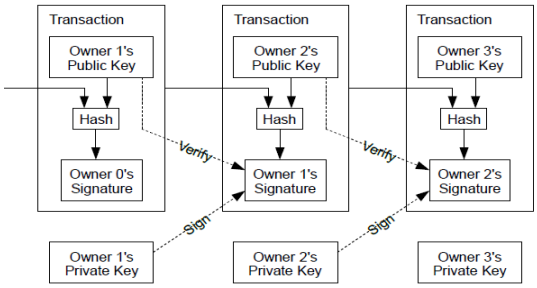
그러나 블록체인의 높은 유용성에도 불구하고, 속도, 보안 등 여러 이슈를 해결하지 못해 실제 서비스에 적용되는 사례는 저조하다. PoW 및 PoS 등 과반이상 합의를 통한 블록체인은 51% hash rate 장악 시 데이터 변조가 가능함에 따라, 해당 블록체인은 대중의 신뢰를 잃게 된다. 또한 비정상 행위를 한 노드에 대한 penalty 모델도 부재하다. PBFT (Practical Byzantine Fault Tolerance) 합의 알고리즘은 2/3 초과의 노드를 확보해야만 데이터 변조가 가능하여 PoS 및 지분증명(PoS : Proof of Stake) 보다 51% 공격에 강하지만, 반면 1/3 이상 노드만 확보해도 합의를 교착상태로 만든다.

따라서 본 논문에서는 PBFT 합의 알고리즘을 기반으로 신뢰 평가 모델을 접목하기 위해, PBFT 합의 알고리즘을 분석하여 문제점 및 제약사항 개선 방안을 검토한다. 이를 통해 비정상 행위에 대한 penalty 모델을 적용하여 합의 성공률 향상 및 합의 교착상태에서 정상 합의로 회귀할 수 있는 Adaptive Consensus Bound PBFT (ACB-PBFT) 합의 알고리즘을 제안한다.

2. 관련 연구

2.1 Blockchain Architecture

블록체인의 데이터 구조는 데이터의 가장 기본 단위인 트랜잭션(Tx : Transaction)을 일정 규모로 묶은 블록과 블록들이 연결되어 구성된 체인 형태로 구성된다. 블록체인의 트랜잭션은 암호화폐를 교환하는 상호 간 거래 정보이며, 네트워크에서 전송되는 메시지다. 그림1은 비트코인 시스템의 트랜잭션 흐름이다.



(Figure 1) Transaction Flow of Bitcoin

블록체인의 트랜잭션은 전자서명을 통해 메시지에 대한 무결성 제공 및 부인 방지 기능을 제공하며, 메시지 전송의 송신자와 수신자 주소의 익명화를 통해 개인정보를 보호한다. 트랜잭션이 요청되면 메시지는 모든 노드에게 전파(broadcast)된다. 트랜잭션은 전자서명의 체인(chain of digital signature) 형태로 구현되며, 각 트랜잭션에는 전자서명과 공개키 1쌍이 부여된다.

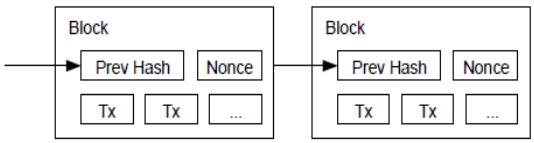
블록은 특정시간(Block Time) 동안 모아진 다수의 트랜잭션의 집합이며, 표1의 비트코인의 블록 구조와 같이 Header와 Body로 구성된다. Header에는 version, previous

block hash, merkle root hash, timestamp, bits, nonce의 6가지 정보가 담겨있고, 블록의 정보를 담고 Body는 거래의 내용인 트랜잭션들의 집합이다. Body 내 트랜잭션들을 binary tree 방식으로 해시해서 merkle root hash라는 최종 해시 다이제스트를 만들어, 트랜잭션의 무결성 검증 기능을 한다[8]. 이렇게 생성된 블록은 Header를 통해 인접 블록들과 연결되며 신뢰성 검증이 이루어진다.

(Table 1) Structure of Block

Category	Destination (size)
Magic Number (4 bytes)	
Block Size (4 bytes)	
Block Header	Version (4 bytes)
	Hash of PrevBlock (32 bytes)
	Hash of MerkleRoot (32 bytes)
	Timestamp (4 bytes)
	Bits (Difficulty) (4 bytes)
	Nonce (4 bytes)
Block Body	Transaction counter (1~9 bytes)
	Coinbase transaction
	Transaction #1~n

블록체인은 블록들이 체인(chain of Blocks) 형태로 연결된 Linked list 구조의 분산 DB이다. 그림2에서와 같이 hash pointer들이 최초의 블록(Genesis Block)부터 바로 최근 블록까지 연결되면서 하나의 DB를 이룬다.



(Figure 2) Transaction Flow of Bitcoin

생성된 블록은 네트워크 내 모든 노드에게 전파되고, 검증 및 승인된 블록은 가장 최근 블록에 연결된다. 추가된 블록은 기본적으로 수정 불가 및 영구 저장된다. 이 과정의 반복을 통해 블록체인이 형성된다. 트랜잭션 관점에서, 트랜잭션 변조를 위해서는 그 트랜잭션이 포함된 블록의 Header를 변조해야하며, 대상 블록부터 가장 최근 블록까지 모두 변조해야하는 많은 자원과 노력이 필요하며 확률이 낮은 행위를 해야 함을 알 수 있다.

2.2 Consensus Algorithm

합의 알고리즘(Consensus Algorithm)은 다수 노드가 존재하는 P2P 네트워크에서 정보 불일치 발생 시 노드 간 하나의 DB를 유지하기 위해 어떤 정보를 선택할지 결정하는 기술이다. 블록체인은 합의 알고리즘을 통해 블록 생성 권한과 분기된 블록체인 선택에 대한 기법을 결정한다. 대표적 합의 알고리즘은 PoW와 PoS, PBFT 등이 있다. 블록 분기 발생 시 PoW와 PoS 등의 경우는 가장 길게 연장된 블록체인을 선택하며, 이는 일시적 정보 불일치가 발생할 수 있다.

2.2.1 FLP Impossibility

합의 알고리즘에서 중요한 요소는 Safety와 Liveness이다. Safety는 노드 간 합의 발생 시, 어느 노드가 접근하든 그 값은 동일해야함을 의미한다. Liveness는 합의 대상에 문제가 없다면, 반드시 합의가 이뤄져야함을 말한다. Fiscer, Lynch, Paterson는 Safety와 Liveness를 모두 완벽히 만족하는 합의 알고리즘 설계는 불가능하다는 것을 증명하였다[9]. 따라서 합의 알고리즘 설계 시 Safety와 Liveness에 대한 trade-off 고려가 매우 중요하다. PoW로 대표되는 최근의 합의 알고리즘들은 'Liveness over Safety' 방식을 채택함으로써, 블록의 분기를 수용하는 대신 Liveness를 극대화하면서 일시적 Safety 문제를 허용한다. Safety를 보완하기 위해 최장 길이 체인을 선택하여 합의한다. BFT (Byzantine Fault Tolerance) 계열 알고리즘은 이와는 반대로 'Safety over Liveness' 방식으로 데이터를 저장함으로써, 추가될 데이터에 대한 완전한 합의 후에 블록을 추가한다. 그러므로 분기를 허용하지 않으며, 완전한 Safety를 확보할 수 있다. 합의가 이뤄지지 않으면 합의 대상이 정상이어도 처리하지 못해 Liveness 손실이 발생한다.

2.2.2 Byzantine General Problem

Byzantine General Problem은 고대 비잔틴 제국을 비유한 시스템 문제로서 상호 간 통신에 의한 합의 상황을 가정한다. Lamport, Shostak와 Pease는 한 리더에 의해 3명

의 장군이 적을 공격 또는 공격하지 않는 결정에 대해 합의 시 한명의 배신자라도 존재하면 합의에 실패하게 됨을 증명했다[10]. 문제 상황은 배신자뿐만 아니라 메시지 전달과정 중 유실, 변조까지도 포함한다. 시스템에서 장군은 합의 노드, 배신자는 Byzantine faulty 노드를 나타낸다. Byzantine fault는 malicious 노드, network failure 및 system error 등을 포괄한다. 이 문제를 해결하기 위해 Byzantine Fault Tolerance (BFT) 모델이 제안되었으나, 동기식 네트워크에서만 정상적으로 동작하는 한계가 있다.

2.2.3 Proof of Work

P2P 네트워크는 정보 전달 시간차에 따른 전송 지연 및 failure가 존재하여, 이중 송신에 따른 중복 처리나 오작동이 발생 가능하다. 이를 해결하기 위한 정보 검증 및 선택 방법이 합의 알고리즘이다. 비트코인의 합의 알고리즘인 작업증명(PoW)을 가능하게 하는 핵심 기술은 해시 함수(SHA-256)이다. 블록체인은 해시로 시작해서 해시로 끝나는 암호 기반 기술이라고 하는 이유가 바로 여기 있다. PoW를 통해 블록을 만듦으로써 블록보상을 얻는 것이 채굴(mining)이다. 채굴은 기술적으로는 '하나의 블록을 생성하여 블록체인의 길이를 연장하는 행위'를 말하며, 블록을 형성하는 방법은 현재 블록에서 정해진 난이도를 만족하는 정답(nonce)을 0에서 시작하여 1씩 더해가는 무차별대입(Brute‐Forcing) 방식으로 수행된다. 이런 이유로 계산량에 의한 증명 즉, 작업증명이라 정의한다. 다시 말해, 블록 생성을 누가할 것이냐의 문제를 작업량에 따른 증명을 통해 블록 생성 권한을 주고 이를 신뢰하는 방식인 것이다[11].

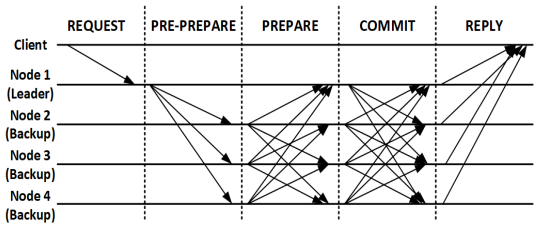
2.2.4 Proof of Stake

PoW의 경우 computing power를 동원한 계산량에 의한 작업증명을 수행하여 시간이 지날수록 과도한 에너지 소비 및 자원 낭비와 hash rate의 독점화에 대한 문제가 발생되었다. 이를 개선하려는 논의가 시작되며 나온 것이 지분증명(PoS : Proof of Stake)이다. PoS는 노드의 소유 지분(Stake)과 소유 기간에 따라 블록 생성 권한에 영향을 주는 난이도를 낮춰, 더 많이 더 오래 지분을 보유한 노드가 더 많이 블록을 생성할 수 있게 하는 방식이다[12]. 블록 생성 및 검증하는 노드가 되기 위해서는 보유하고 있는 자산을 보증금 형태로 rock-up하는 특별한 트랜잭션을 실행하여, 그 이후부터의 새로운 블록을 생성하고 검증하는 절차에 참여하도록 되어있다. 최근 PoS 방식을 활용해 대표 노드들을 선출하여 더 빠른 합의를 수행토록 하는 위임된 지분 증명(DPoS : Delegated Proof of Stake) 알고리즘이 등장했다[13].

2.2.5 Practical Byzantine Fault Tolerance

Castro, Liskov는 BFT의 Liveness 손실을 낮추기 위해 비동기식 네트워크에서도 작동하는 합의 프로토콜을 접목한 PBFT를 제안하였다[14,15]. 다시 말해 Safety를 확보하고 Liveness를 희생하면서도, 비동기 네트워크에서도 합의를 이룰 수 있는 알고리즘인 것이다.

(1) PBFT Description



(Figure 3) Normal operation of PBFT

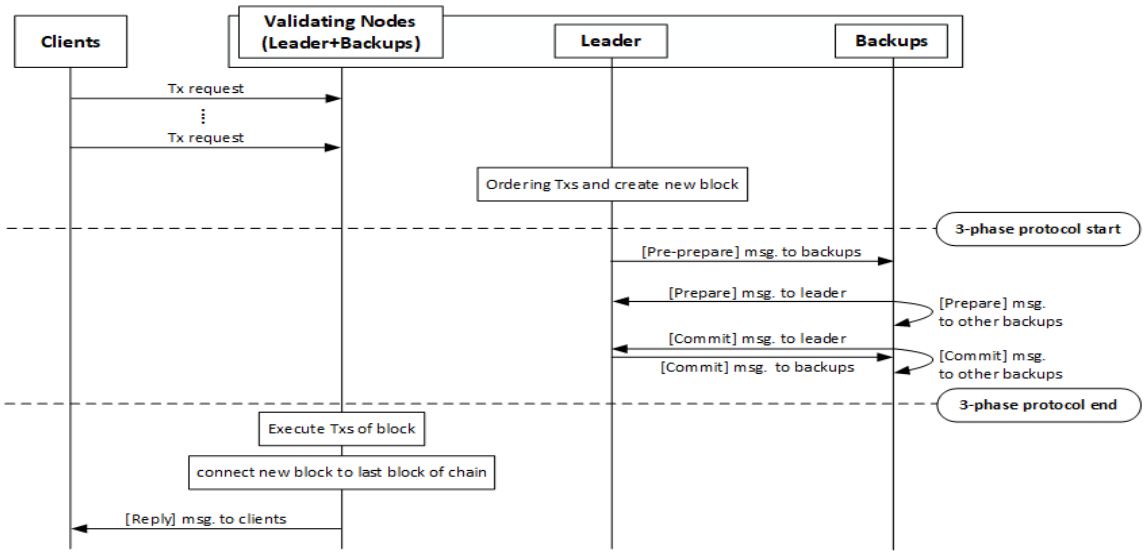
PBFT가 적용된 시스템은 약속된 행동을 하지 않는 Byzantine faulty 노드(이하 Faulty 노드)가 존재할 수 있는 비동기 네트워크에서도 Faulty 노드가 일정 비율 이하에서는 정상 합의가 가능하다. 전체 노드 수 n, Faulty 노드 수 f에 대해, f가 $(n-1)/3$ 까지는 합의에 성공하며, 정상 합의 시 수식(1)을 만족한다.

$$f \le \frac{n-1}{3}, \quad n \ge 3f+1 > 3f \tag{1}$$

이 경우 f의 Faulty 노드가 존재 시, 정상 노드는 $2f+1$ 이상 존재해야 한다. PBFT는 합의 성능 향상을 위해 그림3처럼 pre-prepare, prepare, commit로 진행되는 3-phase protocol을 통해 합의를 시행한다.

(2) PBFT Procedure

그림 4는 PBFT의 세부적인 process를 나타낸다. <request> 단계에서 client가 Leader 노드에게 Tx 실행을 요청한다. <pre-prepare>에서 Leader는 Tx들을 검증·정렬하여 블록을 생성하고, 다른 노드들(backups)에게 전파한다. <prepare>



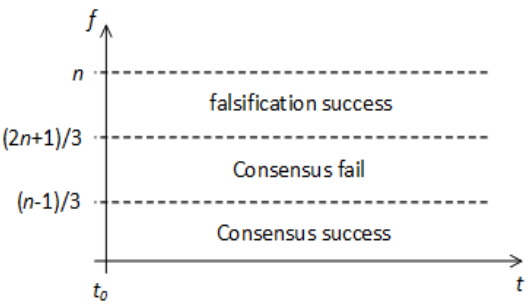
(Figure 4) Overall process of PBFT in blockchain

에서 Leader 메시지를 받은 backup은 검증 후 결과가 참일 경우 다른 노드들에게 재 전파한다. <commit>에서 각 노드는 $2f$ 이상의 노드로부터 같은 값의 prepare 메시지를 받으면, commit 메시지를 다른 노드들에게 전파한다. <reply>에서 각 노드는 $2f+1$ 이상의 노드로부터 같은 값의 메시지를 받으면 블록을 체인에 추가하고, 결과를 client에 전달하고, client는 $f+1$ 이상의 다른 노드들로부터 동일한 결과를 받으면 해당 결과가 처리되었음을 확인한다.

PBFT 블록체인을 대상으로 검증 노드 확보를 통한 데이터 변조 시도가 가능하며, 확보 노드 수에 따라 3가지 상황으로 구분된다. f가 $(n-1)/3$ 이하인 경우 합의에 성공할 수 있으나, $(n-1)/3$ 초과 시 합의에 실패하여 교착상황에 빠진다. f가 더 증가하여 $(2n+1)/3$ 이상이 되면 데이터 변조가 가능해진다. 그림 5에서 t_0는 Faulty 노드가 활동하기 시작한 합의 라운드이며, t은 합의라운드를 의미한다.

(3) PBFT Blockchain

PBFT 알고리즘은 현재 다양한 블록체인 플랫폼에서 시스템에 맞게 변형되어 사용되고 있다. 코스모스는



(Figure 5) The consensus result based on f

Tendermint합의 알고리즘을 사용하고 있는데, 이는 DPoS의 개념과 PBFT를 섞은 알고리즘이다. 먼저, 지분을 기반으로 실시한 투표를 통해서 일정 수의 검증자를 선발한 후, 선발된 검증자 사이에서 PBFT 알고리즘을 통해 블록생성을 합의한다[16,17]. PBFT의 노드 수를 줄여서 통신 복잡도와 합의 시간을 절약할 수 있지만, 보안 위험성이 낮아지게 된다. Zilliqa 블록체인은 PBFT합의 알고리즘에 Sharding을 적용한 합의 방식을 사용하고 있다[18]. 이 알고리즘은 노드들과 트랜잭션들을 Shard로 분할한 후, 블록을 병렬적으로 생성해서 TPS(Transactions per Second) 성능을 상승시킨다. 그러나 노드들이 Shard로 분리되어 적은 수의 노드가 합의하기 때문에 소수의

faulty 노드들로 Shard가 점유될 가능성이 있다. 이 외에도 PBFT 기반 알고리즘은 Hyperledger에서 사용되고 있고, JP Morgan의 Quorum 블록체인은 BFT 기반의 Istanbul BFT와 RAFT 등을 사용하고 있다[19]. 하지만, 위의 합의 알고리즘들은 합의 과정에서 부정행위를 한 노드들에 대한 penalty 시스템은 부족하다.

3. Adaptive Consensus Bound PBFT

PoW 및 PoS 계열 합의 알고리즘들은 부정 행위를 한 노드에 대한 penalty 매커니즘이 부재하다. 따라서 참여 노드가 블록체인을 변조하기 위해 블록을 분기를 시키더라도 합의 알고리즘에 따라 최장길이 체인을 선택하는 방식으로만 블록체인을 유지하고 있을 뿐, 악의적 행위를 한 노드는 여전히 그 지위를 유지할 수 있다. PBFT는 적은 노드 수를 통해 빠른 TPS (Transaction Per Second) 확보가 가능하나, 비잔틴장군문제에 따라 전제 노드 수 n 개에 대하여 $(n-1)/3$ 초과의 노드만 확보하여도 합의에 실패할 수 있어, PoW, PoS 등 보다 더 적은 수의 노드로도 공격이 가능하다. 따라서 악의적 노드에 대한 penalty를 적용하여 정상 합의 상태로 되돌리는 매커니즘이 필요하다. 각 노드에 대한 신뢰도를 평가할 수 있다면, 즉 악의적인 노드의 신뢰를 낮출 수 있다면 합의 robustness를 향상시킬 수 있을 것이다.

3.1 Preliminaries

본 논문에서 사용되는 각종 기호 및 약어들을 표2와 같이 정의하였다. PBFT를 바탕으로 하는 블록체인 시스템은 mesh-type으로 상호 통신이 가능한 n개의 validating 노드로 구성된다. n개 노드 중 일부 Faulty 노드 수는 f이다. 블록체인에 참여하고 있는 모든 validating 노드는 합의라운드마다 3-phase protocol에 참여하며, t_0부터 활동하는 malicious 노드는 블록 변조 시도 또는 합의 미 참여를 수행한다. malicious 노드가 정상적으로 합의에 참여하는 것은 합의에 영향이 없으며, 악의적 의도를 관철하려면 더 많은 노드에게 메시지를 보내야 효과적이므로 phase별로 다른 노드에게 정상 메시지와 변조 메시지를 동시에 보내는 것은 고려하지 않는다. 이때 정상 노드가 네트워크 환경에 따라 time delay, network congestion 등에 의해 합의에 참여 실패하게 되더라도, 합의에 부정적 영향을 미침으로 penalty를 부여한다.

(Table 2) Definition of Symbols

Symbols	Definition
n	Number of all nodes
f	Number of Byzantine faulty nodes (Faulty nodes)
V_k	kth Validating peer
F_k	kth Faulty nodes
R_k	kth Royal node
t	Consensus round from genesis block
t_0	Consensus round where Faulty nodes have started to act
t_m	Consensus round from Faulty nodes have started to act $(t-t_0+1)$
C_i^t	Local Credibility of ith node at t
$C_{i,k}^t$	Local Credibility of ith node for k-th node at t
$\overline{C^t}$	Glocal Credibility at t
$\overline{C_k^t}$	Glocal Credibility for kth node at t
P_f^t	Voting Power of Faulty nodes at t
P_r^t	Voting Power of Royal node at t
D_f^t	Dominance on Consensus of Faulty nodes at t
D_r^t	Dominance on Consensus of Royal node at t
α	Penalty weight, $0<\alpha\leq 1$

n 개의 노드 중 사전에 결정된 Leader 노드가 블록을 생성하며, validating 노드, Faulty 노드, Royal 노드는 각각 $V=\{V_k|k=1,\cdots,n\}$, $F=\{F_k|k=1,\cdots,f\}$, $R=\{R_k|k=1,\cdots,n-f\}$로 정의된다. 각 노드는 commit-phase에서 수집한 투표정보를 바탕으로 신뢰도 평가를 실시하여 Local Credibility $C_{i,k}^t$를 계산한다. Faulty 노드가 발생하기 이전 초기값은 모두 1이다.

$$C_i^t=\{C_{i,k}^t|k=1,\cdots,n\},\ 1\leq i\leq n \text{ and } 2\leq t$$

각 노드는 $t-1$ 라운드에서 투표를 통해 평가한 Local Credibility를 t 라운드 까지 유지한다. Leader는 t 라운드 시 자신의 Local Credibility를 블록과 함께 제안한다. 노드 간 합의로 결정된 Credibility는 Global Credibility로 인정되며 다음과 같이 나타낸다.

$$\overline{C^t} = \left\{ \overline{C_k^t} | k = 1, \cdots, n \right\},\ 2 \le t$$

3.2 Calculation of Credibility

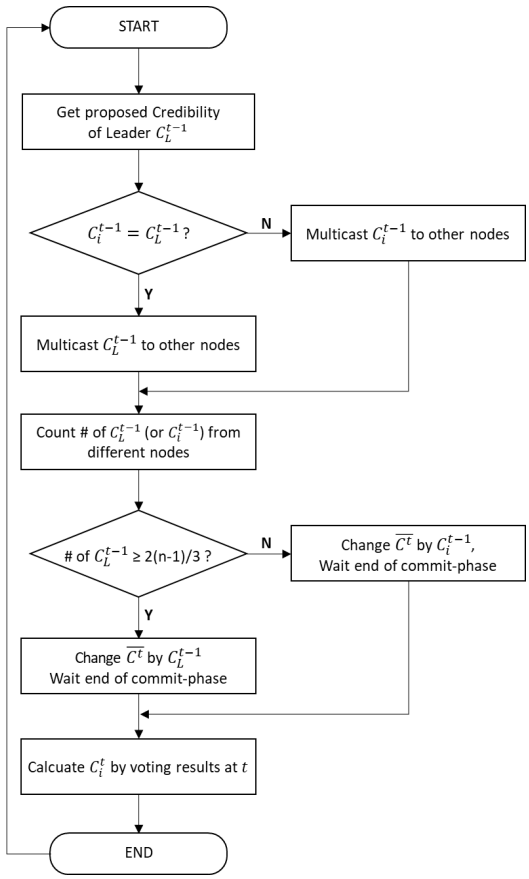
Genesis 블록에서 전 노드의 Credibility는 1이며, 두 번째 블록부터 이전 라운드의 투표결과에 따라 Credibility를 계산한다. 먼저 정상적인 Leader의 제안에 동의하는 투표를 했을 경우 해당 노드는 Royal 노드로 판단하며 이전 라운드의 Credibility를 유지한다. 잘못된 투표를 하거나 투표를 하지 않은 Faulty 노드로 판단되면, 이전 라운드의 전체 Faulty 노드의 Credibility를 전체 노드의 Credibility로 나눈 값에 penalty 가중치 α를 곱한 값만큼 감소시킨다. 이때 Credibility Consensus Procedures 통해 정상적으로 Global Credibility가 결정된 경우, kth 노드의 $t-1$ 라운드 Credibility는 Global Credibility의 kth 노드의 t 라운드 Credibility $\overline{C_k^t}$ 와 같다. 이를 통해 $C_{i,k}^t$는 수식(2)와 같이 계산된다.

$$C_{i,k}^t = \begin{cases} 1 & , t = 1 \\ \overline{C_k^t} & , V_k \in R \\ \overline{C_k^t}\left(1 - \alpha \dfrac{\sum\limits_{\forall F} \overline{C_l^t}}{\sum\limits_{j=1}^{n} \overline{C_j^t}}\right) & , V_k \in F \end{cases} \quad (2)$$

하지만 만약 Global Credibility의 합의가 실패한다면, 이전 라운드의 Local Credibility를 활용하여 수식(3)과 같이 해당 라운드의 Local Credibility를 재계산한다.

$$C_{i,k}^t = \begin{cases} 1 & , t = 1 \\ C_{i,k}^{t-1} & , V_k \in R \\ C_{i,k}^{t-1}\left(1 - \alpha \dfrac{\sum\limits_{\forall F} C_{i,l}^{t-1}}{\sum\limits_{j=1}^{n} C_{i,j}^{t-1}}\right) & , V_k \in F \end{cases} \quad (3)$$

f가 증가할수록 정상 합의에 실패할 확률이 증가한다. 그러므로 Faulty 노드의 Credibility 합의 증가에 비례하여 Faulty 노드들과 전체 노드의 Credibility 합의 비율만큼 penalty를 증가시킴으로써, Faulty 노드 합의 영향력을 감소시켜 합의 성공률을 높일 수 있다.



(Figure 6) Flow chart of Credibility Consensus Procedures.

3.3 Credibility Consensus Procedures

각 노드의 Trust value를 의미하는 Credibility는 각 노드별로 계산된다. 계산된 Credibility를 이용하여 전체 노드가 하나의 Trust value를 공유하기 위해 3-phase protocol로 합의를 수행한다.

그림6은 Credibility Consensus Procedures의 흐름을 보여주며, 각 phase별 상세한 절차는 다음과 같다.

<pre-prepare>에서 Leader는 이전 라운드 $t-1$의 투표 결과로 계산한 Local Credibility를 블록에 포함하여 다른 노드들에게 제안한다. <prepare>에서 나머지 노드들은 자신의 Local Credibility와 비교 후 같으면 수용하고, 다르면 Local Credibility로 변경하여 다른 노드들에게 전파한다. <commit>에서 각 노드는 $2\times(n-1)/3$ 개 이상 노드로부터 동일한 Credibility를 받으면 Trust state로 반영한다. 동일한 Credibility를 보낸 노드가 $2\times(n-1)/3$ 미만인 경우, Trust state를 Local Credibility로 변경한다. <commit>이 종료되면 합의 성공과 상관없이 투표 결과를 통해 전 노드에 대한 Credibility를 재계산한다.

3.4 Credibility-bassed 3-phase protocol

합의된 Global Credibility는 블록 데이터에 대한 합의에 활용된다. 각 노드는 Global Credibility의 각 노드에 대한 Credibility로 노드별 투표영향력(voting power)으로 계산한다. 투표영향력은 합의 과정에서 투표 결과에 영향을 끼치는 힘이다. PBFT에서는, 모든 노드가 동일한 한 표의 투표영향력을 가진다. 따라서 faulty 노드의 수가 f일 때, faulty 노드의 투표영향력은 f이다. 하지만, ACB-PBFT에서는 노드의 투표영향력이 Credibility로, 높은 Credibility를 갖는 노드가 합의 과정에서 더 큰 영향력을 낼 수 있고, faulty 노드들의 투표영향력은 $\sum_{\forall F}\overline{C_j^t}$과 같다. 각 단계별 세부 절차는 다음과 같다. <commit>에서 각 노드는 Global Credibility를 바탕으로 <prepare>에서 동일한 메시지를 보낸 노드들의 Credibility 합이 $2\times(\sum_{k=1}^{n}\overline{C_k^t}-1)/3$ 이상 이면, commit 메시지를 다른 노드들에게 전파한다. <reply>에서 각 노드는 <commit>에서 동일한 메시지를 보낸 노드들(자신 포함)의 Credibility 합이 $2\times(\sum_{k=1}^{n}\overline{C_k^t}-1)/3+1$ 이상일 경우 블록을 체인에 추가하고, 결과를 client에 전달한다. 위와 같이 수행되는 ACB-PBFT는 Consensus Bound가 adaptive하게 변화하게 되며, 표3에서 보는 바와 같이 PBFT와는 큰 차이를 보인다. PBFT에서는 faulty 노드의 수 f가 전체 노드의 수의 $(n-1)/3$ 이하인 경우에는 정상적인 합의를 할 수 있지만, f가 $(n-1)/3$ 초과 시 정상인 블록을 만드는 합의를 실패시켜 교착상황에 빠진다. 그리고, f가 더 증가하여 $(2n+1)/3$ 이상이 되면 변조된 블록을 만들 수 있다. ACB-PBFT에 경우는, 이러한 Consensus Bound가 faulty 노드의 수와 전체 노드 수를 대신해서 faulty node의 투표영향력 $\sum_{\forall F}\overline{C_j^t}$ 과 전체 노드의 투표영향력 $\sum_{i=1}^{n}\overline{C_i^t}$에 의해서 계산된다.

(Table 3) Comparison of Consensus Bound

Consensus result	PBFT	ACB-PBFT
Consensus success	$f \le \frac{n-1}{3}$	$\sum_{\forall F}\overline{C_j^t} \le \frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$
Consensus failure	$f > \frac{n-1}{3}$	$\sum_{\forall F}\overline{C_j^t} > \frac{\sum_{i=1}^{n}\overline{C_i^t}-1}{3}$
Falsification success	$f \ge \frac{2n+1}{3}$	$\sum_{\forall F}\overline{C_j^t} \ge \frac{2\sum_{i=1}^{n}\overline{C_i^t}+1}{3}$

4. 성능평가

4.1 Simulation Scenarios

ACB-PBFT의 성능 평가를 위해 모의실험에서 고려하는 시스템 모델은 PBFT 알고리즘의 메시지 통신 방식을 차용하였으며, 파라미터는 표4와 같이 설정했다.

PBFT는 Faulty 노드 존재를 예상하고 노드 구성을 하므로 최소 1개 이상 Faulty 노드를 설정해야한다. PBFT 노드 구성은 최소 4개부터 가능하며, 이는 가장 기본적 구성으로 PBFT와 ACB-PBFT의 성능 확인이 가능하다. 더 세부적 성능 평가를 위해서는 적절한 노드 수 판단이 필요하다. PBFT는 Leader에 의한 합의로 매우 높은 TPS 구현이 가능하나, 전파 지연에 따른 블록 분기 방지를 위해 수식(4)로 표현되는 매우 높은 통신복잡도를 가져, 노드 증가 시 통신량이 급증한다.

$$O(2(n-1)+2(n-1)^2+N_T) \approx O(n^2) \qquad (4)$$

N_T는 블록 당 포함된 Tx 수이다. ACB-PBFT는 PBFT의 통신 모델에서 메시지 포맷 내 Credibility만 추가하므로 PBFT와 동일한 통신량을 가지며, 추가적 통신 부하는 없다. Credibility 계산을 위한 추가적 계산복잡도 증가는 발생하나, 시스템에 미치는 영향은 미비하다. 실제 시스

템에서는 PBFT의 통신복잡도를 고려해 통신량이 일정 이하로 유지되는 노드 규모로 구현된다. PBFT 알고리즘에서 faulty 노드 수가 f일 때, 합의가 정상적으로 진행되려면 전체 노드는 $3f+1$이 필요하다[10]. 본 실험에서 전체 노드 수는 n이 4인 경우로 가장 적은 통신량 경우의 성능을 비교하고, n이 31인 경우를 통해 실제 시스템에 가장 알맞은 성능을 평가한다. 또한 n이 301인 경우를 설정하여 fault tolerance를 극대화한 경우까지 평가한다. 또한, faulty 노드 비율이 과반 이상 상황까지 실험하여 penalty 매커니즘이 설계와 같이 작동하는지 확인한다. Penalty weight는 credibility의 감쇠상수로 값이 클수록 faulty 노드의 credibility는 많이 감소하게 된다.

(Table 4) Prefixed parameter values

Parameters	Symbols	Value
Number of all nodes	n	4, 31, 301
Density of faulty nodes	f/n	0 ~ 0.6
Max. Consensus Rounds from t_0	t_m	100
Penalty weight	α	0.1

4.2 Performance Evaluation Indicator

ACB-PBFT의 성능을 평가·비교를 위해 Faulty 노드의 투표영향력(Voting power)과 합의 점유율(Dominance on Consensus)을 평가지표로 사용하였다. PBFT의 합의 성공 여부는 전체 노드와 Faulty 노드의 비율로 결정된다. PBFT는 Consensus failure와 Falsification success의 정해진 전체 노드와 Faulty 노드 비율이 존재하며, 이는 Consensus의 bound이다. 그러나 ACB-PBFT는 합의가 진행됨에 따라 Consensus Bound를 변화시킨다. 이를 확인하기 위해 합의 라운드 진행에 따른 전체 노드 중 Faulty 노드의 Voting Power (P_f^t) 변화를 살펴본다. P_f^t는 합의 진행 시 제안된 데이터의 검증결과 불일치 발생 시 Royal 노드와 Faulty 노드의 투표 영향력으로서 합의 결과에 대한 신뢰도 및 합의 성공에 직접적 영향을 미치는 요인이다. PBFT의 P_f^t는 f로 합의 진행과 무관하다. 반면 ACB-PBFT의 P_f^t는 다음과 같다.

$$P_f^t = \sum_{\forall F} \overline{C_i^t},\ V_k \in F \tag{5}$$

Faulty 노드의 Dominance on Consensus (D_f^t)는 전체 노드 중 Faulty 노드들의 합의 점유율 즉 P_f^t가 차지하는 비율을 의미한다. PBFT의 D_f^t는 f/n로 와 마찬가지로 t의 변화와 무관하게 전체 노드와 Faulty 노드 수의 변화에 종속된다. 반면 ACB-PBFT의 D_f^t는 다음과 같다.

$$D_f^t = \frac{\sum_{\forall F} \overline{C_j^t}}{\sum_{i=1}^{n} C_i^t} = \frac{P_f^t}{\sum_{i=1}^{n} C_i^t} \tag{6}$$

4.3 Simulation Results

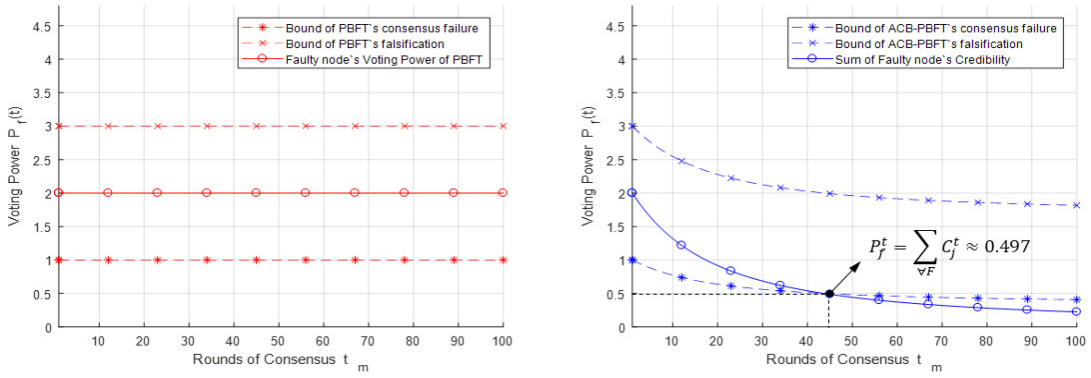
Voting Power 평가는 n이 각각 4, 31, 301 경우별로 PBFT가 Consensus failure에 빠지게 되는 Faulty 노드 수가 전체 노드의 과반 이상인 경우를 가정했고, Faulty 노드 활동 이후 합의라운드 t_m는 수식(7)과 같다.

$$t_m = t - t_0 + 1 \tag{7}$$

그림7은 n이 4, f가 2인 경우의 Faulty 노드들의 투표 영향력을 나타내는 그래프이다. PBFT는 Royal 노드 수가 합의 성공을 위한 quorum을 넘기지 못해 합의 교착상태에서 있으며 라운드가 진행되어도 변하지 못한다. 반면 ACB-PBFT는 malicious 노드들이 활동을 시작한 t_0에서는 PBFT와 마찬가지로 합의 교착상태에 있지만, 라운드가 진행됨에 따라 malicious 노드의 Credibility가 감소하여 t_m이 45인 라운드에서 P_f^t가 bound of consensus failure와 같아짐을 확인 할 수 있다. 따라서 그 다음 합의 라운드부터 정상적인 합의가 가능해진다.

그림 8은 n이 31, f가 16인 경우이며, 앞의 실험과 마찬가지로 PBFT는 합의 교착 상태이나, ACB-PBFT는 t_m이 21인 순간에 P_f^t가 약 6.974으로 bound of consenus failure와 만나게 된다.

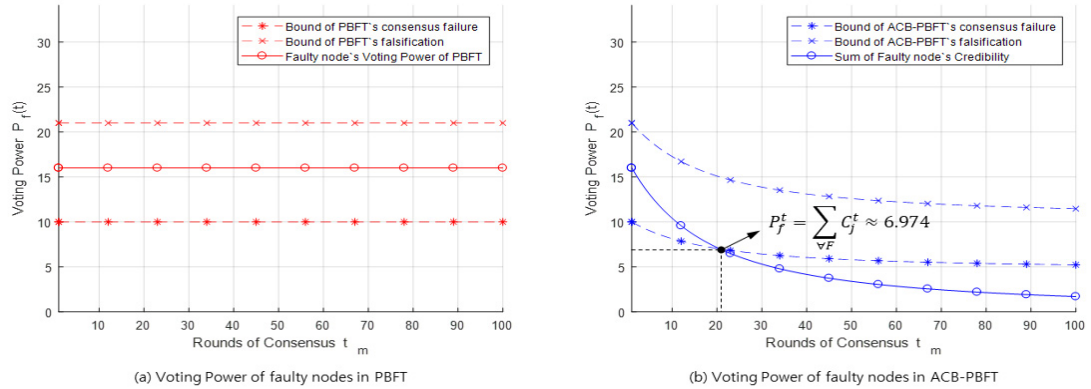
그림 9는 n이 301, f가 151인 경우의 모의실험으로, ACB - PBFT는 t_m이 18에서 P_f^t가 약 74.246로 bound of consensus failure와 만나게 된다. 위 세 가지 실험을 통해 노드 수 증가와 상관없이 합의라운드 진행에 따라 ACB - PBFT는 adaptive하게 Consensus Bound가 변화하며,



(a) Voting Power of faulty nodes in PBFT

(b) Voting Power of faulty nodes in ACB-PBFT

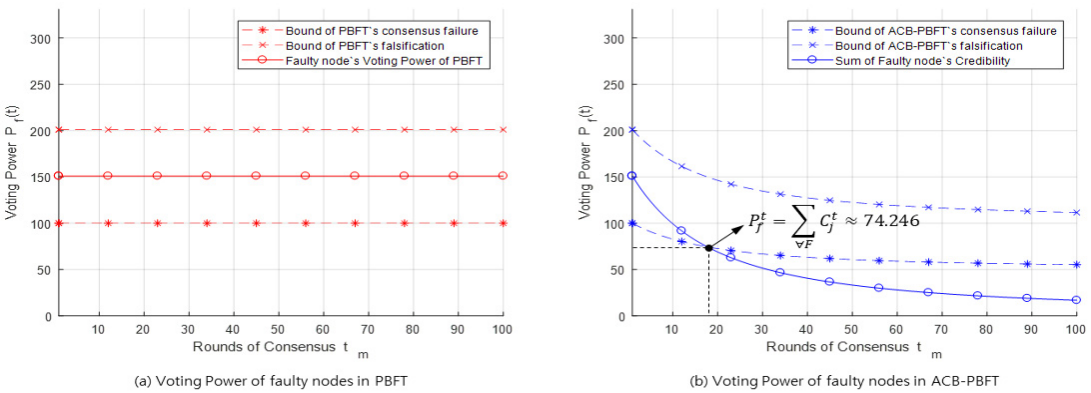
(Figure 7) Voting Power in case n=4, f=2



(a) Voting Power of faulty nodes in PBFT

(b) Voting Power of faulty nodes in ACB-PBFT

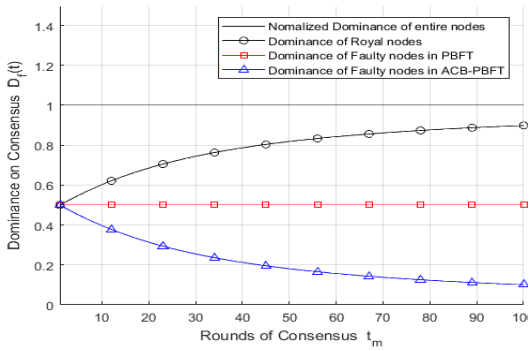
(Figure 8) Voting Power in case n=31, f=16



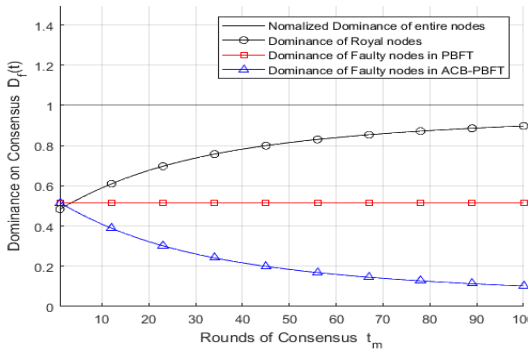
(a) Voting Power of faulty nodes in PBFT

(b) Voting Power of faulty nodes in ACB-PBFT

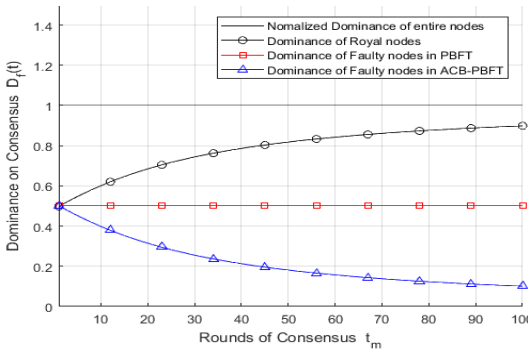
(Figure 9) Voting Power in case n=301, f=151



(a) n=4, f=2



(b) n=31, f=16



(c) n=301, f=151

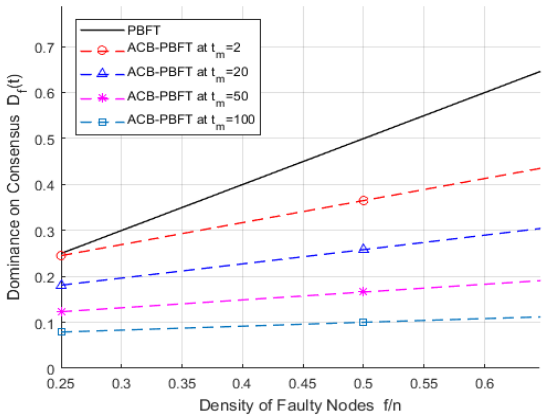
(Figure 10) Dominance on Consensus

Faulty 노드의 Credibility를 감소시키는 penalty 부여를 통해 consensus failure 상황을 벗어날 수 있음을 확인할 수 있었다. 또한 노드 수가 증가할수록 더 빠르게 교착상황을 벗어날 수 있음이 증명되었다. 이는 노드 수가 증가할수록 validating network의 robustness가 강화됨을 의미한다.

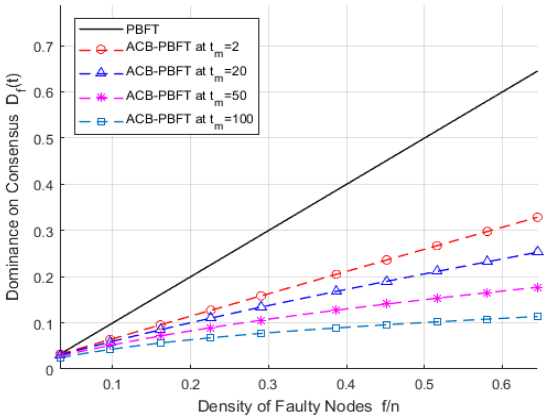
그림 10은 3가지 상황별 Dominance on Consensus (D_f^t)를 계산한 그래프다. 세 경우 모두 합의라운드 진행에 따라 계산된 Credibility의 변화로 Faulty 노드들의 Dominance가 감소함을 보이며, 이에 따라 상대적으로 Royal 노드의 Dominance는 증가함을 알 수 있다. 반면 PBFT의 경우 Faulty 노드들의 Dominance는 변화하지 않음을 알 수 있다. 그림14에서 t_m이 100에서의 $D_f^{t_0+100}$와 $D_r^{t_0+100}$는 (a)의 경우 $D_f^{t_0+100}=0.101$, $D_r^{t_0+100}=0.899$이며, (b)에서는 $D_f^{t_0+100}\simeq 0.102$, $D_r^{t_0+100}\simeq 0.898$이고, (c)에서는 $D_f^{t_0+100}\simeq 0.101$, $D_r^{t_0+100}\simeq 0.899$로, 세 경우 모두 유사한 결과를 보인다. Voting Power 실험에서는 노드 수 증가에 따른 Consensus Bound의 보안성이 강화되어 더 적은 수의 합의로 교착상태를 벗어남을 확인했다. 그러나 Dominance on Consensus는 3가지 상황 모두 전체 노드 수의 변화와는 무관하게 전체 노드와 Faulty 노드의 비율에 의해서만 영향을 받는 것처럼 나타난다.

그림 11은 다른 t_m별로 Faulty 노드의 증가에 따른 Dominance on Consensus 변화를 모의실험 한 것이다. 세 상황 모두 공통으로 확인되는 것은 Faulty 노드에 penalty 매커니즘이 한 번만 적용되어도 Credibility가 크게 감소하여 Dominance를 급격히 감소시키는 효과를 보였다. 이때 Faulty 노드들의 Dominance는 합의 라운드가 진행 될수록 거의 근사치에 가까워짐을 보이지만, t_m이 2인 경우에 Faulty 노드 비율이 50%의 D_f^t를 확인해보면 (a)는 약 0.3651, (b)는 약0.2616 (c)는 약 0.2453를 나타내며, 이는 t_m이 작은 경우는 노드 수가 증가할수록 Faulty 노드의 Dominance가 더 급격히 큰 폭으로 감소함을 확인할 수 있었다.

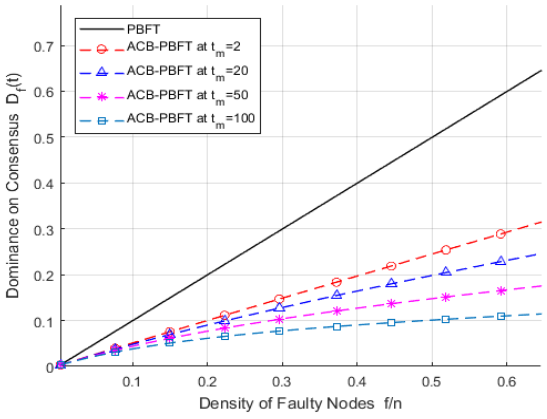
이 모의실험 결과로 기존 PBFT의 경우 악의적 노드 및 Network failure 등에 의한 Faulty 노드 발생 시에 정상 합의 수행을 방해받을 수 있고, Byzantine Faulty 노드 수가 Bound of Consensus failure 이상으로 증가하면 Consensus failure 상태가 해결되지 못하고 교착상태에 머무름을 확인할 수 있었다. 이에 반해 본 논문에서 제안한 ACB-PBFT는 Byzantine Faulty 노드가 발생한 이후 바로 해당 노드의 voting power에 penalty를 부과하여 consensus failure 상태를 벗어나게 됨을 확인하였고, 통신복잡도는 PBFT와 동일하여 통신량 측면의 성능에서는 큰 차이가



(a) n=4



(b) n=31



(c) n=301

(Figure 11) Comparison of Dominance on Consensus

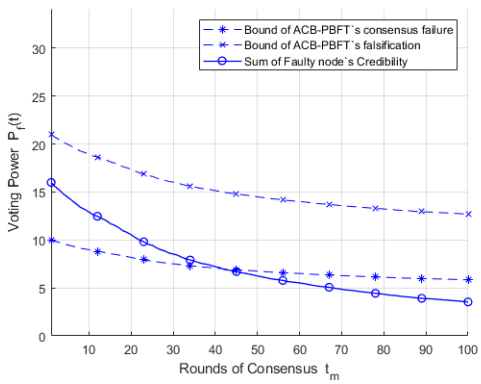
없음을 알게 되었다. 또한 전체 노드 수를 증가시킴에 따라 penalty 매커니즘의 영향이 커져, 더 빠르게 정상 합의로 복귀함을 보여 네트워크의 보안성이 강화됨을 확인했다. 따라서 ACB-PBFT는 PBFT 대비 bound of consensus failure를 높이는 것뿐만 아니라, PBFT에 없던 consensus failure 회피 가능 모델을 보여줌으로써, PBFT 뿐만 아니라 PoW, PoS 등의 다른 블록체인 합의 알고리즘들 보다 우수한 보안성을 보임을 확인하였다.

4.4 Analysis for Inconsistent Attack

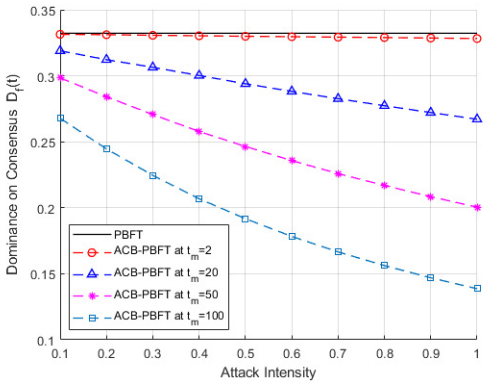
Faulty 노드들은 정상적으로 합의 과정에 참여하다가 어느 순간에 공격을 하거나 확률적으로 공격을 하는 비일관적인 공격을 할 수 있는 가능성이 있다. 따라서 비일관적인 공격에 대한 ACB-PBFT 모델의 성능을 확인하기 위해서 Attack Intensity 변수를 도입했다. Attack Intensity는 0~1의 값을 가지며, faulty 노드들은 비일관적으로 Attack Intensity의 확률로 합의 과정에서 공격을 행한다.

그림 12는 n이 31, f가 16이고, Attack Intensity는 0.5일 때의 투표 영향력을 보여주는 그래프이다. 이 경우에는 faulty 노드들이 50%의 확률에 따라 비일관적으로 malicious 행위를 한다. 그 결과, 그림8의 상황에 비해서 ACB-PBFT의 합의 Bound가 내려가 합의 교착상태 failure 회피가 이루어지는 시점 t_m이 2배 정도 증가했다.

그림 13은 다른 t_m별로 Attack Intensity를 0.1부터 1까지 변화시키며 Dominance on Consensus 변화를 실험한 것이다. Attack Intensity가 높을수록 malicious 행동으로 인해 credibility가 자주 감쇠되어서 faulty 노드들의 합의



(Figure 12) Voting Power in case Inconsistent Attack



(Figure 13) Dominance on Consensus of Inconsistent Attack

점유율이 많이 감소하는 것을 확인할 수 있다. 또한, 시간이 흐름에 따라 드문 확률로 malicious 행동을 하는 경우에도 faulty 노드들의 합의 점유율은 결국 감소하게 된다.

Credibility는 합의 라운드를 진행함에 penalty 매커니즘에 따라 malicious 행동을 할 때마다 누적해서 감쇠되기 때문에 faulty 노드가 정상적으로 합의를 진행하다가 특정 시점에서 malicious 행동을 하는 비일관적인 공격 경우에도 결국 credibility를 penalty한다. faulty 노드들이 정상적으로 행동을 하는 경우에는, 오히려 블록 생성에 도움이 되기 때문에 Transactions per second와 같은 성능에 긍정적인 영향을 끼치므로 credibility에 penalty 매커니즘이 발생하지 않고, 합의 bound도 일정하다. 따라서 ACB-PBFT는 비일관적인 공격에도 penalty 매커니즘이 없는 PBFT의 경우보다 더 우수한 보안성을 가진다.

5. 결 론

본 논문에서는 기존 블록체인 합의알고리즘들이 51% 공격 시 해당 블록체인의 신뢰도를 잃는 문제를 살펴보았고, 2/3 초과의 노드를 확보해야만 데이터 변조가 가능한 PBFT 합의 알고리즘에 대하여 세부적으로 분석하였다. PBFT는 PoW, PoS 등 보다 51% 공격에 대해 무결성 측면에서 보안성이 높은 특징을 갖고 있으나 오히려 1/3 이상의 노드만 확보하면 합의를 교착상태로 만들 수 있음을 확인하였다. 이러한 문제점에 착안하여 비정상 행위를 한 노드에 대한 penalty를 적용하여 합의 교착상태에서 벗어날 수 있는 Adaptive Consensus Bound PBFT (ACB-PBFT)를 제안하였으며, PBFT와의 비교 모의실험을 통해 설계한 모델의 정상 작동 여부 및 PBFT 대비 우수성을 확인하였다.

블록체인이 금융·공공·의류 등 여러 분야에서 실제 서비스에 사용되기 위해서는 정보유통의 실시간성 뿐 아니라 보안성 향상이 필수적이다. 주요 시스템의 데이터 변조·오류가 발생한다면, 그 피해는 판단할 수도 없을 것이다. 본 논문에서는 이를 위해 기존 시스템의 블록체인화를 위한 필수요소인 블록체인 네트워크 보안성 강화 방안을 제안하였다. 제안된 알고리즘을 적용한 블록체인 기술을 실제 네트워크에 접목 시, 기존 대비 블록체인의 무결성도 확보하면서 해킹 등의 공격에 보다 효과적으로 대응할 수 있는 블록체인 네트워크 구축이 가능할 것으로 생각된다.

참고문헌(Reference)

[1] D. Chaum, “Blind signatures for untraceable payments,” in Proc. 2nd Conference on Advances in Cryptology, pp. 199‐203, Santa Barbara, United States, Aug. 1982. http://dx.doi.org/10.1007/978-1-4757-0602-4_18

[2] W. Dai. “B-Money,” 1998. [Online]. Available: http://www.weidai.com/bmoney.txt. [Accessed: Sept. 21. 2018]

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” bitcoin.org, Oct. 31. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Sept. 13. 2018]

[4] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084-2123, Mar. 2016. http://dx.doi.org/10.1109/COMST.2016.2535718

[5] K. Panetta, “Gartner Top 10 Strategic Technology Trends for 2018,” gartner.com, Oct. 3. 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/ [Accessed: Oct. 1. 2018]

[6] W. Lehmacher, Trade Tech ‐ A New Age for Trade and Supply Chain Finance, Geneva, Switzerland: World Economic Forum, 2018.

[7] 과학기술정보통신부, 블록체인 기술 발전전략. 정보통신정책실, 2018.
[8] R. Merkle, “Protocols for public key cryptosystems,” in Proc. IEEE Computer Society Symposium on Security and Privacy, pp. 122-133, Oakland, United States, Apr. 1980. http://dx.doi.org/10.1109/SP.1980.10006
[9] M. Fischer, N. Lynch, and M. Paterson, “Impossibility of Distributed Consensus With One Faulty Process,” Journal of the ACM, vol. 32, no. 2, pp. 374-382, Apr. 1985. http://dx.doi.org/10.1145/588058.588060
[10] L. Lamport, R. Shostak, and M. Pease, “The Byzantine generals problem,” ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382-401, Jul. 1982. http://dx.doi.org/10.1145/357172.357176
[11] Wikipedia, “Proof-of-work system,” wikipedia.org, [Online]. Available: https://en.wikipedia.org/wiki/Proof-of-work_system [Accessed: Oct. 7. 2018]
[12] Wikipedia, “Proof-of-work system,” wikipedia.org, [Online]. Available: https://en.wikipedia.org/wiki/Proof-of-work_system [Accessed: Oct. 9. 2018]
[13] Bitshares, “Delegated Proof-of-Stake Consensus,” bitshares.org, [Online]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/ [Accessed: Oct. 9. 2018]
[14] G. Bracha and S. Toueg, “Asynchronous Consensus and Broadcast Protocols,” Journal of the ACM, vol. 32, no. 4, pp. 824-840, Oct. 1985. http://dx.doi.org/10.1145/4221.214134
[15] M. Castro and B. Liskov, “Practical byzantine fault tolerance,” in Proc. 3rd Symposium on Operating Systems Design and Implementation, pp. 173-186, New Orleans, United States, Feb. 1999. https://dl.acm.org/citation.cfm?id=296824
[16] E. Buchman, “Tendermint : Byzantine Fault Tolerance in the Age of Blockchains,” M.Sc. Thesis, University of Guelph, Canada, Jun. 2016. http://hdl.handle.net/10214/9769
[17] J. Kwon, “Tendermint : Consensus Without Mining.” [Online]. Available: https://cdn.relayto.com/media/files/LPgoWO18TCeMIggJVakt_tendermint.pdf
[18] “The Zilliqa Technical Whitepaper,” Aug, 2017. [Online]. Available: https://docs.zilliqa.com/whitepaper.pdf
[19] “Quorum Whitepaper,” Aug, 2018. [Online]. Available: https://github.com/jpmorganchase/quorum/blob/master/docs/Quorum%20Whitepaper%20v0.2.pdf

◐ 저 자 소 개 ◑

김 형 대(Hyoungdae Kim)
2009년 공군사관학교 전자공학과(공학사)
2019년 연세대학교 대학원 전기전자공학과(공학석사)
관심분야 : 블록체인, Consensus Algorithm, IoT, etc.
E-mail : astrozero@yonsei.ac.kr

◐ 저 자 소 개 ◑

윤 주 식(Jusik Yun)
2016년 연세대학교 전기전자공학과(공학사)
2017~현재 연세대학교 대학원 전기전자공학과 석박통합과정 진행중
관심분야 : 블록체인, 트러스트 시스템, 기계학습, etc.
E-mail : awp212@yonsei.ac.kr

고 윤 영(Yunyeong Goh)
2019년 연세대학교 전기전자공학과(공학사)
2019~현재 연세대학교 대학원 전기전자공학과 석박통합과정 진행중
관심분야 : 블록체인, 증강현실, 엣지/포그 컴퓨팅, 딥러닝, etc.
E-mail : rhdbsdud@yonsei.ac.kr

정 종 문(Jong-Moon Chung)
1992년 연세대학교 전자공학과(공학사)
1994년 연세대학교 전자공학과(공학석사)
1999년 Pennsylvania State University, Electrical Engineering (공학박사)
1997년~1999년 Pennsylvania State University, Electrical Engineering, Faculty Instructor 및 조교수
2000년~2005년 Oklahoma State University, Electrical and Computer Engineering 부교수(정년보장)
2005년~현재 연세대학교 전기전자공학과 교수(정년보장)
2011년~현재 Editor, IEEE Trans. on Vehicular Technology
2013년~현재 KSII Trans. on Internet and Information Systems (TIIS) Co-EiC
2015년~현재 연세대학교 국방융합공학협동과정 주임교수
2017년~현재 Section Editor, Wiley ETRI Journal
2018년~현재 연세대학교 공과대학 부학장
2019년~현재 한국인터넷정보학회 (KSII) 학술부회장
2019년~현재 연세대학교 의과대학 응급의학교실 (겸직)교수
2019년~현재 IEEE Consumer Electronics Society 부회장
2019년~현재 Assoc. Editor, IEEE Trans. on Consumer Electronics
관심분야 : 무선통신, 이동통신망, Ad Hoc망, 정보이론, 통신보안
E-mail : jmc@yonsei.ac.kr