JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 21, No. 1, pp. 229-236, Jan. 2020

Check for updates

거부권 그룹을 포함한 PBFT 기반 블록체인 합의 방식 개선

장윤희[1] · 이상현[3] · 최수혁[3] · 김형중[2*]
[1]고려대학교 정보보호대학원 정보보호학과 석사과정
[2]고려대학교 정보보호대학원 정보보호학과 교수
[3](주)심버스

Improving PBFT-Based Blockchain Consensus Using Veto Group

Yun-Hee Jang[1] · Sang-Hyun Lee[3] · Su-Hyuk Choi[3] · Hyoung-Joong Kim[2*]

[1]Master's Course, Department of Information Security, Korea University, Seoul 02841, Korea

[2]Professor, Department of Information Security, Korea University, Seoul 02841, Korea

[3]Symverse, Seoul 07788, Korea

[요 약]

현재 대중적인 블록체인은 느린 거래 처리 속도와 블록 확정 불확실성 등의 문제가 있어 블록체인을 도입하고자 하는 산업 분야에서 블록체인 기술의 도입에 어려움을 겪고 있다. 이에 본 논문에서는 거래 처리 속도와 확정성, 안전성 보장 관점에서 설계하여 언급되는 블록체인의 문제점을 개선한 합의 방식을 제안한다. 제안하는 합의 방식은 거부권을 행사하는 비토 그룹을 도입한 PBFT 알고리즘 기반의 새로운 합의 방식이다. 본 논문에서는 제안된 합의 방식의 유효성을 평가하기 위해 Istanbul BFT와 비교실험과 노드 수에 따른 비교실험을 진행했다. 본 논문에서 진행된 TPS 측정 및 평가를 통해 제안하는 합의 방식이 기존의 합의 방식보다 개선되었음 보이는 유의미한 수치를 확인할 수 있었다.

[Abstract]

Blockchain, which currently adopts a popular consensus, has problems of slow transaction processing speed and finality uncertainty, making it difficult to adopt blockchain technology in industries that try to introduce blockchain. In this paper, we propose a consensus algorithm that improves the problems of blockchain mentioned earlier by designing it from the viewpoint of finality certainty and safety guarantee as well as improved processing speed. The way we are suggesting is a new PBFT-based consensus that adds the Veto group, which excercise veto power. To verify the validity of the proposed consensus mechanism, we conducted comparison experiments with the Istanbul BFT and the one by the number of nodes. The conducted comparison experiments showed significant results that the proposed consensus mechanism was improved.

색인어 : 블록체인, 블록 신뢰도, 합의, 실용적 비잔틴 장애 허용, 거부권

Key word : Blockchain, Block reliability, Consensus, PBFT, Veto power

http://dx.doi.org/10.9728/dcs.2020.21.1.229

Received 28 November 2019; **Revised** 31 December 2019
Accepted 23 January 2020

***Corresponding Author; Hyoung-Joong, Kim**

Tel: +82-2-3290-4895
E-mail: khj-@korea.ac.kr

Ⅰ. 서 론

'Bitcoin: A Peer-to-Peer Electronic Cash System[1]'을 통해 세상에 알려진 블록체인 기술은 4차 산업혁명의 주요 기반 기술로 주목받고 있다. 세계경제포럼도 블록체인을 미래 12대 유망 기술 중 하나로 선정하고 약 10년 뒤에는 전 세계 GDP (gross domestic product) 의 10%가 블록체인 기술에 기반을 둘 것으로 예측하는 등 블록체인의 미래혁신에 대한 기대는 점점 더 높아지고 있다[2].

현재 블록체인이 가장 빛을 발하는 분야는 금융 서비스 기술 분야이다. IDC (international data corporation) 에 따르면 블록체인은 금융 서비스 시장에서 자주 발생하는 여러 경우에 유용하다. 대표적으로 규제 준수, 국가 간 결제 및 정산, 소유권과 자산 추적, 그리고 무역 금융과 무역, 거래 후 정산 등을 들 수 있다.

관련 분야에서는 적극적으로 도입을 검토하고 있지만, 아직 미성숙한 기술인 블록체인에 존재하는 여러 한계점으로 인하여 도입에 어려움이 따른다. 주요 한계점으로 지적되는 것이 느린 거래 처리 속도와 블록 확정 불확실성이다.

이러한 한계점을 개선하는 한 방법으로 PBFT (practical byzantine fault tolerance) [3] 합의 알고리즘을 기반으로 한 다양한 합의 방식이 등장하고 있다. 대표적으로 Tendermint[4]를 들 수 있는데, Tendermint는 PBFT 알고리즘과 위임지분증명 (DPoS; delegated proof of stake) [5]의 장점을 결합하여 만든 알고리즘이다. 대표자를 선출하고 투표를 진행하여 탈중앙화 규모를 줄이는 방식으로 거래 처리 속도를 높이고 하나의 블록을 선정하는 투표를 진행 하는 과정에 DPoS가 포함되어 지분 기반으로 투표를 진행한다.

본 논문에서는 PBFT 알고리즘의 장점에 거부권 그룹을 도입한 새로운 합의 방식을 제안한다. 제안하는 합의 방식은 거부권을 행사하는 신뢰 받는 그룹 (veto group) 을 도입하여 제안된 블록에 대한 유효성 여부를 결정지어 주어, 다른 PBFT 기반의 합의 알고리즘보다 높은 안전성를 가진다. 게다가 기존 PBFT 합의 알고리즘의 단계에 신뢰성 향상을 위한 단계를 추가하여 비토 그룹과 추가된 단계를 통해 빠른 블록 확정 확실성을 갖는다.

본 논문의 2장에서는 블록체인 합의 알고리즘의 특징과 기반 알고리즘인 PBFT를 살펴보고 대표적인 PBFT 기반 합의 방식인 IBFT를 소개한다. 3장에서 합의 방식을 제안하고 4장에서 이를 평가하며, 5장에서 본 논문을 결론짓는다.

Ⅱ. 블록체인 합의 알고리즘

분산화된 시스템에서는 네트워크 참가자들이 통일된 의사결정을 위한 방법이 필요하다. 다수의 참여자가 통일된 결정을 하고 이에 대한 신뢰를 확보하기 위해 사용되는 방법을 합의 알고리즘 (consensus algorithm) 이라 한다. 블록체인에서 합의 알고리즘은 생성된 블록의 정당성을 검토하고 해당 블록을 블록체인에 연결하기 위해 사용되는 블록체인 네트워크의 핵심적인 요소로서, 분산화된 시스템의 무결성과 보안을 유지하게 시키는 역할을 한다.

분산 시스템의 합의 알고리즘은 일반적으로 안전성과 지속성 특성이 있다. 블록체인 네트워크 또한 안전성과 지속성이 존재하는데 안전성은 특정 시기에 모든 노드가 같은 값을 갖는 것을 의미하고 지속성은 어떠한 일이 있다 하더라도 블록이 생성되어 블록체인이 계속 유지되는 것을 의미한다.

P2P (peer-to-peer) 네트워크를 기반으로 하는 블록체인은 비동기성을 가지고 있어 합의 문제를 완벽히 해결할 수 있는 분산 알고리즘이 없다[6]. 즉, 블록체인에서 사용되는 합의 방식은 안전성 (safety) 과 지속성 (liveness) 두 가지 특성을 완벽하게 만족하지 못한다.

이에 블록체인에서는 네트워크에서 추구하는 특성에 따라 liveness over safety 또는 safety over liveness 방식의 합리적이고 효율적인 의사 결정을 내릴 수 있는 다양한 합의 방식이 등장하고 있다. 대표적으로 사용되는 합의 방식으로는 작업증명 (PoW; proof of work) [1], 지분증명 (PoS; proof of stake) [7], 위임지분증명 (DPoS) , PBFT를 기반으로 응용한 IBFT (istanbul byzantine fault tolerance) [8], Tendermint 등이 있다.

2-1 PBFT(Practical Byzantine Fault Tolerance)

Castro와 Liskov가 1999년 제안한 PBFT 는 비잔틴 장애 허용의 동기식 시스템에서만 구현되고 느린 합의 속도의 문제점을 실용적인 측면에서 개선한 형태이다. 분산 네트워크의 합의에 참여하는 전체 노드의 수 N 중 비잔틴 노드의 개수 f 가 $\left\lfloor \frac{N-1}{3} \right\rfloor$ 이하 존재하는 경우 정상적인 동작이 가능하다[9].

PBFT는 그림 1과 같이 클라이언트로부터 전달받은 request 를 하나의 primary 노드와 나머지 replica 노드들이 pre-prepare, prepare, commit 단계를 거쳐 합의 후 reply한다. 상태 기계를 모델로 하는 PBFT 알고리즘의 각 replica는 결정론적이다. 이에 블록체인 합의 방식의 단점 중 느린 합의 속도와 블록 확정 불확실성 문제를 해결하기 위해 블록체인에서 합의 방식으로 도입되었다.

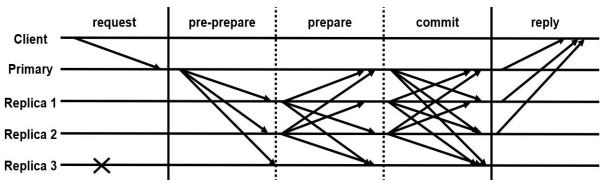

그림 1. PBFT 동작도
Fig. 1. PBFT Normal Case Operation

2-2 IBFT(Istanbul Byzantine Fault Tolerance)

PBFT 기반의 블록체인 합의 알고리즘의 한 예로 PBFT 알고리즘을 Go-Ethereum[10]에 맞게 변형하여 제안된 IBFT 를 들 수 있다. PBFT와 같이 pre-prepare과 prepare, commit의 3단계 합의를 사용하는 IBFT는 PBFT를 블록체인 환경에 맞도록 변경한 것이다.

IBFT는 클라이언트가 따로 존재하지 않고 블록 합의에 참여하는 노드인 검증자 (validator) 를 모두 클라이언트로 한다. 또한 검증자 중 블록을 제안하는 제안자 (proposer) 를 고정된 상태로 진행하지 않고 라운드로빈 방식으로 각 라운드마다 정해진 순서에 따라 새로운 제안자를 선정하여 합의에 대한 블록 제안이 이루어지는 차이점이 있다.

Ⅲ. 제안하는 합의 방식

제안하는 합의 방식을 설명하기 위해 표 1과 같이 용어가 정의되어 있다. 표 2는 상태 기계 복제 알고리즘을 기반으로 하는 제안하는 합의 방식의 프로토콜을 실현하기 위해 각 노드가 지니는 상태이다. 합의가 진행됨에 따라 그림 3과 같은 상태 전이를 가진다. primary와 그 외의 노드의 상태 전이에 차이가 있는데 이는 primary는 자신이 블록과 함께 보낸 메시지인 PROPOSE 메시지와 AGGREGATE 메시지의 검증을 하지 않아 이를 검증하는 단계인 proposed와 aggregated 상태에는 들어가지 않기 때문이다.

표 1. 용어의 정의
Table 1. Terminology

Terminology	Description
Verifier	- Nodes participating in the consensus. - Verifiers verify the block proposed by primary.
Primary	- The node in suggestion group that suggests block in the round. - Every node can calculate primary to the same result through Hash before the next round.
Veto power	- Veto opinion over $\lceil \frac{\lvert G_v \rvert}{2} \rceil$ of verifiers in the veto group about the message from Primary.
Veto Group (G_v)	- The group that exerts veto power. - The group consists of $\lceil \frac{N}{3} \rceil = f+1$ nodes reliable for safety and they make a consensus by a majority vote. - They don't suggest block generation, just verify blocks and exert veto power.
Proposal Group (G_p)	- The nodes not included in veto group. - Primary that suggests block generation is chosen in this group.

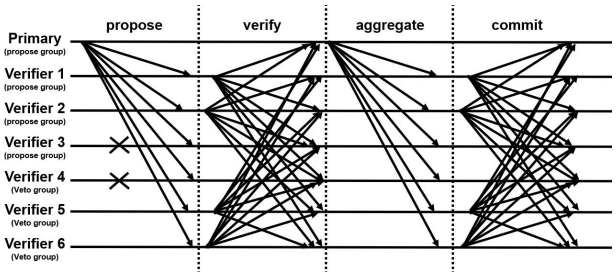

그림 2. 제안하는 합의 방식 동작도
Fig. 2. Proposed Method Normal Case Operation

3-1 프로토콜

PBFT를 개선한 제안하는 합의 방식의 차별점은 다음과 같다. 먼저 프로토콜은 그림 2와 같이 PROPOSE, VERIFY, AGGREGATE, COMMIT의 4단계로 진행된다. AGGREGATE 단계는 VERIFY 메시지에 존재하는 verifier의 서명을 primary가 모으고 이를 이용한 서명을 통해 최종 블록을 생성하기 위해 추가된 단계이다. 블록 내의 서명은 블록 합의에 찬성한 보증 노드들이 생성한 서명을 결합하는 결합 서명 방식을 사용하여 생성된다. AGGREGATE 단계를 진행함으로써 해당 블록 생성에 동의한 verifier를 알려 합의 과정의 투명성을 높이고 결합 서명으로 만들어진 primary의 서명으로 블록의 신뢰성이 향상된다. 또한, 제안하는 합의 방식에서 비토 그룹은 합의에 참여하는 노드 중 신뢰성 있는 노드들로 구성되고 거부권을 행사한다. 비토 그룹의 거부권 행사는 블록 데이터와 전체 네트워크 신뢰성의 향상을 위해 추가되었다.

1) PROPOSE

합의는 new round 상태에서 시작한다. PROPOSE는 블록을 제안하는 단계로 모든 verifier가 같은 블록 높이와 같은 라운드에서 작업하고 있는지 확인한다. PROPOSE 단계가 시작되기 전, verifier는 이전 블록의 해시를 이용하여 이번 라운드에 새로운 블록을 제안할 primary를 알고 있고 트랜잭션의 집합을 공유하고 있다.

primary는 트랜잭션의 집합을 이용하여 블록을 구성하고 이를 포함한 PROPOSE 메시지를 모든 verifier에게 제안한 후 pre-verified로 넘어간다. verifier 들은 primary의 PROPOSE 메시지 수신을 기다리고 PROPOSE 메시지 수신 후 proposed 상태로 들어간다. PROPOSE 메시지를 받은 각 verifier는 공유된 트랜잭션의 집합을 이용하여 제안받은 블록을 검증한다. 검증은 현재 primary가 블록을 생성했는지, 블록의 높이와 이전 블록 해시가 올바른지 확인하고 블록의 메시지가 올바른지 확인하는 과정을 거친다.

표 2. 상태별 정의
Table 2. States

State	Description
new round	- Start of consensus. - Primary broadcasts PROPOSE message, verifier waits for PROPOSE message.
proposed	- The state that comes when verifier receives PROPOSE message. - Verifying PROPOSE message and if verified, broadcasts VERIFY message and it goes to pre-verified state.
pre-verified	- The state VERIFY message or PROPOSE message is broadcasted. - Waiting for enough VERIFY messages.
verified	- The state that verifier receives enough VERIFY messages. - Primary broadcasts AGGREGATE message, verifier waits for AGGREGATE message.
aggregated	- The state that verifier receives AGGREGATE message. - Verifying AGGREGATE message and if verified, sends COMMIT message and it goes to pre-commited state.
pre-committed	- The state AGGREGATE message or COMMIT message is broadcasted. - Waiting for enough COMMIT message.
committed	- The state that received enough COMMIT messages. - Trying adding block to make blockchain possible to add block.
finalized	- Successfully added blocks to the blockchain. - Preparing for the next round.
round change	- The state when appears unexpected situation like timeout, receiving invalid massage from primary, - fail to block insertion and veto power - Ready to run the round again and wait for enough ROUND CHANGE message.

2) VERIFY

VERIFY는 블록 생성에 동의한다는 것을 알리는 단계이다. verifier는 수신한 PROPOSE 메시지를 검증 후, 블록 생성을 동의하는 경우 verifier는 해당 블록에 서명한다. 이를 포함하여 VERIFY 메시지를 구성하고 모든 verifier에게 브로드캐스트 한 후 pre-verified 상태에서 다음 단계를 위한 충분한 VERIFY 메시지를 기다린다. 모든 verifier는 서명 검증을 통해 수신한 메시지가 적법한지 검증한다.

충분한 메시지라 표현하는 이유는 비토 그룹의 의견은 그룹원의 다수결 방식 (majority voting rule) 으로 결정되기 때문이다. 제안하는 합의 방식은 비잔틴 노드가 f 개 존재 시, 비토 그룹의 크기 $|G_v|$ 를 $f+1$ 로 정한다. 다수결 방식으로 의사 결정을 하는 비토 그룹의 특징으로 인해, 비토 그룹원 전체의 의견 $|G_v| = f+1$ 은 $\lceil \frac{|G_v|}{2} \rceil = \lceil \frac{f+1}{2} \rceil$ 개의 비토 그룹의 메시지만으로 알 수 있다.

3) AGGREGATE

AGGREGATE는 블록의 신뢰성을 향상하기 위한 단계로 primary가 블록의 서명 필드를 채우고 이를 AGGREGATE 메시지와 함께 브로드캐스트한다. 블록 서명 필드는 primary가 VERIFY 단계에서 수신하고 검증한 verifier의 서명을 결합하여 생성하는 결합 서명 방식으로 서명을 하여 채운다. primary는 AGGREGATE 메시지를 브로드캐스트 한 후 pre-committed 상태로 이동 한다.

각 verifier는 AGGREGATE 메시지를 받으면 aggregated 상태로 들어간 후 AGGREGATE 메시지를 검증한다. 현재 primary가 보낸 메시지인지, 서명을 제외한 블록의 메시지가 PROPOSE 단계에서 받은 것과 같은지 확인하고 블록에 기록된 primary의 서명을 검증한다. 서명의 검증은 이전 단계에서 블록 합의에 찬성한 verifier의 서명을 이용하여 이루어진다. 이는 primary가 블록의 내용을 조작하여 서명하는 것이 불가능하다는 점을 의미한다.

4) COMMIT

COMMIT은 각 verifier가 제안된 블록을 수락하고 블록을 체인에 추가할 것임을 알리는 단계이다. 충분한 수의 VERIFY 메시지를 수신하고 AGGREGATE 메시지 검증에 성공한 verifier는 COMMIT 메시지를 브로드캐스트한다. 충분한 수의 COMMIT 메시지가 들어오면 블록을 체인에 삽입하여 확정 짓는다. COMMIT 메시지를 브로드캐스트 하는 것은 악의적인 primary에 의한 분기 시도를 막을 수 있는 중요한 과정이다.

AGGREGATE 메시지나 COMMIT 메시지를 브로드캐스트 한 상태에서 이후 VERIFY 단계와 같이 충분한 수의 COMMIT 메시지를 받으면 commited로 넘어간다. commited는 블록체인에 블록을 추가가 가능한 상태로 verifier는 체인에 블록 추가를 시도한다. 블록 추가에 성공한 verifier는 성공적인 기록을 의미하는 finalized에 들어가 다음 라운드를 위한 작업을 한다.

3-2 Primary 교체

Primary의 교체는 매 라운드 이루어진다. 다음 primary는 finalized 상태에서 new round 상태로 넘어가는 과정에 이전 블록의 해시값을 이용하여 결정한다. 이는 primary를 예측하여 공격이 이루어지는 것을 막기 위함이다.

블록 높이가 증가하여 새로운 라운드가 시작 되면 이전 블록의 해시를 이용하여 제안 그룹의 verifier를 후보로 선정하고 순위를 정한다. ROUND CHANGE 발생으로 새로운 라운드 시작 시, 블록 높이가 증가할 때까지 정해진 순위에 따라 차례대로 primary로 지정 된다.

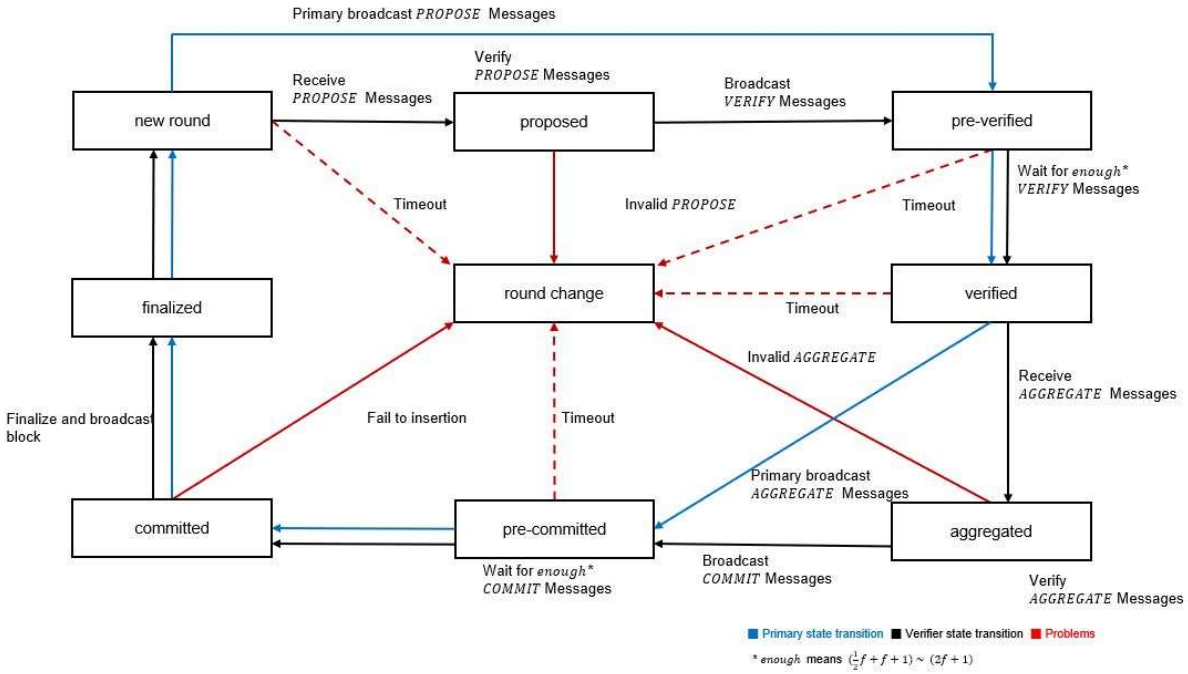

그림 3. 제안하는 합의 방식 상태 전이도
Fig. 3. Proposed Method State Transition

3-3 ROUND CHANGE

ROUND CHANGE는 네트워크가 계속해서 작동할 수 있도록 하는 지속성 (liveness) 을 제공하는 중요한 과정이다. ROUND CHANGE는 timer의 timeout, 유효하지 않은 primary의 message, 블록 추가 실패, 거부권 발효의 경우에 이루어진다. 거부권의 발효는 비토 그룹 내 다수의 verifier가 primary의 메시지를 유효하지 않다고 판단하면 이루어진다. 이 경우에 바로 round change 상태를 벗어나게 된다.

위 경우 중 하나를 만족하는 verifier는 ROUND CHANGE 메시지를 브로드캐스트 하고 round change 상태로 들어가 다른 verifier의 ROUND CHANGE 메시지를 기다린다. 이 상태는 충분한 ROUND CHANGE 메시지, 해당 높이의 블록 동기화, 거부권 발효 등의 조건이 만족하는 경우로 벗어날 수 있다. round change 상태를 벗어난 verifier는 primary 계산과 같은 다음 라운드를 진행할 준비를 끝내고 new round 상태로 이동한다.

Ⅳ. 평 가

4-1 Safety

제안하는 합의 방식에서 안전성 (safety) 의 경우는 비토 그룹의 존재로 인해 더욱 확실하게 보장하려고 한다. 악의적인 primary가 특정 높이 H 에서 분기를 시도하여 블록 B_1 과 블록 B_2 를 동시에 제안하는 경우를 가정할 수 있다. 비토 그룹은 다수결을 통하여 동일한 의견을 내기에 B_1 과 B_2 중 하나로 의견이 일치되게 해야 한다. 이는 정족수 $N-f=2f+1$ 인 네트워크에서 $f+1$ 개의 부분 합의한 결정이 있다는 의미이다.

합의의 정족수가 $2f+1$ 개 일 때, 해당 라운드에 제안된 블록에 대한 결정은 $f+1$ 개 이상으로 부분 합의된 것을 따른다. 이로 인하여 하나의 라운드에서 여러 개의 블록이 제안되어도 높이 H 에 대한 블록은 비토 그룹이 동의한 블록으로 결정되어 블록체인의 분기를 막을 수 있다. 그러나 비토 그룹이 동의한 자발적 분기까지 막을 수 있는 것은 아니다.

4-2 Finality 확실성

기본적으로 투표를 통해 하나의 블록을 제안하여 생성하고 배포하는 PBFT 기반의 합의 방식임에 확정적인 finality 시간이 보장된다. 제안하는 합의 방식은 추가된 AGGREGATE 단계와 비토 그룹으로 인해 기존의 PBFT 기반의 합의 방식보다 빠른 블록 확정 시간을 가진다.

4-1에서 논하였듯이 일반적인 경우 비토 그룹은 높이 H 에 대한 블록이 한 가지만 존재하도록 한다. AGGREGATE 단계 이후 배포되는 블록에는 블록 생성에 동의한 verifier들의 서명과 이를 결합하여 만든 primary의 서명이 들어있다. 블록의 commit은 primary의 서명이 유효한 경우에 이루어지며 이 서명이 유효함은 결합 서명생성에 사용된 verifier의 서명이 유효함을 의미한다. 즉 블록이 배포되는 순간 블록은 확정되었음을 의미한다. 이에 해당 블록을 받은 네트워크 참여자들은 블록에 기

록된 서명들을 검증하는 것만으로 블록을 받아들일 수 있다.

4-3 TPS 측정 및 평가

1) 실험 환경

제안하는 합의 방식의 유효성을 확인하기 위해 TPS (transaction per second) 비교실험을 진행하였으며 실험에 사용한 환경은 표 3과 같다. 실제 블록체인 환경과 유사하게 진행하기 위해 먼 거리에 설치된 다수의 노드 사이에서 실험을 수행해야 하나 수행된 실험은 동일 공간의 여러 대의 PC를 이용했다. 따라서 노드 사이의 전송속도가 고려되지 못한 한계가 존재한다.

실험은 하나의 PC당 최대 7개의 노드를 실행하였으며 노드 수에 따른 TPS 실험을 수행할 때에는 부하 분산을 위하여 동일 성능의 PC를 여러 대 이용하여 진행하였다.

2) 실험 방식

트랜잭션의 배포 및 동기화 시간을 제외하고 순수하게 블록 합의에 걸린 시간만 측정하기 위해 pool에 트랜잭션을 사전 공유하여 시험을 수행하였다.

트랜잭션 풀에 공유된 트랜잭션을 유지하기 위해 트랜잭션 풀과 state 처리 시 nonce를 검사하는 부분을 수정하여 정해진 숫자의 트랜잭션을 유지 및 동기화하는 로컬 네트워크를 구성하였다. 실험은 위와 같이 구성된 네트워크에서 합의를 통해 지속해서 블록을 생성하는 방식으로 진행하였다.

TPS는 이전 블록 생성 완료 시점부터 현재 블록 생성 완료까지의 시간을 처리시간 (elapsed time) 으로 하고 해당 시간 동안 처리된 트랜잭션의 수 (processed transactions) 를 이용하여 계산하였다.

3) IBFT와 비교

제안하는 PBFT 기반의 합의 방식과 기존에 존재하는 PBFT 기반 합의 방식과의 비교실험은 대만 금융기관들이 공동으로 세운 블록체인 전문업체 아미스 (AMIS) 가 개발한 IBFT[11]와 진행하였다.

실험은 하나의 PC에 7개의 노드를 실행하여 네트워크를 구성하고 해당 로컬 네트워크의 트랜잭션 pool에 6000, 6500, 7500개의 트랜잭션을 사전공유 후 유지하며 5000개의 블록을 생성하였을 때의 결과로 비교하였다. 한 블록 생성에 따른 평균 결과는 표 4에 나타나 있다.

표 4를 보면 pool에 존재하는 트랜잭션의 수가 증가함에 따라 트랜잭션 처리 시간이 길어 짐을 확인할 수 있다. 이는 처리된 트랜잭션의 수가 pool에 존재하는 트랜잭션의 수가 같은 것으로 보아 트랜잭션 처리개수 증가에 따른 처리시간 증가로 판단된다. 이를 통해 한 블록에 기록되는 트랜잭션의 수가 블록체인 성능에 영향을 준다는 사실을 알 수 있다.

실험의 결과를 비교해 보면 모든 경우에 대해 제안하는 합의 방식의 처리시간이 빨라 TPS가 높은 것으로 나타났다. 비토 그룹은 의사 결정 과정에서 $\left\lceil \frac{|G_v|}{2} \right\rceil = \left\lceil \frac{f+1}{2} \right\rceil$ 개의 메시지로 $|G_v| = f+1$ 개의 의견을 얻을 수 있어 다음 단계로 진행될 때 필요한 메시지의 수가 기존보다 감소할 수 있다. 개선된 TPS는 이런 과정을 통해 도출된 결과이다.

4) Verifier 수에 따른 비교

보다 공정하고 탈중앙화된 블록체인을 운영하기 위해서는 다수의 노드가 합의에 참여하여야 한다. 이에 합의에 참여하는 노드 수 증가에 따른 TPS 변화를 확인하기 위해 노드 수에 따른 TPS 비교실험을 진행하였다.

구현한 합의를 이용하여 합의에 참여하는 7, 13, 25개의 노드 수에 따른 TPS 비교 측정을 진행하였다. 실험은 부하 분산을 위하여 하나의 PC에 6개 또는 7개의 노드를 실행하여 로컬 네트워크를 구성하고 해당 로컬 네트워크에 6000개의 트랜잭션을 사전공유 후 유지하며 진행되었다. 표 5 는 5000개의 블록을 생성하는 동안 얻은 결과를 이용해 얻은 평균 결과이다.

표 5를 통해서 구현한 합의는 일반적인 PBFT의 특징대로 노드 수의 증가에 따라 처리시간이 증가하여 TPS가 감소함을 확인할 수 있다. 7개에서 13개로 증가했을 때 처리시간은 64.07 ms 정도의 차이를 보였으나 13개에서 25개로 증가한 경우 607.39 ms 로 큰 폭의 처리시간 차이를 보였다. 큰 폭의 증가에도 불구하고 이 결과는 표 4에 있는 6000개의 트랜잭션을 유지하는 네트워크에서 IBFT 합의 방식을 사용하여 7개의 노드로 진행된 결과보다 나은 것을 확인할 수 있다. 따라서 제안하는 합의 방식으로 동작하는 블록체인 네트워크는 기존의 다양한 유형의 합의 방식으로 동작하는 블록체인보다 향상된 성능을 보일 것으로 기대된다.

표 3. 실험 환경
Table 3. Experiment environment

	PC specification
CPU	Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
Memory	DDR4 32GB RAM
OS	Windows 10

표 4. IBFT와 비교실험 결과
Table 4. Comparative Experiment Results with IBFT

No.	Shared Transactions	Test	Processed Transactions	TPS	elapsed time (ms)
1	6000	IBFT	6000	3130.34	1938.69
		Proposed	6000	4729.63	1348.43
2	6500	IBFT	6500	3142.99	2092.22
		Proposed	6500	4509.58	1629.21
3	7500	IBFT	7500	3248.88	2344.74
		Proposed	7500	4498.55	1867.67

표 5. Verifier수 별 비교실험 결과
Table 5. Comparative Experiment Results by Verifier

No.	Verifiers	Processed Transactions	TPS	elapsed time (ms)
1	7	6000	4729.63	1348.43
2	13	6000	4326.25	1412.50
3	25	6000	3573.29	2019.89

Ⅴ. 결 론

본 논문에서는 기존 블록체인을 개선하기 위해 거래 처리 속도, 신뢰할 수 있는 데이터 등을 고려한 합의 방식을 제안하였다. 제안하는 합의 방식은 PBFT 알고리즘을 기반으로 하며 비토 그룹의 거부권 발효를 통해 블록체인의 신뢰성이 향상되도록 설계된 합의 방식이다.

제안하는 합의 방식의 VERIFY와 COMMIT 단계에서 적용되는 비토 그룹의 의사 결정 방식으로 인해 기존에 존재하던 합의 방식보다 적은 수의 메시지로 다음 단계를 진행할 수 있고 추가된 AGGREGATE 단계를 통해 합의된 블록의 신뢰도가 향상되어 기존의 PBFT 기반의 합의 방식보다 블록 확정 시간이 감소하였다. 합의 방식에 도입된 신뢰받는 그룹인 비토 그룹의 거부권 행사는 블록체인의 안전성 보장성 향상, 기록 내용의 신뢰도 개선, 네트워크의 방향성 유지를 통해 거버넌스의 부재로 발생하는 문제점을 해결할 것으로 기대 된다.

제안한 합의 방식은 블록의 확정성과 안정성 보장관점에서 설계되었기에 무역과 같이 기관과 기관이 서로 협업하며 정확한 기록을 필요로 하는 관계에서 사용할 수 있다. 처리 속도 또한 개선되어 실시간 거래를 해야 하는 금융과 같은 분야에서 사용할 수 있다. 단, 비토 그룹의 신뢰성 보장은 제안한 합의 방식을 사용하기 위한 선결 조건이다. 따라서 비토 그룹의 신뢰성 유지가 가능하도록 구성된 컨소시엄이나 프라이빗 네트워크에서 유용하게 활용될 것으로 기대 된다.

본 논문에서 진행된 TPS 측정 및 평가를 통해 제안하는 합의 방식이 기존의 합의 방식보다 개선되었음을 확인할 수 있었다. IBFT와 비교실험 결과를 보면 진행된 3종류의 실험에서 모든 경우에 제안하는 합의 방식의 처리시간이 빨라 TPS가 높은 것으로 나타났다.

향후 높은 개선을 보이는 본 논문의 결과의 세부적 원인을 규명하기 위해 합의 과정의 단계별 처리시간을 비교 측정하는 추가적인 연구가 진행되어야 한다.

참고문헌

[1] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system [Internet]. Available: https://bitcoin.org/bitcoin.pdf.

[2] B. Granetto, R. Kandaswamy, J. D. Lovelock, and M. Reynolds, Forecast: blockchain business value, worldwide, 2017-2030, Gartner Research, Technical Report G00325744, 2017.

[3] M. Castro, and B. Liskov, “Practical Byzantine Fault Tolerance”, Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, pp. 173-186, February 1999.

[4] Tendermint. What is tendermint? [internet]. Available: https://docs.tendermint.com/master/introduction/what-is-tendermint.html.

[5] Bitshare. Delegated proof-of-stake consensus [Internet]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

[6] M. J. Fischer, N. A. Lynch, and M. S. Paterson, “Impossibility of Distributed Consensus with One faulty Process”, *Journal of the Asscktion for Computing Machinery*, vol. 32, No. 2, pp. 374-382, April 1985.

[7] S. King, and S. Nadal, Ppcoin: peer-to-peer crypto-currency with proof-of-stake [Internet]. Available: https://www.peercoin.net/whitepapers/peercoin-paper.pdf/.

[8] Amis team. Istanbul byzantine fault tolerance #650 [Internet]. Available: https://github.com/ethereum/EIPs/issues/650/.

[9] L. lamport, R. shostak, and M. pease, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382-401, July 1982.

[10] Ethereum. Official go implementation of the ethereum protocol [Internet]. Available: https://github.com/ethereum/go-ethereum/.

[11] Amis team. Official go implementation of the ethereum protocol [Internet]. Available: https://github.com/getamis/go-ethereum/.

장윤희(Yun-Hee Jang)

2016년 : 인하대학교 IT공과대학 (공학학사)

2016년~2018년: 고려대학교 정보보호대학원 정보보호학과 석사과정
2018년~현 재: ㈜Symverse 연구원
※관심분야 : 컴퓨터보안, 정보보호기술, 블록체인

이상현(Sang-Hyun Lee)

2000년: 경북대학교(상주) 컴퓨터공학 (학사)

2012년~2013년: New Business Team
2013년~2017년: Inscobee Smart Grid Team
2018년~현 재: ㈜Symverse CTO
※관심분야 : 블록체인, Cryptocurrency, Network Protocol

최수혁(Su-Hyuk Choi)

1992년 : 노스웨스턴대학교 경제학과 (경제학박사)

1992년~1995년: 정보통신정책연구원 연구위원
2016년~현 재: 고려대학교 정보보호대학원 블록체인학과 겸임 교수
2018년~현 재: ㈜Symverse
※관심분야 : 블록체인, Cryptocurrency, Token Economics

김형중(Hyoung-Joong Kim)

1986년 : 서울대학교 제어계측공학과 (공학석사)
1989년 : 서울대학교 제어계측공학과 (공학박사)

1989년~2006년: 강원대학교 교수
2006년~현 재: 고려대학교 정보보호대학원 교수
※관심분야 : 컴퓨터보안, 블록체인, 패턴인식, 가역정보은닉, 머신러닝, 빅데이터분석 등