JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 4, pp. 47-53, April 2020
https://doi.org/10.9708/jksci.2020.25.04.047

Study on the efficient consensus process of PBFT

Youn-A Min*

*Professor, Dept. of Applied Software Engineering, Hanyang Cyber University, Seoul, Korea

[Abstract]

Blockchain is a distributed shared ledger that transparently manages information through verification and agreement between nodes connected to a distributed network. Recently, cases of data management among authorized agencies based on private blockchain are increasing. In this paper, we investigated the application cases and technical processes of PBFT, the representative consensus algorithm of private blockchain, and proposed a modified PBFT algorithm that enables efficient consensus by simplifying duplicate verification and consensus processes that occur during PBFT processing. The algorithm proposed in this paper goes through the process of selecting a delegation node through an authoritative node and can increase the safety of the delegation node selection process by considering an efficient re-election algorithm for candidate nodes. By utilizing this research, it is possible to reduce the burden on the network communication cost of the consensus process and effectively process the final consensus process between nodes.

▸ **Key words**: Blockchain, PBFT

[요 약]

블록체인은 분산 네트워크에 연결된 노드 간 검증과 합의를 통하여 정보를 투명하게 관리하는 분산공유원장이다. 최근에 프라이빗 블록체인을 기반으로 허가된 기관 간 데이터 관리 사례가 증가하고 있다. 본 논문에서는 프라이빗 블록체인의 대표적 합의 알고리즘인 PBFT(Practical Byzantine Fault Tolerance)의 적용 사례 및 기술적 처리과정을 조사하고 PBFT 처리 시 발생하는 중복된 검증과 합의과정을 간소화 하여 효율적인 합의가 가능하도록 수정된 PBFT 알고리즘을 제안하였다. 본 논문에서 제안한 알고리즘은 권위 있는 노드를 통한 위임노드 선출과정을 거치며 후보노드 대상 효율적인 재선출 알고리즘을 고려하여 위임노드선출과정의 안전성을 높일 수 있기 때문에 전반적으로 합의과정의 네트워크 통신비용에 대한 부담을 줄이고 노드 간 최종 합의과정을 빠르게 처리할 수 있다.

▸ **주제어**: 블록체인, PBFT

• First Author: Youn-A Min, Corresponding Author: Youn-A Min
*Youn-A Min (yah0612@hycu.ac.kr), Dept. of Applied Software Engineering, Hanyang Cyber University
• Received: 2020. 01. 30, Revised: 2020. 04. 10, Accepted: 2020. 04. 10.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

Ⅰ. Introduction

블록체인(Blockchain)은 분산 네트워크 상 연결된 모든 노드를 통하여 거래내역(Transaction)을 검증하고 합의하여 동일한 데이터를 공유하는 기술이다[1].

Fig.1은 블록체인을 통한 거래내역의 송금 사례이다.

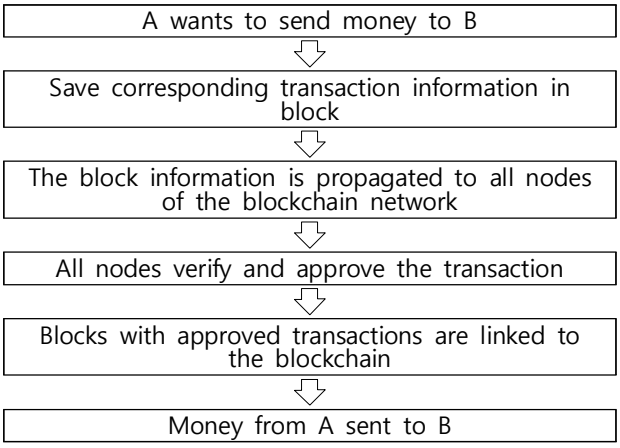

Fig. 1. Blockchain based transaction history remittance case [1]

블록체인은 인터넷상의 이중 거래(Double spending problem)에 대한 해결을 위하여 2008년 사토시 나카모토에 의해 'A Peer-to-Peer Electronic Cash System'의 논문을 통하여 소개되었다. 초기 블록체인 기술은 암호화폐인 비트코인(Bitcoin)을 중심으로 개발되었다[2].

블록체인 1.0이라 불리우는 비트코인은 기존 중앙 집중화 시스템 형태의 데이터 관리에서 벗어나 분산된 네트워크를 통하여 데이터를 관리한다. 비트 코인 이후 블록체인 2.0에 들어서며 스마트 컨트랙트(Smart Contract) 등 추가 기능이 적용되며 이더리움(Ethereum) 및 하이퍼레저(Hyper Ledger) 등으로 발전하였다[3][11].

블록체인은 누구나 노드로 참여하고 합의과정에 참여할 수 있는 퍼블릭 블록체인(Public Blockchain)과 제한된 사용자만이 노드로 참여하고 합의과정에 참여할 수 있는 프라이빗 블록체인(Private Blockchain)으로 구분할 수 있다[4].

Table.1은 블록체인 플랫폼 별 특징과 적용사례를 나타낸 것이다.

블록체인에서는 합의 알고리즘 (Consensus Algorithm)을 통하여 노드 간 거래내역에 대한 검증과 합의가 이루어진다[4].

퍼블릭 블록체인은 각 노드 간 신뢰가 없는 상태에서 네트워크가 구성되기 때문에 네트워크의 신뢰를 유지하기 위하여 블록생성을 원하는 노드들에게 과도한 컴퓨팅 파워 및 지분을 요구한다.

Table 1. Blockchain type[3]

Platform	Characteristic	example
Public Blockchain	● Features open to all. ● Anyone joins PoW with computing power ● Network expansion is difficult ● Slow transaction	Bitcoin, Ripple, Ethereum. etc
Private Blockchain	● Private type blockchain ● One subject manages internal computer network ● Platform service appeared for the relevant chain developmen ● Semi-central blockchain ● Only a small number of pre-selected subjects can participate ● Participation in consensus through agreed rules between participants	Chain, Nasdaq, R3, CEV, Boa. etc

그에 반해 프라이빗 블록체인은 허가된 노드만으로 구성된다는 전제를 기반으로 하기 때문에 블록의 분기(Fork)가 일어나지 않으며 각 노드의 신뢰를 기반으로 합의 알고리즘이 처리된다.

프라이빗 블록체인의 대표적인 합의 알고리즘으로 PBFT(Practical Byzantine Fault Tolerance)을 들 수 있으며 PBFT를 통하여 비동기식 처리가 발생하는 네트워크 상에서 시간상 제약 없이 거래내역을 처리할 수 있다[5]. 또한 PBFT는 악의적 노드가 있는 경우에도 신뢰가능한 노드의 비율을 감안하여 최종합의에 도달 할 수 있으므로 블록 분기를 통한 전체 네트워크의 신뢰도 문제에 대한 문제를 해결할 수 있다[5].

PBFT는 처리과정에서 중복하여 모든 노드를 대상으로 검증 및 인증을 요청한다. 이러한 중복된 처리과정에 의하여 정확한 검증이 가능하지만 순차적 블록생성처리과정을 감안할 경우 블록을 생성하기 위한 대기 시간 고려 등 시간 효율성의 문제 및 대기 병목현상에 대한 문제가 발생할 수 있기 때문에 PBFT의 단점을 해결하기 위한 신뢰기반의 처리 단순화 과정이 필요하다.

Ⅱ. Background

1. Consensus algorithm

블록체인 합의 알고리즘은 사용자 환경에 따라 합의하는 방식이 다르다.

퍼블릭 블록체인의 대표적인 합의 알고리즘으로 PoW(Proof of Work)와 PoS(Proof of Stake) 및 DPoS(Delegated Proof of Stake)를 들 수 있다[4][5]. 프

라이빗 블록체인의 대표적 합의 알고리즘으로 PoA(Proof of Authority) 및 PBFT와 Raft를 들 수 있다[4][5][6].

1) PoW

PoW는 블록체인 네트워크에 참여하는 노드들이 CPU의 컴퓨팅파워를 통하여 주어진 문제를 해결하는 방식이다. PoW를 통하여 블록 생성에 성공한 노드는 다양한 방법으로 보상을 받는다. PoW 방식의 블록체인 네트워크 해킹을 위해서는 PoW에 사용되는 전체 CPU컴퓨팅파워의 51%이상을 확보해야 하므로 사실상 해킹은 불가하다[4]. PoW을 사용하는 대표적 사례는 비트코인을 들 수 있으며 작업 증명을 위한 난이도 조절 알고리즘을 통하여 난이도가 자동 조절된다[4][5].

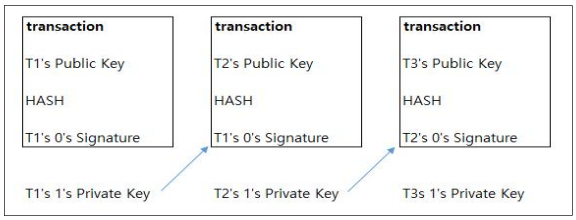

Fig. 2. PoW Process [4][5]

2) PoS and DPoS

PoS에서는 각 노드가 자신이 보유한 지분에 따라 블록 생성권한을 가질 수 있다. PoW와 달리 CPU컴퓨팅 파워에 대한 소모가 없으며 PoS 합의 알고리즘 환경에서 해킹을 하려면 먼저 네트워크의 과도한 지분 및 토큰확보가 필요하기 때문에 자신의 토큰 가치를 하락시키면서까지 해킹을 하려는 노드는 없을 것이라는 개념을 기본으로 한다[4][5][12][13]. PoS에서는 지분이 없는 노드들로만 구성된 경우 Nothing at Stake 문제가 발생할 수 있고 이로 인하여 토큰을 소유하지 않은 노드가 악의적인 선택을 할 수 있다는 위험상황이 늘 존재한다.

DPoS는 PoS의 개념과 비슷하지만 대표노드를 통하여 블록 생성 과정 참여 및 합의가 발생한다. DPoS는 블록검증을 대표노드에게 위임하기 때문에 합의과정이 복잡하지 않고 시간적 효율도 우수하다. 다만 모든 노드의 참여가 불가하다는 단점이 있으며 대표노드들의 악의적 결정을 미리 파악할 수 없다[4][5].

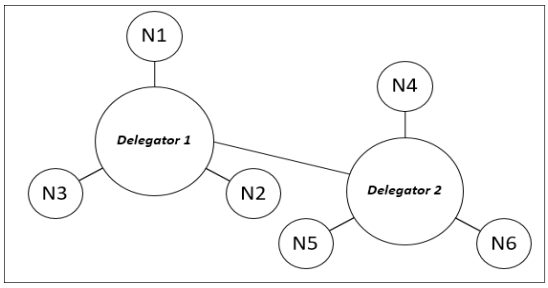

Fig. 3. DPoS Process [4][5]

3) PoA

PoA는 프라이빗 블록체인 플랫폼에서 사용하는 합의 알고리즘으로 노드의 권위에 의한 증명이 가능하다.

PoA는 블록체인 참여자 중 신뢰를 가진 권위자에게 블록생성의 권한을 부여하고 해당 권위자는 명성을 지키기 위하여 블록 검증의 임무를 충실히 수행한다[4][5].

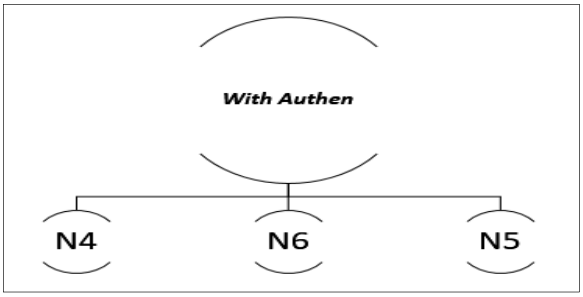

Fig. 4. PoA Process [4][5]

4) PBFT(Practical Byzantine Fault Tolerance)

BFT(Byzantine Fault Tolerance)는 총 노드 중 51%가 악의적 노드일 경우 해킹 등이 발생할 수 있는 비잔틴 장군문제를 동기적으로 해결하여 악의적 노드가 있는 경우에도 총 노드 수 대비 신뢰 가능한 노드 수가 51% 또는 67% 이상일 경우 합의가 가능하다는 이론을 전제로 한다[6].

하지만 다수의 노드가 참여하는 블록체인 네트워크에서는 비동기를 기반으로 비잔틴 장군문제를 해결해야하는 경우가 발생하며 이러한 상황을 위한 합의 알고리즘으로 PBFT가 제안되었다.

PBFT는 텐더민트(Tendermint), 네오(Neo) 등 블록체인 플랫폼에서 사용되고 있으며 하이퍼레져(Hyper ledger)와 R3의 합의 알고리즘으로도 사용하고 있다[5][6]. PBFT는 전체 참여노드 N에 대하여 총 33%의 악의적 노드에 대한 결함을 허용하며 합의가 가능하다.

PBFT는 하나의 리더(Primary)노드와 여러 개의 리플리

카(Replica)노드로 구성되며 Request, Pre-Prepare, Prepare, Commit, Reply의 과정으로 Fig.5와 같은 순서로 합의가 진행된다[6].

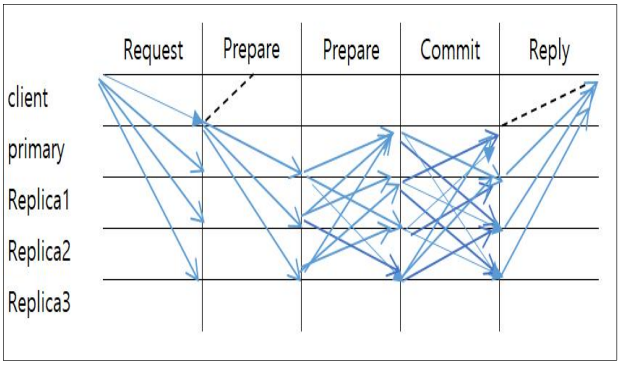

Fig. 5. PBFT Process [6]

Fig.5의 합의과정을 다음과 같이 상세하게 설명할 수 있다[7].

먼저 Request과정에서 Client는 모든 노드에 블록처리를 요청한다. Pre-Prepare과정 에서는 선출된 리플리카 노드(Replica0)를 리더노드로 선출하고 다른 노드들에게 블록 처리에 대한 요청사항을 전파한다. Prepare과정에서 노드들은 요청내용에 대한 수신 여부를 다른 모든 노드들에게 전파한다. Commit과정에서 노드들은 다른 노드의 요청을 취합하여 요청한 노드의 수가 총 노드 수의 2/3 이상일 경우 블록을 검증하고 유효성 검증결과를 다른 노드들에게 전부 전파한다[6][7].

마지막 단계인 Reply에서 각 노드는 다른 노드들이 보낸 블록의 유효성 검증결과를 취합하여 동일 결과가 2/3 초과 시 생성 가능한 블록으로 인정하여 리더를 통하여 해당 상태를 Client에 전송하도록 한다[7].

PBFT의 합의 과정에서 총 노드 N에 대하여 악의적 노드가 없다는 가정 하에 리더 노드를 제외한 노드들은 (N-1)*2번의 통신을 하게 되고 전체 통신량은Client와의 통신까지 포함하여 2N ^ 2번 발생한다[7][8].

일반적 프라이빗 블록체인의 합의 알고리즘이 O(N)임을 감안할 때 노드 수가 증가할수록 네트워크가 부담하는 통신비용의 부담이 커질 수밖에 없다[9][10].

III. Modified PBFT Algorithm

1. Research proposal

2장을 통하여 PBFT의 처리과정을 살펴보았으며 PBFT는 총 노드 수 N과 악의적 노드 x에 대하여 33%의 결함 허용이 가능하며 블록 중간의 분기가 발생하지 않기 때문에 블록의 신뢰를 유지할 수 있음을 확인하였다[6][7].

PBFT의 단점으로 총 노드 N에 대하여 (N-1)/3의 노드에 대한 방어가 가능하기 때문에 51% 미만 악의적 공격 시 합의가 이루어지는 PoW 대비 악의적 공격에 대한 방어가 불리하다는 점과 합의 시 모든 노드 간 중복된 검증 및 합의가 필요하므로 노드 증가 시 네트워크의 통신부담 비용이 커진다는 것을 알 수 있었다[7][8][12][13].

본 논문에서는 PBFT를 통한 합의 시 네트워크 통신비용의 부담을 최소화하기 위하여 수정된 PBFT 알고리즘을 제안하였다.

수정된 PBFT는 PBFT의 통신량 부담에 따른 처리 시간적 및 기능적 제한에 대한 문제를 보완하기 위하여 허가된 노드만 참여한다는 전제를 적극 활용하였다.

수정된 PBFT는 참여노드의 신뢰를 기반으로 유효성 검증을 위한 대표노드를 선출하여 합의과정을 간소화 하였다.

수정된 PBFT의 합의를 위한 프로세스는 다음과 같다.

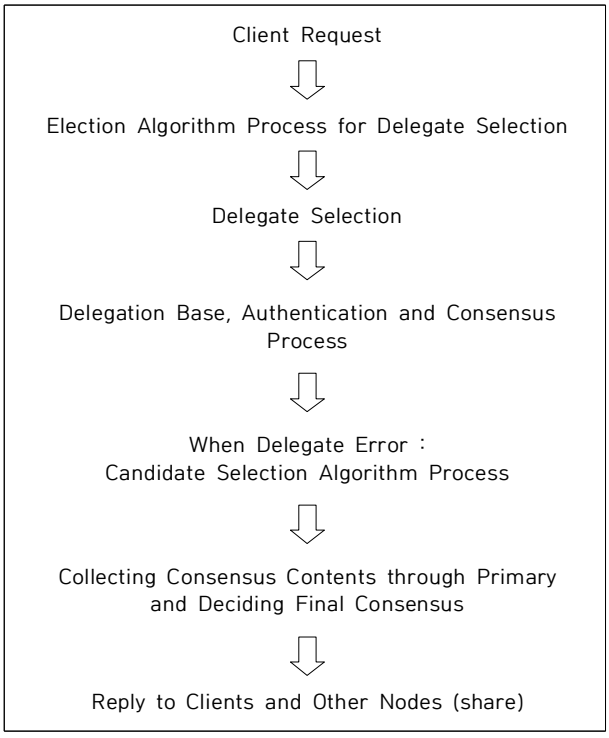

Fig. 6. Modified PBFT Process

Fig.6의 과정에서는 Delegation Selection algorithm을 통하여 대표노드 선출 및 선출내용 공지가 추가되고 이후부터는 선출된 대표노드를 통하여 합의가 진행된다.

이러한 과정을 통하여 PBFT의 모든 노드 대상 브로드캐스트 합의과정을 간소화 할 수 있다.

만일 대표노드 선출과정에서의 오류 및 대표노드의 응답 부재 시 다음과 같은 처리과정을 거쳐 새로운 대표노드를 선출할 수 있다. 해당 과정은 기존 연구된 Raft의 리더 선출 알고리즘과 유사하다[10].

-Select the number of replica nodes as necessary through Primary
-Check the frequency of participation of candidates during the selection process. Through this, it prevents the recurrence of representative nodes of certain nodes.
-Announcement of selection to candidates and selection of automatic representative node if there are no errors

Fig. 7. Representative Leader Re-election Process

2. Performance evaluation

수정된 PBFT의 성능평가를 위하여 2018년 보고된 연구논문의 평가항목을 참고하였다[5][6]. 평가 항목으로 합의 노드 수 대비 네트워크 통신비용, 위임 노드를 고려한 초당 트랜잭션의 처리량을 고려한다.

다음은 성능평가를 위한 항목과 해당 내용이다.

Table 2. Performance Evaluation Item

Item	Contents
TPS(considering Delegation process)	It measures the ability to process and record transactions between participating nodes and is a key performance assessment component of distributed processing algorithms.
Network traffic cost	The number of nodes participating in the consensus process and is related to the speed of consensus and the size of exchange messages in the consensus process, network traffic.

Fig.5와 Fig.6을 통하여 제시한 처리과정의 수를 감안하여 데이터 샘플링 및 단항식을 Fig.8과 같이 유추할 수 있다. 해당 식을 통하여 PBFT의 네트워크 통신비용은 노드 수 x에 대하여 $f(x) \fallingdotseq 2x^2$이며 수정된 PBFT는 각 노드의 신뢰도 α를 고려하여 $f(x) \fallingdotseq 2(1.93)x \pm \alpha(op)$으로 제안할 수 있다.

```
Call: #PBFT
lm(formula = y ~ x)

Coefficients:
(Intercept)                x
      -20.87            19.73
Call: #Modified PBFT
lm(formula = y1 ~ x1)

Coefficients:
(Intercept)               x1
      -0.81             1.93
```

Fig. 8. Unary Expression Generation Process for Visualization

위의 식으로 계산하였을 때 PBFT는 리더를 제외한 다른 노드가 (n-1)*2번의 통신을 수행하고 모든 노드들의 전체 통신량은 2n^2 이므로 노드가 증가할수록 합의에 도달하는 시간의 증가는 $O(N^2)$으로 2차 함수의 형태가 된다. 반면 수정된 PBFT는 노드의 증가에 따른 네트워크 통신량은 O(N)으로 1차 함수의 형태로 나타낼 수 있다.

Fig.9는 노드 수 증가에 따라 네트워트 통신비용의 추이를 그래프로 나타낸 것이다. 노드 수가 증가할수록 네트워크 통신비용의 차이가 벌어지는 것을 알 수 있다.

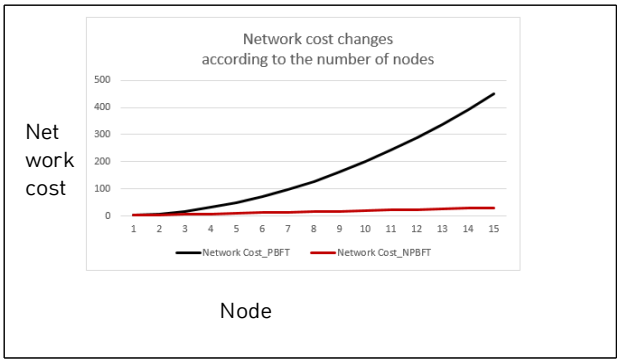

Fig. 9. Network Traffic Cost.(Compared to Agreed Number of Nodes)

초당 트랜잭션 처리량을 계산하기 위하여 기존 연구된 논문의 블록생성시간을 적용하였다[6][7].

블록 생성시간을 t, 블록의 크기를 Sb, 트랜잭션의 크기를 St, 네트워크 통신비용을 ε이라 할 때 기존 연구된 수식에 의하여 $((s_b/s_t)*(1/t))/\varepsilon$과 같이 계산할 수 있다[6][7].

위의 블록 생성시간에 따른 수정된 초당 트랜잭션 처리량 계산식과 그림 8의 네트워크 통신비용을 수식에 적용하여 노드 개수에 따른 초당 트랜잭션 처리량을 다음과 같은 수식으로 제안하여 통계적 특징을 Fig.10과 같이 정리할 수 있다.

```
Call: #PBFT
lm(formula = y1 ~ x)
Residuals:
    1     2     3     4     5
 0.8   2.2 -6.4   3.0   0.4
Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept)     3.600      4.515   0.797    0.484
x               5.600      1.361   4.113    0.026 *
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 4.305 on 3 degrees of freedom
Multiple R-squared:  0.8494,    Adjusted R-squared:  0.7992
F-statistic: 16.92 on 1 and 3 DF,  p-value: 0.02602

Call: #Modified PBFT
lm(formula = y2 ~ x)
Residuals:
    1     2     3     4     5
-0.6   3.4 -2.6 -2.6   2.4
Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept)   -2.400      3.382  -0.710  0.52915
x             10.000      1.020   9.806  0.00225 **
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 3.225 on 3 degrees of freedom
Multiple R-squared:  0.9697,    Adjusted R-squared:  0.9597
F-statistic: 96.15 on 1 and 3 DF,  p-value: 0.002254
```

Fig. 10. Transaction throughput prediction per second

위의 식을 통하여 도출된 계산식은 PBFT의 경우 노드의 수 x를 기준으로 5.6x +3.6의 식을 가지며 수정된 PBFT의 경우 10.0x±α이다. 해당 수식 도출을 위한 데이터 샘플링은 PBFT와 수정된 PBFT의 처리과정을 감안하였다. 수정된 PBFT와 같이 대표노드에 의한 합의과정으로 처리될 경우 Fig.11과 같은 초당 트랜잭션 처리량을 확인할 수 있다.

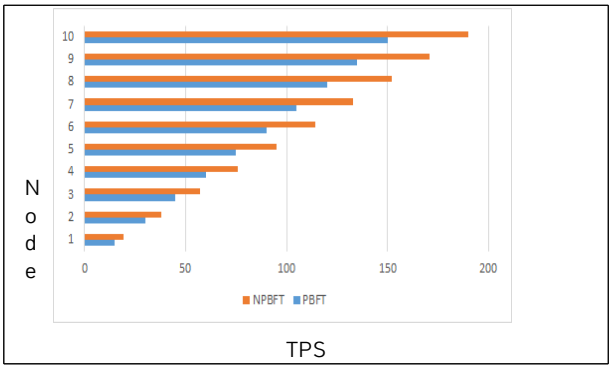

Fig. 11. Compare Transaction throughput per second

IV. Conclusions

프라이빗 블록체인을 통하여 허가된 노드 간 데이터를 공유하고 관리할 수 있으며 공공기관 및 기업을 통한 프라이빗 블록체인 적용사례가 증가하고 있다.

본 논문에서는 프라이빗 블록체인의 대표적 합의 알고리즘인 PBFT의 처리과정 중 중복된 인증과 합의과정에서 발생하는 네트워크 비용 부담을 줄이기 위한 방법으로 노드 중 대표노드들 선출 방법을 제안하여 합의과정의 간소화가 가능하도록 하였다. 대표노드들 선출과정 및 처리과정 중 오류 발생 시 기존 Raft의 노드 선출 알고리즘을 적용하도록 하여 최소한의 연산 시간이 가능하도록 하였다. 본 논문에서는 PBFT와 수정된 PBFT의 각 알고리즘의 처리과정을 분석한 데이터 샘플링을 통하여 네트워크 처리비용과 초당 트랜잭션 처리량을 위한 수식을 제안하였으며 해당 수식을 적용하여 PBFT와 제안한 처리과정의 차이점 및 제안내용의 성능 우수성을 증명할 수 있었다. 먼저 네트워크 통신비용의 경우 PBFT는 노드 수 x에 대하여 $f(x)=f(x) \fallingdotseq 19x$ 이며 수정된 PBFT는 각 노드의 신뢰도 α를 고려하여 $f(x)=1.93x\pm\alpha(op)$으로 유추되었으며 초당 트랜잭션 처리량의 경우 PBFT는 노드 수 x에 대하여 5.6x의 식을 가지며 수정된 PBFT의 경우 $10.0x\pm\alpha(op)$로 유추되었다. 해당 수식으로 그림 9와 11과 같은 성능평가를 분석하였으며 노드 수가 증가될수록 제안 내용에 대한 성능이 우수해 짐을 알 수 있었다.

기존 PBFT의 경우 다수의 브로드케이스 방식의 합의과정을 거치므로 정확성을 보장하는 대신 연산을 위한 비용이 증가할 수 있고 트랜잭션 처리량이 증가할 경우 과부하로 이어질 수 있다. 본 논문에서 제안의 주안점은 사용자 환경의 특징을 고려한 위임 노드의 선정과정을 추가하여 전체 브로드캐스트를 통한 중복된 합의과정을 효율적으로 운영하는 것이다. 제안한 알고리즘을 통하여 합의 과정의 단순화와 노드 간 합의 안정성을 높일 수 있다. 하지만 위임 선정을 위한 알고리즘이 빈번하게 작동되는 경우 합의과정에서의 성능이 떨어질 수 있기 때문에 사용자 환경의 특징을 잘 고려해야한다. 또한 본 논문의 제한점으로 돌발상황에 대한 고려를 고려하지 않았다는 점을 들 수 있다. 네트워크에서 발생할 수 있는 외부요인과 돌발적 이벤트가 다수 발생되는 경우 역시 합의안정성을 저하시킬 수 있다. 향후 대표 노드의 선정 알고리즘의 신뢰도를 높이기 위한 방법을 추가 연구하고 다양한 돌발 상황에서도 합의 안정성을 고려한 위임노드 적용이 가능하도록 연구할 예정이다.

REFERENCES

[1] Bang Jung-ho, Public SW System Application Team Software Industry Promotion Headquarters, Korea IT Industry Promotion Agency, “Blockchain Industry Status and Trends" 2018, No. 17, *https://www.nipa.kr/index.jsp*

[2] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *http://bitcoin.org/bitcoin.pdf*

[3] Buterin Vitalik, “Ethereum white paper,” *https://github.com/ethereum/wiki/wiki/%5BKorean%5D-White-Paper*

[4] *https://www.santanderbank.com/*

[5] Jinseok Kim, “A Design of Secure and Efficient PBFT Consensus Algorithm in Blockchain”, 2019

[6] Do Gyun Kim,.Jin Young Choi,Kiyoung Kim,Jintae Oh,J. Soc. “Performance Improvement of Distributed Consensus Algorithms for Blockchain through Suggestion and Analysis of Assessment Items”, Korea Ind. Syst. Eng Vol. 41, No. 4 : pp.179-188, December 2018, DOI: 10.11627/jkise.2018.41.4.179

[7] Castro M ,Liskov B . "Practical Byzantine Fault Tolerance and Proactive Recovery" ACM transactions on computer systems, VOL.20, NO.4, pp.398-461, November 2002.

[8] Impossibility of Distributed Consensus with One faulty Process, *https://apps.dtic.mil/dtic/tr/fulltext/u2/a132503.pdf*

[9] Huang, D. Ma, X.Zhang, S,"Performance Analysis of the Raft Consensus Algorithm for Private Blockchains",IEEE Transactions on Systems, Man, and Cybernetics: Systems IEEE Trans. Syst. Man Cybern, Syst. Systems, Man, and Cybernetics: Systems, IEEE Transactions ,2020, pp.171-182

[10] Li. Yixin, Wang. Zhen, Fan. Jia, Luo. Yili,Deng. Chunhua,Ding. Jianwei,"An Extensible Consensus Algorithm Based on PBFT", 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019 International Conference, 2019, pp.17-23

[11] Sharma.Tejsi, Satija.Shivangi, Bhushan.Bharat, "Unifying Blockchian and IoT:Security Requirements, Challenges, Applications and Future Trends", 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) Computing, 2019, pp.341-346

[12] Yu, SY, Kim. KT, Yun, HY,“A consensus algorithm based on blockchain”, Proceedings of the Korea Computer Information Society Conference, 2018, pp.17-18

[13] Baek YT, Min, YA, “Modified PBFT research for effective fusion of IoT big data and blockchain technology”, roceedings of the Korea Computer Information Society Conference, 2020, pp.193-194

Authors

Youn-A Min received a Ph.D. in computer science from Dongguk University, Korea, in 2008, 2013. Dr. Min Youn A is a professor of applied software engineering at Hanyang Cyber University, 2020. She is also a visiting professor at Hanyang University. She is interested in embedded system security and blockchain..