프라이빗 블록체인 기반의 사용자 환경을 고려한 수정된 PBFT 연구

(A Study on Modified Consensus Algorithm Considering Private Blockchain Environment-based User Environment)

민 연 아*
(Min Youn-A)

요 약

블록체인은 데이터의 투명성 및 보안성이 뛰어난 분산공유원장으로써 핵심기술인 합의 알고리즘을 통하여 참여 노드에 동일한 데이터를 순차적으로 공유할 수 있도록 한다. 이러한 블록체인 기술의 특징을 활용하고자 최근 기업 및 공공기관을 중심으로 블록체인을 적용하려는 시도가 증가하고 있다.

본 논문에서는 분산 네트워크와 같은 비동기 네트워크 환경에서 활용되는 프라이빗 블록체인의 합의 알고리즘인 PBFT를 수정하여 네트워크 통신비용 및 합의 안정성을 고려한 수정된 PBFT를 제안하였다. 수정된 PBFT는 노드 간 신뢰가 보장된 비동기 네트워크 환경의 특징을 감안하여 클라이언트의 요청 검증에 대하여 기존의 전체 참여 방식을 개선하여 2/N의 Leader (리더)를 통한 합의와 인증을 제안하였다. 해당 과정에서 발생되는 브로드캐스트 과정의 간소화를 통하여 합의를 위한 최소 노드 수 유지가 가능하였으며 네트워크 통신을 위한 효율적 비용관리가 가능하다.

■ 중심어 : 프라이빗 블록체인 ; 합의알고리즘

Abstract

Recently there have been increasing attempts to apply blockchains to businesses and public institutions. Blockchain is a distributed shared ledger with excellent transparency and security of data and through consensus algorithm, the same data can be shared to all nodes in order.

In this paper, Modified PBFT which does not modify the PBFT consensus algorithm is proposed. MPBFT is able to tolerate Byzantine faults on a private blockchain on an asynchronous network. Even with the increase of participating nodes, the network communication cost can be effectively maintained. Modified PBFT takes into account the characteristics of an asynchronous network environment where node-to-node trust is guaranteed. In response to the client's request, PBFT performed the entire participation broadcast several times, but Modified PBFT enabled consensus and authentication through the 2 / N leader.

By applying the Modified PBFT consensus algorithm, the broadcast process can be simplified to maintain the minimum number of nodes for consensus and to efficiently manage network communication costs.

■ keywords : Private Blockchain; consensus algorithm

Ⅰ. 서 론

블록체인은 사카시 나카모토에 의하여 암호화폐의 형태인 비트코인으로 처음 소개되었으나 최근 스마트 계약 등의 새로운 기술이 적용된 다양한 형태의 블록체인으로 발전되고 있다[1-2].

블록체인은 누구나 블록체인 네트워크에 참여하여 거래 내역을 공유하고 합의할 수 있는 퍼블릭 블록체인(Public blockchain)과 허가된 참여자만이 네트워크에 참여하는 프라이빗 블록체인(Private blockchain)으로 구분된다[3][16].

퍼블릭 블록체인은 공개형 분산원장의 형태로 불특정 다수가 네트워크에 참여하며 블록 생성, 합의, 보관을 모든 노드가 함께 처리한다.

이러한 퍼블릭 블록체인의 블록 생성 과정 및 관리 과정의 특징으로 인하여 합의를 위한 과도한 경쟁, 거래의 익명성 보장을 위한 처리 과정, 블록 생성의 한계 등 여러 가지 기술적 문제가 제기되고 있다[4][15].

* 정회원, 한양사이버대학교 응용소프트웨어공학과 조교수

접수일자 : 2020년 02월 19일
수정일자 : 2020년 02월 27일
게재확정일 : 2020년 03월 03일
교신저자 : 민연아 e-mail : jyah0612@hycu.ac.kr

퍼블릭 블록체인 중 비트코인(Bitcoin)은 10분마다 한 개의 블록이 생성되고 이더리움(Ethereum)의 경우 약 12초마다 한 개의 블록이 생성되며 해당 블록이 네트워크를 통하여 모든 노드에 공유되는 시간 역시 2분 남짓하여 중앙 집중 시스템의 처리시간 대비 처리 속도가 매우 느리다[1][4][5].

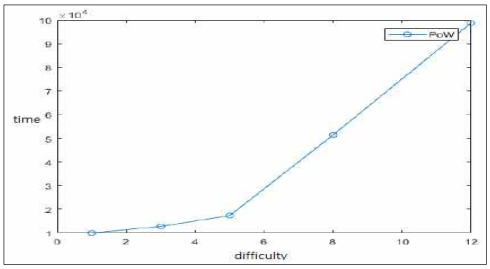

그림 1. PoW 합의 과정[5]

또한 퍼블릭 블록체인 네트워크상에서는 모든 노드에 데이터가 동일하게 저장되어 기록되므로 개인 정보 및 거래에 대한 보안 정보가 블록으로 공유될 경우 치명적인 보안상 문제가 발생할 수 있다[6].

퍼블릭 블록체인의 기술적, 기능적 단점을 보완하고 허가된 노드들 간에 분산 네트워크를 구성하며 보안성과 효율성을 극대화하고자 하는 노력의 일환으로 다양한 합의 알고리즘, 저장 방식의 다양화 등이 제기되고 있으나 퍼블릭 블록체인의 특징인 모두에게 개방된 참여 방식 및 원장관리의 방식으로 인하여 근본적인 기술의 한계는 극복하기 힘들다[7].

프라이빗 블록체인은 허가된 노드들만이 참여하므로 퍼블릭 블록체인과 달리 각 노드에 대한 신뢰를 기반으로 네트워크가 구성된다. 신뢰 기반의 프라이빗 블록체인 네트워크를 통하여 빠른 커뮤니케이션, 데이터 처리 속도 증가 및 업무 효율을 증대할 수 있다.

이러한 프라이빗 블록체인의 특징으로 인하여 기업 및 공공기관의 데이터 처리를 위한 새로운 인프라로 프라이빗 블록체인을 적용하고자 하는 시도가 활발하게 진행 중이다.

그림 2는 시장조사 기관인 Tractica에서 조사한 기업 용도인 프라이빗 블록체인 적용 예측의 그래프이며 2025년 199억 달러를 전망하였다[8].

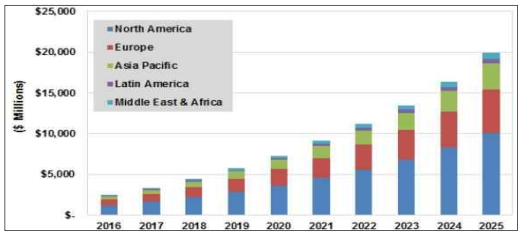

그림 2. 기업용도 블록체인 시장전망[8]

그림 2와 같이 프라이빗 블록체인의 활용 가능성이 높아짐에 따라 블록체인 합의 알고리즘도 지속적으로 발전하고 있다.

블록체인에서는 합의 알고리즘(Consensus Algorithm)에 의하여 거래의 정확성을 유지하기 위하여 모든 노드 또는 대표 노드들이 블록 생성의 정당성을 검토하고 전체 네트워크에 블록을 공유한다.

블록체인의 합의 알고리즘은 블록체인의 특징인 데이터의 정확성 및 무결성 등을 보장하는 핵심기술이다.

Ⅱ. 연구 배경

1. 합의 알고리즘

분산 네트워크 환경에서는 데이터 전달의 지연 등에 따른 이중 지불 및 악의적 노드에 의한 데이터 위조, 변조에 의한 데이터 오작동의 위협이 늘 존재한다[3].

블록체인에서는 불가피한 데이터 전송의 지연 및 보안성 위협에 대처하여 블록의 정확성을 보장하고 전체 노드에 동일한 데이터를 공유하기 위하여 합의 알고리즘을 적용한다.

합의 알고리즘은 플랫폼을 구성하는 구성원의 특징에 따라 다양하게 나누어진다[3].

가. 퍼블릭 블록체인 합의 알고리즘

퍼블릭 블록체인에서는 익명의 다수의 노드에 의하여 연결되어 있으므로 블록 생성 및 정확한 합의를 위한 방법으로 참여 노드의 과도한 컴퓨팅 파워 또는 지분을 요구한다.

힘든 마이닝을 통하여 블록체인에 블록을 연결한 노드들은 인센티브를 받음과 동시에 힘든 노동 또는 자신의 지분의 대가인 블록체인 네트워크의 신뢰를 유지하려 노력한다.

퍼블릭 블록체인의 대표적 합의 알고리즘인 PoW(Proof of Work)는 블록을 생성하고자 하는 노드들이 특정한 난이도의 작업을 수행하기 위하여 해시값을 찾는 채굴 과정을 수행한다.

PoW의 해시함수는 다음과 같다.

$$\text{hash}(B) < M/D(\text{difficulty}) \quad (1)$$

[4]

M은 난이도 D의 최댓값(2 256 - 1)이다[4].

PoW의 과도한 컴퓨팅 파워 낭비를 해결하기 위하여 제시된 방법이 PoS(Proof of Stake)이며 PoS는 블록을 생성하고자 하는 노드의 지분에 기반하여 블록 생성 기회를 부여한다.

PoS의 해시함수는 수식(1)과 같다.

hash(hash(pre_B),A,t))<balance(A)M/D[4] (2)

수식(2)와 같이 A의 잔고에 따라 블록 생성 기회는 비례한다.

퍼블릭 블록체인의 합의 알고리즘은 합의를 위한 과도한 컴퓨팅 파워 및 지분 확보 경쟁이 유발될 수 있으며 동시에 블록이 생성되는 경우가 발생하기 때문에 블록체인의 신뢰성 문제도 발생할 수 있다[5].

나. 프라이빗 블록체인의 합의 알고리즘

프라이빗 블록체인은 허가된 노드들만으로 구성된 네트워크라는 점에서 기본적으로 퍼블릭 블록체인의 과도한 채굴 경쟁 및 분기 등을 고려하지 않아도 된다.

또한 프라이빗 블록체인의 경우 노드의 신뢰를 기반으로 하기 때문에 블록체인의 분기를 전혀 고려하지 않거나 비동기적 네트워크상에서의 비잔틴 장애를 허용하기도 한다. 비잔틴 장애 허용이란 네트워크에 구성된 노드들 중 악의를 가진 노드의 비율에 따라 합의를 허용하는 것이다.

블록체인의 분기를 전혀 고려하지 않은 상황에서는 단순히 노드의 고장만을 오류 상황으로 인식하여 합의 과정에 반영한다. 이러한 상황을 실패-종료(이하 fail-stop)이라 한다.

비잔틴 장애 허용이 가능한 상황에서는 악의적 노드의 비율을 고려하여 합의하기 위한 다수의 브로드캐스트를 통한 정확한 데이터 전달 확인 과정이 포함된다. 이러한 상황을 비잔틴 폴트(이하 Byzantine fault)라 한다[9].

프라이빗 블록체인의 대표적 합의 알고리즘으로 Paxos와 Raft, PBFT(Practical Byzantine Fault Tolerance)를 들 수 있다.

이 중 Paxos와 Raft는 fail-stop의 상황을 고려한 합의 알고리즘이며 PBFT는 Byzantine fault의 상황을 고려한 합의 알고리즘이다[10-12].

다. PBFT

PBFT는 비동기 네트워크에서 발생할 수 있는 악의적 노드에 대하여 비잔틴 장애 허용이 가능한 합의 알고리즘으로써 하이퍼 레저와 R3 등에서 적용된 바 있다[4].

PBFT는 총 노드 N개 중 악의를 가진 노드 f개 포함 N=3f+1 이상이면 합의가 가능한 상태의 알고리즘이라 설명할 수 있다[9-10].

PBFT는 Request, Pre-prepare, Prepare, Commit, Reply의 5단계를 거쳐 실행된다[13].

실행 과정은 다음과 같다.

- Request 과정에서는 클라이언트의 상태 변환 요청 메시지 MM을 Primary에 전송한다.

Primary는 해당 Request에 대응하는 Sequencial Number인 i를 생성하여 네트워크의 모든 노드에게(Primary 제외) 메시지를 전송한다.

- Pre-prepare 메시지 구조는 <Pre-pare, V, N, D(MM)>이며 V는 메시지의 View, N은 Sequential Number, D(MM)은 메시지 MM의 description이다.

- Pre-prepare에서 전송한 메시지를 임의의 노드 temp에게 전송한 후 D(MM)과 V, N의 관계를 검증하여 검증결과가 참인 경우 Prepare 메시지를 생성하여 모든 노드에게 검증 내용을 전송한다. Prepare의 메시지 구조는 <Prepare, V, N, D(MM), temp)의 형태이며 temp는 Pre-prepare 메시지 검증 노드의 index이다.

-네트워크에 연결된 각 노드는 Pre-prepare 메시지와 Prepare 메시지를 수집하여 Prepare 메시지가 2f 이상인 경우 prepared certificate 한 후 해당 노드는 prepared the request 상태가 된다. 합의되지 않은 Request는 기각된다.

PBFT는 33%의 장애 허용범위를 가지고 있으며 여러 차례 모든 노드에 메시지를 브로드캐스트 하는 등의 합의 과정을 통하여 블록생성의 정확성을 보장할 수 있으나 네트워크에 참여하는 노드가 증가할 경우 네트워크 통신 속도가 느려질 수 있다는 단점이 있다.

라. 합의 알고리즘의 속성

일반적으로 합의 알고리즘은 Safety와 Liveness의 시스템 속성에 대한 시스템 손실을 최소화하는 것이 목적이다. 하지만 비동기 네트워크상에서는 아래의 속성을 모두 만족하는 합의 알고리즘은 없음이 증명되었다[14].

표 1. 합의 알고리즘의 속성[4]

Property	Contents	Performance Evaluation
Safety	All normal nodes must share the same content for the transaction.	Consistency of agreement
Liveness	All nodes must be alive, and if there is no problem with the content of the agreement (block), then an agreement must be made.	Recognition of all created and agreed blocks

위에서 설명한 블록체인의 합의 알고리즘 중 퍼블릭 블록체인 합의 알고리즘의 대부분은 Safety와 Liveness를 고루 만족시킬 수 있도록 고안되었고 이 중 Liveness를 보장하기 위하여 분기(Fork)를 선택할 수 있도록 하였다.

퍼블릭 블록체인의 합의 알고리즘과 같은 경우 분기를 선택할 수 있게 함으로써 블록체인의 신뢰를 떨어뜨릴 수 있으며 프라이빗 블록체인은 Liveness를 희생함으로 Safety를 보장하고 최종적으로 블록체인의 최종성(Finalty)을 보장할 수 있다[4].

III. MPBFT의 제안과 성능평가

1. 연구의 개요

본 논문에서는 프라이빗 환경이 허가된 정직한 노드만으로 구성되었다는 환경적 특징을 고려하여 합의 알고리즘의 만족 조건 중 Safety의 최적화를 지향하고 네트워크 비용의 효율적 운영이 가능한 상태를 목표로 한 합의 알고리즘을 제안하였다.

제안한 내용을 토대로 블록체인 네트워크의 비용 효율성 및 안정성을 유지할 수 있도록 하였으며 이를 위하여 기존의 프라이빗 블록체인의 대표 합의 알고리즘인 PBFT를 수정한 MPBFT(Modified PBFT)를 제안하였다.

먼저, 2장에서 살펴본 PBFT의 합의 알고리즘의 처리 과정에서 나타나는 합의 조건과 네트워크 통신비용을 다음과 같이 정리할 수 있다.

가. 기존 합의알고리즘의 성능

(1) 합의를 위한 노드의 개수

PBFT 과정에서 합의를 위한 조건은 다음과 같이 계산된다.

메시지 전달 오류를 가진 노드 f에 대하여 N-f 만족 시 합의 가능하다.

위의 경우를 포함 (N-f)개의 노드 중 비잔틴 장군 문제가 있는 악의적 노드 f에 대하여 (N-f)-f>f인 상황을 만족해야 한다.

따라서 N>3f의 상황으로 PBFT는 합의 상황을 도출할 수 있다.

(2) 합의 과정에서 발생하는 네트워크 통신비

PBFT의 네트워크 통신비는 다음과 같이 계산된다.

Prepare에서 모든 노드에게 브로드캐스트 한다. 이후 Commit 과정에서 모든 노드에게 브로드캐스트 한다. 따라서 해당 과정에서 발생하는 네트워크 통신비용을 $2N^2$으로 계산할 수 있다.

(3) PBFT 합의 알고리즘의 특징

위의 정리로 알아본 PBFT 합의 알고리즘의 처리 시 발생하는 특징은 다음과 같다.

- PBFT는 블록체인 합의를 위한 두 가지 조건인 Safety와 liveness 중 Safety의 조건을 만족시키기 위한 합의 조건으로 N=3f+1을 고려하였으며 이를 통하여 33.3%의 Liveness를 희생하였다.
- PBFT 합의 알고리즘은 블록체인 네트워크 참여 노드의 수가 증가되면 네트워크 통신비용 역시 증가하게 되어 비용의 부담이 발생한다.

나. MPBFT

본 논문에서 제안한 MPBFT의 핵심 고려사항은 프라이빗 블록체인의 환경이다.

신뢰 기반 노드들로만 구성된 프라이빗 네트워크의 특징을 적극 활용하여 블록체인 네트워크에 허가된 정직한 노드만이 존재한다는 가정을 기본으로 하여 Safety와 처리과정의 단순화를 제안하였다.

MPBFT는 노드 간 신뢰를 기반으로 네트워크의 통신비용을 효율적으로 관리하기 위하여 기존 PBFT의 처리과정 중 Prepare와 Commit 과정에서 발생하는 브로드캐스트의 수를 최소화하고 그 과정을 신뢰기반으로 처리하기 위하여 투표를 통하여 선출된 N/2의 노드가 PL_ID(PBFT Leader ID)가 된다. PL_ID 선출 및 Primary 재선출의 프로세스는 다음과 같다.

① 0th node becomes Primary.

② Primary designates N / 2 Random node as PL_ID and designates the remaining N / 2 node as Follower, and delivers the relevant message to all nodes.

-If: If there is no 'permit' reception from the node designated as PL_ID, or if communication between PL_IDs is lost,

③ Re-elect PL_ID

- candidate conversion process

Convert entire Follower to Candidate

Select as many PL_IDs as needed during the calendar.

- Election Process

The candidate who voted first is selected as PL_ID.

④ In case of primary error, process same as above process.

그림 3. 대표노드 선출 알고리즘

제안하는 MPBFT의 처리 과정은 다음과 같다.

assumption:
Network configuration with authorized honest nodes

Request occurred:
-The client sends the request message MM requesting state transition to the primary node.
-Network communication cost: 1 (constant)

Pre-prepare treatment:
Generate a sequential number N corresponding to the request
-Select PL_ID (PBFT_Leader) by voting
Message <Pre-pare, V (View The message is being sent), N, D (Descriotion of message), PLID) to node 2 / N, and message <Pre-pare, Random Node Id> to 2 / N send
Network communication cost: N-1

Prepare processing:
-Node of the requested random number sends <Prepare, V, N, D (MM), PL_ID) to PL_ID
Network communication cost: 2 / N-1

Commit:
-PL_ID transmits the verification to PL_ID and Primary
-Primary sends all nodes verified
Network communication cost: 2 / N

Reply:
Send the result of request to Client
-Network communication cost: 1 (constant)

그림 4. MPBFT 처리 과정

위와 같은 처리 과정을 통하여 MPBFT 처리가 가능하며 비잔틴 결합 허용 비율 및 노드 수 증가에 따른 네트워크 통신의 효율적 활용이 가능하다.

2. 성능평가

MPBFT를 적용하였을 경우 합의 노드 비율과 네트워크 통신 비용을 수식(3)과 같이 계산할 수 있다.

합의 노드 비율은 기존 PBFT에서 악의 노드를 가정하고 33%의 Liveness를 희생하였으나 본 논문에서는 허가된 정직한 노드들만의 구성을 가정한다.

단 노드 자체의 결함에 의한 오류의 발생을 염두에 둔다.

가. 합의 노드 비율의 우수성

$$2/N = 3f+1$$
$$N=6f+2$$
$$FT >= 16.6666..\% \quad (3)$$

이를 통하여 PBFT는 33.3%의 노드 희생이 필요하고 MPBFT는 16.7%의 희생이 필요한 것으로 계산된다.

표 2. Fault Tolerance Comparison

Node	PBFT	MPBFT
4	1.332	0.66664
5	1.665	0.8333
6	1.998	0.99996
7	2.331	1.16662
8	2.664	1.33328

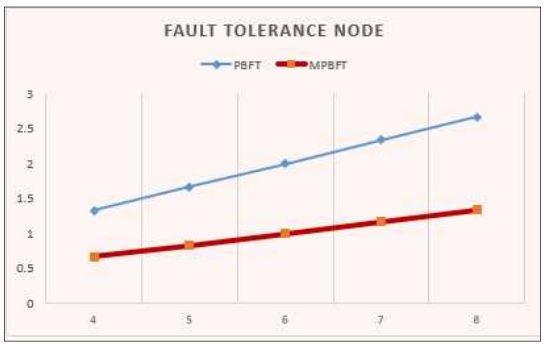

그림 5. Fault Tolerance Comparison

나. 네트워크 통신비용 (N_2C, Network Communication Cost)

$$N\_2C = N-1+1+(N/2)*2 - 1 +1$$
$$N\_2C=2N \quad (4)$$

이를 통하여 PBFT는 $2N^2$의 네트워크 통신비용이 필요하고 MPBFT는 2N의 통신비용이 필요한 것으로 계산된다.

표 3. Network Communication Cost Comparison

Node	PBFT	MPBFT
1	2	2
2	8	4
3	18	6
4	32	8
5	50	10

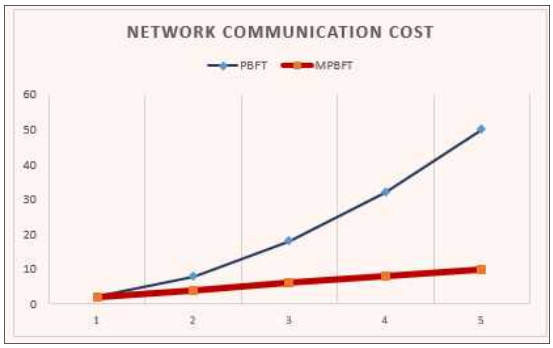

그림 6. Network Communication Cost Comparison

다. TPS

위의 계산식을 토대로 제안 내용의 성능평가를 위하여 블록체인 네트워크의 노드의 수를 조절하며 PBFT와 본 논문에서 제안한 MPBFT의 초당 트랜잭션 처리량(TPS)를 측정하였다.

측정 결과는 다음과 같다.

표 4. TPS Comparison

Node	PBFT	MPBFT
1	14000	13500
2	10500	13000
3	11500	12000
4	9900	11000
5	1000	9000

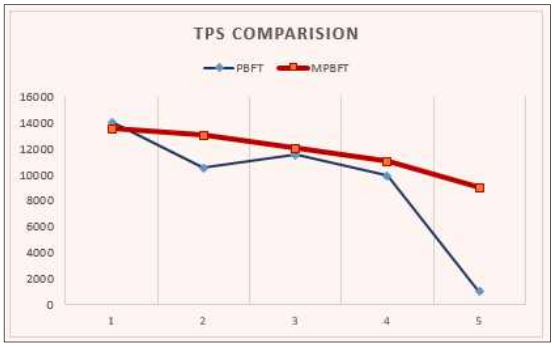

그림 7. TPS Comparison

위의 성능평가를 통하여 제안하는 내용에 대하여 결합 허용 노드 수의 감소 및 네트워크 비용의 감소, TPS의 증가를 확인할 수 있다.

Ⅳ. 결 론

4차 산업혁명의 핵심기술로 부상하고 있는 블록체인은 암호화폐의 활용을 넘어 기업과 공공기관의 데이터 관리 및 공유를 위한 새로운 인프라로 자리매김하고 있다.

블록체인 기술 중 합의 알고리즘은 블록체인의 특징인 데이터의 투명한 관리를 위한 핵심기술이다.

기업 및 공공기관에서 주로 활용하는 프라이빗 블록체인은 신뢰기반의 허가된 노드로 네트워크가 구성되며 프라이빗 블록체인의 대표 합의 알고리즘 중 PBFT는 비동기적 네트워크를 고려한 비잔틴 장애 허용을 통하여 기존 퍼블릭 블록체인의 단점이었던 블록의 분기 문제를 해결하였고 정확한 데이터 합의를 이끌어 내기 위하여 여러 차례의 합의 과정을 거친다.

전술한 바와 같이 PBFT는 정확한 데이터 공유를 위하여 네트워크에서 여러 차례 모든 노드들과 통신을 하는 과정을 거친다. 이러한 과정은 노드의 증가에 대하여 네트워크 통신비용의 부담을 줄 수 있다.

본 논문에서는 사용자의 환경적 특성을 고려하여 PBFT 합의 알고리즘에 합의 및 인증을 위한 대표 노드 선출 알고리즘을 추가하여 브로드캐스트 하는 노드의 수를 감소함으로써 네트워크 통신비용의 효율적 활용을 가능하게 하였고 가용 노드의 수를 2/N으로 조절함으로써 비잔틴 결함 허용 노드 비율을 낮출 수 있었다.

또한 네트워크 상 불가피한 돌발 상황이 발생하지 않는다면 PBFT 대비 TPS 역시 증가하는 것을 확인할 수 있었다.

하지만 합의를 위한 사용자의 다양한 환경적 요구 사항 분석이 미흡하며 향후 해당 분야에 대한 연구가 필요하다.

REFERENCES

[1] Bitcoin: A Peer-to-Peer Electronic Cash System(2008), http://nakamotoinstitute.org/static/docs/bitcoin.pdf (accessed Jan., 24, 2020).

[2] Don Tapscott, Alex Tapscott, *Blockchain Revolution*, Eulyoo Publishing Co, 2017.

[3] D.H Lee, H.S Kim, "Analysis of Blockchain Research Trends: Focusing on Consensus Algorithms," *Journal of the Korea Institute of Information Security and Cryptology*, 28(3), pp. 5-10, June 2018.

[4] J.C. Yim, H,Y, Yoo, J.Y. Kwak, S.M. Kim, "Blockchain and Consensus Algorithm," *Electronic and Telecommunications Trends*, vol. 33, no. 1, 2018.

[5] S.H.Yoo, "Safe and Efficient System Construction Using Blockchain Consensus Algorithm in D2D Communication Environment," Ehwa Woman Univ, 2018.

[6] Khan Minhaj Ahmad, Salah Khaled, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[7] Why Private Blockchain(2018), http://internetplus.co.kr/wp/?p=183(accessed Jan, 25, 2020).

[8] Blockchain Revenue by Industry, World Markets: 2017-2025(2018), https://www.tractica.com/newsroom/press-releases/enterprise-blockchain-revenue-to-surpass-20-billion-by-2025/(accessed Jan., 25, 2020).

[9] GUEL CASTRO, BARBARA LISKOV, "Practical Byzantine Fault Tolerance and Proactive Recovery," *OSDI*, pp. 173-186 1999.

[10] L. Lamport, "The Part-Time Parliament," *ACM Trans. Comput. Syst.*, vol. 16, no.2, pp. 133-169, 1998.

[11] L. Lamport, "Paxos Made Simple," *ACM SIGACT News*, vol. 32, no.4, pp. 18-25, 2001.

[12] D. Ongaro, J.K. Ousterhout, "In Search of and Understandable Consensus Algorythm," *USENIX Annu. Technical Conf.*, Philadelphia, PA, USA, pp. 305-319, 2014.

[13] BFT Consensus(2018), https://docs.google.com/presentation/d/10W7gKEvk_6XRIlSdiKwnwP9gVzo5Re5m_24QzLGaqvk/edit (accessed Jan., 25, 2020).

[14] MICHAEL J. FISCHER 'Impossibility of Distributed Consensus with One Faulty Process', 1985.

[15] Yeong-Tae Baek , Youn-A Min, Modified PBFT Study for Effective Convergence of IoT Big Data and Blockchain Technology. *Korean Society of Computer Information*, vol. 28, no. 1, pp. 193-194, 2020.

[16] S.W. Jang, Y.C. Kim, "Study IoT Asset Management System Based on Block-Chain Framework," *Smart media journal*, vol. 33, no. 2, pp. 94-98, 2019.

[17] Woo-Jin Joe, Hyong-Shik Kim, "A Malware Variants Detection Method based on Behavior Similarity," *Smart Media Journal*, vol. 8, no. 4, pp. 25-32, 2019.

저 자 소 개

민연아(정회원)

2013년 동국대학교 컴퓨터공학과 공학박사.
2019~2019년 가천대학교 소프트웨어학과 조교수.
2020년 한양사이버대학교 응용소프트웨어공학과 조교수.

<주관심분야 : 임베디드시스템 보안, 블록체인, IoT>