Journal of KIIT. Vol. 18, No. 4, pp. 101-107, Apr. 30 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.4.101

블록체인 네트워크의 통신비용 효율성을 고려한 PBFT 합의과정 연구

민 연 아*

A Study on PBFT Consensus Process Considering Communication Cost Efficiency of Blockchain Network

Min Youn-A*

요 약

최근 공공기관 및 기업 등에서 데이터의 투명성 및 무결성 보장을 위하여 프라이빗 블록체인을 활용하는 사례가 증가하고 있다. 블록체인의 핵심기술은 합의 알고리즘이며 합의를 통하여 블록체인 네트워크의 모든 노드에게 동일한 데이터를 정확하고 안전하게 저장하고 관리할 수 있다. 프라이빗 블록체인 환경에서 가장 많이 사용되는 합의 알고리즘인 PBFT(Practical Byzantine Fault Tolerance)는 악의를 가진 노드가 네트워크에 존재하여도 안정적인 합의가 가능하도록 설계되었다. 하지만 PBFT는 여러 번 중복되는 브로드캐스트 형식의 검증 및 인증 과정이 필요하며 이러한 PBFT의 처리 프로세스는 네트워크 통신비용을 가중할 수 있다. 본 논문에서는 PBFT의 효율적 네트워크 통신비용 관리를 위하여 Raft의 장점을 일부 적용한 RB_PBFT(Raft Based PBFT) 알고리즘을 제시하였다. 제시한 내용을 통하여 기존 $O(N^2)$의 통신비용을 최대 O(N)으로 비용 절감 가능하며 초당 트랜잭션의 처리량도 향상됨을 확인하였다.

Abstract

Recently, the use of the private blockchain to ensure the transparency and integrity of data in public institutions and enterprises are increasing. The core technology of blockchain is consensus algorithm, and consensus can save and manage the same data accurately and safely to all nodes of blockchain network. PBFT, the most popular consensus algorithm in private blockchain environment, is designed to enable stable consensus even if malicious nodes exist in the network. However, PBFTs require redundant verification and certification processes, which can add to network communication costs. In this paper, we propose RB_PBFT (Raft Based PBFT) algorithm that applies some of the advantages of Raft for efficient network communication cost management of PBFT. Based on the suggested contents, the communication cost of the existing $O(N^2)$ can be reduced to the maximum O(N).

Keywords
blockchian, consensus algorithm

* 한양사이버 대학교 응용소프트웨어공학과 조교수
- ORCID: https://orcid.org/0000-0003-3259-5929

· Received: Mar. 04, 2020, Revised: Mar. 16, 2020, Accepted: Mar. 19, 2020
· Corresponding Author: Min Youn-A
Department of Applied Software Engineering, Hanyang Cyber University, 220 Wangsimniro, Seongdong-gu, Seoul, Korea
Tel.: +82-2-2290-0872, Email: yah0612@naver.com

Ⅰ. 서 론

4차 산업혁명의 핵심기술로 소개되며 차세대 기술로써 인정받은 블록체인은 발표 초기 비트코인과 같은 암호화폐 기술을 위주로 소개되었으나 이더리움(Ethereum), 하이퍼 레저(Hyper ledger)등의 기술의 발전에 힘입어 최근에는 금융, 공유경제, IoT, 물류 등 여러 분야에 걸쳐 활용되고 있다[1].

Grand View Research의 보고서는 블록체인의 2015년 시장규모가 509백만 달러 규모이고 연평균 37.2% 성장을 거듭하여 2027년에는 7,592백만 달러까지 성장할 것으로 전망하였다[2].

블록체인은 분산된 네트워크에 연결된 모든 노드에 동일한 데이터를 분산저장 및 공유하는 기술이다[3].

블록체인은 기록된 내용에 대하여 모든 노드가 동일한 데이터를 저장할 수 있도록 검증하고 합의한다. 이러한 합의 과정은 합의 알고리즘(Consensus algorithm)을 통하여 처리되며 합의 알고리즘을 통하여 데이터의 정확성이 유지되므로 합의 알고리즘은 블록체인의 핵심기술이라 할 만큼 중요하다[4].

블록체인은 사용자 범위에 따라 퍼블릭(Public) 블록체인과 프라이빗(Private) 블록체인으로 구분할 수 있다[4].

퍼블릭 블록체인은 비허가(Permissionless) 방식이라 하며 허가받지 않은 임의의 다수가 참여할 수 있다. 프라이빗 블록체인은 허가(Permissioned) 방식이라 하며 허가된 노드들만의 참여로 이루어진다. 블록체인 플랫폼의 형태가 비허가 또는 허가 방식인지에 따라 사용자 환경이 달라지므로 전혀 다른 형태의 합의 알고리즘을 사용할 수 있다.

비허가 방식의 경우 노드들의 채굴을 위한 과도한 노력과 지분 보유를 요구하는데 반해 허가 방식은 신뢰기반의 노드들만이 참여하기 때문에 채굴 등의 노력이 필요 없으며 선출된 대표 노드들을 통한 인증 및 합의를 통하여 투명한 거래내역 합의가 가능하다.

표 1은 블록체인의 타입에 대하여 표로 정리한 것이다. 본 논문에서는 허가된 사용자들만으로 구성된 프라이빗 블록체인의 합의 알고리즘 중 대표적으로 사용되는 PBFT의 처리 프로세스 및 활용 사례를 살펴보고 PBFT의 단점인 네트워크 통신비용의 효율적 관리를 위하여 수정된 PBFT를 제안한다.

표 1. 블록체인 종류[5]
Table 1. Blockchain type[5]

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 development	Chain, Nasdaq. R3, CEV, Boa. etc

Ⅱ. 연구 배경

최근 공공기관, 기업을 중심으로 프라이빗 블록체인을 활용한 활용이 증가하고 있다. 2장에서는 공공기관의 블록체인 활용 사례와 프라이빗 블록체인의 합의 알고리즘을 상세하게 살펴본다.

2.1 공공기관의 블록체인 활용

Maximize market Research의 2017년 보고서는 공공분야의 블록체인 활용 시장규모에 대하여 2017년 1억 달러에서 2024년에는 75억 달러의 규모로 성장할 것으로 전망하였다[6].

국내 공공기관의 블록체인은 대부분 신원인증, 온라인 투표, 의료 정보 공유, 복지 급여 관련 데이터공유 등이다.

표 2. 공공기관의 블록체인 적용 사례[7]
Table 2. Blockchain application cases of public institutions[7]

Government(local government)	Contents
Police	Build a digital evidence management platform
Rural development administration	Field crop production. Distribution management platform
Ministry of health and Welfare	Welfare benefit redundancy management platform
Busan	Waterworks smart water management system

표 2는 2020년 KISA에서 추진하는 공공기관 블록체인 시범사업의 사례 중 일부이다. 표 2의 사례는 대부분 신뢰기반 노드 간 연결을 기반으로 하는 프라이빗 블록체인 플랫폼을 사용하여 각 노드 간 투명한 데이터 공유, 데이터 이력 관리, 인증 등의 서비스 제공을 목적으로 한다.

최근에는 디지털 ID를 활용하여 블록체인에 도입하는 사례가 소개되었으며 경상남도는 분산형 신원증명(DID)을 기반으로 시민 및 학생카드를 제작하고 공공시설을 활용할 수 있도록 하는 플랫폼을 추진할 예정이다. 공공기관 중 보건복지부는 다수의 정부 지자체와 중복으로 관리되는 서비스에 대한 정부 재정의 효율적 운영을 위하여 중복서비스 지급 지자체 및 정부 부처 간 블록체인으로 연결하여 복지 급여의 중복 지급을 개선할 예정이다.

2.2 프라이빗 블록체인 합의 알고리즘

퍼블릭 블록체인은 모든 노드가 신뢰가 없다는 가정에 기반하며 신뢰가 없는 네트워크에서 신뢰를 유지하는 방법으로 블록 생성 시 작업 증명방식 등과 같이 과도한 노력을 통하여 채굴을 하도록 하여 네트워크의 가치를 지키려는 노력을 한다[8]. 그에 반해 프라이빗 블록체인은 모든 노드가 신뢰를 가지고 있다는 가정에 기반 한다. 따라서 과도한 컴퓨팅 파워나 지분확보를 위한 노력이 필요 없다.

프라이빗 블록체인 합의 알고리즘은 Paxos, Raft, PBFT로 나눌 수 있다[9].

Paxos는 악의적 노드가 존재한다는 가정을 기반으로 하는 fault Tolerance System에서 여러 프로세스들 간에 동일한 값을 정확하게 합의하기 위한 프로토콜이다.

Paxos는 여러 개의 값이 합의를 기다리지만 결국에는 하나의 값이 선택되며 이를 위하여 제안자(Proposer), 투표자(Accepter), 학습자(Learner)의 역할로 나누어진다. Paxos는 여러 단계 역할에 의하여 다중의 합의와 인증이 이루어지므로 정확한 데이터 관리가 가능하다. 하지만 프로토콜 동작이 복잡하고 연산을 위한 노력이 필요하여 많이 적용되지 않는다[9].

Raft는 Paxos의 단점을 보완하여 보다 간단하게 개발되었다. Raft는 클라이언트의 블록 생성 요청에 대하여 선출된 리더(Leader)에 의하여 처리되고 해당 결과가 로그(Log)에 쓰이게 되어 리플리카(Replica)라 불리는 개별 노드에 반영된다. 리더에 오류가 발생할 경우 리더 선출 프로토콜에 의해 빠르게 리더가 재선출 된다는 장점이 있다[10][11].

선출된 리더는 각 리플리카에게 메시지를 전송하며 확인된 결과는 클라이언트에게 Reply 된다. 이 과정에서 리더의 오류 등에 대한 돌발 상황이 발생할 수 있다.

프라이빗 블록체인 환경에서 모든 노드는 신뢰를 가지고 있다고 가정하므로 Raft합의 알고리즘에서 사용하는 리더 선정 및 리더 주도의 합의 과정은 네트워크 통신 시간을 크게 단축할 수 있다는 장점을 지닌다. 그림 1은 Raft 서버 노드간 상태 전이를 나타낸다.

2.3 PBFT

PBFT는 비잔틴 장애 허용을 위하여 비동기적 방식으로 구현되는 프로토콜이다.

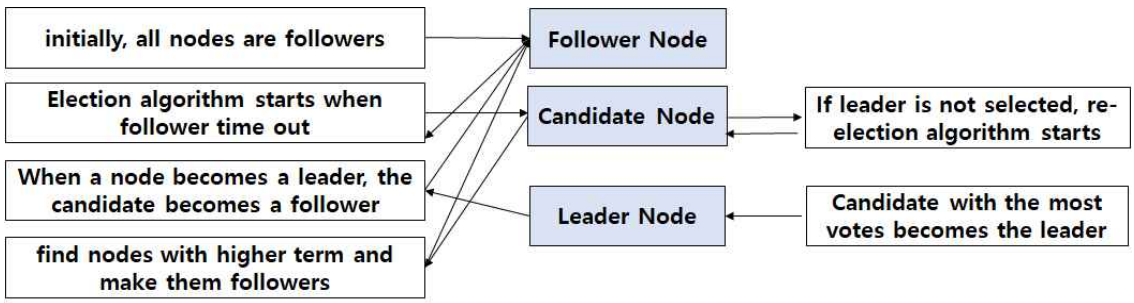

그림 1, Raft 서버 노드 상태 전이[11]
Fig. 1. Raft server node state metastasize[11]

최종 확정성이 보장되며 퍼블릭 블록체인의 합의 알고리즘 보다는 성능이 개선되었지만 합의 과정에서 발생하는 중복 확인 및 인증으로 인하여 인증 시간이 길어질 수 있다[12].

PBFT는 그림과 같이 브로드캐스트 과정이 중복하여 발생하며 이러한 중복 인증 과정을 통하여 네트워크의 전체 노드들과 합의 과정을 거친다.

PBFT의 중복 인증 과정을 통하여 총 노드 수 N에 대하여 발생되는 네트워크 통신비용은 $O(N^2)$이다. N의 증가에 따라 합의를 위하여 거치는 네트워크의 통신비용이 2차 함수로 증가하여 통신비용에 대한 부담이 커진다.

또한 악의를 가진 노드의 수 f에 대하여 N=3f+1의 수식으로 운영되므로 33%의 노드가 반대하거나 투표하지 않으면 시스템이 정지될 수 도 있다[13].

그럼에도 불구하고 PBFT는 IBM, R3 등에서 사용되며 프라이빗 블록체인의 대표적 합의 알고리즘으로 활용되고 있다[13].

PBFT의 장점으로는 유연성과 신뢰성을 들 수 있다. PBFT는 악의를 가진 노드 f에 대하여 3f+1개의 형태가 유지되면 합의가 가능하므로 비잔틴 장애에 유연할 수 있으며 합의를 위한 여러 개의 블록이 존재하지 않기 때문에 Fork가 발생하지 않는다. 또한 한번 연결된 블록이 지속 유지되므로 블록의 신뢰 유지가 가능하다.

PBFT의 단점으로는 최종성을 확보하기 위한 방어의 문제와 통신비용의 부담을 들 수 있다. PBFT의 경우 33%의 노드에 대한 방어가 가능하며 PoW 대비 악의를 가진 노드의 공격에 대한 방어가 불리하다. 또한 PBFT는 네트워크 전체 노드 간 두 번의 브로드 캐스팅이 이루어진다. 따라서 노드 증가 시 네트워크의 통신 부담 비용이 커진다.

III. 블록체인 성능 평가를 위한 요소

3.1 수정된 PBFT 개요

2.3절에서 살펴본 바와 같이 PBFT는 다양한 장점이 존재하는 반면 노드 수 증가에 따라 네트워크 통신비용이 증가한다는 단점을 지닌다.

본 논문에서는 프라이빗 블록체인 환경 기반 허가된 노드에 대한 신뢰를 전제로 하여 기존 PBFT의 기술에 Raft의 리더 선출 알고리즘을 적용한 수정된 PBFT(이하 RB_PBFT, Raft Based PBFT)를 제안하였다.

RB_PBFT의 프로세스는 다음과 같다.

- Request : Client가 모든 노드에게 블록 Confirm을 요청한다.
- Delegate Selection : 선출된 Primary 노드는 연결 노드 중 기존 명성을 고려하여 유효성 검증을 위한 위임자를 선정한다.
- Pre-prepare : Primary 노드는 모든 노드에 블록 Confirm을 요청하고 위임자에게는 별도의 권한을 부여한다.
- Prepare : Replica들의 요청 확인을 취합한다.
- Commit : Replica의 요청 확인 건수와 위임자의 검증 확인에 따라 블록 생성 여부에 대한 상태를 Client에 전달한다.
- Reply : 위임자의 검증 확인을 다른 노드에게 전파한다.

위의 프로세스에 따라 그림 2와 같이 Delegate Selection Pre-prepare 과정을 추가하고 Prepare, Commit 과정에서의 권위가 있는 노드 중심의 인증 과정이 진행된다. 이를 통하여 합의과정에서의 네트워크 통신비용에 대한 부담을 줄이고 인증과정에서의 노드 간 신뢰 확보 및 최종성(Finality)을 보장할 수 있다.

제안 내용은 기존 PBFT 대비 브로드캐스팅을 통한 합의 절차가 간소화됨에 따라 네트워크 통신비용이 최소 O(N)으로 나타낼 수 있다.

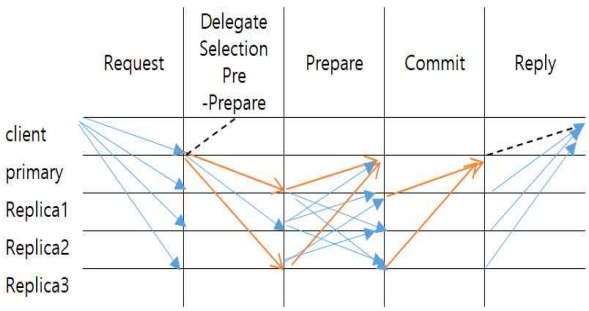

그림 2. RB_PBFT 처리과정
Fig. 2. RB_PBFT process

3.2 성능 평가

본 논문에서는 기존 연구된 수식을 기반으로 수정된 PBFT의 특징인 선출알고리즘을 적용하여 수식을 변형하여 평가할 수 있도록 한다. 따라서 성능평가를 위한 별도의 실험환경은 필요하지 않으며 PBFT와 비교분석을 목적으로 한다.

RB_PBFT의 성능 평가를 위하여 2018년 보고된 연구논문의 평가항목을 참고하였다[2][14].

평가항목으로 권위 있는 노드 비율을 고려한 노드 수 대비 네트워크 통신비용과 초당 트랜잭션의 처리량을 적용하였다. 표 3의 평가요소는 네트워크 통신비용과 TPS이다. 상세 내용은 다음과 같다.

표 3. 성능평가 요소[2][14][15]
Table 3. Performance evaluation factor[2][14][15]

Factor	Measurement content
Network traffic cost against authoritative number of nodes	When calculating network traffic, the formula includes the number of authoritative nodes as variables.
Transaction throughput per second	Measures transaction throughput per second between participating nodes and increases in proportion to the number of authoritative nodes.

① 네트워크 통신비용

전체 노드 수가 N으로 주어졌을 때 노드 간 합의 및 인증건수는 4, 16, 36 …이다.

샘플 데이터를 통하여 R을 통하여 예측치를 계산하였을 때 f(x)=16x - 13.33(≒$2x^2$)를 유도할 수 있다. 동일한 조건에서 RB_PBFT의 네트워크 통신비용을 구하기 위한 수식을 그림 3과 같이 유도하였다.

도출된 수식에 의하여 PBFT와 RB_PBFT의 네트워크 비용 증가량을 확인하기 위하여 다음과 같이 그래프로 노드 수 증가 대비 네트워크 통신비용을 특정하였다.

그림 4는 그림 3의 수식에 대하여 노드수를 1~11까지 증가하며 네트워크 통신비용을 측정한 것이다. RB_PBFT의 경우 PBFT 대비 노드수 증가에 따라 통신비용의 차이가 더욱 큰 것을 알 수 있다.

sampling about
explanatory variable, response variable X, Y
X={1,2,3...}
Y={2.5, 4.1,6.4..}
Find f(x) Model Fitting & training set
f(x)=1.6x + 0.9

그림 3. 데이터 샘플링과 수식도출과정
Fig. 3. Data sampling and formula extraction process

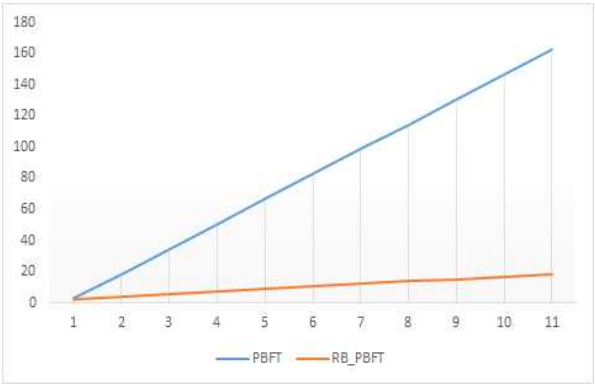

그림 4. 네트워크 통신비용 비교분석
Fig. 4. Network communication cost comparison analysis

② 초당 트랜잭션 처리량

총 노드 수 N에 대하여 블록 생성 시간을 t, 블록의 크기를 s_b, 트랜잭션의 크기를 s_t라 하고 네트워크 비용을 적용하여 다음과 같은 수정된 TPS 계산이 가능하다. 식 (1)은 기존 논문에 제시된 수식[17]을 적용하였으며 제안한 합의 알고리즘에 의하여 합의에 참여하는 노드의 비율인 ①을 반영하였다.

$$((s_b/s_t)*(1/t)) \,/\, network\ cost \quad (1)$$

* network cost : proportional to the number of authorized nodes, delegation time, etc.

위의 수식에 의하여 샘플 데이터를 활용한 PBFT와 RB_PBFT의 처리량 계산 수식을 R을 통하여 예측하고 다음과 같이 도출하였다. PBFT의 샘플 데이터에 의한 수식은 1.5x+3.178e-14((≒1.5x+3.2) 정도에 해당하며 RB_ PBFT는 13x+2의(≒x^2) 수식이 도출된다. 다만 네트워크 상황에 따른 샘플 데이터의 변화 고려가 필요하다.

그림 6은 그림 5의 수식에 대하여 노드수를 1~11까지 증가하여 트랜잭션 처리량을 측정한 것이다.

```
#PBFT
> lm(y.2~x)
Coefficients:
(Intercept)                x
  3.178e-14       1.500e+01
# RB_PBFT
# Let α is Fluid
> lm(y.3~x)
Coefficients:
(Intercept)                x
          2               13
```

그림 5. 트랜잭션 처리량 계산을 위한 수식
Fig. 5. Formula for transaction throughput

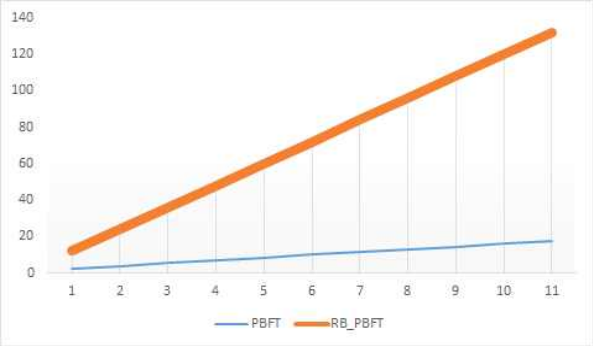

그림 6. 트랜잭션 처리량 비교분석
Fig. 6. Transaction throughput analysis

RB_PBFT의 경우 PBFT 대비 노드수 증가에 따라 트랜잭션 처리량이 더욱 증가함을 알 수 있다. 하지만 본 논문에서 제안한 바와 같이 합의 알고리즘에 참여하는 노드 중 리더의 오류율에 대한 반영이 제외되어 있어 해당 사항을 포함하였을 경우 연산 비용이 증가할 수 있다.

Ⅳ. 결 론

본 논문에서는 대표적인 프라이빗 블록체인의 합의 알고리즘인 PBFT를 수정한 형태인 RB_PBFT를 제안하였다.

RB_PBFT는 PBFT 알고리즘의 장점인 데이터의 정확한 관리와 단점인 네트워크 통신비용 증가의 특징을 고려하여 Raft의 리더 선출 알고리즘을 적용시킨 형태이다. 제안한 내용은 프라이빗 블록체인은 허가된 노드들만 참여하는 네트워크라는 점을 고려하였으며 Raft의 리더 선출 알고리즘에 의하여 기존 PBFT에서 네트워크에 참여하는 모든 노드를 대상으로 진행한 검증 및 인증 과정을 단순화하였다.

RB_PBFT의 성능 평가를 위하여 네트워크 통신비용과 초당 트랜잭션 처리량으로 제한하여 수식을 통하여 PBFT와 RB_PBFT를 비교하였다. 성능 평가 시 권위 있는 노드의 비율이 적용될 수 있도록 기존 수식을 변형하였으며 돌발 상황이 발생하지 않는다는 가정 하에 데이터를 샘플링하고 새로운 수식을 도출하였다. 성능 평가의 결과 네트워크 통신비용은 PBFT 대비 RB_PBFT가 $O(N^2)$과 $O(N)$의 결과로 분석되었으며 초당 트랜잭션 처리량 역시 1.5x와 13x의 비율로 변화됨을 분석하였다.

본 논문의 제한점은 네트워크에서 발생할 수 있는 외부요인과 돌발 상황을 고려하지 않았다는 점이다.

향후 권위 있는 노드의 발굴 및 해당 노드로의 통신에 대한 과부하가 요구될 경우 제시하는 수식에 해당 요인에 대한 변수가 추가되어야 할 것이다.

References

[1] Don Tapscott, "Alex Tapscott, Blockchain Revolution", Eulyoo Publishing Co, 2017.

[2] https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market [accessed: Mar. 03, 2020].

[3] 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. [accessed: Mar. 03, 2020]

[4] https://www.santanderbank.com/ [accessed: Mar. 03, 2020]

[5] Buterin Vitalik, "Ethereum white paper", https://github.com/ethereum/wiki/wiki/%5BKorean%5D-White-Paper. [accessed: Mar. 03, 2020]

[6] Yonatan Sompolinsky and Aviv Zohar, "Secure High-Rate Transaction Processing in Bitcoin", https://fc15.ifca.ai/preproceedings/paper_30.pdf.

[accessed: Mar. 03, 2020]

[7] https://www.kisa.or.kr/notice/bid_View.jsp?cPage=1&mode=view&p_No=35&b_No=35&d_No=6995&ST=&SV= [accessed: Mar. 03, 2020]

[8] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", ttps://git.dhimmel.com/bitcoin-whitepaper/, [accessed: Mar. 03, 2020]

[9] Dongyan Huang, Xiaoli Ma, and Shengli Zhang "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.

[10] Raft.github.io/Raft.pdf [accessed: Mar. 03, 2020]

[11] https://www.geeksforgeeks.org/Raft-consensus-algorithm/ [accessed: Mar. 03, 2020]

[12] Yixin Li, Zhen Wang, Jia Fan, Yili Luo, Chunhua Deng, and Jianwei Ding, "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

[13] Crunchbase, Available: http://www.crunchbase.com [accessed: Mar. 03, 2020]

[14] Jinseok Kim, "A Design of Secure and Efficient PBFT Consensus Algorithm in Blockchain", Master's Thesis for Soongsil University, 2019.

[15] S. H. Yoo, "Blockchain Consensus in D2D Communication Environment Safe and efficient using algorithm", Master Thesis for Ewha Womans University, 2018.

저자소개

민 연 아 (Min Youn-A)

2002년 2월 : 동국대학교 컴퓨터교육학과
2013년 2월 : 동국대학교 컴퓨터공학과 (공학박사)
2016년 ~ 2019년 : 가천대학교 소프트웨어학과 조교수
2020년 1월 ~ 현재 : 한양사이버대학교 응용소프트웨어학과 조교수
관심분야 : 임베디드시스템 보안, 블록체인, IoT