The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 22, No. 2, pp.151-157, Apr. 30, 2022. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2022.22.2.151
JIIBC 2022-2-22

NFT 거래 안정성을 고려한 합의알고리즘 성능분석

Performance Analysis of Consensus Algorithm considering NFT Transaction Stability

민연아*, 임동균**

Youn-A Min*, Dong-Kyun Lim**

요 약 본 논문에서는 NFT 거래 시 거래비용과 처리시간의 증가 및 스마트 계약 실행 시 발생하는 거래 안정성 요구을 높이기 위한 방법으로 다양한 블록체인 합의알고리즘의 성능을 비교 분석하였다. 성능 비교를 위한 평가항목으로 네트워크 신뢰성, TPS, 합의알고리즘의 안정성의 세 가지 평가항목에 대하여 제시하였다. 각 평가항목에 대한 정형화된 식을 수립하기 위하여 연산식에 노드의 신뢰도와 스마트 계약 성공률 등을 변수로 고려하였으며 동일 조건하에 PoW와 Raft, PBFT 세 개 그룹의 합의알고리즘에 대하여 성능을 비교하고 분석하였다. 성능평가 결과 네트워크 신뢰도는 세 그룹의 성능이 유사하였으며 나머지 두 개의 평가항목의 경우 다른 합의알고리즘 대비 PBFT 합의알고리즘이 우수한 것으로 분석되었다. 본 연구의 성능평가 연산식과 결과를 통하여 PBFT 합의 시 본 연구에서 제안한 처리 과정을 합의 과정에 반영하여 처리할 경우 네트워크 신뢰성을 보장하고 합의 알고리즘의 안정성과 경제적 효율성을 높일 수 있는 것으로 분석되었다.

Abstract In this paper, the performance of various blockchain consensus algorithms was compared and analyzed as a method to increase the transaction cost and processing time during NFT transactions and to increase the transaction stability requirements that occur during smart contract execution. Network reliability and TPS are evaluation items for performance comparison. TPS and the stability of the Consensus algorithm are presented for three evaluation items. In order to establish a standardized expression for each evaluation item, the reliability of the node and the success rate of the smart contract were considered as variables in the calculation formula, and the performance of the consensus algorithm of the three groups, PoW/PoS, Paxos/Raft and PBFT, was compared under the same conditions. / analyzed. As a result of the performance evaluation, the network reliability of the three groups was similar, and in the case of the remaining two evaluation items, it was analyzed that the PBFT consensus algorithm was superior to other consensus algorithms. Through the performance evaluation equations and results of this study, it was analyzed that when the PBFT consensus processing process is reflected in the consensus process, the network reliability can be guaranteed and the stability and economic efficiency of the consensus algorithm can be increased.

Key Words : Blockchain, consensus algorithm, NFT(Non Fungible Tokens)

*정회원, 한양사이버대학교 응용소프트웨어공학과
**정회원, 한양사이버대학교 컴퓨터소프트웨어공학과
접수일자 2021년 9월 9일, 수정완료 2022년 3월 3일
게재확정일자 2022년 4월 8일

Received: 9 September, 2021 / Revised: 3 March, 2022 / Accepted: 8 April, 2022
*Corresponding Author: yah0612@hycu.ac.kr
Dept. of Computer Science Engineering, Hanyang Cyber University, Korea

Ⅰ. 서 론

정보통신 기술의 발전에 따라 디지털 콘텐츠 제작 및 거래 활동이 활발해지고 온라인을 통한 디지털 콘텐츠 거래가 증가하며 디지털 콘텐츠 거래 시 발생할 수 있는 다양한 보안 위협 요인을 최소화하고 거래 투명성을 보장하기 위한 관심이 높아지고 있다[1]. 최근 거래의 투명성 보장을 위한 탈중앙화 기술로 블록체인기술에 대한 연구가 한창이다[2]. 블록체인 기술은 거래의 투명성과 정확성 및 무결성 보장이 가능한 기술로써 거래를 위한 네트워크에 포함된 모든 노드에 의해 거래검증 및 합의가 진행되며 거래내역이 공유되어 관리된다[2,3].

블록체인 기술기반 거래를 위한 방법으로 최근 대체불가 코인기반 기술인 NFT(Non Fungible Tokens)에 대한 관심이 높아지고 있다[3]. NFT는 블록체인 이더리움 기술 기반 디지털 자산이다. NFT는 고유한 식별값을 통한 대체불가특성을 지니며 블록체인 고유특징을 기반으로 거래내역에 대한 고유 식별값이 블록체인상에서 관리된다[3,4]. 블록체인의 특징을 기반으로 하기 때문에 NFT기반 거래는 위·변조가 불가능하며 디지털 콘텐츠가 NFT 형태로 거래될 경우 동일 내용 복사 및 합의 없는 거래가 불가하기 때문에 디지털 콘텐츠의 고유한 가치를 관리할 수 있다[4]. NFT 시장분석업체인 넌펑저블(NonFungible)에 의하면 2021년 1분기 NFT 거래 규모는 약 2조 2000억원으로 전분기 대비 22배 증가한 수치이다[5]. NFT를 통하여 거래되는 사례는 다양하다. NFT기반 기술로 디지털 콘텐츠의 고유 가치인증, 오프라인상의 자산관리 등 온·오프라인의 자산에 대한 거래가 가능하다[6]. 향후 다양한 형태의 자산에 대한 투명한 거래기술로 NFT 기술이 제시되기 위해서는 보다 안전한 합의 과정이 필요하다. 본 논문에서는 NFT를 기반으로 디지털 콘텐츠 거래 시 안전성과 익명성을 보장하기 위하여 안정성과 보안 측면을 고려한 다양한 합의알고리즘을 성능 평가 한다.

본 논문의 2장에서는 블록체인과 합의알고리즘을 살펴보고 NFT의 다양한 활용 사례에 대하여 살펴본다. 3장에서는 거래자 메타데이터를 기반으로 블록체인의 다양한 합의알고리즘을 적용하고 거래의 경제적·시간적 효율성 측면을 고려하여 합의알고리즘의 성능을 측정 및 평가 한다.

Ⅱ. 연구배경

1. 블록체인과 합의 알고리즘

가. 블록체인

블록체인 기술은 중앙집중시스템 관리방식을 탈피하여 탈중앙화 방식으로 네트워크에 연결된 모든 노드를 대상으로 트랜잭션 승인과 합의 가능하다는 특징을 가진다[2,7]. 분산원장관리라는 블록체인의 특징으로 인하여 각 노드에서 생성된 트랜잭션 생성 및 거래내역에 대하여 투명한 관리가 가능하며 하다[7].

블록체인 기술은 누구나 블록체인 네트워크 참여가 가능한 퍼블릭 블록체인과 허가된 노드만 네트워크 참여가 가능한 프라이빗 블록체인으로 구분된다. 퍼블릭 블록체인 플랫폼으로 비트코인(Bitcoin)과 이더리움(Ethereum)이 대표적이며 프라이빗 블록체인 플랫폼으로 하이퍼레져 프로젝트(Hyper Ledger Project)가 대표적이다[7-9].

나. 합의알고리즘

블록체인 생성 및 합의를 위한 기술로는 합의알고리즘과 해시함수 등을 들 수 있으며 그 중 합의알고리즘은 블록 생성을 위한 합의 과정에 사용되는 알고리즘이므로 블록체인의 핵심 기술이라 할 수 있다[9].

블록체인 합의 알고리즘은 블록 생성을 위한 합의를 얻기 위한 알고리즘이다[10]. 합의 알고리즘은 블록체인 네트워크에 참여한 모든 노드가 검증과 합의에 참여하는PoW, PoW과 블록 생성 합의를 도출하는 알고리즘과 대표노드 선출과정을 통하여 신뢰를 기반으로 합의과정을 도출하는 리플리카 시스템(replica system) 기반의 PBFT, Raft 알고리즘으로 구분이 가능하다[11]. 리플리카 시스템은 Fail-Stop과 비잔틴폴트(Byzantine Fault)라는 두 가지의 비정상적인 상황을 가질 수 있다. Fail-Stop는 단순한 시스템의 고장을 의미하고 비잔틴폴트는 악의를 지닌 노드에 의해 임의로 동작이 발생할 수 있는 상태를 말한다. Fail-Stop를 고려한 합의알고리즘은 Paxos, Raft이며[12-14]. 비잔틴폴트를 고려한 합의알고리즘은 PBFT이다[15]. 다음 절에서 대표적인 합의 알고리즘인 PoW, PoS, Paxos, PBFT, Raft에 대한 상세 설명을 한다.

1) PoW (Proof of Work)

PoW는 퍼블릭 블록체인에 주로 사용하는 알고리즘으로 비트코인과 이더리움의 합의알고리즘으로 주로 사용한다. PoW는 네트워크상에서 블록생성을 원하는 노드들이 블록 해시값을 만족하는 넌스(Nonce) 값을 찾는 연산을 컴퓨팅파워를 통하여 실행하는 방법이다. 네트워크에 참여한 모든 노드에 의해 합의 과정이 이루어지는 방식이기 때문에 연산을 위한 시간이 다수 소모되며 연산 추진을 위한 처리비용이 소모된다[16]. 또한 PoW를 통한 합의 과정에서 다수의 채굴자가 블록 생성을 위하여 경쟁하므로 컴퓨팅 파워에 대한 부담이 크다. 수식(1)은 PoW의 채굴을 위한 해시함수 hash-f 관련 연산식이다[2,10].

$$hash - f \leq M/D \quad (1)$$

해시함수 hash-f의 값은 M/D보다 작거나 같도록 넌스값을 구하며 이때 사용되는 D는 난이도(difficult)이며 M은 난이도에서 나타낼 수 있는 최대값이다.

PoW는 반복된 연산을 다수 진행하므로 연산량이 많고 모든 노드에 의해 합의가 결정되므로 트랜잭션의 처리시간이 다수 소모된다는 단점이 있다[2,10]. NFT 자산생성을 위하여 사용하는 합의알고리즘의 대부분은 PoW이며 향후 NFT의 효율적 활용을 위해서는 과도한 컴퓨팅파워와 연산 지연 시간에 대한 해결이 필요하다.

2) PoS(Proof of Stake)

PoS는 참여자의 소유 지분에 대한 판단을 근거로 블록 생성에 대한 권한 지분이 결정되는 방식으로써 PoW의 과도한 컴퓨팅파워에 대한 해결이 가능하다[16].

수식(2)는 PoS를 위한 해시함수 hash-f 관련 연산식이다[2,9-10].

$$hash - f(hash - f(B_{prev}), A, T) \leq f2(A)M/D \quad (2)$$

해시함수 hash-f의 변수가 되는 A는 계정을 의미하고 t는 타임 스탬프를 의미하며 B_{prev}는 이전 블록 f2(A)는 A의 지분, M은 최대 난이도, D는 난이도이다. B의 해시값은 A가 보유한 지분의 보유량이 많을수록 난이도가 낮아짐을 알 수 있다. 하지만 PoS는 지분이 많은 소수의 노드의 의해 합의가 도출될 수 있다는 단점이 있으며 만일 해당 노드가 악의를 가진 노드일 경우 더 많은 문제가 발생할 수 있다[2,9-10].

3) Paxos

Paxos는 신뢰할 수 없는 여러 프로세서가 있는 네트워크에서 합의를 위한 알고리즘이다[13,17]. Prepare와 Accepter, Learner의 역할로 구분하여 합의 과정을 도출하며 대표적인 리플리카 시스템의 처리 과정을 가지며 프로토콜의 동작과 연산이 복잡하다[13,17].

4) PBFT(Practical Byzantine Fault Tolerance)

PBFT는 비잔틴장군문제의 해결을 위해 제안된 알고리즘이며 총 노드 N개 중 F개의 오류를 가정하여 N=3F+1의 환경에서 정상적인 동작이 보장된다. PBFT는 여러 개의 리플리카 중 리더(Primary)를 선출하여 합의의 결정을 하도록 하며 리더 오류 발생 시 빠르게 리더 변경이 가능한 알고리즘을 적용한다[15, 18-20].

5) Raft

Raft는 Paxos를 수정하여 쉽게 연산이 가능하도록 고안된 알고리즘이다. Raft는 합의를 위하여 전체 노드가 합의 과정에 참여하는 것이 아니고 리더 노드에 의한 대표 합의가 가능하다. Raft 합의알고리즘 적용 시 클라이언트가 트랜잭션 처리를 요청하면 선출된 하나의 리더가 요청 내용을 복사하여 로그 내용을 전체 노드에 전송하고 전송된 내용을 받은 노드 중 전체의 50%에 해당하는 노드가 수신했음을 확인하면 요청 내용을 확정하는 과정을 거친다. 리더 오류 발생 시 선출프로토콜에 의해 다수 후보노드 중 리더의 선출을 빠르게 갱신하는 과정을 가진다[13-15,19].

2. NFT

블록체인 플랫폼의 한 종류인 이더리움은 암호화폐 기능만을 가진 비트코인과 달리 스마트 컨트랙트를 기반으로 조건에 따라 자동 계약이 가능하기 때문에 다양한 분야에서 활용 가능하다. 이더리움은 ERC-20과 ERC-721 두 종류의 발행 프로토콜이 가능하며 그 중 NFT는 ERC-721의 발행토큰이다. 이더리움 기술기반으로 NFT는 스마트 컨트랙트를 활용하여 발행되고 거래지원이 가능한 플랫폼에 등록되어 거래 가능한 대체 불가능 자산이다. NFT 거래 시 이더리움 스마트 컨트랙트의 가스비(Gas Limit)가 소모되며 거래가 성사되지 않을 경우에도 거래를 위한 물품 등록 비용 및 거래추진 비용 등이 이더리움 가스비로 소모

된다[4, 20].

그림 1은 스마트 컨트랙트를 통한 트랜잭션 처리 시 가스비 소모과정을 나타낸다.

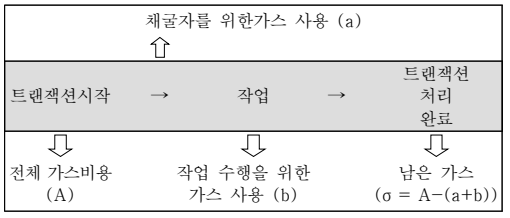

그림 1. 가스 소모과정
Fig. 1. gas consumption process

또한 거래를 위한 합의 과정에서 사용되는 알고리즘이 PoW임을 감안하여 네트워크에 연결된 모든 노드를 통한 합의 과정이 필요하므로 트랜잭션의 최소 거래시간이 최소 15초 이상 소모된다[16-19].

합의 알고리즘으로 PoW와 PoS를 사용하는 비트코인은 평균 7TPS이고 이더리움은 15 ~20TPS이며 Paxos와 Raft, PBFT 등은 평균 1000TPS로 처리 속도는 50~ 100배 정도 차이를 보인다[2,15].

NFT 시장은 2020년 대비 2021년 10배 이상 증가하여 향후 온라인시장의 새로운 자산 시장으로 형성될 것이 유추되고 있으나 그 거래 과정에서 발생하는 시간적, 비용적 부담이 존재한다[16-19]. 또한 NFT 처리 시 이더리움 스마트 컨트랙트 기반의 자동 계약이 사용되므로 스마트 컨트랙트에서 자동 처리될 트랜잭션 및 다양한 변수에 대한 안정성 확보를 위하여 처리 요구자의 정직성과 스마트 컨트랙트 평균 성공률에 대한 안정성 확보가 필요하다[3,20].

Ⅲ. NTF 거래 안정성을 고려한 합의 알고리즘 성능 분석

NFT는 이더리움 기반 스마트 컨트랙트를 사용하여 거래가 진행된다. 이더리움은 퍼블릭 블록체인에 포함되어 네트워크에 참여한 전체 노드에 의해 합의가 진행되는 PoW 합의알고리즘을 주요 적용하므로 경제적. 시간적 손실이 발생한다.

본 논문에서는 NFT에 대한 거래 효율성을 높이기 위하여 다수의 합의알고리즘을 비교·분석하여 NFT 자산을 위한 최적의 합의알고리즘 상태를 연구한다.

본 논문에서는 NFT 자산 거래 시 중요한 요소인 네트워크 신뢰성과 트랜잭션 처리량, 합의 알고리즘의 실행 안정성이 중요한 요소가 될 수 있다. 본 논문에서는 네트워크에 연결된 노드들의 역할을 구분하여 활동 횟수를 확인한다. 전체 수식에서 사용할 변수 중 N은 총 노드 수를 의미하며 a는 활동 횟수가 많은 노드 중 신뢰가 가능한 정직한 노드의 수를 의미한다.

다음과 같이 제안한 성능평가 요소에 대하여 상세 설명한다.

1. 네트워크 신뢰성 평가

합의 알고리즘에서 합의 과정에 참여하는 전체 노드 수는 보통 상수로 표기한다.

노드 정직성을 고려한 네트워크 신뢰성 체크를 위하여 δ= 1/(N/a)를 각 합의알고리즘의 합의 가능 노드 수에 더하여 연산한다. 먼저, PoW와 PoW는 전체 노드수 N에 대하여 50% 이상 확인 후 합의가 가능하므로 N=(N*0.5) * δ이며 Paxos와 Raft는 N = (2f+1) * δ, PBFT는 N=(3f+1) *δ의 식으로 표현 가능하며 a의 증가에 따른 네트워크의 신뢰를 평가할 수 있다.

2. 초당 트랜잭션 처리량(TPS)

프라이빗 블록체인 환경의 특성을 고려하여 다음과 같이 초당 트랜잭션 처리량의 수식을 변경할 수 있다. t는 블록생성 시간이고 B는 블록의 크기, T는 트랜잭션의 크기를 나타낸다. α는 블록 평균 생성시간이며 δ는 합의 가능 노드 수/전체 노드 수를 나타낸다.

$$TPS = ((B/T) \times (1/t) \times (\delta \times \alpha)) \quad (3)$$

수식 (3)은 기존에 공개된 수식[2,10] 에 대하여 a의 비율을 반영하여 계산한다.

3. 합의 알고리즘 실행 안정성

기존 연구[2,10]에서 공개된 블록체인 생성 가능성의 수식을 변형하여 합의 알고리즘 실행 시 안정성 측면을 고려할 수 있다.

해당 수식은 네트워크 내 노드의 정직한 노드의 수와 스마트 컨트랙트 실행 및 실패 여부에 따라 안정성이 증가 또는 감소할 수 있다.

$$Result = 1 - \sum_{b=0}^{a} \frac{c^d e^{-c}}{b!} (1-(q-p)^{(a-b)}) \times s \times \delta \quad \text{v} \quad (4)$$

수식 (4)의 식에서 사용한 변수 중 Result는 합의결정

을 위한 시간을 의미하며 p는 정직한 노드가 블록을 생성할 확률을 의미한다. 또한 q는 악성 노드가 블록을 생성할 확률로 전체 노드에서 p의 확률을 차감하여 연산한다. a는 합의를 대기하는 블록 수이다. σ는 합의를 대기하는 블록 a와 (q / p)를 곱한 값을 대입한다. δ는 실제 연산 시 정직한 노드들의 비율을 의미하며 (정직한 노드의 수 / 모든 노드의 수)로 연산한다. S는 스마트 컨트랙트 실행 성공률을 평균값으로 대입하여 계산한다. PoW는 각각 N=N*0.5의 비율을 가지며 PBFT는 총 노드 수 N과 악의적 의도를 가진 노드 수 f에 대하여 N=3f+1이며 Raft는 N=2f+1임을 고려할 때 각 합의알고리즘의 실행 안정성은 표 1과 같이 정리할 수 있다.

표 1. 합의 알고리즘 실행안정성 평가를 위한 수식
Table 1. Equation for Evaluating Consensus Algorithm Execution Stability

합의 알고리즘	실행 안정성
PoW, PoS	δ*(N / 2) + 1 time
PAXOS, Raft	δ* at least N times
PBFT	δ*(N / 2) + 1 time

합의 가능한 정직한 노드 수에 대한 가중치 δ에 대한 비율이 적용되어 합의를 위한 실행 안정성을 연산할 수 있다.

4. 노드 수에 따른 합의알고리즘 성능 비교

성능평가 항목인 네트워크 신뢰성을 test_1, 초당 트랜잭션 처리량을 test_2, 합의 알고리즘의 실행 안정성을 test_3이라 하였을 때 전술한 성능평가 항목에 대한 수식에 의해 표 2와 같이 합의알고리즘의 성능을 비교한다.

표 2. 합의알고리즘의 성능평가 항목별 수식
Table 2. Equation for each performance evaluation item of each consensus algorithm

항목	public blockchin-PoW	private blockchain -Raft	private blockchain -PBFT
test_1	(N*0.5) *δ	(2f+1)*δ	(3f+1) *δ
test_2	((B/T)*(1/t)*δ	((B/T)*(1/t)*δ	((B/T)*(1/t)*δ
test_3	((N*0.5)*S)*δ	((2f+1)*S)*δ	((3f+1)*S)*δ

전체 노드의 수 N이 평균 10 이상이고, 정직한 노드의 수가 평균 50% 이상일 경우, 블록 생성시간 t의 계산을 위하여 PoW의 t를 1로 보았을 때 리더노드에 의해 빠르게 블록 합의가 가능한 Raft, PBFT는 평균 1/10 이상으로 적용이 가능하다. 또한 스마트 컨트랙트 실행 성공률 S에 대하여, PoW에 1을 대입하였을 경우, 프라이빗 블록체인의 허가된 노드들 간 거래의 경우 실행 및 합의가 빠르게 증가함을 고려하여 PoW 대비 10배 이상으로 적용 가능하다.

네트워크와 노드에 대한 가정이 위와 같을 때 성능 비교에 대한 그래프는 그림 2와 같다.

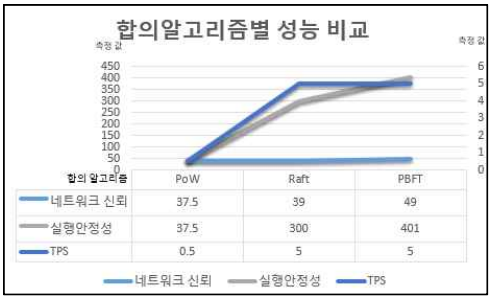

그림 2. 합의알고리즘 성능 비교
Fig. 2. Consensus Algorithm Performance Comparison

그림2와 같이 퍼블릭 블록체인의 대표적인 합의알고리즘인 PoW와 프라이빗 블록체인의 대표적 합의알고리즘인 Raft 및 PBFT를 대상으로 네트워크 신뢰성, 합의알고리즘 실행 안정성, 초당 트랜잭션 처리량의 평가 요소로 성능을 비교한 결과 네트워크 신뢰성 측면에서는 여러 합의알고리즘이 유사한 성능을 보였으나 PBFT가 PoW대비 50% 정도 성능이 좋은 것으로 나타났으며 실행 안정성과 초당 트랜잭션 처리량의 경우 PoW대비, Raft가 10배 이상 우수하고 PBFT는 12-13 우수한 것으로 확인되었다. 해당 실험의 경우

노드 수와 트랜잭션 크기에 비례하여 PBFT의 효율성이 더욱 높아질 것으로 유추할 수 있다.

다양한 사용자 환경에서 제안한 성능평가 요소를 적용함으로써 효율적 합의알고리즘 선택이 가능하다.

Ⅴ. 결 론

디지털 콘텐츠 등 온라인을 통한 거래가 활발해지며 투명하고 정확하며 안정적 환경 기반의 거래에 관심이 높아지고 있다. 최근 NFT를 통한 거래가 증가하고 있다. NFT는 이더리움 기반 PoW 합의알고리즘을 주로 활용하고 있으나 그로 인한 거래비용 및 처리시간의 비효율성에 대한 문제가 발생할 수 있으므로 안정성과 효율성 측면을 고려한 블록체인 합의 알고리즘 제시가 필요하다.

본 논문에서는 NFT 기반 거래에서 시간과 비용 등 경제적 효율성을 높이고 안정성을 보장하기 위한 효율적인 블록체인 합의알고리즘 선정을 위하여 동일한 거래환경에서 거래 합의 시 발생하는 다양한 성능평가항목을 수식의 연산을 통하여 계산하고 성능 평가하였다.

본 논문에서 제시한 성능평가 요소는 네트워크 신뢰성, 초당 트랜잭션 처리량, 합의 알고리즘의 실행 안정성이며 각 항목에 대하여 다양한 합의 알고리즘 성능평가를 위한 수식을 제시하였다. 본 논문에서 제시한 항목은 NFT 거래 및 합의 시 발생 가능한 요구조건에서 중요한 항목이다. 성능평가 항목을 토대로 각 합의알고리즘의 성능을 비교한 결과는 다음과 같다. 네트워크 신뢰성은 전체 노드 중 활동 빈도가 높은 노드 중 정직한 노드의 비율과 해당 비율 대비 합의결정이 가능한 노드의 수를 기반으로 하며 대부분의 합의알고리즘에 대한 큰 편차가 발생하지 않았으나 PBFT가 다소 높게 나타났다. 초당 트랜잭션 처리시간은 블록 생성시간과 트랜잭션의 처리시간을 기반으로 합의 가능 노드 수의 비율을 연산한 것으로 PoW 대비 Raft는 10배 정도 우수한 것으로 평가되었으며 PBFT는 더욱 효율이 우수한 것으로 평가되었다. 합의 알고리즘 실행 안정성은 전체 노드 중 정직한 노드의 비율과 트랜잭션의 성공적 처리를 위한 스마트 컨트랙트 실행 성공률을 수식에 반영하였으며 PoW 대비 Raft는 10배 정도 우수하였으며 Raft와 PBFT는 유사한 성능을 보이는 것으로 평가되었다. 해당 연구를 통해 제안한 성능평가항목에 의한 합의알고리즘 비교 결과 PBFT의 합의 과정을 반영하여 알고리즘 처리 시 네트워크 신뢰성을 보장하고 합의 알고리즘의 안정성과 경제적 효율성을 높일 수 있는 것으로 분석되었다.

본 논문에서는 네트워크 상황에서 발생 가능한 돌발 상황 등에 대해서는 고려하지 않았으나 향후 대표적 돌발 상황을 고려한 추가 연구를 진행할 예정이다.

References

[1] Online Shopping Trends docs – Available : http://kostat.go.kr/portal/korea/eng_nw/1/12/3/index.board

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

[3] Non-fungible tokens (NFT) web-site, Available at : https://ethereum.org/en/nft

[4] Siho Kim, “NFT and Smart Contracts”, 2021 KISA Report, Vol 7, pp.1-9, 2021.

[5] Non fungible Tokens web-site, Available at : http://NonFungible.com

[6] News web-site, Available at : https://www.fnnews.com/news/202105261520512661

[7] Ethereum Smart Contract web-site, Available at : https://ethereum.org/en/developers/docs/smart-contracts/

[8] Youn-A Min, "A study on the Application of Distributed ID Technology based on blockchain for Welfare Blind Spot Management for details in a new window", Journal of the Korea Internet and Communications Society, Issue 6, p. 145-150, 2020.
DOI: https://doi.org/10.7236/JIIBc.2020.20.6.145

[9] Alrumaih et al., “Introducing contemporary blockchain Platforms”, International Journal of computer Science & Network Security, Vol.21, No.4, pp.9-18, 2021.
DOI: 10.15813/kmr.2018.19.4.007

[10] Youn-A Min, " A study on the performance evaluation items of the private blockchain consensus algorithm considering consensus stability", Journal of the Korea Society of computer and Information, Vol.25, No.4, pp.71-77, 2020.
DOI: https://doi.org/10.9708/JKScI.2020.25.04.071

[11] Zheng, Kai et al., “Model checking PBFT consensus Mechanism in Healthcare blockchain Network”, International conference on Information Technology in Medicine and Education, pp.877-881, 2018.
DOI: 10.1109/ITME.2018.00196

[12] L. Lamport et al., “The Part-Time Parliament”, AoM

Books, pp.277-317, 2019.
DOI:10.1145/3335772.3335939

[13] Liu, Yanhong A et al., "Moderately complex Paxos Made Simple: High-Level Executable Specification of Distributed Algorithms", Proceedings of the 21st International Symposium on Principles and Practice of Declarative Programming, pp. 1-15, 2019.
DOI: http://dx.doi.org/10.1145/3354166.3354180

[14] Huang, D. et al., "performance Analysis of the Raft consensus Algorithm for Private blockchains", IEEE Transactions, Vol.50, No.1, pp.172-181, 2020.
DOI: 10.1109/TSMc.2019.2895471

[15] Konczak, J. et al., "Recovery Algorithms for Paxos-Based State Machine Replication", IEEE Transactions, Vol. 18, No.2, pp.623-640, 2021.
DOI:10.1109/TDSc.2019.2926723

[16] castro, Miguel et al., "Practical byzantine fault tolerance and proactive recovery", AcM Transactions on computer Systems, Vol. 20, No. 4, pp. 398-461, 2002.
DOI:10.1145/571637.571640

[17] L. Lamport, "The Part-Time Parliament", AcM Trans, AcM transactions on computer systems, VOL.16, NO.2, pp. 133-169, 1998.
https://lamport.azurewebsites.net/pubs/lamport-paxos.pdf

[18] Li, Yuxi et al., "An Optimized Byzantine Fault Tolerance Algorithm for consortium blockchain.", Peer-to-Peer Networking & Applications, Vol. 14, Issue 5, pp.2826-2839, 2021.
DOI:10.1007/s12083-021-01103-8

[19] Practical Byzantine Fault Tolerance web-site, Available at : https://www.usenix.org/legacy/events/osdi99/full_papers/castro/castro_html/castro.html

[20] Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and challenges web-site, Available at : https://arxiv.org/abs/2105.07447

저 자 소 개

민 연 아(정회원)

- 2002년 2월 : 동국대학교 컴퓨터교육학과 석사
- 2013년 2월 : 동국대학교 컴퓨터공학과 박사
- 2020년 1월 ~ 현재 한양사이버대학교 응용소프트웨어공학과 조교수
- 관심분야 : Blockchain, NFT, DID

임 동 균(정회원)

- 1987년 2월 한양대학교 전자통신공학과 석사
- 2001년 2월 한양대학교 전자통신공학과 박사
- 2003년 3월 ~ 현재 한양사이버대학교 컴퓨터 소프트웨어 공학부 교수
- 관심분야 : Blockchain, 온라인교육