Journal of Korean Society of Industrial and Systems Engineering
https://doi.org/10.11627/jksie.2022.45.1.001

Vol. 45, No. 1 : 1-9, March 2022
ISSN : 2005-0461 / EISSN : 2287-7975

Decentralization Analysis and Control Model Design for PoN Distributed Consensus Algorithm

Jin Young Choi*† · Young Chang Kim** · Jintae Oh** · Kiyoung Kim**

*Department of Industrial Engineering, Ajou University
**Electronics and Telecommunications Research Institute

PoN 분산합의 알고리즘 탈중앙화 분석 및 제어 모델 설계

최진영*† · 김영창** · 오진태** · 김기영**

*아주대학교 산업공학과
**한국전자통신연구원

The PoN (Proof of Nonce) distributed consensus algorithm basically uses a non-competitive consensus method that can guarantee an equal opportunity for all nodes to participate in the block generation process, and this method was expected to resolve the first trilemma of the blockchain, called the decentralization problem. However, the decentralization performance of the PoN distributed consensus algorithm can be greatly affected by the network transaction transmission delay characteristics of the nodes composing the block chain system. In particular, in the consensus process, differences in network node performance may significantly affect the composition of the congress and committee on a first-come, first-served basis. Therefore, in this paper, we presented a problem by analyzing the decentralization performance of the PoN distributed consensus algorithm, and suggested a fairness control algorithm using a learning-based probabilistic acceptance rule to improve it. In addition, we verified the superiority of the proposed algorithm by conducting a numerical experiment, while considering the block chain systems composed of various heterogeneous characteristic systems with different network transmission delay.

Keywords : Blockchain, Distributed Consensus Algorithm, Trilemma, Decentralization, Nonhomogeneous Network

1. 서 론

4차 산업혁명의 핵심 인프라 기술의 하나인 블록체인은 P2P 네트워크로 연결된 노드들이 분산된 환경에서 트랜잭션 데이터를 공유하고 인증하는 방식으로 블록을 만들고 분산 저장함으로써 데이터의 신뢰성을 제공할 수 있는 기술이다. 이 때, 분산합의 알고리즘은 각 노드들이 생성하는 트랜잭션을 기반으로 블록이 검증되고 생성되는 합의 과정을 제어하는 역할을 수행한다[3, 7, 8].

블록체인 시스템을 효율적으로 구축하기 위해서는 탈중앙화, 확장성, 보안성의 3가지 특징을 동시에 만족시켜야 한다. 그러나 지금까지 제안된 다양한 블록체인 시스템들은 적어도 하나 이상의 부문에서 한계점을 보였으며, 이 세 가지를 블록체인 트릴레마라고 정의하였다[4, 6]. 이 중에서 탈중앙화(Decentralization)는 네트워크에 포함된 모든 노드들이 공정하게 합의에 참여하는 현상을 의미한다. 즉, 블록 생성을 위한 합의에 참여하는 주체가 일부 제한된 노드들에 집중되지 않는 특성이다. 또한, 확장성은 블록체인 노드 수가 증가하더라도 블록체인 성능이 크게 영향을 받지 않는 특성이다. 마지막으로 보안성은 비잔틴 노

Received 15 December 2021; Finally Revised 14 January 2022; Accepted 19 January 2022
† Corresponding Author : choijy@ajou.ac.kr

드와 같은 악의적인 노드의 공격에도 블록이 안전하게 생성되고 저장될 수 있는 특성을 의미한다[6].

이러한 블록체인의 트릴레마를 해결하기 위한 방안으로 PoN(Proof of Nonce) 분산합의 알고리즘이 제안되었다[2, 5]. PoN 분산합의 알고리즘은 분산합의를 위한 합의체(Congress) 선정 단계와 선출된 합의체로부터 위원회(Committee)를 구성하고 블록을 합의하는 단계로 구성된다. 이 때, 기본적으로는 모든 노드에게 공평한 참여 기회를 보장할 수 있는 비경쟁 합의 방식을 사용하며, 이러한 방식은 첫 번째 트릴레마인 탈중앙화 문제를 해결할 수 있을 것으로 기대된다. 또한, 블록 합의 단계에서 교환되는 메시지 복잡도가 $O(n)$ (n은 노드 수)이기 때문에 매우 효율적이며, n이 증가하더라도 높은 수준의 성능을 제공할 수 있는 확장성이 보장될 수 있다. 보안성의 경우, 넌스 체인을 이용한 블록 생성 자격 검증을 통해 제공될 수 있다.

그러나 PoN 분산합의 알고리즘의 탈중앙화 성능은 블록체인을 구성하고 있는 노드들의 네트워크 트랜잭션 전송 지연 특성에 큰 영향을 받을 수 있다. 특히, 합의 과정에서 선착순에 의한 합의체 및 위원회 구성은 네트워크 노드 성능에 따른 차이가 크게 영향을 줄 수도 있다. 따라서 본 논문에서는 PoN 분산합의 알고리즘의 탈중앙화 성능을 분석하여 문제점을 제시하고, 이를 개선하기 위한 학습기반 확률적 채택 규정을 이용한 공정성 제어 알고리즘(FCA-LPAR: Fairness control algorithm using learning-based probabilistic acceptance rule)을 제안하였다. 또한, 다양한 이종 특성 시스템으로 구성된 블록체인 시스템을 고려한 수치 실험을 수행하여 제안된 알고리즘의 우수성을 검증하였다.

본 논문의 구성은 다음과 같다. 먼저 제2장에서는 블록체인 시스템의 탈중앙화 정도를 측정하기 위해서 제안된 다양한 지표를 소개한다. 제3장에서는 PoN 분산합의 알고리즘의 탈중앙화 성능을 분석하고, 이를 개선하기 위한 제어 모델을 설계한다. 재4장에서는 제안된 알고리즘의 성능 검증을 위한 수치 실험을 설명하고, 마지막으로 제5장에서 결론과 향후 연구 방향을 제시한다.

2. 분산합의 알고리즘 탈중앙화 지표

일반적으로 블록체인 시스템의 탈중앙화 정도는 관리 계층(Governance layer)과 네트워크 계층(Network layer)으로 나누어 측정될 수 있다. 관리 계층은 블록 생성을 위한 논리적 합의를 만드는 계층을 의미하며, 분산합의 알고리즘 단계에서 측정할 수 있다. 네트워크 계층은 네트워크 토폴로지(Topology)와 서비스 품질(Quality of Service: QoS)과 같이 네트워크 단계에서 측정될 수 있다. 지금까지 각각에 대해 다음과 같은 탈중앙화 지표가 제안되었다[1].

2.1 관리 계층의 탈중앙화 지표

• 공정성 지표(Fairness metrics)

블록체인 네트워크에서 자원 할당에 대한 결정의 공정성을 측정하는 지표로 식 (1)과 같이 계산된다. 이 때, X는 블록체인 네트워크, N은 노드 수, p_i는 노드 i가 채굴한 블록의 비율을 의미한다. 만일, 모든 노드가 같은 비율로 채굴하였다면 이 값은 1이 되며, 완전히 중앙화되었을 경우 1/N의 값을 가진다.

$$F(X) = \frac{(\sum_{i=1}^{N} p_i)^2}{N\sum_{i=1}^{N} p_i^2} \tag{1}$$

• 엔트로피(Entropy)

엔트로피는 일반적으로 어떤 사건이나 메커니즘의 불확실성이나 무작위성을 정량화하는 지표이지만, 채굴 혹은 합의에 참여한 비율을 이용하여 샤논 엔트로피를 식 (2)와 같이 측정할 수 있다. 채굴이나 합의에 참여한 비율 p_i가 균등하면 엔트로피가 높아지며, 반대로 비균등이면 엔트로피는 낮아진다.

$$H(X) = \sum_{i=1}^{N} -p_i \log(p_i) \tag{2}$$

• 지니 계수(Gini coefficient)

경제학에서 소득 분배의 균등을 측정하는 지표로 사용되는 지니 계수는 합의 참여 또는 채굴 비율 p_i를 이용하여 식 (3)과 같이 불균등 지수를 평가할 수 있다. 만일, 모든 노드의 점유율이 균등할 때 지니 계수는 0이며, 한 개의 노드가 완전히 독점할 경우에는 $1-1/N$의 값을 가진다.

$$G = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} |p_i - p_j|}{2N\sum_{j=1}^{N} p_j} \tag{3}$$

• 거리 측정(Distance measures)

유클리디안 거리 또는 민코프스키 거리 등의 기하학적 최단 거리와 p-norm을 활용하여 탈중앙화를 측정한다. 식 (4)는 유클리디안 거리를 이용한 탈중앙화 지표이며, s_i는 노드 i의 목표 점유율을 나타낸다.

$$ED = \sqrt{\sum_{i=1}^{N} (p_i - s_i)^2} \tag{4}$$

• 유사성 계수(Similarity coefficient)

이 방법은 실제 점유율과 목표 점유율 간의 유사도를

계산하여 탈중앙화를 측정한다. 코사인 유사도는 식 (5)와 같이 표현될 수 있는데, 완전히 탈중앙화되었을 때 0의 값을 갖고 중앙화되었을 때 1의 값을 갖는다. 식 (6)은 KL-발산(divergence)을 이용한 유사성 계수를 계산한 식을 나타내며, 값이 클수록 중앙화 정도가 강하고 낮을수록 탈중앙화가 이루어진 것을 나타낸다. 식에서 P와 S는 각각 p_i와 s_i에 대한 벡터를 나타낸다.

$$Cos(P, S) = \frac{\sum_{i=1}^{N} (p_i, \cdot s_i)}{\sum_{i=1}^{N} p_i \cdot \sum_{i=1}^{N} s_i} \quad (5)$$

$$D_{KL} = (P \| S) \sum_{i=1}^{N} p_i \cdot \log\left(\frac{p_i}{s_i}\right) \quad (6)$$

2.2 네트워크 계층의 탈중앙화 지표

• 연결 중심성(Degree centrality)

블록체인 네트워크의 한 노드가 몇 개의 노드와 직접 연결되어 있는지를 측정하는 지표로서 식 (7)과 같이 나타낼 수 있다. 이 때, a_{ij}는 노드 i가 노드 j에 직접 연결되었는지를 표현하며, 연결되었을 경우 $a_{ij}=1$의 값을 가진다.

$$C_d(n_i) = \frac{\sum_{j=1}^{N} a_{ij}}{N-1} \quad (7)$$

• 사이 중심성(Betweeness centrality)

이 지표는 노드 간의 최단 경로를 이용하는데, 노드 i의 중요성을 다른 두 개의 노드 j와 k의 최단 경로에 노드 i가 포함된 비율을 이용하여 식 (8)과 같이 계산한다. 이 때, $g_{jk}(i)$는 노드 i를 경유하는 노드 j와 노드 k의 최단 거리를 의미하며, g_{jk}는 단순히 노드 j와 노드 k의 최단 거리를 의미한다. 모든 거리는 홉 수(hop count)를 이용하여 계산한다.

$$C_b(n_i) = \frac{\sum_{j=1}^{N} \sum_{k>j}^{N} \frac{g_{jk}(i)}{g_{jk}}}{\frac{1}{2}N(N-1)} \quad (8)$$

• 근접 중심성(Closeness centrality)

이 지표는 중요한 노드일수록 다른 노드들까지의 거리가 짧을 것이라는 가정하에 식 (9)와 같은 식을 이용하여 계산된다. 이 때, $d(n_i, n_j)$는 두 개의 노드 i와 j의 최단 거리를 나타내며, 중심성 척도가 낮을수록 탈중앙화 되었음을 의미한다.

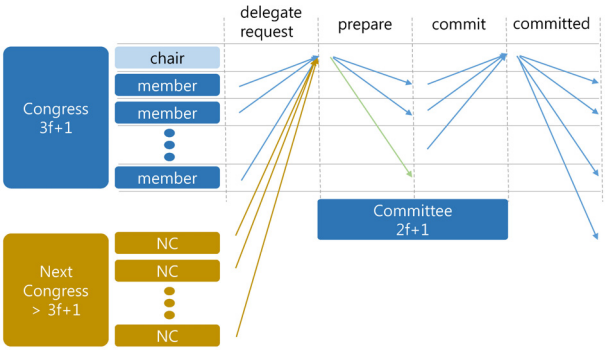
$$C_c(n_i) = \sum_{j=1, j\neq i}^{N} \frac{N-1}{d(n_i, n_j)} \quad (9)$$

3. PoN 분산합의 알고리즘 탈중앙화 성능 분석 및 제어 모델 설계

3.1 특징 및 합의 절차

PoN 분산합의 알고리즘은 PoW(Proof of Work), PoS(Proof of Stake)[8] 등의 기존 분산합의 알고리즘의 한계점으로 지적되고 있는 탈중앙화 문제 및 합의 시간, TPS(Transactions Per Second) 등의 성능을 개선하기 위해서 제안된 효율적인 방법이다. 특히, 넌스 체인을 이용하여 비잔틴 노드가 존재하는 네트워크 환경에서 분산된 노드 간의 합의를 도출할 수 있으며, 모든 노드에 공평한 참여 기회를 보장할 수 있는 비경쟁 합의 방식으로 탈중앙화를 제공한다. 또한 최소 5개의 노드만으로도 블록 합의를 도출할 수 있으며, 합의를 위해 교환되는 메시지 복잡도가 $O(n)$으로 매우 효율적이다. 추가적으로, 합의에 참여하는 노드를 예측하는 것이 불가능하며, 비잔틴 노드 감내 확률도 1.1×10^{-16}으로 매우 큰 보안성을 제공한다[5].

이러한 PoN 분산합의 알고리즘의 블록 합의 과정은 크게 합의체(Congress) 선정 과정과 블록 합의 과정으로 구성된다[2, 5]. 먼저, 합의체 선정 과정에서는 각 노드가 각자 보유하고 있는 넌스 체인을 이용하여 해쉬 함수를 계산하고, 합의에 참여할 수 있는 특정 조건을 만족하는 경우에만 참여 자격을 획득한다. 참여 자격을 획득한 노드들은 의장 노드에게 Next Congress Request(NCR) 메시지를 보내고, 의장 노드는 이러한 요청들 중에 $3f+1$개의 요청을 선착순으로 선정하여 블록 합의를 위한 합의체를 확정한다. 이 때, f는 비잔틴 노드의 수를 나타내며, 매 블록 합의 때마다 새로 구성된 합의체 노드들 중에서 해쉬 값이 가장 작은 노드가 새로운 의장 노드로 선출된다.



<Figure 1> Block Agreement Procedure of PoN

다음으로, 합의체를 이용하여 수행되는 블록 합의 과정은 <Figure 1>과 같이 Delegated Request(DR), Prepare, Commit, Committed의 4단계로 구성되어 있다[5]. 먼저, 합

의체에 포함된 각 노드는 의장 노드에게 DR 메시지를 보낸다. DR 메시지에는 자신의 멤풀(Mempool)에 저장되어 있던 트랜잭션의 번호와 트랜잭션 정보가 포함된다. 의장 노드는 수신된 메시지를 검토한 후, $f+1$개 이상의 메시지에 공통적으로 포함된 트랜잭션 번호와 내용만을 선택하여 최종 블록의 내용으로 확정한다. 두 번째로 Prepare 단계에서는 의장 노드가 수신되는 DR 메시지 중에서 선착순으로 $2f+1$개를 선정하여 이에 해당하는 노드들로 위원회(Committee)를 구성한다. 또한, 위원회에 포함된 노드들에게 확정된 블록의 내용을 포함하는 Prepare 메시지를 전송한다. 이를 수신한 위원회 노드들은 수신된 후보 블록의 내용을 자신들의 멤풀에 있는 트랜잭션과 비교하여 검증한다. 세 번째로 Commit 단계에서는 위원회 노드들이 블록 검증에 대한 다중 서명을 생성하여 의장 노드에게 Commit 메시지를 보내고, 의장 노드는 모든 메시지를 수신한 후 블록을 최종적으로 확정한다. 마지막으로 Committed 단계에서는 의장 노드가 모든 노드들에게 최종 블록을 전파하고, 이를 수신한 노드들은 블록에 포함된 결과를 원장에 반영한다.

3.2 탈중앙화 성능 분석

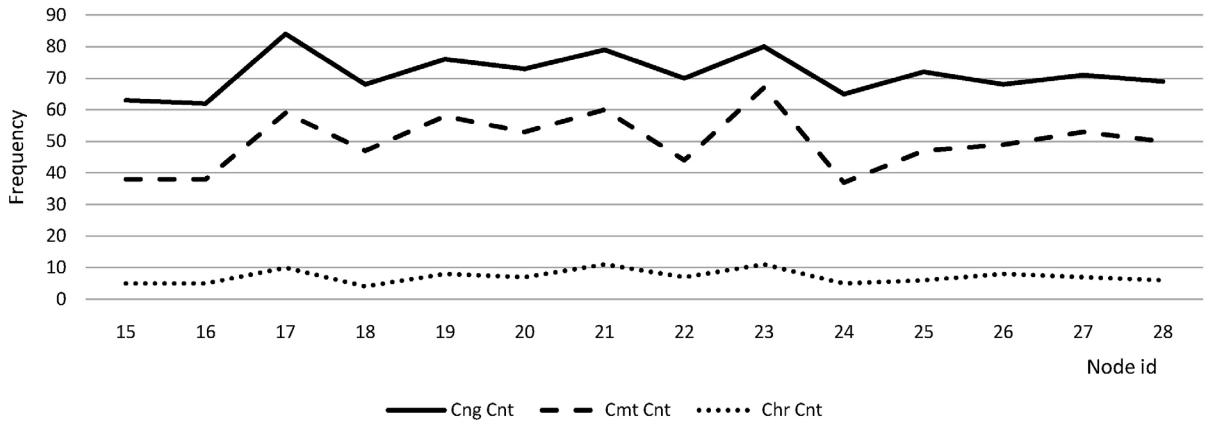
이러한 PoN 분산합의 알고리즘의 블록 합의 과정에서 블록체인 시스템의 중요한 성능 요구 사항인 탈중앙화에 영향을 미치는 여러 요소가 있다. 먼저, 의장의 선출이 랜덤하게 이루어지며, 합의체 구성이 넌스 체인을 이용한 해쉬 함수 계산 결과를 통해 랜덤하게 진행된다. 또한, 최종 블록 확정을 위해 필요한 위원회 구성은 선착순으로 수신된 DR 메시지를 통해 선정이 된다. 이러한 블록 합의를 위해 필요한 요인들의 선출 방식으로 인해 PoN 블록체인 시스템의 탈중앙화 성능은 블록체인 네트워크를 구성하는 노드들의 성능 특성에 많은 영향을 받을 수 있다.

<Table 1> Experimental results for 14 nodes

nodeID	Chr Cnt	Cng Cnt	Cmt Cnt	
15	5	63	38	0.38
16	5	62	38	0.38
17	10	84	59	0.59
18	4	68	47	0.47
19	8	76	58	0.58
20	7	73	53	0.53
21	11	79	60	0.6
22	7	70	44	0.44
23	11	80	67	0.67
24	5	65	37	0.37
25	6	72	47	0.47
26	8	68	49	0.49
27	7	71	53	0.53
28	6	69	50	0.5

따라서 본 논문에서는 이러한 특성을 갖는 PoN 분산합의 알고리즘의 탈중앙화 성능을 평가하기 위해 네트워크를 구성하는 노드들의 성능 특성에 따라 PoN 블록체인 네트워크 시스템을 i) 동종(Homogeneous) 특성 시스템과 ii) 이종(Non-homogeneous) 특성 시스템으로 나누어 실험을 진행하였다. 탈중앙화 성능 평가를 위한 수치 실험은 [2]에서 설계하고 구현한 BADA 분산합의 시뮬레이터를 활용하였는데, 이 시스템은 네트워크로 연결된 다수의 컴퓨터들이 분산 환경에서 <Figure 1>과 같이 정의된 블록 합의 과정을 수행하도록 구현되었다. 또한, PoN 블록체인 시스템의 탈중앙화 성능에 대한 지표는 각 노드들이 최종적으로 블록 합의에 영향을 미치는 위원회에 선정된 비율을 이용하였고, 제2장에서 소개된 다양한 탈중앙화 지표 중에서 공정성 지표를 이용하여 탈중앙화 성능을 평가하였다.

먼저, 동종 특성 시스템으로 구성된 PoN 블록체인 네트



<Figure 2> Participation frequency for 14 nodes

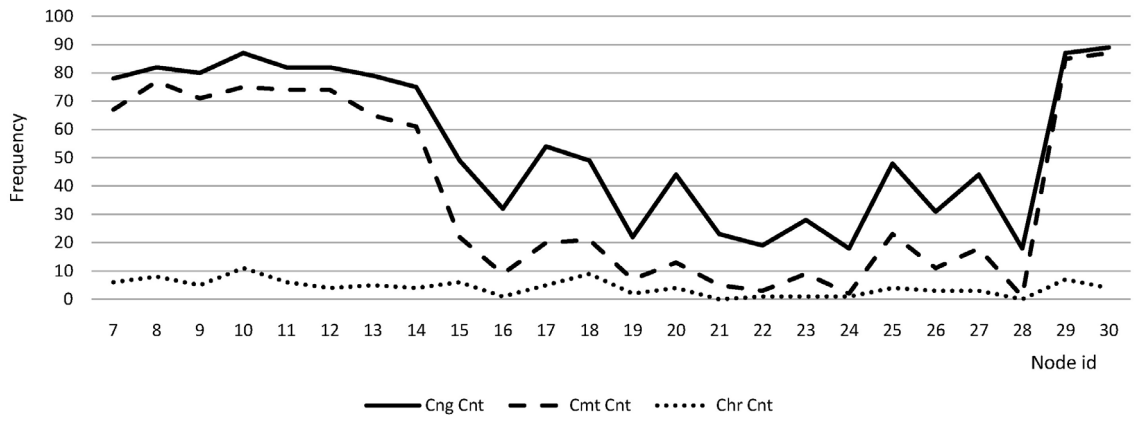
워크에 대한 탈중앙화 성능 평가 수치 실험을 다음과 같이 수행하였다. BADA 분산합의 시뮬레이터에서 동일한 성능 특성을 갖는 14개의 노드들로 블록체인 네트워크를 구성하여 100번의 블록 합의 절차를 진행하였다. 이 때, 블록체인 네트워크에 비잔틴 노드가 어느 정도 존재하더라도 합의에 실패할 확률이 1.1×10^{-16} 보다 작은 것이 보장될 수 있도록 합의체와 위원회를 구성하는 노드의 수를 각각 10개와 7개로 구성하였다[5]. <Figure 2>는 100개 블록의 합의 과정에서 각 노드가 의장, 합의체 및 위원회에 참여한 빈도 수를 나타내며, 각각 Chr Cnt, Cng Cnt, Cmt Cnt로 표현되었다. 그림에서처럼 모든 노드가 동일한 비율을 갖지는 않지만, 어느 정도 유사한 비율로 합의를 위한 과정에 참여하고 있는 것으로 보이며, 이를 통해 탈중앙화 성능이 어느정도 제공됨을 확인할 수 있다.

<Table 1>은 실험 결과로 얻은 값을 나타낸다. 첫 번째 열(nodeID)은 노드 번호, 두 번째 열(Chr Cnt)은 의장에 선출된 횟수, 세 번째 열(Cng Cnt)은 합의체에 포함된 횟수, 네 번째 열 (Cmt Cnt)은 위원회에 포함된 횟수, 마지막 열(p_i)은 위원회에 포함된 비율을 나타낸다. 이 p_i값을 이용하여 탈중앙화 지표를 계산하면, 공정성 지표는 $F(X)=0.97$이다. 따라서, 동종 특성 시스템으로 구성된 블록체인 네트워크에서 PoN 분산합의 알고리즘은 탈중앙성을 제공한다고 할 수 있다.

다음으로, 이종 특성 시스템으로 구성된 PoN 블록체인 네트워크에 대한 탈중앙화 성능 평가 수치 실험을 다음과 같이 수행하였다. 앞에서와 마찬가지로 BADA 분산합의 시뮬레이터에서 24개의 노드들로 블록체인 네트워크를 구성하여 100번의 블록 합의 절차를 진행하였다. 이 중에서 14개의 노드는 앞에서 수행한 동종 특성 시스템에 대한 성능 실험에 사용되었던 동일한 노드이며, 나머지 10개의 노드들은 이들보다 높은 성능을 갖는 유사한 노드들로 구성하였다. 앞에서와 같은 이유로 합의체와 위원회를 구성하는 노드의 수는 각각 13개와 9개로 구성하였다[2]. <Figure 3>은 100개 블록의 합의 과정에서 각 노드가 의장, 합의체 및 위원회에 참여한 빈도수를 나타낸다. 그림에서처럼 의장에 선출되는 비율은 모든 노드가 거의 유사하지만, 합의체와 위원회에 참여하는 비율은 성능이 높은 10개의 노드들(7번 ~ 14번, 29, 30번)이 훨씬 높은 값을 갖는다.

<Table 2> Experimental Results for 24 Nodes

nodeID	Chr Cnt	Cng Cnt	Cmt Cnt	
7	6	78	67	0.67
8	8	82	77	0.77
9	5	80	71	0.71
10	11	87	75	0.75
11	6	82	74	0.74
12	4	82	74	0.74
13	5	79	65	0.65
14	4	75	61	0.61
15	6	49	22	0.22
16	1	32	9	0.09
17	5	54	20	0.2
18	9	49	21	0.21
19	2	22	7	0.07
20	4	44	13	0.13
21	0	23	5	0.05
22	1	19	3	0.03
23	1	28	9	0.09
24	1	18	2	0.02
25	4	48	23	0.23
26	3	31	11	0.11
27	3	44	18	0.18
28	0	18	1	0.01
29	7	87	85	0.85
30	4	89	87	0.87



<Figure 3> Participation frequency for 24 nodes

<Table 2>는 실험 결과로 얻은 의장, 합의체, 위원회에 선출된 횟수와 비율을 나타낸다. 앞에서와 마찬가지로 마지막 열에 있는 p_i 값을 이용하여 탈중앙화 지표를 계산하면 공정성 지표는 $F(X)=0.59$이다. 따라서 이종 특성 시스템으로 구성된 블록체인 네트워크의 경우에 PoN 분산합의 알고리즘은 탈중앙화를 제공하는데 한계점이 있으며 이를 보완하기 위한 방안이 필요하다.

3.3 탈중앙화 제어 모델 설계

이러한 PoN 분산합의 알고리즘의 탈중앙화 한계점을 개선하기 위한 공정성 제어 모델로써 본 논문에서는 학습기반 확률적 채택 규정을 이용한 공정성 제어 알고리즘(FCA-LPAR)을 설계하였다. 제안된 알고리즘은 다음과 같이 (i) 공정성 지표 학습 단계와 (ii) 공정성 제어 단계로 구성된다.

[1단계] 공정성 지표 학습 단계
(ⅰ) 합의체 선정 후, Cng Cnt 업데이트
(ⅱ) 노드 i가 합의체에 선출된 비율 r_i업데이트
(ⅲ) 의장 선출
(ⅳ) 위원회 선출 후, Cmt Cnt 업데이트
(ⅴ) 노드 i가 위원회에 선출된 비율 p_i업데이트
(ⅵ) 탈중앙화 지표 $F(X)$ 업데이트
(ⅶ) $F(X)$가 수렴할 때 학습 종료

[2단계] 공정성 제어 단계
확률적 채택 규정을 적용하면서 위의 세부 절차 (i)~(vi)을 반복적으로 적용

먼저, 공정성 지표 학습 단계에서는 PoN 블록체인 시스템의 블록 합의 과정을 진행하면서 탈중앙화 지수, 즉 노드들이 블록 생성 합의에 직접적으로 관여할 수 있는 합의체와 위원회에 선정된 비율인 r_i와 p_i를 계산한다. 그리고 이를 이용하여 PoN 블록체인 네트워크를 구성하고 있는 노드들의 성능 특성을 반영한 탈중앙화 지표인 $F(X)$를 학습하게 된다.

다음으로, 공정성 제어 단계에서는 확률적 채택 규정을 적용하면서 위의 세부 절차 (i) ~ (vi)을 반복적으로 적용한다. 구체적으로, (i) 합의체 선정과 (iv) 위원회 선출 시, 노드 i가 합의체 또는 위원회 선정 후보이더라도 이를 그대로 수락하지 않고 각각 $1-r_i$와 $1-p_i$의 확률로 수락한다. 거절된 노드는 해당 블록의 생성에 참여할 수 없으며, 의장은 다시 새로운 후보 노드를 선택한다. 만일, 이러한 과정에서 많은 노드가 거절되고, 합의체나 위원회 구성에 꼭 필요한 수만큼의 노드만 남아있다면, 남아있는 모든 노드를 합의체나 위원회로 선출한다. 이 과정에서 r_i와 p_i는 매 블록 생성 시마다 업데이트된다.

이러한 확률적 채택 규정은 합의체 또는 위원회에 적게 선정된 노드들에게 보다 많은 선정 기회를 제공해 줄 수 있다. 이로 인해, 노드 간 공정성의 개선을 유발할 수 있게 되고, 점차적으로 블록체인 네트워크에 참여하는 노드들 간에 탈중앙화가 달성될 수 있도록 할 수 있다.

4. 수치 실험

4.1 실험 설계

본 논문에서 제안된 학습기반 확률적 채택 규정을 이용한 공정성 제어 알고리즘(FCA-LPAR)의 탈중앙화 성능을 평가하기 위한 수치 실험을 위해 이종 특성 시스템으로 구성된 6가지 네트워크 구성 Conf 1부터 Conf 6을 <Table 3>과 같이 설계하였다. 두 번째 열은 각각의 구성(Configuration)에 대해 블록체인 네트워크에 포함된 이종 특성 시스템 그룹의 수를 나타낸다. 각 그룹은 10개의 노드로 구성되며, 세 번째 열은 각각의 구성에 대한 전체 노드 수를 나타낸다. 예를 들면, Conf 1은 그룹 수가 2이므로 20개의 노드로 구성된 2가지 종류의 이종 특성 시스템으로 구성된 블록체인 네트워크를 의미한다. 이 때, 각 그룹 수에 속하는 그룹 번호는 1번부터 시작해서 그룹 수에 해당하는 번호까지 포함하는 것을 가정한다. 즉, 그룹 수가 5이면, 그룹 1 ~ 그룹 5까지로 구성된 이종 특성 시스템이 하나의 블록체인 네트워크를 구성하고 있는 것을 의미한다.

<Table 3> Network Configuration

Config.	# of groups	# of nodes
Conf 1	2	20
Conf 2	3	30
Conf 3	4	40
Conf 4	5	50
Conf 5	10	100
Conf 6	15	150

한편, 수치 실험을 위한 각 노드의 성능을 네트워크 지연시간을 반영한 가중치로 표현하였다. 즉, 가중치가 높은 노드가 고성능을 보유한 것으로 가정하였고, 결과적으로 네트워크 지연이 적어 합의체 구성에 빠르게 지원할 수 있도록 하였다. 구체적으로, 본 논문에서는 이종 특성 시스템 간의 성능 차이를 <Table 4>와 같이 노드 그룹 별

가중치의 차이로 표현하였다. 예를 들면, 그룹 1에 속한 10개의 노드는 $i=1$을 대입하면 1 ~ 5 사이의 값을 가중치로 랜덤하게 가지며, 그룹 2에 속한 10개의 노드는 $i=2$를 대입하면 11 ~ 15 사이의 값을 가중치로 랜덤하게 갖는다. 즉, 그룹 2에 속한 노드들이 그룹 1에 속한 노드들보다 더 좋은 성능을 가진다. 결과적으로, 모든 경우에 대해 그룹 번호가 더 높은 그룹에 속한 노드들의 성능이 더 좋은 결과를 갖게 된다.

<Table 4> Range of weights for group

Group number	Range of weights
Group i	$(10 \times i - 9) \sim (10 \times i - 5)$

4.2 수치 실험 및 결과 분석

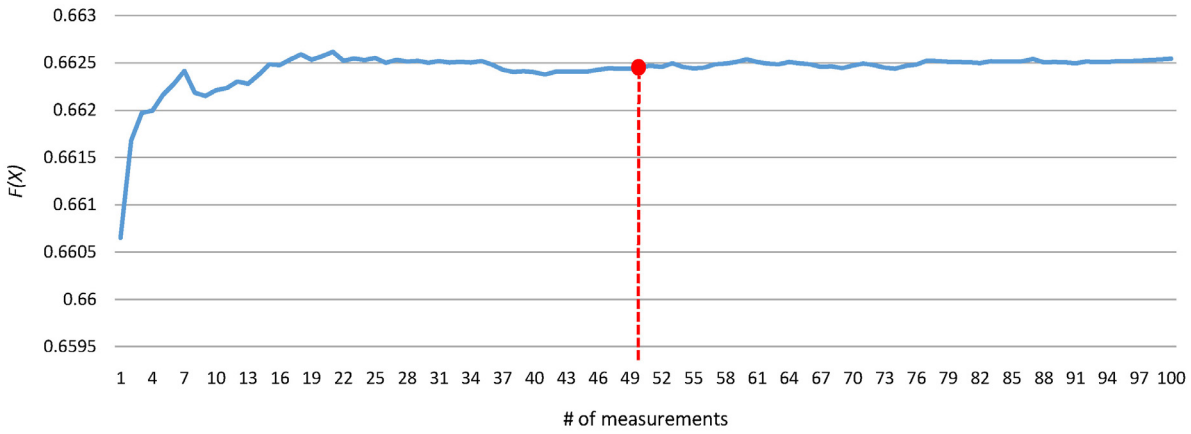
먼저, 이종 특성 시스템으로 구성된 블록체인 네트워크에서 현재의 PoN 분산합의 알고리즘이 공정성 제어 없이 그대로 적용될 때, 탈중앙화 지표가 수렴하기까지 걸리는 시간을 파악하기 위한 실험을 수행하였다. 이를 위해 이종 특성 시스템으로 구성된 블록체인 네트워크를 랜덤하게 구성하고, PoN 분산합의 알고리즘의 탈중앙화 성능 변동을 관찰하였다. 구체적으로, <Table 3>에서 정의된 네트워크 구성 중에서 Conf 2에 해당되는 2개의 그룹(20개의 노드)으로 구성된 이종 특성 시스템에 대해서 100만개의 블록을 생성하였으며, 10,000번 마다 공정성 지표 $F(X)$를 계산하여 기록하였다. 총 20회의 실험을 수행하였으며, <Figure 4>는 100번의 측정치에 대한 결과 그래프의 대표적 예시를 나타낸다. 공정성 지표 값이 수렴하기 전에 변동이 어느 정도 지속되다가 평균적으로 50만개 정도의 블록을 생성한 후에 수렴하는 것으로 파악되었다. 공정성 지표 값도 3.2절에서와 유사하게 0.7 이하의 수준을 보이면서 탈중앙화를 달성할 수 없는 것으로 나타났다. 이를 기반으로 본 논문에서는 제안된 탈중앙화 제어 모델의 1단계인 공정성 지표 학습 단계의 블록 생성 수를 50만개로 정하였다.

다음으로, 제안된 탈중앙화 제어 모델의 성능을 평가하기 위한 실험을 수행하였다. 각 실험 구성에 해당하는 그룹 수를 갖는 이종 특성 시스템으로 구성된 블록체인 네트워크에 대해 랜덤하게 예시(instance)를 30개씩 생성하고, 각 예시에 대해 FCA-LPAR 제어 모델을 결합한 PoN 분산합의 알고리즘을 적용하여 블록 합의를 진행하였다. 제3.3절에서 제안된 알고리즘이 적용되었으며, 1단계인 공정성 지표 학습 단계에서 50만 개의 블록을 생성하면서 노드의 특성을 학습한 후, 2단계인 공정성 제어 단계로 전환되었다. 이때, 평가의 정확성을 높이기 위해서 각 예시에 대한 공정성 지표 값은 10회 반복 평가 후 평균 값을 활용하였다.

또한, 각각의 실험 구성에서 생성된 30개의 예시에 대해 공정성 제어 기능이 없는 PoN 알고리즘을 적용하여 공정성 지표 값을 구하였다. 즉, 각각의 실험 구성에서 동일한 예시에 대해 두 가지 방법, 즉 제어 모델이 적용되는 경우와 적용되지 않는 경우를 각각 적용한 공정성 지표 값을 구하였다. 그리고 그 결과를 이용하여 제안된 FCA-LPAR 제어 모델의 효과를 검증하기 위한 쌍체 t-검정을 수행하였다.

<Table 5> Results of Numerical Experiments

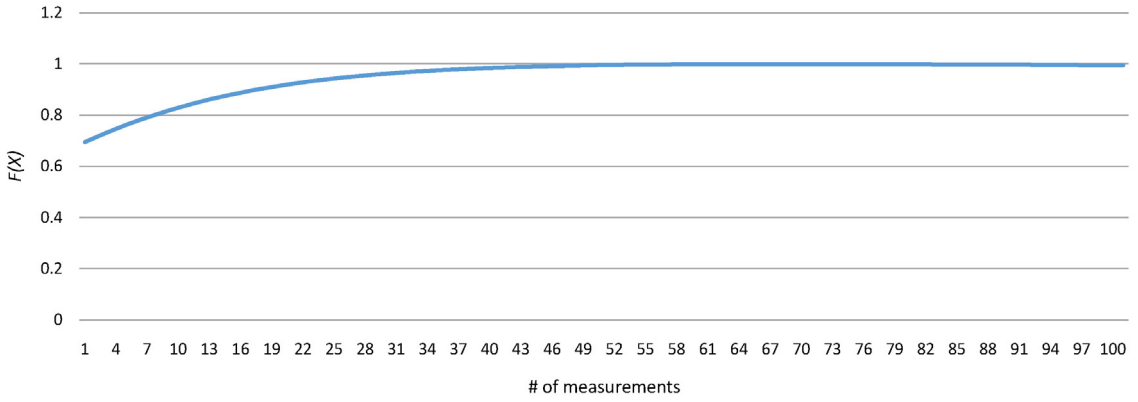
Config.	PoN + PCA-LPAR	PoN w/o control	p-value
Conf 1	0.9960	0.6797	0
Conf 2	0.9929	0.6899	0
Conf 3	0.9924	0.7019	0
Conf 4	0.9909	0.7043	0
Conf 5	0.9884	0.7122	0
Conf 6	0.9871	0.7146	0



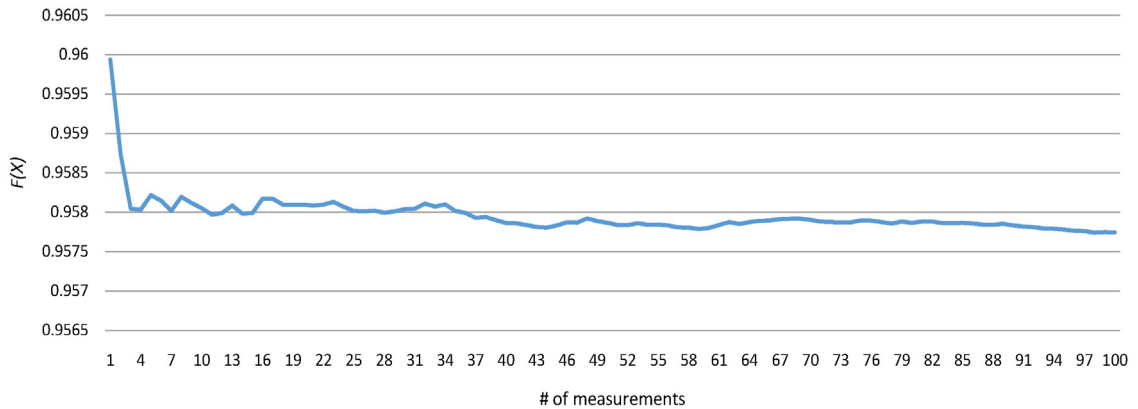
<Figure 4> Fairness variation for PoN without fairness control

<Table 5>는 수치 실험의 결과를 나타낸다. 두 번째 열과 세 번째 열은 각각 FCA-LPAR 제어 모델을 결합시킨 PoN 분산합의 알고리즘과 공정성 제어 기능이 없는 PoN 알고리즘에 대한 공정성 지표 실험 결과로써, 30개의 예시에 대한 평균값을 나타낸다. 마지막 열은 제안된 FCA-LPAR 제어 모델이 우수하다는 가설 검정에 대한 p 값을 나타낸다. Conf 1에서 Conf 6까지의 모든 경우에 대해 제안된 탈중앙화 제어 모델의 탈중앙화 공정성 지표 값 $F(X)$가 0.985 이상이었으며(공정성 지표는 탈중앙화가 높을수록 1에 가까운 값을 가짐), 모든 경우에 대해 p 값이 0이었다. 따라서 제안된 탈중앙화 제어 모델의 성능이 매우 우수함을 검증할 수 있었다. 또한, Conf 5와 Conf 6은 다른 실험 구성에 비해 그룹 수가 2배에서 7배까지 큰 경우인데도 불구하고, 제안된 탈중앙화 제어 모델 성능의 우수함이 지속적으로 유지되었고, 이를 통해 제안된 FCA-LPAR 제어 모델 성능의 확장성도 확인할 수 있었다.

추가적으로, 제안된 제어 모델에서 고려한 공정성 지표의 학습에 대한 효과를 검증하기 위한 실험을 수행하였다. 구체적으로, FCA-LPAR에서 확률적 채택 규정을 적용할 때, 학습을 하고 적용하는 경우와 학습을 하지 않고 적용하는 경우로 나누어 실험을 진행하고 공정성 지표를 비교하였다. 이 때, 학습을 수행하지 않는 경우란 제안된 제어 모델에서 공정성 제어 단계만을 수행하는 경우를 의미한다. 이를 위한 실험은 공정성 지표 수렴 시간 측정에 대한 실험과 마찬가지로, Conf 2에 해당하는 2개의 그룹(20개의 노드)으로 구성된 이종 특성 시스템에 대해서 100만 개의 블록을 생성하였으며, 10,000번 마다 공정성 지표 $F(X)$를 계산하여 기록하였다. <Figure 5>는 실험 결과로 얻은 공정성 지표의 변화를 나타낸다. <Figure 5>의 (a)는 학습을 적용했을 경우의 변화를 나타내는데, 0.7 정도의 값에서 시작해서 점차로 1에 가깝게 수렴하는 것을 볼 수 있다. 반면, <Figure 5>의 (b)는 학습을 적용하지 않는 경우의 변화를 나타내는데, 0.96 정도의 값에서 시작해서 0.957에 가깝게 수렴하는 것을 확인할 수 있다. 실험 결과, 학습을 수행하지 않는 경우에는 최종 공정성 지표의 수렴 값이 0.99에 수렴하지 못하고, 0.95 ~ 0.96 사이에 머무는 것을 확인할 수 있었다. 따라서 제안된 제어 모델에서 고려한 공정성 지표의 학습에 대한 효과가 유효하다고 할 수 있다.



<Figure 5> (a) Fairness variation with learning phase



<Figure 5> (b) Fairness variation without learning phase

5. 결 론

PoN 분산합의 알고리즘은 기본적으로 모든 노드에게 공평한 참여 기회를 보장할 수 있는 비경쟁 합의 방식을 사용하며, 이러한 방식은 블록체인의 첫 번째 트릴레마인 탈중앙화 문제를 해결할 수 있을 것으로 기대되었다. 그러나 PoN 분산합의 알고리즘의 탈중앙화 성능은 블록체인을 구성하고 있는 노드들의 네트워크 트랜잭션 전송 지연 특성에 큰 영향을 받을 수 있다. 특히, 합의 과정에서 선착순에 의한 합의체 및 위원회 구성은 네트워크 노드 성능에 따른 차이가 크게 영향을 줄 수도 있다. 따라서 본 논문에서는 PoN 분산합의 알고리즘의 탈중앙화 성능을 분석하여 문제점을 제시하고, 이를 개선하기 위한 학습기반 확률적 채택 규정을 이용한 공정성 제어 알고리즘(FCA-LPAR)을 제안하였다. 또한, 다양한 이종 특성 시스템으로 구성된 블록체인 시스템을 고려한 수치 실험을 수행하여 제안된 알고리즘의 우수성을 검증하였다.

이러한 연구 결과를 기반으로 PoN 분산합의 알고리즘의 합의체 및 위원회 구성 방식의 다양성을 반영한 효율적 탈중앙화 제공 방안에 대한 연구를 고려할 수 있다. 이에 대한 세부 연구 내용으로 단일 동적 합의체 탈중앙화 정도에 대한 핵심 인자 민감도 분석 및 탈중앙화를 위한 인센티브 적용 구조 설계 등을 추후 연구로 수행하고자 한다.

Acknowledgements

This work was supported by the Institute of Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No. 2021-0-00118, Development of decentralized consensus composition technology for large-scale nodes)

References

[1] Gochhayat, S., Shetty, S., Mukkamala, R., Foytik, P., Kamhoua, G. and Njilla, L. Measuring Decentrality in Blockchain Based Systems, IEEE Access, 2020, Vol.8, 10.1109/ACCESS.2020.3026577.

[2] Kim, Y.C., Kim, K.Y., Oh, J.T., Kim, D.G. and Choi, J.Y., Simulator design and performance analysis of BADA distributed consensus algorithm, *Journal of Society of Korea Industrial and Systems Engineering*, 2020, Vol.43, No.4, 168-177.

[3] Kimani, D., Adams, K., Attah-Boakye, R., Ullah, S., Frecknall-Hughes, J. and Kim, J., Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how?, *Technol Forecast Soc Change*, 2020, Vol. 161, pp. 143-174.

[4] Kwon, Y., Liu, J., Kim, M., Song, D. and Kim, Y., Impossibility of full decentralization in permissionless blockchains, *Proc. 1st ACM Conference on Advances in Financial Technologies*, Zurich, Switzerland, 2019.

[5] Oh, J.T., Park, J.Y., Kim, Y.C., and Kim K.Y., Algorithm based on Byzantine agreement among decentralized agents (BADA), *ETRI Journal*, 2020, pp. 1-14.

[6] Viswanathan, S. and Shah, A. The Scalability Trilemma in Blockchain, https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df, 2018.

[7] Yoo, S. M., 4th industrial revolution and blockchain: Focusing on data economics, *The Journal of The Korean Institute of Communication Sciences*, 2020, Vol. 37, No. 2, pp. 23-30.

[8] Zheng, Z., Xie, S., Dai H., and Wang, H., An overview of blockchain technology: Architecture consensus and future trends, *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Honolulu, USA, 2017, pp. 557-564.

ORCID

Jin Young Choi | http://orcid.org/0000-0001-6397-3107
Young Chang Kim | http://orcid.org/0000-0002-9694-1483
Jintae Oh | http://orcid.org/0000-0002-4372-0943
Ki Young Kim | http://orcid.org/0000-0001-5059-2284