ISSN 1229-1889(Print)
ISSN 2287-9005(Online)
J Korean Soc Qual Manag Vol. 49, No.4: 527-537, December 2021
https://dx.doi.org/10.7469/JKSQM.2021.49.4.527

반응표면분석을 이용한 PoN 블록체인 시스템 합의품질 개선

최진영*† · 김영창** · 오진태** · 김기영**

* 아주대학교 산업공학과
** 한국전자통신연구원

Improvement of Consensus Quality for PoN Blockchain System Using Response Surface Methodology

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

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

ABSTRACT

Purpose: The purpose of this study was to suggest an improved version of Proof-of-Nonce (PoN) algorithm, which is a distributed consensus algorithm used for block chain system.

Methods: First, we used response surface method for design of experiment that is to generate experimental points considering non-linear relationship among variables. Then, we employed overlapped contour plots for visualizing the impact of control variables to performance target.

Results: First, we modified the consensus procedure of the existing PoN algorithm by diminishing the content of the exchanged message. Then, we verified the performance improvement of the new PoN algorithm by performing a numerical experiment and paired t-test. Finally, we established new regression models for consensus time and Transactions per second (TPS) and proposed a method for optimizing control variables for obtaining performance target.

Conclusion: We could improve the performance of the previous version of PoN algorithm by modifying the content of the exchanged message during 4-steps of consensus procedure, which might be a stepping stone for designing an efficient and effective consensus algorithm for blockchain system with dynamic operation environment.

Key Words: Blockchain, Proof-of-Nonce, Distributed Consensus Algorithm, Consensus Qualtiry, Response Surface Method

● Received 9 October 2021, 1st revised 18 October 2021, accepted 19 October 2021
† Corresponding Author(choijy@ajou.ac.kr)

* This work was supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government. [No. 2018-0-00201, Development of High Confidence Information Trading Platform Based on block chain (PON algorithm)]

1. 서 론

최근 들어 블록체인(blockchain) 기술은 디지털 기술과 통신 기술의 발달을 기반으로 금융, 의료, 물류, 교육 등의 다양한 분야에서 신뢰 기반의 데이터 공유 및 인증을 위한 기반 기술로써 활용도가 높아지고 있다(Kimani et al., 2020; Yoo, 2020). 블록체인 기술은 P2P 네트워크를 통해 연결된 모든 노드들이 트랜잭션 데이터를 일정 크기의 블록(block) 형태로 저장하고, 암호화 기술을 통해 저장된 블록들을 연결하여 하나의 체인으로 관리하는 기술이다. 체인에 등록된 블록은 검증 가능하며 비가역적(irreversible) 방법으로 기록되어 있기 때문에 한번 입력된 데이터의 수정이 거의 불가능하게 되고, 이를 통해서 기존의 중앙집중적 관리가 아니라 신뢰를 기반으로 한 데이터 공유 및 더 나아가서는 개인 대 개인의 직접 거래도 가능해질 수 있게 된다. Figure 1은 중앙 기관이 존재하는 중앙집중적 네트워크에서의 트랜잭션 관리 방법과 중앙 기관이 없는 분산된 P2P 네트워크에서의 트랜잭션 관리 방법 간의 차이를 나타낸다. 그림에서 Ledger로 표시된 부분이 트랜잭션 정보가 기록된 원장을 나타내며, 블록체인은 분산된 P2P 네트워크 형태로 구현되어 모든 노드가 이러한 정보를 분산 원장의 형태로 공유한다(Zheng et al., 2017).

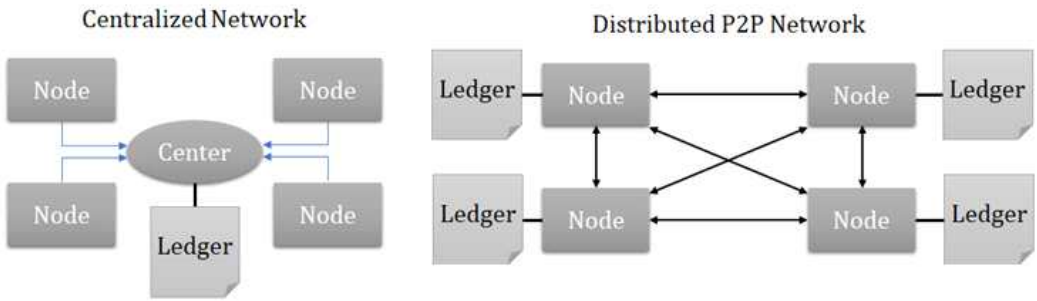

Figure 1. Comparison of centralized network vs. distributed P2P network

이러한 블록체인에서 참여하는 모든 노드가 분산된 원장에 동일한 데이터를 공유하고 저장하기 위해서 사용되는 방법이 분산합의 알고리즘이다. 즉, 분산합의 알고리즘은 분산된 환경에서 각각의 노드들 사이에서 이루어진 트랙잭션에 대한 기록이나 블록 생성 및 검증 등의 과정에서 발생할 수 있는 노드 간 블록 정보의 불일치 문제를 해결해 주는 역할을 수행한다. 분산합의 알고리즘은 블록 생성을 위해 참여할 수 있는 권한을 주는 노드들의 범위에 따라 크게 경쟁적 방법(퍼블릭 블록체인)과 비경쟁적 방법(프라이빗/컨소시움 블록체인)으로 나눌 수 있으며 지금까지 많은 방법들이 제안되었다. 대표적 경쟁적 방식 분산합의 알고리즘으로는 가장 잘 알려진 비트코인이나 이더리움에서 사용하는 작업증명(Proof-of-Work, PoW) 알고리즘(Nakamoto, 2008)과 지분 증명(Proof-of-Stake, PoS) 알고리즘(Buterin, 2013) 등이 있다. 또한, 대표적 비경쟁적 분산합의 알고리즘으로는 비잔틴 노드라 불리는 악의적 노드가 존재할 경우에도 합의를 도출할 수 있는 Practical Byzantine Fault Tolerance(PBFT) 알고리즘(Castro and Liskov, 1999), 위임된 지분 증명(Delegated Proof-of-Stake, DPoS) 알고리즘(Kim et al., 2020) 등이 있다.

그러나 이러한 분산합의 알고리즘들은 각각의 성능 한계점으로 인해 다양한 응용 분야에 범용적으로 사용되기보다는 프라이빗 블록체인의 형태로 제한된 환경에서 사용되는 경우가 많이 있다. 구체적으로, PoW 분산합의 알고리즘은 성능 효율성 지표인 초당 트랜잭션 수(Transactions Per Seconds, TPS)가 최대 7 TPS 정도로 매우 낮고, 10분이라는 긴 합의 시간을 필요로 한다. 이러한 PoW의 단점을 보완하기 위해서 제안된 PoS 분산합의 알고리즘도 수십 TPS 수준의 성능을 갖기 때문에 실시간 서비스 제공에 한계를 갖고 있다. 대표적인 비경쟁적 분산합의 알고리즘

인 PBFT 알고리즘은 합의에 참여하는 노드들의 가 동의하면 합의에 도달할 수 있지만, 합의에 참여하는 모든 노드가 브로드캐스팅을 통해 합의 메시지를 전달하기 때문에 메시지 복잡도가 으로 증가함에 따라 참여 노드의 수가 많아질수록 합의 시간이 증가하고 TPS 성능이 저하된다. 한편, 퍼블릭 블록체인에서 탈중앙화 보장을 위해 제안된 Algorand 알고리즘도 PBFT와 마찬가지로 합의 단계의 메시지 브로드케스팅으로 인해 의 메시지 복잡도를 가지며, 22초의 합의 시간이 소요되어 실시간 서비스 제공에 제약이 따른다(Chen and Micali, 2019).

이러한 기존 분산합의 알고리즘의 한계를 극복하기 위해서 제안된 Proof-of-Nonce(PoN) 분산합의 알고리즘은 각 합의 단계에서 교환되는 메시지 복잡도가 매우 효율적이며, 이를 기반으로 수초 이내의 합의 시간과 수천 TPS 수준의 성능을 제공이 가능하였다(Oh et al., 2020). 그러나 하나의 블록에 포함되는 트랜잭션의 크기와 수가 블록 합의를 위해 필요한 4단계의 합의 과정 동안에 전송되는 메시지 크기에 영향을 미치며, 전체 노드 수 증가로 인한 합의 참여 노드 수의 증가는 발생하는 메시지 총량이나 처리 시간의 증가에 매우 큰 영향을 줄 수 있다. 따라서 본 논문에서는 이를 개선하기 위한 경량화된 PoN 분산합의 알고리즘의 블록 합의 과정을 제안하였으며, 기존 PoN 분산합의 알고리즘과의 성능 비교를 통해 개선 결과를 검증하였다. 또한, 반응표면분석을 이용한 수치 실험을 통해, 제어 인자에 기반하여 성능 목표를 예측하는 비선형 예측 모델을 수립하고, 특정한 성능 목표 조건을 달성하기 위해 최적 인자 조합을 도출하는 방법에 대해서도 제안하였다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 PoN 분산합의 알고리즘의 개요에 대해서 소개한다. 3장에서는 PoN 분산합의 알고리즘의 단점과 이를 개선하기 위한 경량화된 PoN 분산합의 알고리즘의 합의 과정을 기술하고 성능 비교를 수행한다. 4장에서는 제안된 PoN 분산합의 알고리즘의 성능 최적화를 위한 반응표면분석 기반 실험 설계 및 합의 품질 최적화에 대해서 설명하고, 마지막으로 5장에서는 결론과 향후 연구 방향을 제시한다.

2. PoN 분산합의 알고리즘 개요

2.1 트릴레마 특성

PoN 분산합의 알고리즘은 기존에 제안된 다른 분산합의 알고리즘들에 비해 블록체인 트릴레마 이슈를 해결하기 위한 장점을 많이 보유하고 있다. 블록체인 트릴레마란 블록체인 시스템이 기본적으로 제공해야 하는 특성으로서 탈중앙화, 확장성, 보안성으로 정의된다(Viswanathan and Shah, 2018). 탈중앙화는 합의에 참여하는 자격이 일부 노드들에 집중되지 않으며 거래가 발생할 때 중개 권한을 갖는 노드를 거치지 않으면서도 노드 간 거래의 신뢰성을 보장하기 위한 특성이다. PoN 분산합의 알고리즘은 기본적으로 모든 노드가 합의에 참여하는 것이 아니라, 일부 노드로 구성된 합의체(Congress)를 통해 합의를 수행하는 비경쟁적 방식을 제공한다. 이 때, 모든 노드는 합의에 참여하는 자격을 확률적으로 공평하게 얻을 수 있다. 또한, 각각의 노드는 넌스 체인(nonce-chain)을 생성하고, 이를 해쉬 체인(hash-chain)으로 사용하여 합의체 참여를 위한 해쉬 함수 계산에 활용하는 방법을 적용함으로써 합의체 자격 참여 및 검증이 가능한 방법을 제공한다. 따라서 이를 통해 PoN 분산합의 알고리즘은 탈중앙성을 효과적으로 제공할 수 있다(Oh et al., 2020).

확장성은 블록체인 네트워크에 참여하는 노드 수가 증가하더라도 합의 시간 또는 TPS 등의 블록체인 성능에 대한 저하가 크게 발생하지 않는 특성을 나타낸다. PoN 분산합의 알고리즘에서는 블록 합의를 위해서 필요한 최소 위원회의 크기가 5개이며, 합의를 위한 메시지 교환의 복잡도가 으로서 비용 효율적인 네트워크 확장성을 제공할 수 있다. 보안성은 비잔틴 노드와 같은 악의적인 노드의 공격에 대해서 트랜잭션이 왜곡되지 않고 안전하게 저장되어

처리될 수 있는 특성이다. PoN 분산합의 알고리즘에서는 합의를 위한 합의체에 참여한 결과를 어떤 노드도 예측할 수가 없으며, 노드의 수가 증가하거나 비잔틴 노드의 수()가 증가하더라도 합의체 구성이 실패할 확률을 보다 작게 하는 것이 가능하다. 따라서 PoN 분산합의 알고리즘은 Liveness 보장을 위한 비잔틴 공격 또는 장애에 대한 보안성 제공이 가능하다(Oh et al., 2020).

2.2 합의 절차

PoN 분산합의 알고리즘의 합의 절차는 기본적으로 분산합의를 진행하기 위한 합의체를 선출하는 단계와 선출된 합의체로부터 위원회(Committee)를 구성하고 블록을 합의하는 단계로 구성된다(Kim et al., 2020). 합의체 선정 과정에서는 탈중앙와와 보안성 보장을 위해 각각의 노드가 넌스 체인 정보를 공개하고, 이를 이용하여 합의체 참여 자격을 얻는다. 구체적으로 모든 노드가 넌스 체인의 넌스 값을 이용하여 해쉬 함수를 계산하고, 조건을 만족하여 합의체 참여 자격을 얻은 노드들이 의장 노드에게 Next Congress Request(NCR) 메시지를 보내어 합의체 참여 자격을 얻게 되어 최종적으로 개의 노드가 선정된다. 블록 합의 과정에서는 Figure 2와 같이 Delegated Request(DR), Prepare, Commit, Committed의 4단계의 합의 과정을 통해 블록 합의를 달성한다. 먼저, DR 단계에서는 합의체에 선정된 개의 모든 노드가 자신의 멤풀(Mempool)에 저장된 트랜잭션을 의장 노드에게 전달한다. 이 때, 전달되는 트랜잭션에는 트랜잭션 번호(Identification: ID)와 트랜잭션 정보가 포함된다. 의장 노드는 모든 수신된 메시지를 검토하고, 이 중에서 번 이상 공통적으로 포함된 트랜잭션만을 선택하여 최종 블록의 내용으로 확정한다. 또한, 다음 블록의 합의를 위해 모든 노드가 NCR 메시지를 의장 노드에게 보내어 새로운 합의체 구성을 위한 절차도 수행된다.

Prepare 단계에서는 의장 노드가 개의 위원회를 구성하고, 이 노드들에게 Prepare 메시지를 전송한다. 이 메시지에는 의장 노드가 확정한 블록의 내용이 포함되어 있으며, 이를 수신한 위원회 구성 노드들은 수신된 후보 블록을 검증한다. Commit 단계에서는 블록 검증을 완료한 위원회 노드들이 다중 서명을 생성하여 의장 노드에게 Commit 메시지를 보내고, 의장 노드는 이를 통합하여 최종 블록을 생성한다. Committed 단계에서는 의장 노드가 블록체인에 연결된 모든 노드들에게 최종 블록을 전파하고, 블록을 수신한 노드들은 블록에 저장된 결과를 원장에 반영하고 다음 블록 합의를 시작한다.

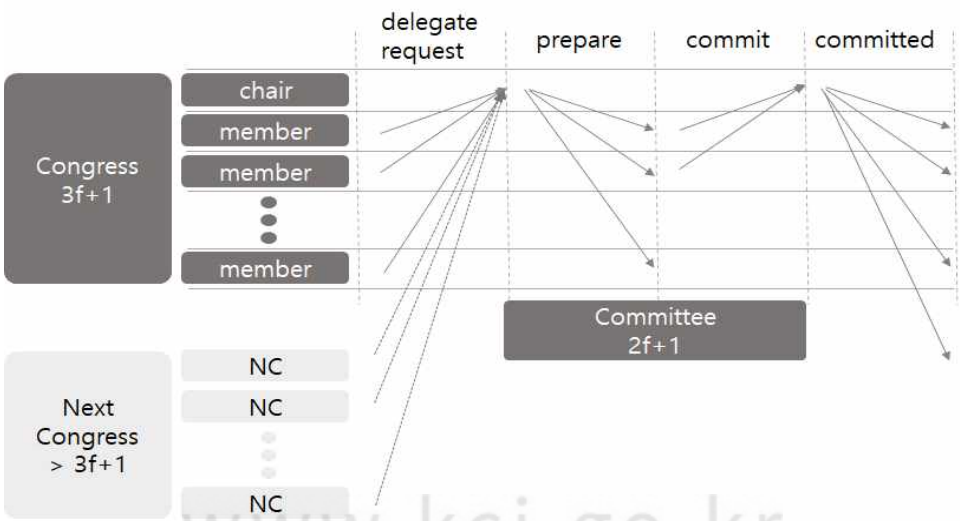

Figure 2. Consensus procedure of PoN algorithm

3. PoN 합의 성능 개선

3.1 개선된 PoN 분산합의 알고리즘

Kim et al.(2020)은 PoN 분산합의 알고리즘의 합의 성능 분석 및 최적화를 위한 연구를 수행하였다. 분산합의 성능에 영향을 줄 수 있는 제어 변수로써 네트워크 노드 수(단위: 개), 트랜잭션 크기(단위: byte), 트랜잭션의 수(단위: 개)를 선택하였으며, 합의 성능으로 합의 시간과 TPS를 고려하였다. 반응표면분석 방법을 적용하여 제어 변수의 실험 조건을 Table 1과 같이 선정하였으며, 네크워크 노드 수에 따른 (i) 트랜잭션 크기와 트랜잭션 수에 대한 합의 시간 및 TPS 예측 모델 수립과 (ii) 합의 시간과 TPS 목표 달성을 위한 트랜잭션 크기 및 트랜잭션 수의 최적화 방안 등을 제안하였다.

Table 1. Levels of design parameters

Variable	Level				
	-1.732	-1	0	1	1.732
Size of transaction (tx_size, X_1)	250	317	409	500	567
The number of transactions (tx_num, X_2)	2,000	2,317	2,750	3,183	3,500
The number of nodes $(node\_num, X_3)$	6	10	15	20	24

그러나 현재의 PoN 분산합의 알고리즘은 합의 과정에서 전송되는 트랜잭션의 크기와 수가 합의 수행을 위해 DR, Prepare, Commit, Committed 단계에서 주고 받는 메시지 크기에 영향을 주며, 전체 노드 수 증가로 인한 합의체와 위원회 크기의 증가는 발생하는 메시지 총량이나 처리 시간의 증가에 매우 큰 영향을 줄 수 있다. 따라서 이에 대한 개선이 필요하며, 본 논문에서는 경량화된 PoN 분산합의 알고리즘의 블록 합의 과정을 제안하였다. 개선된 PoN 분산합의 알고리즘의 블록 합의 단계는 Figure 2와 동일하며, 기존 PoN 알고리즘과 비교할 때 다음과 같은 차이가 있다.

- DR 단계에서 합의체에 포함된 각 노드가 의장 노드에게 자신의 멤풀에 있는 모든 정보를 보내는 것이 아니라, 오직 트랜잭션 ID 리스트만 보낸다.
- Prepare 단계에서 의장 노드는 수신된 트랜잭션 ID 리스트들을 검색하고, 이 중에서 번 이상 공통적으로 포함된 트랜잭션만을 선택한 후, 자신이 보유하고 있는 멤풀의 트랜잭션 ID 리스트와 공통된 것만을 선택하여 최종 블록을 구성하는 트랜잭션 ID 리스트로 확정한다.

3.2 성능 비교

본 논문에서는 먼저 개선된 PoN 분산합의 알고리즘의 성능을 기존 PoN 분산합의 알고리즘의 성능과 비교하기 위한 실험을 수행하였다. 실험 수행을 위한 블록체인 시스템 환경은 Kim et al.(2020)에서 설계하고 구현한 BADA 분산합의 시뮬레이터를 활용하였다. 이 시스템은 네트워크로 연결된 다수의 분산 노드 상에서 합의를 위한 트랜잭션을 생성하고 노드 간에 전달하면서 PoN에서 정의된 합의 과정을 수행할 수 있도록 구현되어 있다. 성능 실험을 위한 응용 서비스는 Kim et al.(2020)에서와 동일하게 금융 거래 기능을 제공하는 Smallbank 블록체인 시스템(Kim et al., 2020)을 고려하였다. Smallbank 트랜잭션은 실제 금융 환경에서 기본적으로 발생하는 6가지 종류의 거래 데이터로 구성되며, 자세한 구성은 Table 2와 같다.

Table 2. Definition of financial service for smallbank

Service name	Description
Balance(N)	Checking the remaining balance of account N
Withdraw(N, V)	Decreasing the balance of account N by V
Deposit(N, V)	Increasing the balance of account N by V
Transfer(N1, N2, V)	Increasing the balance of account N1 and deceasing that of account N2 by V
Merge(N1, N2)	Amalgamating the balance of N1 and N2 into N1

기존 PoN 분산합의 알고리즘을 적용한 Smallbank 블록체인 시스템에 대해 Kim et al.(2020)에서 선정한 반응표면분석 기반 실험점을 이용하여 PoN 분산합의 알고리즘의 합의 시간 및 TPS에 대한 성능 실험을 수행한 결과는 Table 3과 같다. BADA 분산합의 시뮬레이터 구동 환경이 네트워크로 연결된 다수의 분산 노드 상에서 합의를 위한 트랜잭션 생성과 노드 간 전송이 수행되기 때문에 성능 비교의 공정성을 위하여 기존 PoN 알고리즘에 대해서도 동일한 실험점에서 성능 실험을 재수행하였다. 1열은 실험점 번호를 나타내고, 2열~4열은 제어 변수의 값을 나타낸다. 5열~8열은 기존 PoN 알고리즘과 개선된 PoN 알고리즘의 성능을 나타내는데, 각각의 실험점에 대해서 100번의 합의를 수행한 후 측정된 값들의 평균을 구한 결과이다.

Table 3. Experimental results of performance for two versions of PoN

Exp. No.	X_1	X_2	X_3	Perf. of old PoN		Perf. of new PoN	
				y_{11} (Consensus time)	y_{21} (TPS)	y_{12} (Consensus time)	y_{22} (TPS)
1	-1	-1	-1	0.137	2,315	0.125	2,377
2	1	-1	-1	0.161	2,342	0.134	2,349
3	-1	1	-1	0.171	3,202	0.153	3,171
4	1	1	-1	0.199	3,198	0.156	3,211
5	-1	-1	1	0.332	2,310	0.311	2,319
6	1	-1	1	0.399	2,315	0.331	2,321
7	-1	1	1	0.514	3,172	0.393	3,175
8	1	1	1	1.073	3,144	0.453	3,178
9	-1.732	0	0	0.251	2,762	0.214	2,767
10	1.732	0	0	0.343	2,736	0.268	2,754
11	0	-1.732	0	0.209	2,018	0.197	1,998
12	0	1.732	0	0.404	3,492	0.299	3,520
13	0	0	-1.732	0.092	2,760	0.088	2,854
14	0	0	1.732	0.481	2,733	0.395	2,737
15	0	0	0	0.290	2,738	0.238	2,743
16	0	0	0	0.285	2,741	0.234	2,765
17	0	0	0	0.299	2,739	0.238	2,746
18	0	0	0	0.277	2,756	0.241	2,754
19	0	0	0	0.294	2,740	0.232	2,737
20	0	0	0	0.285	2,749	0.237	2,758

개선된 PoN 분산합의 알고리즘의 성능을 검증하기 위해 유의 수준 0.05를 기준으로 가설 검정을 수행하였다. 각각의 실험점에 대해서 개선 전(old PoN)과 후(new PoN)의 성능을 비교하는 것이 목적이기 때문에 쌍체 t-검정(Paired t-test)을 적용하였다. 먼저, 합의 시간에 대한 쌍체 t-검정에서는 i번째 실험점에서의 개선 전과 후에 대한 합의 시간의 차이를 $D_1^i = y_{11}^i - y_{12}^i$라 정의하였다. 이 때, y_{11}^i과 y_{12}^i는 각각 i번째 실험점에서의 개선 전과 후에 대한 합의 시간을 나타낸다. 가설 검정을 위한 귀무가설은 합의 시간에 차이가 없다($H_0 : \mu_{D_1} = 0$)로 하고, 대립가설을 차이 > 0 ($H_1 : \mu_{D_1} > 0$)로 정하였다. 그 결과, p-value = 0.016으로 대립가설이 채택되었으며, 이는 개선된 PoN 알고리즘의 합의 시간이 더 감소했음을 의미한다. 다음으로, TPS에 대한 쌍체 t-검정에서는 i번째 실험점에서의 개선 전과 후에 대한 TPS의 차이를 $D_2^i = y_{21}^i - y_{22}^i$라 정의하였다. 이 때, y_{21}^i과 y_{22}^i는 각각 i번째 실험점에서의 개선 전과 후에 대한 TPS를 나타낸다. 가설 검정을 위한 귀무가설은 TPS에 차이가 없다($H_0 : \mu_{D_2} = 0$)로 하고, 대립가설을 차이 < 0 ($H_1 : \mu_{D_2} < 0$)로 정하였다. 그 결과, p-value = 0.036으로 대립가설이 채택되었으며, 이는 개선된 PoN 알고리즘의 TPS가 증가했음을 의미한다. 따라서 이를 기반으로 경량화된 PoN 알고리즘의 합의 시간과 TPS에 대한 성능이 개선되었음을 검증하였다.

4. 반응표면분석 기반 실험 및 최적화

4.1 반응표면분석 기반 실험점 설계

본 논문에서는 개선된 PoN 분산합의 알고리즘에 대해 네크워크 노드 수에 따른 (i) 트랜잭션 크기와 트랜잭션 수에 대한 새로운 합의 시간 및 TPS 예측 모델 수립과 (ii) 합의 시간과 TPS 목표 달성을 위한 트랜잭션 크기 및 트랜잭션 수의 최적화 방안 등에 대한 연구를 다음과 같이 수행하였다. 먼저, 합의 시간 및 TPS 성능 지표와 핵심 인자 간의 관계를 나타내는 예측 모델 수립을 위해서 제어 인자들의 유의미한 범위를 실험을 통해 정하였다. 블록체인 네트워크에 포함되는 노드의 수는 최소 6개에서 최대 24개까지의 범위로 정하였다. 트랜잭션 크기(단위: byte)의 경우, 비트코인의 트랜잭션 크기인 250 바이트를 기본으로 해서 최대 630 바이트까지 증가할 수 있는 것으로 정하였다. 트랜잭션 수의 경우, 노드 수가 가장 작은 6개일 때, 트랜잭션 크기를 250 바이트로 하면 트랜잭션의 수를 9,000개까지 증가시켜도 합의 시간과 TPS 성능의 저하가 거의 발생하지 않았다. 그러나 노드 수가 증가하거나 트랜잭션 크기가 커지게 되면 9,000개의 트랙잭션을 처리하기 위한 합의 시간과 TPS 성능이 매우 저하되기 때문에 예측 모델 수립에 유의하지 않다. 따라서 본 연구에서는 여러 제어 변수의 다양한 조합에 대해서 실험점을 정하는 반응표면분석에서 유의미한 성능을 갖는 파라메타 범위를 실험에 포함시키도록 하였고, 그 결과 트랜잭션의 수는 3,000 ~ 5,000 개를 기본으로 하여 감소 또는 증가할 수 있도록 하였다.

Table 4. Levels of design parameters for new experiment

Variable	Level				
	-1.732	-1	0	1	1.732
Size of transaction (tx_size, X_1)	250	330	440	550	630
The number of transactions (tx_num, X_2)	5,732	5,000	4,000	3,000	2,268
The number of nodes $(node\_num, X_3)$	6	10	15	20	24

이러한 파라메타 범위를 기반으로 반응표면분석 방법 중에서 외접원 방식을 사용하는 중심 합성 설계(Circumscribed Central Composite)를 사용하여 실험 요인을 Table 4와 같이 설계하였다(Anderson and Whitcomb, 2000; Kim, 2002; Le and Shin, 2018; Myers et al., 2016). 이 때, α값은 1.732로 정하였으며, 이를 이용하여 생성되는 실험점은 기본적으로 Table 3의 2열 ~ 4열까지의 코드(coded) 값과 동일하게 된다. 그러나 기존 PoN 분산합의 알고리즘의 성능 최적화를 위해서 선정된 실험점과 비교했을 때, Table 4에 표현된 것과 같이 노드 수는 동일한 범위이지만, 블록 합의 성능이 좋아졌기 때문에 트랜잭션의 크기나 트랜잭션의 수의 범위가 넓어졌다. 특히, 트랜잭션의 수는 기존 실험에 사용된 수의 2배까지 증가시킬 수 있었다. 따라서 실제로 실험에 사용된 트랙잭션의 크기와 수의 제어 변수 범위는 기존 PoN 분산합의 알고리즘과 비교할 때, 매우 넓어졌음을 확인할 수 있다. 또한 기존 Kim et al.(2020)의 결과와 비교할 때, 트랜잭션 수의 범위를 작은 수준에서 더 큰 값을 갖도록 설계하였다. 예를 들면, 제어 변수 수준이 -1.732일 때 트랜잭션 수가 5,732개이고, 1.732일 때 2,268개이다. 이를 통해 유의미한 합의 시간과 TPS 성능을 발휘할 수 있는 제어 변수의 범위 내에서 성능 최적화를 달성할 수 있는 예측 모델 수립을 위한 실험 설계가 가능하였다.

4.2 성능 예측 모델 및 최적화

새롭게 정한 실험점에 대한 실험을 통해 Table 5와 같은 결과를 얻었다. 이는 20개의 실험점 각각에 대해서 100번의 합의를 수행한 후 측정된 합의 시간과 TPS의 평균을 구한 값이다. 이를 이용하여, 본 논문에서는 먼저 노드 수, 트랜잭션 크기, 트랜잭션 수에 대한 새로운 합의 시간 및 TPS 예측 모델을 미니탭 19를 이용하여 수립하였으며, 그 결과는 Table 6과 같다. 이 때, 유의수준 값은 0.05를 사용하였으며, Table 6 (a)와 (b)는 각각 합의 시간과 TPS에 대한 비선형 회귀 모델의 회귀 계수와 p-value를 나타낸다. 일반적으로, p-value 값이 작을수록 성능 지표에 큰 영향을 미친다고 해석할 수 있으므로, 트랜잭션 수와 노드 수가 합의 시간과 TPS에 큰 영향을 준다고 할 수 있다. 특히, 제어 변수의 비선형적 효과는 합의 시간의 경우에 트랜잭션의 수에 큰 영향을 받으며, TPS는 트랜잭션 수와 노드 수의 교호작용에 영향을 받는 것을 알 수 있다.

Table 5. Experimental results of new PoN

Exp. No.	X_1	X_2	X_3	y_1 (Consensus time)	y_2 (TPS)
1	-1	-1	-1	0.314	5,017
2	1	-1	-1	0.408	5,022
3	-1	1	-1	0.185	3,076
4	1	1	-1	0.206	3,051
5	-1	-1	1	1.140	4,955
6	1	-1	1	2.930	4,840
7	-1	1	1	0.427	3,019
8	1	1	1	0.509	3,008
9	-1.732	0	0	0.378	4,022
10	1.732	0	0	0.576	3,981
11	0	-1.732	0	1.725	5,679

Exp. No.	X_1	X_2	X_3	y_1 (Consensus time)	y_2 (TPS)
12	0	1.732	0	0.265	2,309
13	0	0	-1.732	0.148	4,042
14	0	0	1.732	0.919	3,975
15	0	0	0	0.479	4,006
16	0	0	0	0.475	3,991
17	0	0	0	0.447	4,023
18	0	0	0	0.461	4,031
19	0	0	0	0.457	4,026
20	0	0	0	0.454	4,007

Table 6. Coefficients of regression models for consensus time and TPS

(a) Coefficients for consensus time

Term	Coefficient	p-value
Constant	0.5131	0.000
$X_1 - \ tx\_size$	0.1664	0.030
$X_2 - \ tx\_num$	-0.4281	0.000
$X_3 - \ node\_num$	0.3735	0.000
X_2^2	0.1887	0.011
X_1X_2	-0.2226	0.028
X_1X_3	0.2196	0.030
X_2X_3	-0.3504	0.002

(b) Coefficients for TPS

Term	Coefficient	p-value
Constant	4,004.00	0.000
$X_1 - \ tx\_size$	-15.50	0.033
$X_2 - \ tx\_num$	-965.51	0.000
$X_3 - \ node\_num$	-32.86	0.000
X_2X_3	18.00	0.058

한편, 회귀식을 이용하여 특정한 성능 목표를 달성하기 위한 제어 인자의 최적 조건을 설정하는 것이 가능하다. 일반적으로 네트워크 노드 수는 주어지는 조건이므로 나머지 제어 변수인 트랜잭션 크기와 수에 대한 합의 시간과 TPS의 회귀식 그래프를 등고선도로 나타내면 합의 시간과 TPS의 목표 성능에 대한 두 제어 변수의 범위를 구할 수 있다. Figure 3은 노드 수가 15개 일 때($x_3 = 1$), Table 6에 표현된 비선형 회귀식에 대한 중첩 등고선도를 나타낸다. 예를 들면, 합의 시간 0.5초와 3000 TPS를 달성하기 위해서는 적색 실선과 청색 점선이 만나는 교점에 해당되는 트랜잭션 크기 = 1.3, 즉 583 바이트, 트랜잭션 수 = 1.1, 즉 2,900개가 최적 조건이 된다. 이러한 결과는 Kim et al.(2020)의 결과와 비교할 때 트랜잭션의 크기가 약 140바이트 정도 증가된 것이다. 또한, Kim et al.(2020)에서는 합의 시간 0.5초와 3,000 TPS를 달성하기 위한 조건이 트랜잭션 크기 = 440바이트, 트랜잭션 수 = 3,000이었는데, 이러한 조건에서 새로운 PoN 분산합의 알고리즘은 0.5초보다 더 작은 합의 시간을 달성할 수 있음을 Figure 3에서 알 수 있다.

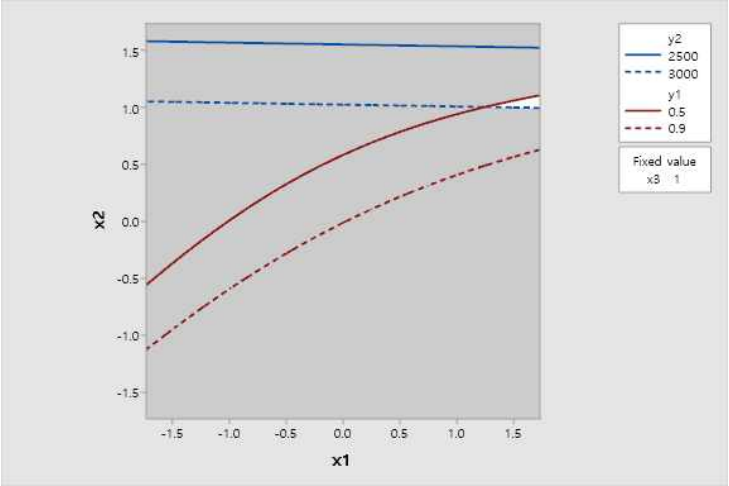

Figure 3. Overlapped contour plot of consensus time and TPS

5. 결 론

PoN 분산합의 알고리즘은 각 합의 단계에서 교환되는 메시지 복잡도가 $O(n)$으로 매우 효율적이며, 이를 기반으로 수초 이내의 합의 시간과 수천 TPS 수준의 성능을 제공이 가능하였다. 그러나 하나의 블록에 포함되는 트랜잭션의 크기와 수가 블록 합의를 위해 필요한 4단계의 합의 과정 동안에 전송되는 메시지 크기에 영향을 미치며, 전체 노드 수 증가로 인한 합의 참여 노드 수의 증가는 발생하는 메시지 총량이나 처리 시간의 증가에 매우 큰 영향을 줄 수 있다. 따라서 본 논문에서는 이를 개선하기 위한 경량화된 PoN 분산합의 알고리즘의 블록 합의 과정을 제안하고, 기존 PoN 분산합의 알고리즘과의 성능 비교를 통해 개선 결과를 검증하였다. 또한, 반응표면분석을 이용한 수치실험을 통해, 제어 인자에 기반하여 성능 목표를 예측하는 비선형 예측 모델을 수립하고, 특정한 성능 목표 조건을 달성하기 위해 최적 인자 조합을 도출하는 방법에 대해서도 제안하였다.

한편, 블록체인 시스템에서는 합의 시간이나 TPS 등의 성능 지표를 최적화하는 것도 중요하지만, 블록체인 트릴레마 이슈를 잘 해결하는 것도 매우 중요할 수 있다. 블록체인 트릴레마란 블록체인 시스템이 기본적으로 제공해야 하는 특성으로서 탈중앙화, 확장성, 보안성으로 정의된다. PoN 분산합의 알고리즘은 일부 노드로 구성된 합의체(Congress)를 통해 합의를 수행하는 비경쟁적 방식을 제공하기 때문에 모든 노드가 합의에 참여하는 자격을 확률적으로 공평하게 얻을 수 있다. 그러나 합의 과정에서 선착순에 의한 합의체 및 위원회를 구성하기 때문에 네트워크 노드 성능에 따른 차이가 발생할 수도 있다. 따라서 PoN 분산합의 알고리즘의 탈중앙화 지표를 정의하고 분석하는 것을 추후 연구로 진행하고자 한다.

REFERENCES

Anderson, M. J. and Whitcomb, P. J. 2000. Design of experiments. Kirk-Othmer Encyclopedia of Chemical Technology:1-22.

Buterin, V. 2013. What proof of stake is and why it matters. Bitcoin Magazine:1-3.

Castro, M. and Liskov, B. 1999. Practical Byzantine fault tolerance. OSDI, 99:173-186.

Chen, J. and Micali, S. 2019. Algorand: A secure and efficient distributed ledger. Theoretical Computer Science 777:155-183.

Kim, Y. 2002. Response Surface Approach to Integrated Optimization Modeling for Parameter and Tolerance Design. Journal of Korean Society for Quality Management 30(4):58-67.

Kim, Y.C., Kim, K.Y., Oh, J.T., Kim, D.G., and Choi, J.Y. 2020. Simulator design and performance analysis of BADA distributed consensus algorithm. Journal of Society of Korea Industrial and Systems Engineering 43(4):168-177.

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

Le, Tuan-Ho and Shin, Sangmun. 2018. A literature review on RSM-based robust parameter design (RPD): Experimental design, estimation modeling, and optimization methods. Journal of Korean Society for Quality Management 46(1):39-74.

Myers, R. H., Montgomery, D. C., and Anderson-Cook, C. M. 2016. Response surface methodology: process and product optimization using designed experiments, John Wiley & Sons:43-49.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.

Oh, Jintae, Park, Joonyoung, Kim, Youngchang, and Kim Kiyoung. 2020. Algorithm based on Byzantime agreement among decentralized agents (BADA). ETRI Journal 42(6):872-885.

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

Yoo, S. M. 2020. 4th industrial revolution and blockchain: Focusing on data economics. The Journal of The Korean Institute of Communication Sciences 37(2):23-30.

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

저자소개

최진영 한양대학교 산업공학과에서 학사, KAIST 산업공학과에서 석사, Georgia Institute of Technology 산업시스템공학과(ISyE)에서 박사학위를 취득하였다. 현재 아주대학교 산업공학과 교수로 재직 중이며, 주요 관심분야는 Industrial AI Optimization, Quality Control, Blockchain, Smart Factory, Modeling & Simulation 등이다.

김영창 전북대학교 컴퓨터공학과에서 학사, 석사, 박사학위를 취득하였다. 현재 한국전자통신연구원 인공지능연구소 블록체인·빅데이터연구단 블록체인연구실 선임연구원으로 재직 중이며, 주요 관심분야는 Database, Distributed Computing, Blockchain 등이다.

오진태 경북대학교 전자공학과에서 학사, 석사, 충남대학교 컴퓨터공학과에서 박사학위를 취득하였다. 현재 한국전자통신연구원 인공지능연구소 블록체인·빅데이터연구단 블록체인연구실 실장으로 재직 중이며, 주요 관심분야는 Network Security, Blockchain 등이다.

김기영 전남대학교 전산통계학과에서 학사, 석사, 충북대학교 컴퓨터과학과에서 박사학위를 취득하였다. 현재 한국전자통신연구원 인공지능연구소 블록체인·빅데이터연구단 단장으로 재직 중이며, 주요 관심분야는 Smartphone Security, Blockchain 등이다.