(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0120071
(43) 공개일자 2024년08월07일

(51) 국제특허분류(Int. Cl.)
H04L 67/1042 (2022.01) *G06F 16/27* (2019.01)
G06N 3/098 (2023.01)
(52) CPC특허분류
H04L 67/1051 (2013.01)
G06F 16/27 (2019.01)
(21) 출원번호 10-2023-0012432
(22) 출원일자 2023년01월31일
심사청구일자 2023년01월31일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 1703호 (송도동, 더샵 센트럴파크2)
양단아
서울특별시 마포구 월드컵북로 502-36, 1003동 802호 (상암동, 상암월드컵파크10단지)
채기준
서울특별시 강남구 강남대로136길 34, 402호 (논현동, 월드노블레스빌)
(74) 대리인
김연권

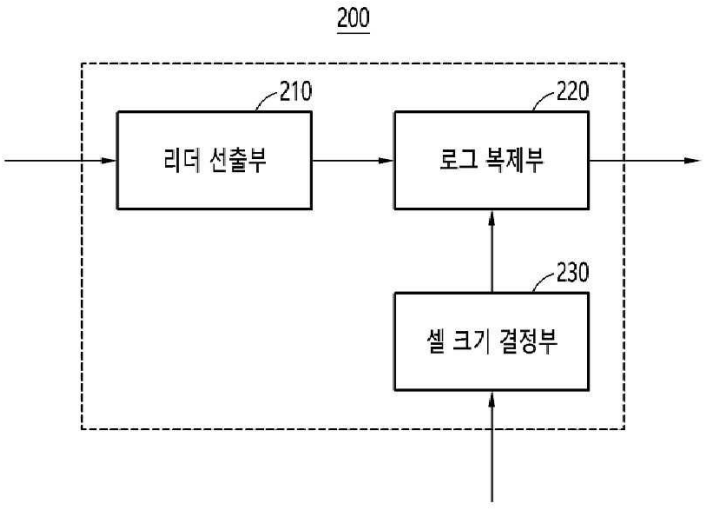
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **셀 기반의 래프트 알고리즘을 이용하는 블록체인 시스템 및 그 동작방법**

(57) 요 약

본 발명은 블록체인 시스템 및 그 동작방법에 관한 것으로서, 일실시예에 따른 블록체인 시스템은 복수의 블록체인 노드 중 어느 하나의 노드가 리더 노드로 선출되고 복수의 블록체인 노드 중 리더 노드를 제외한 복수의 노드가 팔로워 노드로 설정 되도록 제어하는 리더 선출부 및 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 노드가 클라이언트 단말로부터 트랜잭션을 수신하면, 리더 노드와 복수의 팔로워 노드 간의 로그 복제 과정이 수행되도록 제어하되, 사전에 결정된 크기의 셀(cell)의 단위로 로그 복제 과정이 수행되도록 제어하는 로그 복제부를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
G06N 3/098 (2023.01)
H04L 67/1053 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711154280
과제번호	2020R1A2C1006497
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	이공분야기초연구사업(통합)-중견연구자지원사업-(유형1-1)중견연구
연구과제명	UAV를 활용한 모바일 IoT 환경에서 효율적이고 안전한 노드 및 데이터 프라이버시 보장 기법
기 여 율	1/1
과제수행기관명	이화여자대학교
연구기간	2020.03.01 ~ 2023.02.28

명 세 서

청구범위

청구항 1

복수의 블록체인 노드 중 어느 하나의 노드가 리더 노드로 선출되고 상기 복수의 블록체인 노드 중 상기 리더 노드를 제외한 복수의 노드가 팔로워 노드로 설정 되도록 제어하는 리더 선출부 및

상기 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 노드가 클라이언트 단말로부터 트랜잭션을 수신하면, 상기 리더 노드와 상기 복수의 팔로워 노드 간의 로그 복제 과정이 수행되도록 제어하되, 사전에 결정된 크기의 셀(cell)의 단위로 상기 로그 복제 과정이 수행되도록 제어하는 로그 복제부

를 포함하는 블록체인 시스템.

청구항 2

제1항에 있어서,

상기 리더 선출부는,

상기 복수의 블록체인 노드 중 어느 하나의 노드가 후보 노드로 전환되면, 상기 후보 노드에서 상기 복수의 블록체인 노드 중 상기 후보 노드를 제외한 복수의 투표 대상 노드 각각으로, 상기 후보 노드의 현재 텀(term)의 번호와 상기 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호를 포함하는 투표 요청 메시지를 전송하도록 제어하는

블록체인 시스템.

청구항 3

제2항에 있어서,

상기 리더 선출부는,

상기 복수의 투표 대상 노드 각각에서, 상기 후보 노드의 현재 텀의 번호 및 상기 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호에 기초하여 상기 후보 노드에 대한 투표 결과를 포함하는 투표 응답 메시지를 생성하고, 상기 생성된 투표 응답 메시지에 기초하여 상기 후보 노드를 상기 리더 노드로 선출 되도록 제어하는

블록체인 시스템.

청구항 4

제3항에 있어서,

상기 복수의 투표 대상 노드 중 어느 하나의 투표 대상 노드는,

상기 후보 노드의 현재 텀의 번호가 상기 어느 하나의 투표 대상 노드의 현재 텀의 번호 보다 크고, 상기 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호가 상기 어느 하나의 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호 보다 크거나 같으면, 상기 후보 노드를 상기 리더 노드로 선출하는데 동의하는 결과를 포함하는 상기 투표 응답 메시지를 생성하는

블록체인 시스템.

청구항 5

제1항에 있어서,

상기 복수의 블록체인 노드의 개수에 기초하여 상기 셀의 크기를 결정하도록 제어하는 셀 크기 결정부

를 더 포함하는 블록체인 시스템.

청구항 6

제5항에 있어서,

상기 셀 크기 결정부는,

기 설정된 시간동안 상기 복수의 블록체인 노드로부터 TPS(transaction per second) 정보, 커밋 실패 메시지 중 적어도 하나의 정보를 수집하고, 상기 수집된 정보와, 상기 복수의 블록체인 노드의 개수를 입력 데이터로 수신하는 연합 학습 모델을 통해 상기 셀의 크기를 결정하도록 제어하는

를 더 포함하는 블록체인 시스템.

청구항 7

제5항에 있어서,

상기 셀 크기 결정부는,

상기 복수의 블록체인 노드의 개수가 5개 내지 20개인 경우, 상기 셀의 크기가 65개 내지 80개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하고,

상기 복수의 블록체인 노드의 개수가 21개 내지 40개인 경우, 상기 셀의 크기가 50개 내지 70개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하며,

상기 복수의 블록체인 노드의 개수가 41개 내지 60개인 경우, 상기 셀의 크기가 40개 내지 55개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하는

블록체인 시스템.

청구항 8

제5항에 있어서,

상기 셀 크기 결정부는,

상기 복수의 블록체인 노드의 개수가 61개 내지 80개인 경우, 상기 셀의 크기가 35개 내지 45개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하고,

상기 복수의 블록체인 노드의 개수가 81개 내지 100개인 경우, 상기 셀의 크기가 25개 내지 35개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하는

블록체인 시스템.

청구항 9

제1항에 있어서,

상기 로그 복제부는,

상기 리더 노드 및 복수의 팔로워 노드 각각에서, 상기 클라이언트 단말로부터 트랜잭션을 수신할 때 마다 상기 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 팔로워 노드 각각에 구비된 로컬 스토리지에 상기 트랜잭션에 대응되는 트랜잭션 로그를 저장하고, 상기 리더 노드 및 적어도 하나의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그의 크기가 상기 셀의 크기에 도달하면 상기 리더 노드 및 복수의 팔로워 노드 각각에 구비된 상태 머신에 상기 리더 노드 및 복수의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋되도록 제어하는

블록체인 시스템.

청구항 10

제9항에 있어서,

상기 로그 복제부는,

상기 리더 노드의 n번째(여기서, n은 양의 정수) 셀의 해시 값과 상기 적어도 하나의 팔로워 노드의 n번째 셀의 해시 값을 각각 비교하고, 상기 비교 결과가 일치하면 상기 리더 노드 및 상기 적어도 하나의 팔로워 노드 각각에 구비된 상태 머신에 상기 리더 노드 및 상기 적어도 하나의 팔로워 노드의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어하는

블록체인 시스템.

청구항 11

제10항에 있어서,

상기 로그 복제부는,

상기 비교 결과가 일치하지 않는 것으로 나타나면, 상기 리더 노드의 n번째 셀에 저장된 트랜잭션 로그를 상기 비교 결과가 일치하지 않는 팔로워 노드에 전송하도록 제어하는

블록체인 시스템.

청구항 12

리더 선출부에서, 복수의 블록체인 노드 중 어느 하나의 노드가 리더 노드로 선출되고 상기 복수의 블록체인 노드 중 상기 리더 노드를 제외한 복수의 노드가 팔로워 노드로 설정 되도록 제어하는 단계 및

로그 복제부에서, 상기 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 노드가 클라이언트 단말로부터 트랜잭션을 수신하면 상기 리더 노드와 상기 복수의 팔로워 노드 간의 로그 복제 과정이 수행되도록 제어하되, 사전에 결정된 크기의 셀 단위로 상기 로그 복제 과정이 수행되도록 제어하는 단계

를 포함하는 블록체인 시스템의 동작방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 시스템 및 그 동작방법에 관한 것으로, 보다 상세하게는 래프트 알고리즘을 이용하는 블록체인 시스템의 기술적 사상에 관한 것이다.

배 경 기 술

[0002] 래프트(raft) 알고리즘은 분산 조정 서비스 및 분산 데이터베이스 분야의 블록체인 시나리오에 주로 활용되고 있는 알고리즘으로, 블록체인 시나리오 처리에 대한 효율성 및 일관성을 보장한다.

[0003] 그러나, 기존의 래프트 알고리즘은 하나의 로그가 하나의 트랜잭션으로 정의가 되어 처리 되므로, 실시간으로 다수 트랜잭션이 발생하는 스마트 데이터 시장에 기초하는 블록체인 시나리오에 적용 시 네트워크 과부하 및 이에 다른 성능 저하를 야기할 수 있다.

[0004] 또한, 기존 래프트 알고리즘은 팔로워 노드의 수가 증가하는 경우에 네트워크의 통신량이 증가하여 커밋(commit) 속도가 제한될 수 있으며, 이 경우 절반 이상의 팔로워 노드가 병목 현상으로 리더 노드에 의해 제어되지 않는 네트워크 분할(network division) 현상이 발생될 수 있으며, 이로 인한 트랜잭션의 처리량이 큰 감소는 트랜잭션에 대한 실시간 처리를 불가하게 만드는 요인으로 작용할 수 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국공개특허 제10-2022-0141170호, "프라이빗 블록체인에서 연합학습을 이용한 리더 선출 방법, 이를 수행하기 위한 기록 매체 및 장치"

(특허문헌 0002) 한국등록특허 제10-2150210호, "블록체인 네트워크"

(특허문헌 0003) 한국등록특허 제10-2314495호, "래프트 합의를 이용한 블록체인 동기화 방법 및 블록체인 시스템"

발명의 내용

해결하려는 과제

[0006] 본 발명은 셀 기반의 래프트 알고리즘(cell based raft algorithm; CBR)을 이용하여 트랜잭션에 대한 커밋 처리를 크기가 최적화된 셀 단위로 수행하여, 시스템의 과부하 및 병목 현상을 최소화할 수 있는 블록체인 시스템 및 그 동작방법을 제공하고자 한다.

[0007] 또한, 본 발명은 TPS(transaction per second) 정보에 기반하는 연합 학습을 통해 커밋 처리를 위한 셀의 크기를 최적화하여 트랜잭션 처리의 정확도를 향상시킬 수 있는 블록체인 시스템 및 그 동작방법을 제공하고자 한다.

[0008] 또한, 본 발명은 셀의 해시 값에 대한 비교 동작에 기초하여 로컬 오류(local failure)의 발생 여부를 판단하고 이에 대응함으로써, 트랜잭션 처리의 정확도를 향상시킬 수 있는 블록체인 시스템 및 그 동작방법을 제공하고자 한다.

과제의 해결 수단

[0009] 본 발명의 일실시예에 따른 블록체인 시스템은 복수의 블록체인 노드 중 어느 하나의 노드가 리더 노드로 선출되고 복수의 블록체인 노드 중 리더 노드를 제외한 복수의 노드가 팔로워 노드로 설정 되도록 제어하는 리더 선출부 및 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 노드가 클라이언트 단말로부터 트랜잭션을 수신하면, 리더 노드와 복수의 팔로워 노드 간의 로그 복제 과정이 수행되도록 제어하되, 사전에 결정된 크기의 셀(cell)의 단위로 로그 복제 과정이 수행되도록 제어하는 로그 복제부를 포함할 수 있다.

[0010] 일측에 따르면, 리더 선출부는 복수의 블록체인 노드 중 어느 하나의 노드가 후보 노드로 전환되면, 후보 노드에서 복수의 블록체인 노드 중 후보 노드를 제외한 복수의 투표 대상 노드 각각으로, 후보 노드의 현재 텀(term)의 번호와 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호를 포함하는 투표 요청 메시지를 전송하도록 제어할 수 있다.

[0011] 일측에 따르면, 리더 선출부는 복수의 투표 대상 노드 각각에서, 후보 노드의 현재 텀의 번호 및 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호에 기초하여 후보 노드에 대한 투표 결과를 포함하는 투표 응답 메시지를 생성하고, 생성된 투표 응답 메시지에 기초하여 후보 노드를 리더 노드로 선출 되도록 제어할 수 있다.

[0012] 일측에 따르면, 복수의 투표 대상 노드 중 어느 하나의 투표 대상 노드는 후보 노드의 현재 텀의 번호가 어느 하나의 투표 대상 노드의 현재 텀의 번호 보다 크고, 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호가 어느 하나의 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호 보다 크거나 같으면, 후보 노드를 리더 노드로 선출하는데 동의하는 결과를 포함하는 투표 응답 메시지를 생성할 수 있다.

[0013] 일측에 따르면, 블록체인 시스템은 복수의 블록체인 노드의 개수에 기초하여 셀의 크기를 결정하도록 제어하는 셀 크기 결정부를 더 포함할 수 있다.

[0014] 일측에 따르면, 셀 크기 결정부는 기 설정된 시간동안 복수의 블록체인 노드로부터 TPS(transaction per second) 정보, 커밋 실패 메시지 중 적어도 하나의 정보를 수집하고, 수집된 정보와, 복수의 블록체인 노드의 개수를 입력 데이터로 수신하는 연합 학습 모델을 통해 셀의 크기를 결정하도록 제어할 수 있다.

[0015] 일측에 따르면, 셀 크기 결정부는 복수의 블록체인 노드의 개수가 5개 내지 20개인 경우, 셀의 크기가 65개 내지 80개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하고, 복수의 블록체인 노드의 개수가 21개 내지 40개인 경우, 셀의 크기가 50개 내지 70개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하며, 복수의 블록체인 노드의 개수가 41개 내지 60개인 경우, 셀의 크기가 40개 내지 55개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어할 수 있다.

[0016] 일측에 따르면, 셀 크기 결정부는 복수의 블록체인 노드의 개수가 61개 내지 80개인 경우, 셀의 크기가 35개 내지 45개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하고, 복수의 블록체인 노드의 개수가 81개 내지 100개인 경우, 셀의 크기가 25개 내지 35개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어할 수 있다.

[0017] 일측에 따르면, 로그 복제부는 리더 노드 및 복수의 팔로워 노드 각각에서, 클라이언트 단말로부터 트랜잭션을

수신할 때 마다 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 팔로워 노드 각각에 구비된 로컬 스토리지에 트랜잭션에 대응되는 트랜잭션 로그를 저장하고, 리더 노드 및 적어도 하나의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그의 크기가 셀의 크기에 도달하면 리더 노드 및 복수의 팔로워 노드 각각에 구비된 상태 머신에 리더 노드 및 복수의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어할 수 있다.

[0018] 일측에 따르면, 로그 복제부는 리더 노드의 n번째(여기서, n은 양의 정수) 셀의 해시 값과 적어도 하나의 팔로워 노드의 n번째 셀의 해시 값을 각각 비교하고, 비교 결과가 일치하면 리더 노드 및 적어도 하나의 팔로워 노드 각각에 구비된 상태 머신에 리더 노드 및 적어도 하나의 팔로워 노드의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어할 수 있다.

[0019] 일측에 따르면, 로그 복제부는 비교 결과가 일치하지 않는 것으로 나타나면, 리더 노드의 n번째 셀에 저장된 트랜잭션 로그를 비교 결과가 일치하지 않는 팔로워 노드에 전송하도록 제어할 수 있다.

[0020] 본 발명의 일실시예에 따른 블록체인 시스템의 동작방법은 리더 선출부에서, 복수의 블록체인 노드 중 어느 하나의 노드가 리더 노드로 선출되고 복수의 블록체인 노드 중 리더 노드를 제외한 복수의 노드가 팔로워 노드로 설정 되도록 제어하는 단계 및 로그 복제부에서, 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 노드가 클라이언트 단말로부터 트랜잭션을 수신하면 리더 노드와 복수의 팔로워 노드 간의 로그 복제 과정이 수행되도록 제어하되, 사전에 결정된 크기의 셀 단위로 로그 복제 과정이 수행되도록 제어하는 단계를 포함할 수 있다.

발명의 효과

[0021] 일실시예에 따르면, 본 발명은 셀 기반의 래프트 알고리즘(CBR)을 이용하여 트랜잭션에 대한 커밋 처리를 크기가 최적화된 셀 단위로 수행하여, 시스템의 과부하 및 병목 현상을 최소화할 수 있다.

[0022] 일실시예에 따르면, 본 발명은 TPS(transaction per second) 정보에 기반하는 연합 학습을 통해 커밋 처리를 위한 셀의 크기를 최적화하여 트랜잭션 처리의 정확도를 향상시킬 수 있다.

[0023] 일실시예에 따르면, 본 발명은 셀의 해시 값에 대한 비교 동작에 기초하여 로컬 오류(local failure)의 발생 여부를 판단하고 이에 대응함으로써, 트랜잭션 처리의 정확도를 향상시킬 수 있다.

도면의 간단한 설명

[0024] 도 1은 일실시예에 따른 블록체인 네트워크의 적용 환경에 대한 예시를 설명하기 위한 도면이다.

도 2는 일실시예에 따른 블록체인 시스템을 설명하기 위한 도면이다.

도 3a 내지 도 3d는 일실시예에 따른 블록체인 시스템을 보다 구체적으로 설명하기 위한 도면이다.

도 4a 내지 도 4g는 일실시예에 따른 블록체인 시스템의 성능 시험 결과를 설명하기 위한 도면이다.

도 5는 일실시예에 따른 블록체인 시스템의 동작방법을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0026] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[0027] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 구성요소들은 용어들에 의해 한정되어서는 안 된다. 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만, 예를 들면 본 발명의 개념에 따른 권리 범위로부터 이탈되지 않은 채, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0028] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에

직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 표현들, 예를 들면 "~사이에"와 "바로~사이에" 또는 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0029] 본 명세서에서 사용한 용어는 단지 특정한 실시예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 설시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0030] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0032] 이하, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0034] 도 1은 일실시예에 따른 블록체인 네트워크의 적용 환경에 대한 예시를 설명하기 위한 도면이다.

[0035] 도 1을 참조하면, 일실시예에 따른 블록체인 네트워크(100)는 스마트 데이터 시장의 환경에 적용되어, 각 엔티티들(일례로, hospital, smart farm, smart mall, smart parking, transport agencies 등)로부터 다양한 트랜잭션이 수집될 수 있다.

[0036] 구체적으로, 블록체인 네트워크(100)는 하나의 리더 노드 및 리더 노드에 의해 제어되는 복수의 팔로워 노드를 포함하며, 셀 기반의 래프트 알고리즘(CBR)에 기초하여 블록체인 시나리오가 제어될 수 있다.

[0037] 여기서, 리더 노드 및 복수의 팔로워 노드는 블록체인 네트워크(100)를 구성하는 각 엔티티들에 구비된 블록체인 서버일 수 있다.

[0038] 이를 위해, 일실시예에 따른 블록체인 시스템은 리더 선출 과정 및 트랜잭션의 발생에 따른 로그 복제 과정을 수행할 수 있다.

[0039] 일실시예에 따른 블록체인 시스템은 이후 실시예 도 2 내지 도 3d를 통해 보다 구체적으로 설명하기로 한다.

[0041] 도 2는 일실시예에 따른 블록체인 시스템을 설명하기 위한 도면이다.

[0042] 도 2를 참조하면, 일실시예에 따른 블록체인 시스템(200)은 셀 기반의 래프트 알고리즘(CBR)을 이용하여 트랜잭션에 대한 커밋 처리를 크기가 최적화된 셀 단위로 수행하여, 시스템의 과부하 및 병목 현상을 최소화할 수 있다.

[0043] 또한, 블록체인 시스템(200)은 TPS(transaction per second) 정보에 기반하는 연합 학습을 통해 커밋 처리를 위한 셀의 크기를 최적화하여 트랜잭션 처리의 정확도를 향상시킬 수 있다.

[0044] 또한, 블록체인 시스템(200)은 셀의 해시 값에 대한 비교 동작에 기초하여 로컬 오류(local failure)의 발생 여부를 판단하고 이에 대응함으로써, 트랜잭션 처리의 정확도를 향상시킬 수 있다.

[0045] 이를 위해, 블록체인 시스템(200)은 리더 선출부(210), 로그 복제부(220) 및 셀 크기 결정부(230)를 포함할 수 있다.

[0046] 예를 들면, 일실시예에 따른 리더 선출부(210) 및 로그 복제부(220)는 복수의 블록체인 노드와는 별도로 구축된 제어 서버에 구비될 수 있으나, 바람직하게는 복수의 블록체인 노드 각각에 구비될 수 있다.

[0047] 또한, 셀 크기 결정부(230)는 복수의 블록체인 노드와는 별도로 구축된 제어 서버에 구비될 수 있으며, 이 경우 셀 크기 결정부(230)는 리더 노드 및 복수의 팔로워 노드 각각에 결정된 셀의 크기 정보를 제공할 수 있다.

[0048] 일실시예에 따른 리더 선출부(210)는 복수의 블록체인 노드 중 어느 하나의 노드가 리더 노드로 선출되고 복수의 블록체인 노드 중 리더 노드를 제외한 복수의 노드가 팔로워 노드로 설정 되도록 제어할 수 있다.

[0049] 일측에 따르면, 리더 선출부(210)는 복수의 블록체인 노드 중 어느 하나의 노드가 후보 노드로 전환되면, 후보 노드에서 복수의 블록체인 노드 중 후보 노드를 제외한 복수의 투표 대상 노드 각각으로, 후보 노드의 현재 텀(term)의 번호와 후보 노드의 상태 머신(state machine)에 커밋된 마지막 셀의 번호를 포함하는 투표 요청 메시지를 전송하도록 제어할 수 있다.

[0050] 또한, 리더 선출부(210)는 복수의 투표 대상 노드 각각에서 후보 노드의 현재 텀의 번호 및 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호에 기초하여 후보 노드에 대한 투표 결과를 포함하는 투표 응답 메시지를 생성하고, 생성된 투표 응답 메시지에 기초하여 후보 노드를 리더 노드로 선출 되도록 제어할 수 있다.

[0051] 예를 들면, 복수의 투표 대상 노드 중 어느 하나의 투표 대상 노드는 후보 노드의 현재 텀의 번호가 어느 하나의 투표 대상 노드의 현재 텀의 번호 보다 크고, 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호가 어느 하나의 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호 보다 크거나 같으면, 후보 노드를 리더 노드로 선출하는데 동의하는 결과를 포함하는 투표 응답 메시지를 생성할 수 있다.

[0052] 일실시예에 따른 로그 복제부(220)는 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 노드가 클라이언트 단말로부터 트랜잭션을 수신하면, 리더 노드와 복수의 팔로워 노드 간의 로그 복제 과정이 수행되도록 제어하되, 사전에 결정된 크기의 셀(cell)의 단위로 로그 복제 과정이 수행되도록 제어할 수 있다.

[0053] 일측에 따르면, 로그 복제부(220)는 리더 노드 및 복수의 팔로워 노드 각각에서 클라이언트 단말로부터 트랜잭션을 수신할 때 마다 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 팔로워 노드 각각에 구비된 로컬 스토리지에 트랜잭션에 대응되는 트랜잭션 로그를 저장하고, 리더 노드 및 적어도 하나의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그의 크기가 셀의 크기에 도달하면 리더 노드 및 복수의 팔로워 노드 각각에 구비된 상태 머신에 리더 노드 및 복수의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어할 수 있다.

[0054] 일측에 따르면, 로그 복제부(220)는 리더 노드 및 복수의 팔로워 노드 각각에서의 셀의 해시 값에 대한 비교 동작에 기초하여 로컬 오류(local failure)의 발생 여부를 판단하고, 판단 결과에 기초하여 리더 노드의 로컬 스토리지에 저장된 트랜잭션 로그를 로컬 오류가 발생된 팔로워 노드의 로컬 스토리지에 저장할 수 있으며, 예를 들면, 리더 노드의 로컬 스토리지에 저장된 트랜잭션 로그는 셀 단위로 처리될 수 있다.

[0055] 구체적으로, 로그 복제부(220)는 리더 노드의 n번째(여기서, n은 양의 정수) 셀의 해시 값과 적어도 하나의 팔로워 노드의 n번째 셀의 해시 값을 각각 비교하고, 비교 결과가 일치하면 리더 노드 및 적어도 하나의 팔로워 노드 각각에 구비된 상태 머신에 리더 노드 및 적어도 하나의 팔로워 노드의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어할 수 있다.

[0056] 또한, 로그 복제부(220)는 해시 값에 대한 비교 결과가 일치하지 않는 것으로 나타나면, 리더 노드의 n번째 셀에 저장된 트랜잭션 로그를 비교 결과가 일치하지 않는 팔로워 노드에 전송하도록 제어할 수 있다.

[0057] 한편, 셀 크기 결정부(230)는 복수의 블록체인 노드의 개수에 기초하여 셀의 크기를 결정하도록 제어할 수 있다.

[0058] 일측에 따르면, 셀 크기 결정부(230)는 기 설정된 시간동안 복수의 블록체인 노드로부터 TPS(transaction per second) 정보, 커밋 실패 메시지 중 적어도 하나의 정보를 수집하고, 수집된 정보와, 복수의 블록체인 노드의 개수를 입력 데이터로 수신하는 연합 학습 모델을 통해 셀의 크기를 결정하도록 제어할 수 있다.

[0059] 예를 들면, 셀 크기 결정부(230)는 복수의 블록체인 노드의 개수가 5개 내지 20개인 경우, 셀의 크기가 65개 내지 80개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하고, 복수의 블록체인 노드의 개수가 21개 내지 40개인 경우, 셀의 크기가 50개 내지 70개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하며, 복수의 블록체인 노드의 개수가 41개 내지 60개인 경우, 셀의 크기가 40개 내지 55개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어할 수 있다.

[0060] 또한, 셀 크기 결정부(230)는 복수의 블록체인 노드의 개수가 61개 내지 80개인 경우, 셀의 크기가 35개 내지

45개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어하고, 복수의 블록체인 노드의 개수가 81개 내지 100개인 경우, 셀의 크기가 25개 내지 35개의 트랜잭션 로그에 대응되는 크기로 결정 되도록 제어할 수 있다.

[0062] 도 3a 내지 도 3d는 일실시예에 따른 블록체인 시스템을 보다 구체적으로 설명하기 위한 도면이다.

[0063] 도 3a 내지 도 3d를 참조하면, 도 3a는 일실시예에 따른 블록체인 시스템의 리더 선출 과정을 예시하고, 도 3b는 일실시예에 따른 블록체인 시스템의 로그 복제 과정을 예시한다.

[0064] 또한, 도 3c는 일실시예에 따른 블록체인 시스템에서 새 로그가 시작되기 전 리더 노드의 표준 로그와 복수의 팔로워 노드의 로그를 예시하고, 도 3d는 일실시예에 따른 블록체인 시스템에서 새로운 셀이 커밋되기 전 리더 노드의 표준 로그와 복수의 팔로워 노드의 로그를 예시한다.

[0065] 도 3a에 따르면, 복수의 블록체인 노드 중 어느 하나의 노드가 후보 노드로 전환되면, 후보 노드는 복수의 투표 대상 노드 각각으로 후보 노드의 현재 텀(term)의 번호와 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호(lastCell)를 포함하는 투표 요청 메시지(RequestVote RPC 메시지)를 전송하도록 제어할 수 있다.

[0066] 구체적으로, 복수의 블록체인 노드 중 후보 노드를 제외한 복수의 투표 대상 노드 각각으로 후보 노드의 상태 머신(state machine)에 커밋(commit)된 마지막 텀의 번호(term)와 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호(lastCell)를 포함하는 투표 요청 메시지(RequestVote RPC 메시지)를 전송할 있다.

[0067] 또한, 복수의 투표 대상 노드 각각은 후보 노드의 현재 텀의 번호 및 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호에 기초하여 후보 노드에 대한 투표 결과를 포함하는 투표 응답 메시지를 생성하고, 생성된 투표 응답 메시지에 기초하여 후보 노드를 리더 노드로 선출 되도록 제어할 수 있다.

[0068] 예를 들면, 투표 대상 노드는 후보 노드의 현재 텀의 번호(term)가 투표 대상 노드의 현재 텀(term)의 번호 보다 크고, 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호(lastCell)가 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호 보다 크거나 같으면, 후보 노드를 리더 노드로 선출하는데 동의하는 결과(voteGranted)를 포함하는 투표 응답 메시지(response message)를 생성하고, 생성된 투표 응답 메시지를 후보 노드에 전송할 수 있다.

[0069] 구체적으로, 리더 선출 과정에서는 처음에 모든 서버가 팔로워 노드(즉, 투표 대상 노드)의 상태에 있으며, 로그의 인수(argument)에 필요한 용어, 셀 및 로그 인덱스의 값을 0으로 초기화할 수 있으며, 최초에는 리더 노드가 없기 때문에 투표 대상 노드는 리더 노드로부터 heartbeat 메시지를 수신할 수 없으며(도면부호 311), 이 경우 모든 투표 대상 노드들은 리더 선출 모드로 전환되며, 처음의 리더 노드의 부재를 알아차린 투표 대상 노드는 리더 노드가 되기 위해 후보 노드로 전환될 수 있다.

[0070] 다음으로, 후보 노드는 복수의 투표 대상 노드 각각으로 투표 요청 메시지(Request Vote RPC message)를 전송할 수 있으며(도면부호 312), 투표 요청 메시지(Request Vote RPC message)를 수신한 투표 대상 노드들을 각각 수신된 메시지에 대응되는 응답 메시지(Response message)를 후보 노드에게 전송할 수 있다(도면부호 314 및 315).

[0071] 예를 들면, 투표 요청 메시지(Request Vote RPC message) 및 투표 요청 메시지(Request Vote RPC message)에 대응되는 응답 메시지(Response message)는 하기 표1에 도시된 정보를 포함할 수 있다.

표 1

[0072]

type	Arguments	Description
Request Vote RPC message	term	후보자가 팔로워 노드(즉, 투표 대상 노드) 상태일 때 보유하고 있던 텀 값에서 1을 올림하여 얻은 텀 번호
	candidateID	블록체인 네트워크에 참여하는 서버의 고유 아이디
	lastTerm	후보 노드의 상태 머신에 커밋된 마지막 텀의 번호
	lastCell	후보 노드의 상태 머신에 커밋된 마지막 셀의 번호
	lastIndex	후보 노드의 상태 머신에 커밋된 마지막 로그 인덱스의 번호

Response message	term	팔로워 노드가 자체적으로 업데이트하는 텀의 번호
	voteGranted	true 또는 false (후보 노드가 리더가 되는 데 동의하면 'true', 반대하면 'false')
	lastCellHash	팔로워 노드의 상태 머신에 커밋된 마지막 셀의 해시 값
	current Cell Hash	팔로워 노드의 현재 셀의 해시 값

[0073] 구체적으로, 투표 대상 노드는 투표 요청 메시지(Request Vote RPC message)가 수신되면(도면부호 313), 투표 요청 메시지(Request Vote RPC message)에 포함된 후보 노드의 현재 텀의 번호(term)와 투표 대상 노드의 현재 텀 번호(term)을 비교하고(도면부호 314), 투표 요청 메시지(Request Vote RPC message)에 포함된 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호(lastCell)와 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호를 비교하며(도면부호 315), 비교 결과에 기초하여 'true' 또는 'false' 값의 voteGranted을 포함하는 투표 응답 메시지(Response message)를 후보 노드에 전송할 수 있다.

[0074] 예를 들면, 투표 대상 노드는 후보 노드의 현재 텀의 번호(term)가 투표 대상 노드의 현재 텀 번호(term) 보다 크고, 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호(lastCell)가 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호 보다 크거나 같으면 'true' 값의 voteGranted을 포함하는 투표 응답 메시지(Response message)를 생성할 수 있다.

[0075] 또한, 투표 대상 노드는 후보 노드의 현재 텀의 번호(term)가 투표 대상 노드의 현재 텀 번호(term) 보다 크지 않거나, 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호(lastCell)가 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호 보다 작으면 'false' 값의 voteGranted을 포함하는 투표 응답 메시지(Response message)를 생성할 수 있다.

[0076] 여기서, 투표 대상 노드는 voteGranted의 값이 'false'이면 현재 텀 값에 1을 올림한 값으로 업데이트하고, 이후 텀 값이 업데이트된 투표 대상 노드는 후보 노드로 전환될 수 있다.

[0077] 다음으로, 후보 노드는 수신된 투표 응답 메시지(Response message)에 포함된 voteGranted의 값이 'false'이면, 후보 노드는 다시 투표 대상 노드로 전환될 수 있다(도면부호 316).

[0078] 또한, 후보 노드는 복수의 투표 대상 노드로부터 voteGranted의 'true' 값이 과반 이상이면(즉, 투표 대상 노드로부터 동의 응답('true' 값)을 절반 이상 획득하면), 리더 노드로 전환될 수 있다(도면부호 317).

[0079] 다음으로, 복수의 투표 대상 노드는 팔로워 노드가 될 수 있으며, 리더 노드 및 복수의 팔로워 노드는 로그 복제 과정을 수행할 수 있다.

[0080] 이후, 기 설정된 리더 노드의 재결정 조건에 부합하는 상황이 발생되면(도면부호 318), 리더 노드는 다시 투표 대상 노드로 전환되어 리더 선출 모드가 재수행될 수 있으며, 예를 들면, 리더 노드의 재결정 조건은 네트워크 충돌(crash)이 발생된 후 재시작이되는 조건 및 텀(term)의 번호 및 마지막 셀의 번호(lastCell) 중 적어도 하나의 번호가 리더 노드보다 높은 다른 노드가 검색이 되는 조건 중 적어도 하나의 조건을 포함할 수 있다.

[0081] 한편, 새로운 리더가 선출될 때마다 각 노드의 셀 번호는 초기화될 수 있으며, 이를 통해 의미없는 번호의 증가에 따른 시스템 오류의 발생을 방지할 수 있다.

[0082] 도 3b에 따르면, 리더 노드 및 복수의 팔로워 노드 각각에서 클라이언트 단말로부터 트랜잭션을 수신할 때 마다 리더 노드 및 복수의 팔로워 노드 각각은 로컬 스토리지에 트랜잭션에 대응되는 트랜잭션 로그를 저장하고, 리더 노드 및 팔로워 노드 각각은 로컬 스토리지에 저장된 트랜잭션 로그의 크기가 셀의 크기에 도달하면 리더 노드 및 복수의 팔로워 노드 각각에 구비된 상태 머신에 리더 노드 및 복수의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어할 수 있다.

[0083] 구체적으로, 클라이언트 단말에서 이벤트로 인해 트랜잭션이 발생되면, 클라이언트 단말은 리더 노드에 트랜잭션을 발생에 따른 알림 정보를 제공할 수 있다(도면부호 321).

[0084] 다음으로, 리더 노드는 리더 노드에 구비된 로컬 스토리지에 트랜잭션 로그를 기록하고(도면부호 322), 기록된 로그를 포함하는 AppendEntries RPC 메시지를 복수의 팔로워 노드 각각에 전송할 수 있다(도면부호 323).

[0085] 예를 들면, AppendEntries RPC 메시지 및 AppendEntries RPC 메시지에 대응되는 팔로워 노드의 응답 메시지(response message)는 하기 표2에 도시된 정보들을 포함할 수 있다.

표 2

[0086]

type	Arguments	Description
Append Entries RPC message	term	리더 노드의 현재 텀의 번호
	cell	리더노드의 현재 셀의 번호
	lastCellHash	리더노드의 상태 머신에 커밋된 마지막 셀의 해시 값
	leaderID	블록체인 네트워크에 참여하는 노드(서버)의 고유 아이디
	logEntries	상태 머신에 추가해야 하는 로그 항목(heartbeat 메시지의 경우 이 배열은 제외됨)
	prevTerm	새 로그 바로 이전 로그 항목에 대한 텀의 번호
	prevCell	새 로그 바로 이전 로그 항목에 대한 셀의 번호
	prevIndex	새 로그 바로 이전 로그 항목에 대한 인덱스의 번호
response message	term	팔로워 노드의 현재 텀의 번호
	cell	팔로워 노드의 현재 셀의 번호
	logGranted	true 또는 false(로그가 성공적으로 저장되면 true, 반대이면 false)
	lastCellHash	팔로워 노드의 상태 머신에 커밋된 마지막 셀의 해시 값
	currentCellHash	팔로워 노드의 상태 머신에 커밋된 현재 셀의 해시 값

[0087] 다음으로, 팔로워 노드는 리더 노드로부터 수신한 로그를 팔로워 노드에 구비된 로컬 스토리지에 기록할 수 있으며(도면부호 324), 상술한 도면부호 321 내지 324의 과정은 로그가 미리 정해진 셀 크기로 채워질 때까지 반복 수행될 수 있다.

[0088] 한편, 리더 노드와 복수의 팔로워 노드 각각은 셀의 해시 값에 대한 비교 동작에 기초하여 로컬 오류(local failure)의 발생 여부를 판단하고, 판단 결과에 기초하여 리더 노드의 로컬 스토리지에 저장된 트랜잭션 로그를 로컬 오류가 발생된 팔로워 노드의 로컬 스토리지에 저장할 수 있다.

[0089] 구체적으로, 리더 노드와 팔로워 노드는 로그가 셀의 크기만큼 채워지면, 셀에 있는 모든 로그를 수집하여 수집된 로그의 해시 값(n번째 셀의 해시값 $H(C_n)$)을 도출할 수 있다(도면부호 325-1, 325-2).

[0090] 다음으로, 팔로워 노드는 $H(C_n)$를 포함하는 응답 메시지를 리더 노드에 전송할 수 있으며(도면부호 326, 327), 리더 노드는 팔로워 노드의 $H(C_n)$가 리더 노드의 $H(C_n)$와 일치하면 커밋을 준비하고(도면부호 328), 일치하지 않으면 리더 노드의 현재 셀에 저장된 현재 로그를 팔로워 노드에 전송하여 리더 노드의 현재 셀에 저장된 현재 로그를 팔로워 노드의 로컬 스토리지에 저장할 수 있다.

[0091] 다음으로, 리더 노드는 트랜잭션에 대한 처리 결과를 클라이언트 단말에 통지할 수 있다.

[0092] 보다 구체적으로, 도 3c 및 도 3d에 따르면, 로그 복제 과정에서 로그는 도면부호 330에 도시된 바와 같이 리더 노드의 로그 순서대로 각 노드에 저장되고, 셀의 크기는 CBR에 기초하는 일실시예에 따른 블록체인 시스템이 시작될 때 서버에서 지정되며, 이전 리더의 충돌로 인해 'Term 1'의 마지막 셀이 현재 리더의 로그 시퀀스를 기반으로 커밋될 수 있다.

[0093] 로그 인덱스가 일치하지 않는 오류를 로컬 오류(local failure)라 하며, 로그 인덱스가 일치하더라도 셀 번호 등이 일치하지 않는 경우에도 로컬 오류로 간주되며, 이때 팔로워 노드는 리더 노드부터의 새로운 로그의 수신 동작을 정지할 수 있다.

[0094] 이러한 경우는 heartbeat 메시지의 인수로 식별되며 리더가 이전 셀의 로그를 로컬 오류가 발생한 팔로워 단말에게 전송하여 로컬 오류 문제를 해결할 수 있다.

[0095] 여기서, 이전 셀의 로그가 내용과 순서가 완전히 일치하면 'lastCellHash'의 값은 $H(C_{n-1})$의 값이 되며(도면부호 340의 $H(C_0)$의 값), 그런 다음 리더 노드는 로그가 셀 크기만큼 채워질 때까지 팔로워에게 로그를 보낼 수 있다.

[0096] 다음으로, 리더 노드는 셀의 크기로 로그가 채워질때까지 팔로워 노드에 로그를 전송하며 리더 노드를 기준으로

현재 셀이 모두 채워지면, 리더 노드는 'lastCellHash'를 $H(C_1)$로 변경하고 AppendEnries RPC 메시지의 'cell' 및 'prevCell' 값을 올릴 수 있다.

[0097] 또한, 팔로워 노드에 저장된 현재 셀의 로그가 리더 노드와 완벽하게 일치하면, 팔로워는 logGranted 값으로 'true'를 응답하고 lastCellHash로 $H(C_1)$을 응답할 수 있다.

[0098] 그러나, 팔로워 노드는 현재 셀의 로그가 비어 있거나 순서가 잘못된 경우에는 $H(C_1)$ 값이 리더 노드의 $H(C_1)$과 다르며, 이때 팔로워 노드는 커밋할 수 없는 실패(fail) 상태이므로 logGranted 값을 'false'로 응답하며, 응답 메시지에서 logGranted로 'false'를 받은 리더 노드는 자신의 셀의 모든 로그를 전송하여 팔로워 노드가 이 로그를 덮어 쓰도록 제어할 수 있다.

[0100] 도 4a 내지 도 4g는 일실시예에 따른 블록체인 시스템의 성능 시험 결과를 설명하기 위한 도면이다.

[0101] 도 4a 내지 도 4g를 참조하면, 도면부호 410은 기존 래프트 알고리즘을 이용하는 블록체인 시스템의 노드 수에 따른 AppendEntries RPC 메시지 수를 예시하고, 도면부호 420은 기존 래프트 알고리즘에 기반하는 블록체인 시스템의 노드 수에 따른 TPS 값을 예시한다.

[0102] 또한, 도면부호 430은 셀 기반 래프트 알고리즘을 이용하는 일실시예에 따른 블록체인 시스템에서 셀 크기의 변화에 따른 TPS 및 실패(fail) 응답 메시지 간의 상관관계를 예시하고, 도면부호 440은 일실시예에 따른 블록체인 시스템에서 수행되는 연합 학습에 사용된 에폭(epochs)의 평균 정확도 값을 예시하며, 도면부호 450은 일실시예에 따른 블록체인 시스템에서 수행되는 연합 학습에 의한 훈련 손실(training loss) 값을 예시한다.

[0103] 또한, 도면부호 460은 일실시예에 따른 블록체인 시스템의 노드 수에 따른 AppendEntries RPC 메시지 수를 예시하고, 도면부호 470은 일실시예에 따른 블록체인 시스템의 노드 수에 따른 TPS 값을 예시한다.

[0104] 도면부호 410 및 420에 따르면, 기존 블록체인 시스템은 노드 수가 일정한 크기로 증가함에 따라 AppendEntries RPC 메시지 또한 점진적으로 증가하는 것을 확인할 수 있으며, 반면 TPS는 노드 수가 증가함에 따라 지속적으로 감소되는 것을 확인할 수 있다.

[0105] 이러한 결과는 기존 래프트 알고리즘을 이용하는 블록체인 시스템이 리더 노드의 로드 밸런싱 문제로 인해 전체 시스템에 영향을 미칠 수 있음을 의미하며, 이는 블록체인 시스템에서 심각한 과부하로 이어질 수 있음을 시사한다.

[0106] 이에, 일실시예에 따른 블록체인 시스템은 최적화된 크기를 갖는 셀 기반의 래프트 알고리즘을 이용하여 상술한 문제를 최소화할 수 있다.

[0107] 도면부호 430에 따르면, 일실시예에 따른 블록체인 시스템은 셀의 개수가 45개를 초과하면서부터 실패 응답 메시지 수가 급격히 증가하는 것을 확인할 수 있으며, 이는 셀의 크기가 무조건 커지면 안되고 리더 노드와 팔로워 노드가 모두 수용할 수 있는 최적의 셀 크기를 확보해야함을 의미한다.

[0108] 도면부호 440 및 450에 따르면, 일실시예에 따른 블록체인 시스템은 연합 학습을 통해 노드의 로컬 모델이 업데이트될수록 최적화된 셀의 크기를 확보할 수 있음을 확인할 수 있다.

[0109] 구체적으로, 일실시예에 따른 블록체인 시스템은 기 설정된 시간동안 복수의 노드로부터 TPS 정보, 커밋 실패 메시지(즉, 실패 응답 메시지)를 수집하고, 수집된 정보와 복수의 블록체인 노드의 개수를 입력 데이터로 수신하는 연합 학습 모델을 통해 셀의 크기를 최적화할 수 있다.

[0110] 바람직하게는, 일실시예에 따른 블록체인 시스템은 연합 학습을 통해 하기 표3과 같이 평균 정확도(average accuracy)를 고려한 노드의 개수에 따른 최적화된 셀의 크기(average accuracy)를 도출할 수 있다.

표 3

[0111]

Node	optimized cell size	average accuracy
5	80	99.82%
10	75	98.49%
15	75	99.50%
20	65	98.66%
25	70	96.22%

30	55	95.59%
35	60	98.76%
40	50	97.80%
45	50	97.89%
50	55	98.75%
55	50	99.44%
60	40	96.67%
65	45	98.27%
70	40	99.59%
75	40	99.68%
80	35	98.87%
85	30	96.57%
90	35	98.11%
95	20	97.68%
100	25	99.19%

[0112] 도면부호 460에 따르면, 'proposed optimal CBR'은 연합 학습을 통해 최적화된 셀 크기에 기반하는 CBR 알고리즘을 적용하였을 때의 AppendEntries RPC 메시지의 개수를 나타내고, 'proposed static CBR'은 셀의 크기가 40으로 고정된 CBR을 적용하였을 때의 AppendEntries RPC 메시지의 개수를 나타내며, 'traditional Raft'는 기존의 래프트 알고리즘을 적용하였을 때의 AppendEntries RPC 메시지의 개수를 나타낸다.

[0113] 구체적으로, 두 CBR은 기존 래프트 알고리즘 보다 시스템의 과부하가 현저히 감소(평균 45.03% 감소)하는 것을 확인할 수 있으며, 여기서 두 CBR은 메시지 수의 차이가 거의 없음을 확인할 수 있는데, 이는 기본적으로 노드 수가 같을 때 셀 크기가 크면 교환되는 메시지의 수가 필연적으로 줄어들게 되기 때문엔 것으로 분석된다.

[0114] 도면부호 470에 따르면, 노드의 수가 증가함에 따라 두 CBR과 기존 래프트 알고리즘 모두 TPS가 감소하는 것을 확인할 수 있다.

[0115] 특히 블록체인 시스템이 리소스 허용 범위를 벗어나면 TPS가 급격하게 낮아져 거의 로그 처리가 불가능해지며, 이 경우 연합 학습을 통해 셀 크기를 결정하거나 최적화된 셀 값을 얻는 경우 TPS 값이 기존 라프트 알고리즘 보다 높게 나타나는 것을 확인할 수 있다. 즉, 일실시예에 따른 CBR은 기존 래프트 알고리즘 보다 안정적인 성능을 보장하는 것을 확인할 수 있다.

[0117] 도 5는 일실시예에 따른 블록체인 시스템의 동작방법을 설명하기 위한 도면이다.

[0118] 다시 말해, 도 5는 도 1 내지 도 4g를 통해 설명한 일실시예에 따른 블록체인 시스템의 동작방법을 설명하는 도면으로, 이하에서 도 5를 통해 설명하는 내용 중 도 1 내지 도 4g를 통해 설명한 내용과 중복되는 설명은 생략하기로 한다.

[0119] 도 5를 참조하면, 510 단계에서 동작방법은 셀 크기 결정부에서, 복수의 블록체인 노드의 개수에 기초하여 셀의 크기를 결정하도록 제어할 수 있다.

[0120] 일측에 따르면, 510 단계에서 동작방법은 셀 크기 결정부에서, 기 설정된 시간동안 복수의 블록체인 노드로부터 TPS(transaction per second) 정보, 커밋 실패 메시지 중 적어도 하나의 정보를 수집하고, 수집된 정보와, 복수의 블록체인 노드의 개수를 입력 데이터로 수신하는 연합 학습 모델을 통해 셀의 크기를 결정하도록 제어할 수 있다.

[0121] 다음으로, 520 단계에서 동작방법은 리더 선출부에서, 복수의 블록체인 노드 중 어느 하나의 노드가 리더 노드로 선출되고 복수의 블록체인 노드 중 리더 노드를 제외한 복수의 노드가 팔로워 노드로 설정 되도록 제어할 수 있다.

[0122] 일측에 따르면, 520 단계에서 동작방법은 리더 선출부에서, 복수의 블록체인 노드 중 어느 하나의 노드가 후보 노드로 전환되면, 후보 노드에서 복수의 블록체인 노드 중 후보 노드를 제외한 복수의 투표 대상 노드 각각으로, 후보 노드의 현재 텀(term)의 번호와 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호를 포함하는 투표 요청 메시지를 전송하도록 제어할 수 있다.

[0123] 또한, 520 단계에서 동작방법은 리더 선출부에서, 복수의 투표 대상 노드 각각에서, 후보 노드의 현재 텀의 번호 및 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호에 기초하여 후보 노드에 대한 투표 결과를 포함하는 투표 응답 메시지를 생성하고, 생성된 투표 응답 메시지에 기초하여 후보 노드를 리더 노드로 선출 되도록 제어할 수 있다.

[0124] 예를 들면, 복수의 투표 대상 노드 중 어느 하나의 투표 대상 노드는 후보 노드의 현재 텀의 번호가 어느 하나의 투표 대상 노드의 현재 텀의 번호 보다 크고, 후보 노드의 상태 머신에 커밋된 마지막 셀의 번호가 어느 하나의 투표 대상 노드의 상태 머신에 커밋된 마지막 셀의 번호 보다 크거나 같으면, 후보 노드를 리더 노드로 선출하는데 동의하는 결과를 포함하는 투표 응답 메시지를 생성할 수 있다.

[0125] 다음으로, 530 단계에서 동작방법은 로그 복제부에서, 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 노드가 클라이언트 단말로부터 트랜잭션을 수신하면 리더 노드와 복수의 팔로워 노드 간의 로그 복제 과정이 수행되도록 제어하되, 셀 크기 결정부를 통해 결정된 크기의 셀 단위로 로그 복제 과정이 수행되도록 제어할 수 있다.

[0126] 일측에 따르면, 530 단계에서 동작방법은 로그 복제부에서, 리더 노드 및 복수의 팔로워 노드 각각에서, 클라이언트 단말로부터 트랜잭션을 수신할 때 마다 리더 노드 및 복수의 팔로워 노드 중 적어도 하나의 팔로워 노드 각각에 구비된 로컬 스토리지에 트랜잭션에 대응되는 트랜잭션 로그를 저장하고, 리더 노드 및 적어도 하나의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그의 크기가 셀의 크기에 도달하면 리더 노드 및 복수의 팔로워 노드 각각에 구비된 상태 머신에 리더 노드 및 복수의 팔로워 노드 각각의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어할 수 있다.

[0127] 일측에 따르면, 530 단계에서 동작방법은 로그 복제부에서, 리더 노드의 n번째(여기서, n은 양의 정수) 셀의 해시 값과 적어도 하나의 팔로워 노드의 n번째 셀의 해시 값을 각각 비교하고, 비교 결과가 일치하면 리더 노드 및 적어도 하나의 팔로워 노드 각각에 구비된 상태 머신에 리더 노드 및 적어도 하나의 팔로워 노드의 로컬 스토리지에 저장된 트랜잭션 로그가 커밋 되도록 제어할 수 있다.

[0128] 또한, 530 단계에서 동작방법은 로그 복제부에서, 비교 결과가 일치하지 않는 것으로 나타나면, 리더 노드의 n번째 셀에 저장된 트랜잭션 로그를 비교 결과가 일치하지 않는 팔로워 노드에 전송하도록 제어할 수 있다.

[0130] 결국, 본 발명을 이용하면, 셀 기반의 래프트 알고리즘(CBR)을 이용하여 트랜잭션에 대한 커밋 처리를 크기가 최적화된 셀 단위로 수행하여, 시스템의 과부하 및 병목 현상을 최소화할 수 있다.

[0131] 또한, 본 발명을 이용하면, TPS(transaction per second) 정보에 기반하는 연합 학습을 통해 커밋 처리를 위한 셀의 크기를 최적화하여 트랜잭션 처리의 정확도를 향상시킬 수 있다.

[0132] 또한, 본 발명을 이용하면, 셀의 해시 값에 대한 비교 동작에 기초하여 로컬 오류(local failure)의 발생 여부를 판단하고 이에 대응함으로써, 트랜잭션 처리의 정확도를 향상시킬 수 있다.

[0134] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들면, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 장치, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0135] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

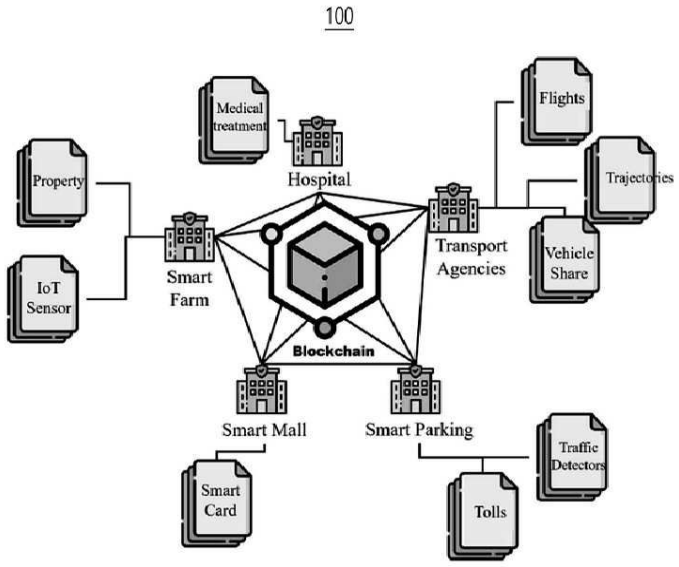
부호의 설명

[0136] 200: 블록체인 시스템 210: 리더 선출부

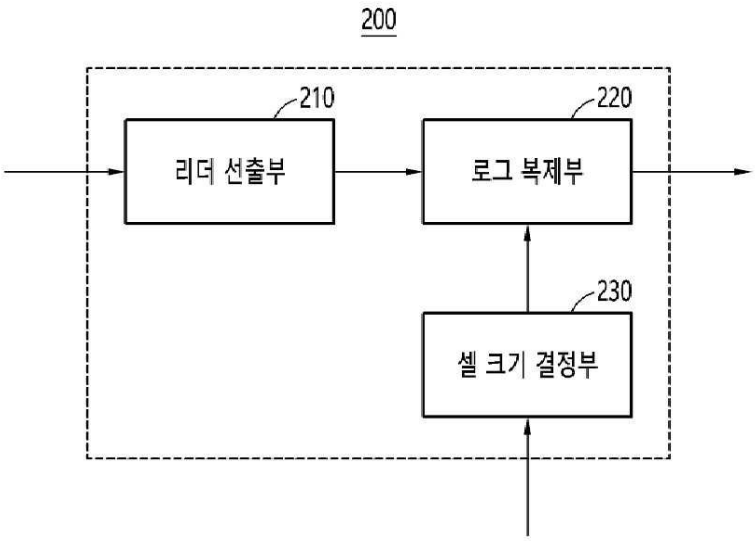
220: 로그 복제부 230: 셀 크기 결정부

도면

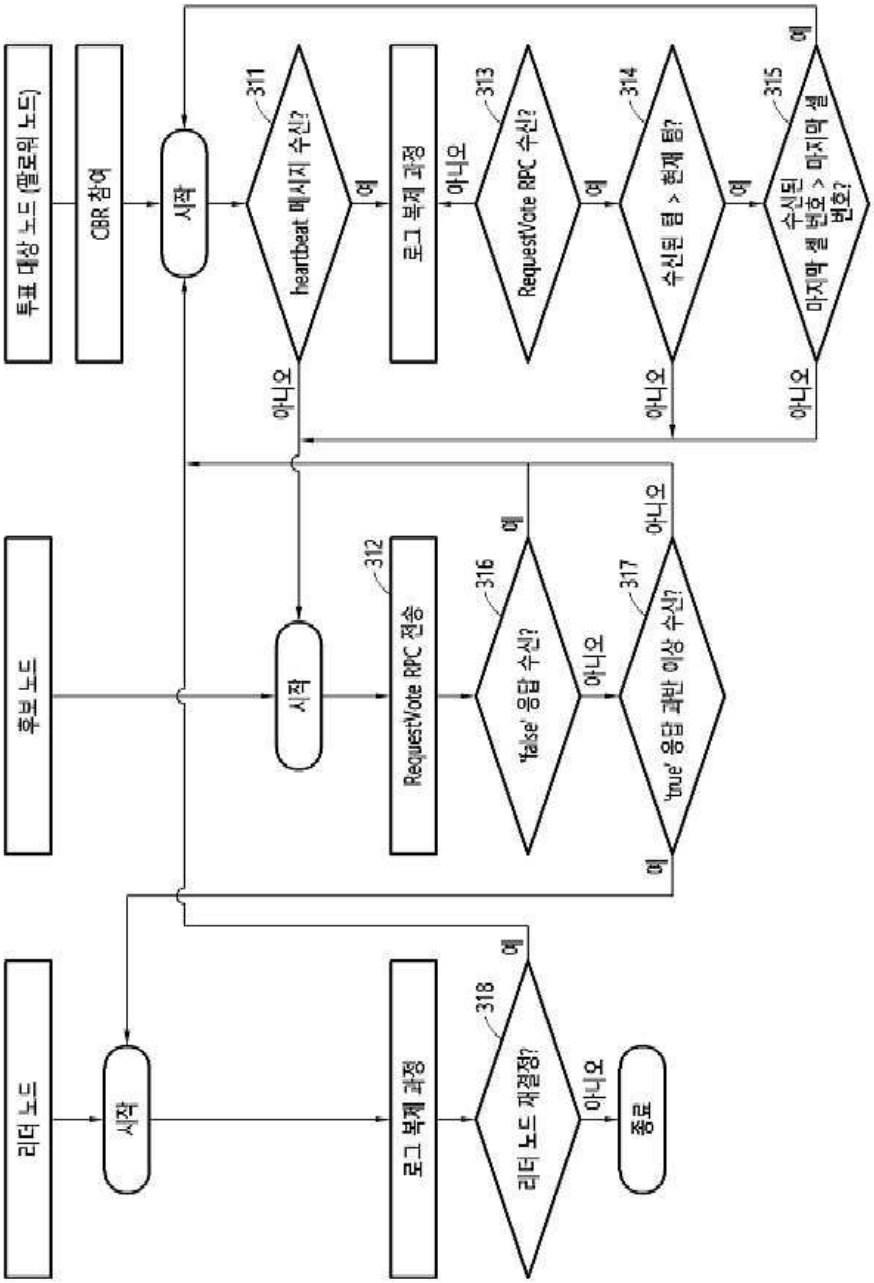
도면1


100
Medical treatment
Hospital
Property
Flights
Trajectories
Smart Farm
Transport Agencies
Vehicle Share
IoT Sensor
Blockchain
Smart Mall
Smart Parking
Traffic Detectors
Smart Card
Tolls

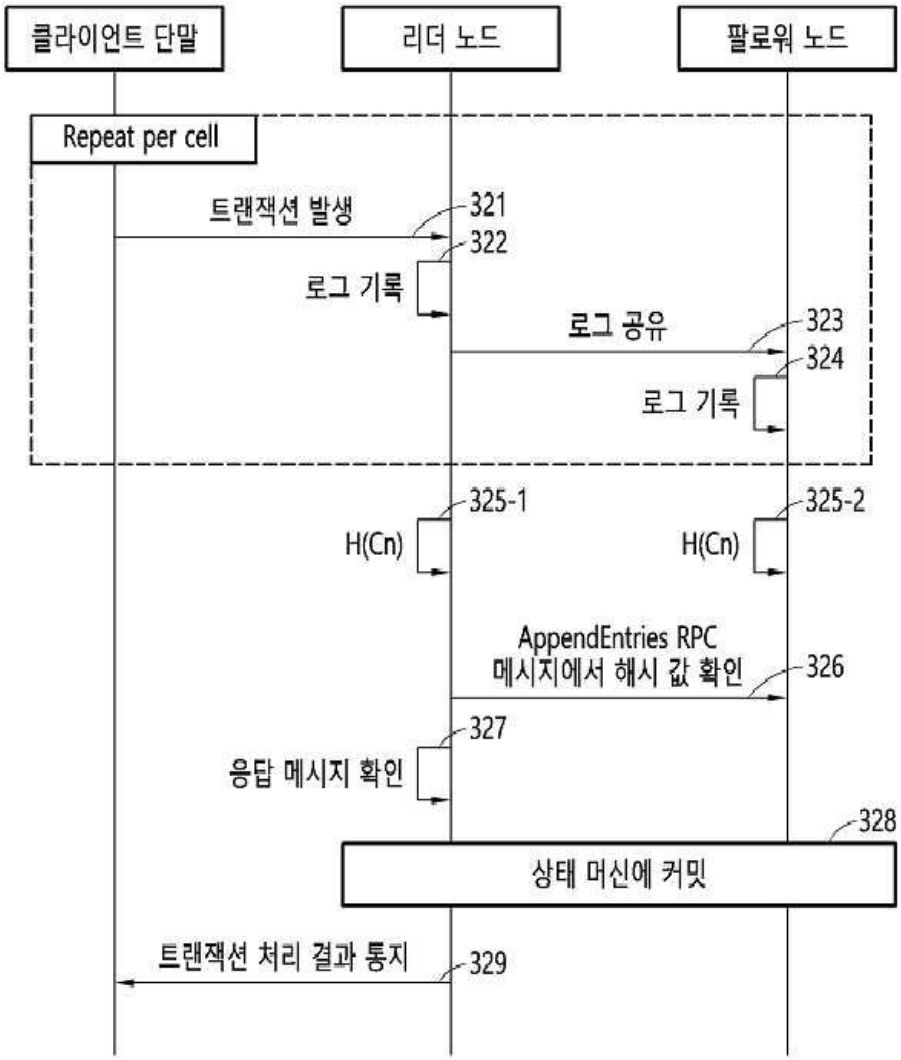
도면2


200
210
리더 선출부
220
로그 복제부
230
셀 크기 결정부

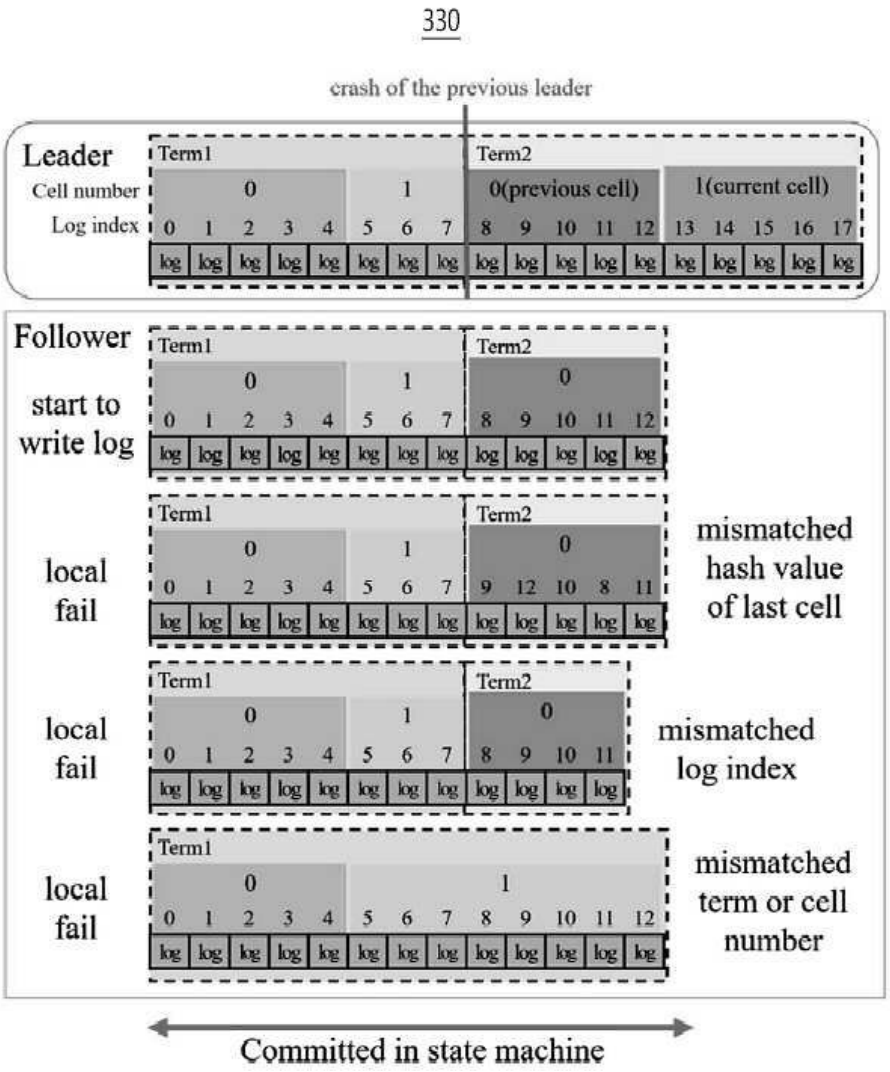
도면3a


투표 대상 노드 (팔로워 노드)
CBR 참여
시작
311
heartbeat 메시지 수신?
여
아니오
로그 복제 과정
313
RequestVote RPC 수신?
여
아니오
314
수신된 텀 > 현재 텀?
여
아니오
315
수신된 마지막 셀 번호 > 마지막 셀 번호?
예
아니오
후보 노드
시작
312
RequestVote RPC 전송
316
'false' 응답 수신?
예
아니오
317
'true' 응답 과반 이상 수신?
아니오
예
리더 노드
시작
로그 복제 과정
318
리더 노드 재결정?
예
아니오
종료

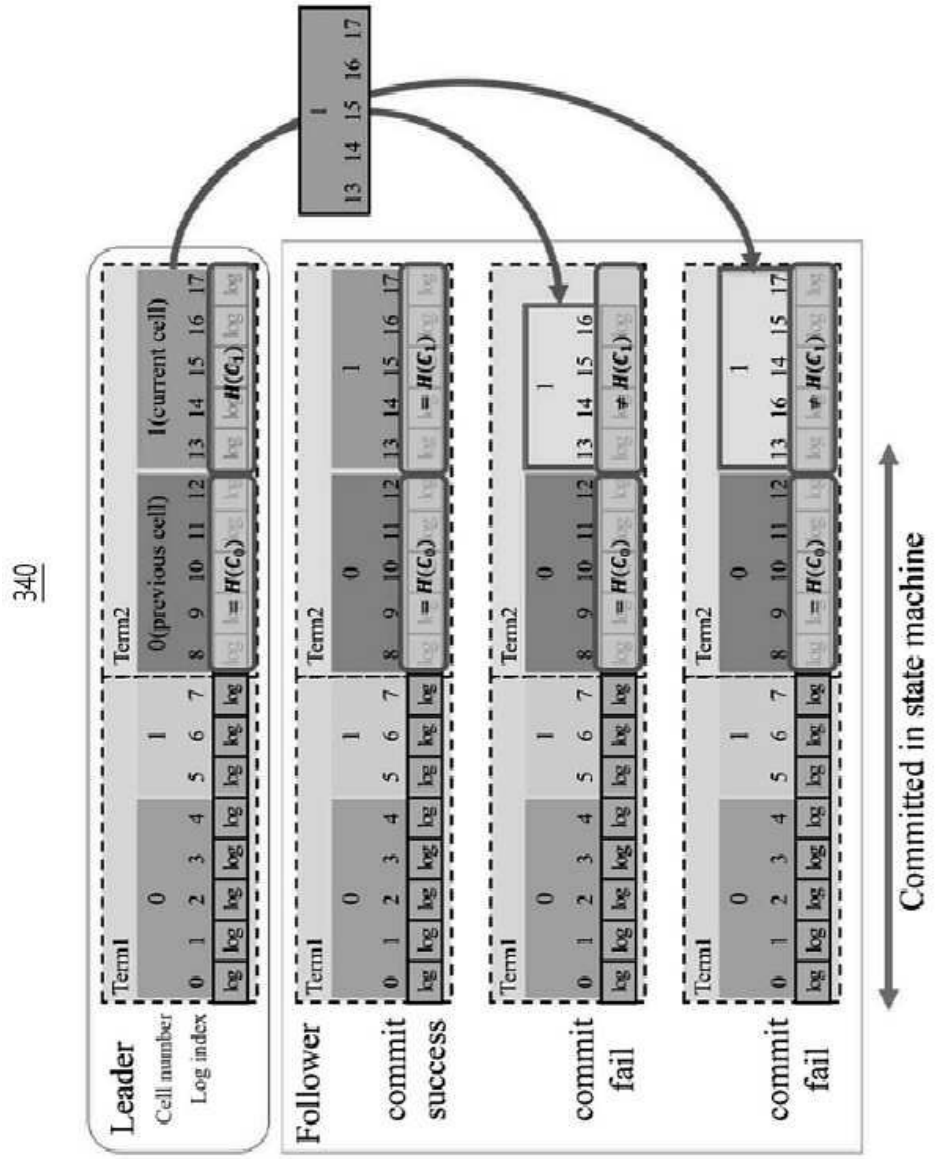
도면3b


클라이언트 단말
리더 노드
팔로워 노드
Repeat per cell
트랜잭션 발생
321
322
로그 기록
로그 공유
323
324
로그 기록
325-1
325-2
H(Cn)
H(Cn)
AppendEntries RPC
메시지에서 해시 값 확인
326
327
응답 메시지 확인
328
상태 머신에 커밋
트랜잭션 처리 결과 통지
329

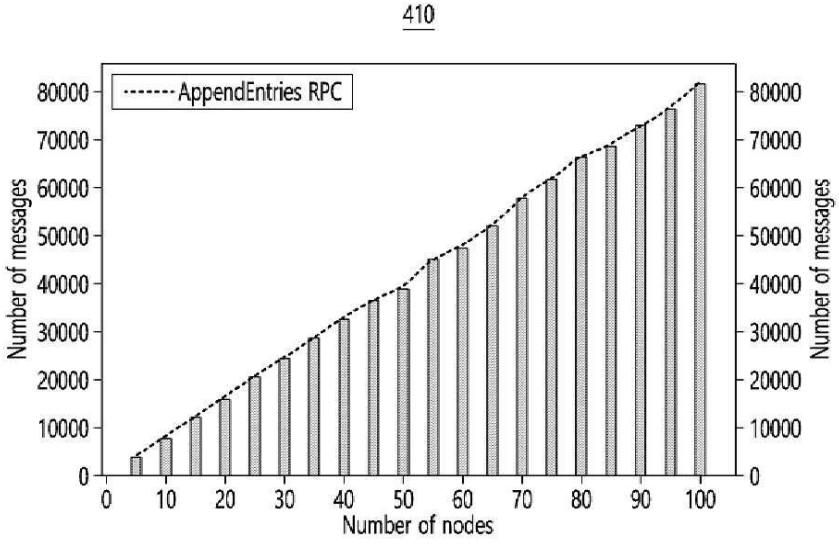
도면3c


330
crash of the previous leader
Leader
Cell number
Log index
Term1
Term2
0
1
0(previous cell)
1(current cell)
Follower
start to write log
local fail
mismatched hash value of last cell
mismatched log index
mismatched term or cell number
Committed in state machine

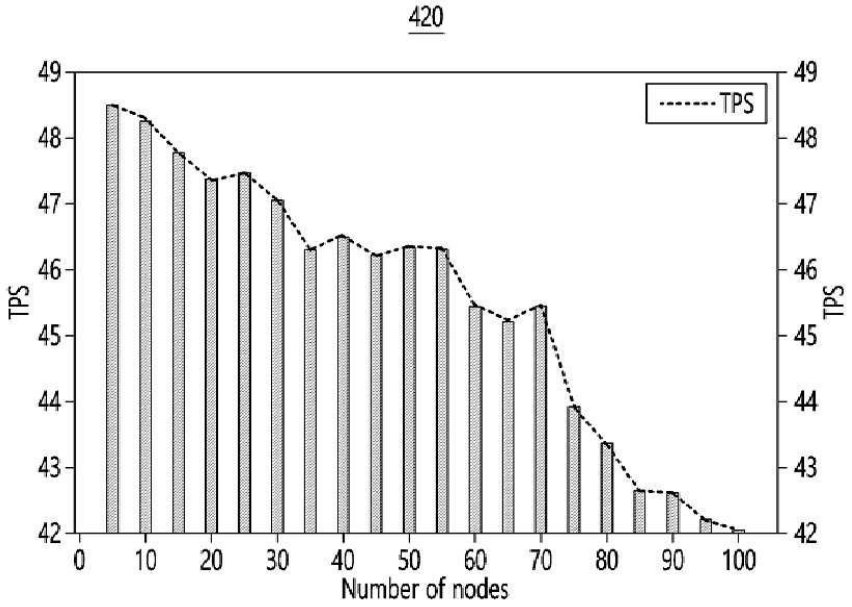
도면3d


340
Leader
Cell number
Log index
Term1
Term2
0(previous cell)
1(current cell)
Follower
commit success
commit fail
commit fail
Committed in state machine

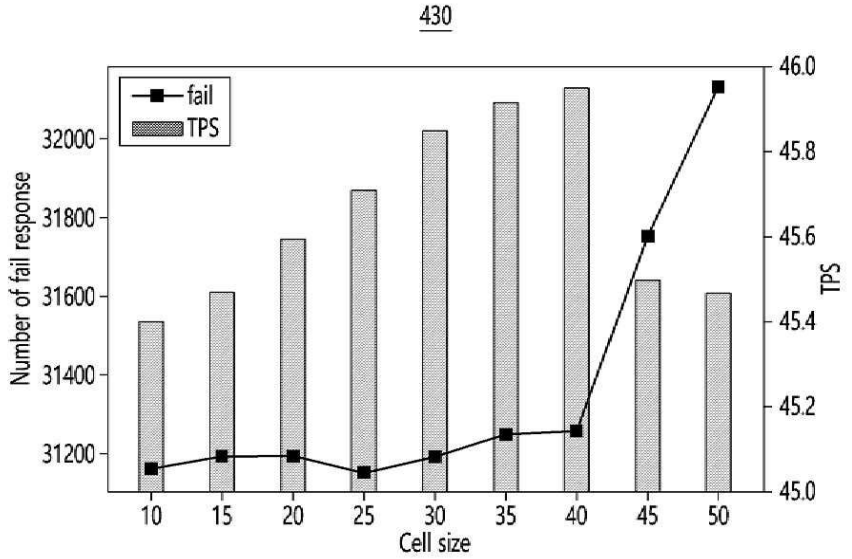
도면4a


410
AppendEntries RPC
Number of messages
Number of nodes
0
10000
20000
30000
40000
50000
60000
70000
80000
0
10
20
30
40
50
60
70
80
90
100

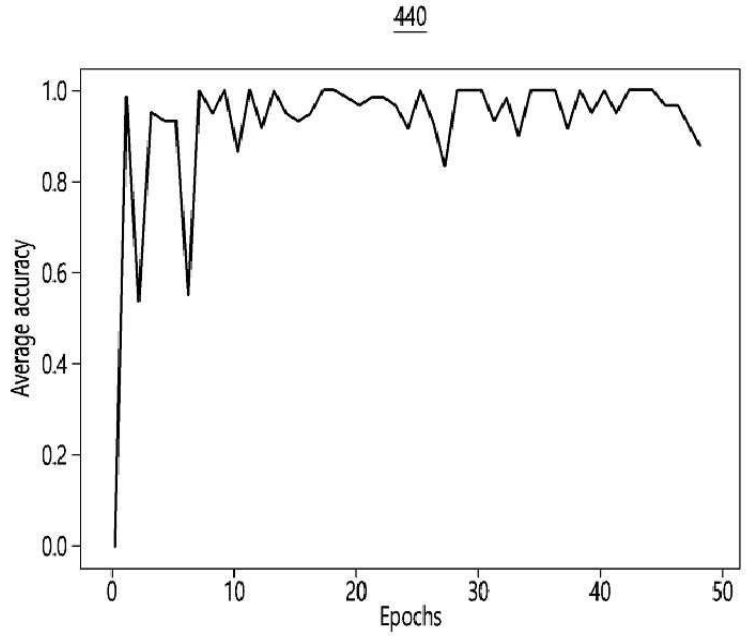
도면4b


420
TPS
49
48
47
46
45
44
43
42
0
10
20
30
40
50
60
70
80
90
100
Number of nodes

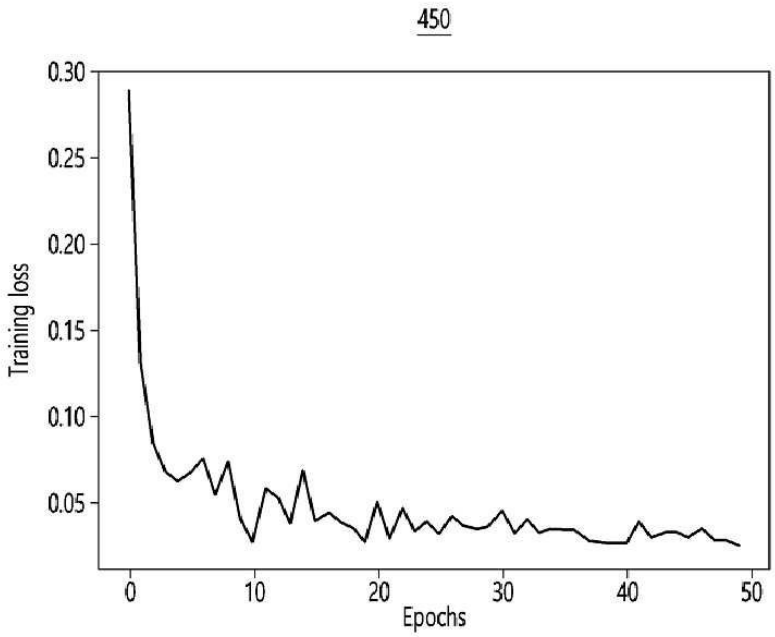
도면4c


430
fail
TPS
Number of fail response
32000
31800
31600
31400
31200
46.0
45.8
45.6
45.4
45.2
45.0
10
15
20
25
30
35
40
45
50
Cell size

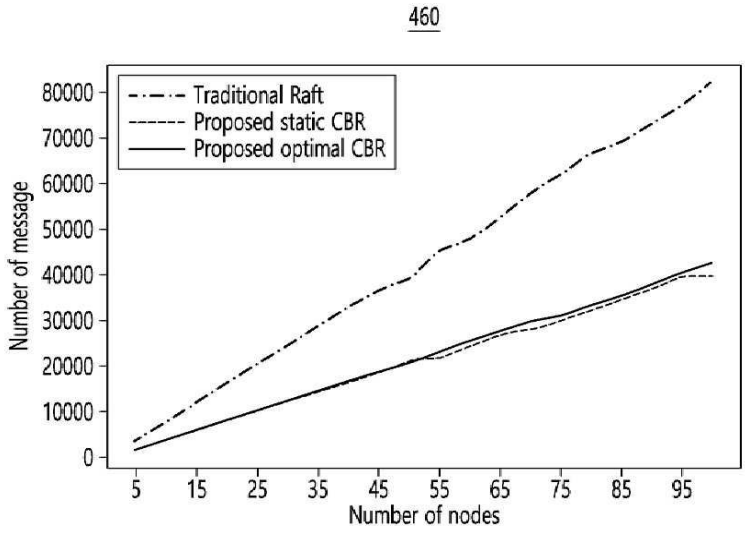
도면4d


440
Average accuracy
1.0
0.8
0.6
0.4
0.2
0.0
0
10
20
30
40
50
Epochs

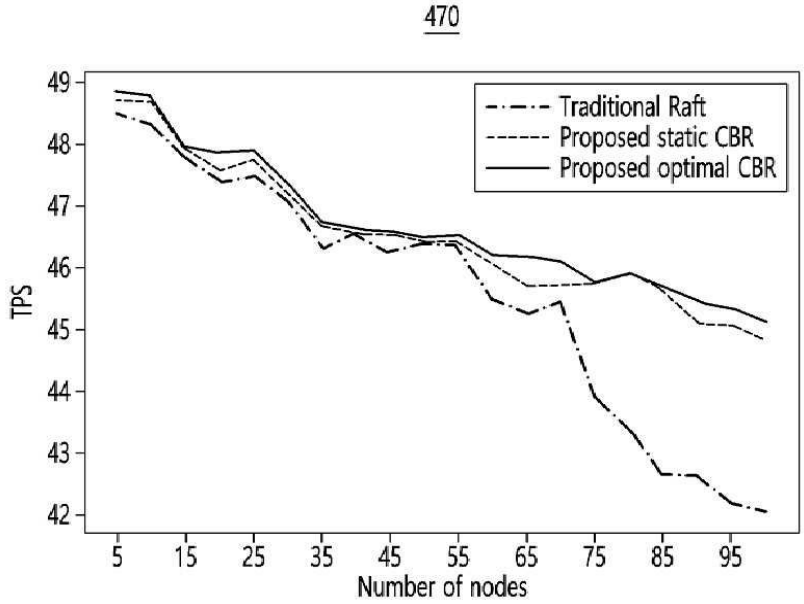
도면4e


450
Training loss
0.30
0.25
0.20
0.15
0.10
0.05
0
10
20
30
40
50
Epochs

도면4f


460
Traditional Raft
Proposed static CBR
Proposed optimal CBR
Number of message
80000
70000
60000
50000
40000
30000
20000
10000
0
5
15
25
35
45
55
65
75
85
95
Number of nodes

도면4g


470
Traditional Raft
Proposed static CBR
Proposed optimal CBR
TPS
49
48
47
46
45
44
43
42
5
15
25
35
45
55
65
75
85
95
Number of nodes

도면5

