(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년08월05일
(11) 등록번호 10-2285882
(24) 등록일자 2021년07월29일

(51) 국제특허분류(Int. Cl.)
G06F 11/18 (2006.01) *G06F 11/14* (2006.01)
G06Q 20/06 (2012.01) *G06Q 20/38* (2012.01)
H04L 29/08 (2006.01)
(52) CPC특허분류
G06F 11/183 (2013.01)
G06F 11/1433 (2013.01)
(21) 출원번호 10-2020-0044613
(22) 출원일자 2020년04월13일
심사청구일자 2020년04월13일
(65) 공개번호 10-2021-0061243
(43) 공개일자 2021년05월27일
(30) 우선권주장
1020190149136 2019년11월19일 대한민국(KR)
(56) 선행기술조사문헌
JP2019012510 A
CN110445619 A
KR1020190088530 A
KR1020190054738 A

(73) 특허권자
한양대학교 산학협력단
서울특별시 성동구 왕십리로 222(행당동, 한양대학교내)
(72) 발명자
정성욱
서울특별시 성동구 사근동10가길 18, 203호
유민수
서울특별시 서초구 강남대로61길 23, 2201호(서초동, 현대성우주상복합아파트)
(74) 대리인
정성준, 윤종원, 최영수

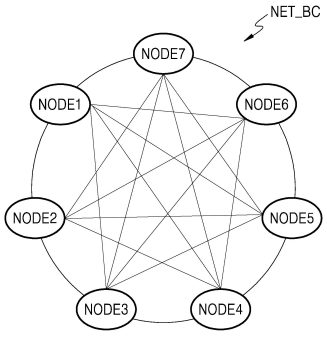
전체 청구항 수 : 총 15 항 심사관 : 김계준

(54) 발명의 명칭 **가변 정족수 기반의 블록체인 합의 방법, 이를 이용하는 블록체인 노드 및 프로그램**

(57) 요 약

본 발명의 실시 예에 따른 가변 정족수 기반의 블록체인 합의 방법은 리더 블록체인 노드로부터 전송된 신규 생성 블록과 상기 신규 생성 블록에 대한 합의 요청 메시지에 따라, 상기 리더 블록체인 노드와 참여 블록체인 노드들이 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트(broadcast)하는 단계, 상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 단계 및 상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
G06F 11/187 (2018.01)
G06Q 20/065 (2013.01)
G06Q 20/382 (2013.01)
H04L 67/104 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093529
과제번호	2019-0-00458-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발(R&D)
연구과제명	블록체인 확장성 개선을 위한 위임형 비잔틴 합의 알고리즘 개발과 검증
기 여 율	1/1
과제수행기관명	한양대학교 산학협력단
연구기간	2019.04.01 ~ 2019.12.31

명 세 서

청구범위

청구항 1

리더 블록체인 노드로부터 전송된 신규 생성 블록과 상기 신규 생성 블록에 대한 합의 요청 메시지에 따라, 상기 리더 블록체인 노드와 참여 블록체인 노드들이 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트(broadcast)하는 단계;

상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 단계; 및

상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 단계를 포함하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 2

제1항에 있어서,

상기 신규 생성 블록과 상기 합의 요청 메시지는 서로 분리되어 전송되는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 3

제1항에 있어서,

상기 참여 블록체인 노드들은,

정해진 시간 내에 상기 신규 생성 블록과 상기 합의 요청 메시지를 수신하지 못한 경우에 상기 무효의 투표 메시지를 브로드캐스트 하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 4

제1항에 있어서,

상기 비잔틴 오류가 발생한 경우는,

비정상적인 메시지를 전송한 경우, 정해진 시간 내에 메시지를 전송하지 않은 경우, 또는 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우인, 가변 정족수 기반의 블록체인 합의 방법.

청구항 5

제4항에 있어서,

상기 비정상적인 메시지를 전송한 경우는,

블록체인의 프로토콜(protocol)에 어긋나는 메시지를 전송한 경우인, 가변 정족수 기반의 블록체인 합의 방법.

청구항 6

제4항에 있어서,

두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우는,

상기 정상적인 메시지들 각각은 블록체인의 프로토콜에 맞게 작성되었으나, 이중으로 투표한 경우인, 가변 정족수 기반의 블록체인 합의 방법.

청구항 7

제1항에 있어서,

상기 기설정된 정족수를 변경하는 단계는,

상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수는 상기 기설정된 정족수에서 빼지 않고, 상기 비잔틴 오류가 발생한 블록체인 노드의 수만 상기 기설정된 정족수에서 뺀 값으로 상기 기설정된 정족수를 변경하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 8

제4항에 있어서,

상기 기설정된 정족수를 변경하는 단계는,

상기 비정상적인 메시지를 전송한 경우 또는 정해진 시간 내에 메시지를 전송하지 않은 경우의 상기 비잔틴 오류를 검출하여, 상기 기 설정된 정족수를 변경하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 9

제8항에 있어서,

상기 가변 정족수 기반의 블록체인 합의 방법은,

상기 리더 블록체인 노드와 상기 참여 블록체인 노드들 각각이 수신한 모든 투표 메시지와 자신이 전송한 투표 메시지를 모아서 추가적으로 브로드캐스트하는 단계를 더 포함하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 10

제9항에 있어서,

상기 가변 정족수 기반의 블록체인 합의 방법은,

상기 추가적으로 브로드캐스트하는 단계 이후에,

상기 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우의 상기 비잔틴 오류를 검출하여, 변경된 상기 정족수를 추가적으로 변경하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 11

제10항에 있어서,

상기 변경된 상기 정족수를 추가적으로 변경하는 단계는,

네트워크 오류에 의하여 투표에 참여하지 못하였던 참여 블록체인 노드를 포함시켜, 상기 변경된 상기 정족수를 추가적으로 변경하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 12

제11항에 있어서,

상기 합의 여부를 결정하는 단계는,

상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 추가적으로 변경된 상기 정족수 이상인지에 따라 상기 합의 여부를 결정하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 13

제1항에 있어서,

상기 가변 정족수 기반의 블록체인 합의 방법은,

상기 리더 블록체인 노드가 정해진 시간 내에 상기 신규 생성 블록과 상기 합의 요청 메시지를 전송하지 않는 경우에, 상기 리더 블록체인 노드를 변경하는 단계를 더 포함하는, 가변 정족수 기반의 블록체인 합의 방법.

청구항 14

신규 생성 블록에 대한 합의 요청 메시지를 생성하는 합의 요청 메시지 생성 모듈;

상기 신규 생성 블록과 상기 합의 요청 메시지를 브로드캐스트하고, 참여 블록체인 노드들이 상기 신규 생성 블록과 상기 합의 요청 메시지에 응답하여 전송한 동의, 거절, 또는 무효의 투표 메시지를 수신하는 통신 인터페이스;

상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 정족수 변경 모듈; 및

상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 합의 결과 처리 모듈을 포함하는, 블록체인 노드.

청구항 15

프로세서(processor)와 결합되어 가변 정족수 기반의 블록체인 합의 방법을 수행하기 위한 컴퓨터 기록 매체에 저장된 프로그램으로서,

리더 블록체인 노드로부터 전송된 신규 생성 블록과 상기 신규 생성 블록에 대한 합의 요청 메시지에 따라, 상기 리더 블록체인 노드와 참여 블록체인 노드들이 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트(broadcast)하는 단계;

상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 단계; 및

상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 단계를 수행하는, 컴퓨터 기록 매체에 저장된 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 가변 정족수 기반의 블록체인 합의 방법, 이를 이용하는 블록체인 노드 및 프로그램에 관한 것으로, 보다 상세하게는 비잔틴 오류가 발생한 참여 블록체인 노드의 수와 무효의 투표 메시지를 발행한 참여 블록체인 노드의 수에 기초하여 정족수를 변경하여 합의 여부를 결정할 수 있는 가변 정족수 기반의 블록체인 합의 방법,

이를 이용하는 블록체인 노드 및 프로그램에 관한 것이다.

배 경 기 술

[0003] 블록체인이란 익명성과 무결성이 보장되면서도 모든 데이터가 암호화되어 블록이라는 구조체에 기록되어 데이터의 신뢰성을 확보할 수 있는 분산 플랫폼이다.

[0004] 블록체인은 거래에 참여하는 모든 사용자에게 거래 명세를 공유하며, 거래가 진행될 때마다 거래 명세를 대조하여 데이터 위조를 막을 수 있다. 블록체인 내의 사용자들은 각자 자신의 원장(ledger)을 가지며, 원장의 내용은 합의 알고리즘에 의하여 동일하게 유지될 수 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 기술적 사상이 이루고자 하는 과제는 비잔틴 오류가 발생한 참여 블록체인 노드의 수와 무효의 투표 메시지를 발행한 참여 블록체인 노드의 수에 기초하여 정족수를 변경하여 합의 여부를 결정할 수 있는 가변 정족수 기반의 블록체인 합의 방법, 이를 이용하는 블록체인 노드 및 프로그램을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 일 실시 예에 따른 가변 정족수 기반의 블록체인 합의 방법은 리더 블록체인 노드로부터 전송된 신규 생성 블록과 상기 신규 생성 블록에 대한 합의 요청 메시지에 따라, 상기 리더 블록체인 노드와 참여 블록체인 노드들이 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트(broadcast)하는 단계, 상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 단계 및 상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 단계를 포함할 수 있다.

[0009] 실시 예에 따라, 상기 신규 생성 블록과 상기 합의 요청 메시지는 서로 분리되어 전송될 수 있다.

[0010] 실시 예에 따라, 상기 참여 블록체인 노드들은, 정해진 시간 내에 상기 신규 생성 블록과 상기 합의 요청 메시지를 수신하지 못한 경우에 상기 무효의 투표 메시지를 브로드캐스트 할 수 있다.

[0011] 실시 예에 따라, 상기 비잔틴 오류가 발생한 경우는, 비정상적인 메시지를 전송한 경우, 정해진 시간 내에 메시지를 전송하지 않은 경우, 또는 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우일 수 있다.

[0012] 실시 예에 따라, 상기 비정상적인 메시지를 전송한 경우는, 블록체인의 프로토콜(protocol)에 어긋나는 메시지를 전송한 경우일 수 있다.

[0013] 실시 예에 따라, 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우는, 상기 정상적인 메시지들 각각은 블록체인의 프로토콜에 맞게 작성되었으나, 이중으로 투표한 경우일 수 있다.

[0014] 실시 예에 따라, 상기 기설정된 정족수를 변경하는 단계는, 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수는 상기 기설정된 정족수에서 빼지 않고, 상기 비잔틴 오류가 발생한 블록체인 노드의 수만 상기 기설정된 정족수에서 뺀 값으로 상기 기설정된 정족수를 변경할 수 있다.

[0015] 실시 예에 따라, 상기 기설정된 정족수를 변경하는 단계는, 상기 비정상적인 메시지를 전송한 경우 또는 정해진 시간 내에 메시지를 전송하지 않은 경우의 상기 비잔틴 오류를 검출하여, 상기 기 설정된 정족수를 변경할 수 있다.

[0016] 실시 예에 따라, 상기 가변 정족수 기반의 블록체인 합의 방법은, 상기 리더 블록체인 노드와 상기 참여 블록체인 노드들 각각이 수신한 모든 투표 메시지와 자신이 전송한 투표 메시지를 모아서 추가적으로 브로드캐스트하는 단계를 더 포함할 수 있다.

[0017] 실시 예에 따라, 상기 가변 정족수 기반의 블록체인 합의 방법은, 상기 추가적으로 브로드캐스트하는 단계 이후에, 상기 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우의 상기 비잔틴 오류를 검출하여, 변경된 상기 정족수를 추가적으로 변경할 수 있다.

[0018] 실시 예에 따라, 상기 변경된 상기 정족수를 추가적으로 변경하는 단계는, 네트워크 오류에 의하여 투표에 참여

하지 못하였던 참여 블록체인 노드를 포함시켜, 상기 변경된 상기 정족수를 추가적으로 변경할 수 있다.

[0019] 실시 예에 따라, 상기 합의 여부를 결정하는 단계는, 상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 추가적으로 변경된 상기 정족수 이상인지에 따라 상기 합의 여부를 결정할 수 있다.

[0020] 실시 예에 따라, 상기 가변 정족수 기반의 블록체인 합의 방법은, 상기 리더 블록체인 노드가 정해진 시간 내에 상기 신규 생성 블록과 상기 합의 요청 메시지를 전송하지 않는 경우에, 상기 리더 블록체인 노드를 변경하는 단계를 더 포함할 수 있다.

[0021] 본 발명의 실시 예에 따른 블록체인 노드는, 신규 생성 블록에 대한 합의 요청 메시지를 생성하는 합의 요청 메시지 생성 모듈, 상기 신규 생성 블록과 상기 합의 요청 메시지를 브로드캐스트하고, 참여 블록체인 노드들이 상기 신규 생성 블록과 상기 합의 요청 메시지에 응답하여 전송한 동의, 거절, 또는 무효의 투표 메시지를 수신하는 통신 인터페이스, 상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 정족수 변경 모듈 및 상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 합의 결과 처리 모듈을 포함할 수 있다.

[0022] 본 발명의 실시 예에 따른 프로세서(processor)와 결합되어 가변 정족수 기반의 블록체인 합의 방법을 수행하기 위한 매체에 저장된 프로그램은 리더 블록체인 노드로부터 전송된 신규 생성 블록과 상기 신규 생성 블록에 대한 합의 요청 메시지에 따라, 상기 리더 블록체인 노드와 참여 블록체인 노드들이 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트(broadcast)하는 단계, 상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 단계 및 상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 단계를 수행할 수 있다.

발명의 효과

[0024] 본 발명의 실시 예에 따른 방법과 장치는 무효의 투표 메시지를 발행한 참여 블록체인 노드의 수를 반영하여 정족수를 변경하여 합의 여부를 결정함으로써, 비잔틴 오류가 발생한 블록체인 노드 수의 예측이 어려운 블록체인에서 효과적으로 합의과정을 수행할 수 있다.

[0025] 또한, 본 발명의 실시 예에 따른 방법과 장치는 무효의 투표 메시지를 발행한 참여 블록체인 노드의 수를 반영하여 정족수를 변경하여 합의 여부를 결정함으로써, 과반 미만의 비잔틴 오류에는 충분히 견딜 수 있는 효과가 있다.

도면의 간단한 설명

[0027] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 간단한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 블록체인 네트워크의 개념도이다.

도 2는 도 1에 도시된 블록체인 네트워크에서 리더 블록체인 노드의 일 실시 예에 따른 블록도이다.

도 3은 도 1에 도시된 블록체인 네트워크에서 수행되는 합의 과정의 일 실시 예에 따른 플로우차트이다.

도 4는 도 3의 합의 과정의 구체적인 예시를 나타낸 도면이다.

도 5는 본 발명의 실시 예에 따라 설정될 수 있는 타이머의 예시를 나타낸 도면이다.

도 6은 본 발명의 실시 예에 따른 가변 정족수 기반의 블록 체인 합의 방법의 플로우차트이다.

발명을 실시하기 위한 구체적인 내용

[0028] 본 발명의 기술적 사상은 다양한 변경을 가할 수 있고 여러 가지 실시 예를 가질 수 있는 바, 특정 실시 예들을 도면에 예시하고 이를 상세한 설명을 통해 상세히 설명하고자 한다. 그러나, 이는 본 발명의 기술적 사상을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 기술적 사상의 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0029] 본 발명의 기술적 사상을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 본 명세서의 설명 과정에서 이용되는

숫자(예를 들어, 제1, 제2 등)는 하나의 구성요소를 다른 구성요소와 구분하기 위한 식별기호에 불과하다.

[0030] 또한, 본 명세서에서, 일 구성요소가 다른 구성요소와 "연결된다" 거나 "접속된다" 등으로 언급된 때에는, 상기 일 구성요소가 상기 다른 구성요소와 직접 연결되거나 또는 직접 접속될 수도 있지만, 특별히 반대되는 기재가 존재하지 않는 이상, 중간에 또 다른 구성요소를 매개하여 연결되거나 또는 접속될 수도 있다고 이해되어야 할 것이다.

[0031] 또한, 본 명세서에 기재된 "~부", "~기", "~자", "~모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 프로세서(Processor), 마이크로 프로세서(Micro Processer), 마이크로 컨트롤러(Micro Controller), CPU(Central Processing Unit), GPU(Graphics Processing Unit), APU(Accelerate Processor Unit), DSP(Drive Signal Processor), ASIC(Application Specific Integrated Circuit), FPGA(Field Programmable Gate Array) 등과 같은 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있으며, 적어도 하나의 기능이나 동작의 처리에 필요한 데이터를 저장하는 메모리(memory)와 결합되는 형태로 구현될 수도 있다.

[0032] 그리고 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다.

[0033] 이하, 본 발명의 기술적 사상에 따른 실시 예들을 차례로 상세히 설명한다.

[0035] 도 1은 본 발명의 일 실시 예에 따른 블록체인 네트워크의 개념도이다.

[0036] 도 1을 참조하면, 블록체인 네트워크(block chain network, NET_BC)에는 복수의 블록체인 노드들(NODE1~NODE7)이 포함될 수 있다.

[0037] 복수의 블록체인 노드들(NODE1~NODE7) 중에서 어느 하나의 블록체인 노드(예컨대, NODE1)는 리더 블록체인 노드로 동작할 수 있으며, 리더 블록체인 노드의 주도 하에서 신규 생성 블록에 대한 합의 과정이 수행될 수 있다.

[0038] 실시 예에 따라, 블록체인 네트워크(NET_BC)는 투표를 통한 합의 방식을 사용하는 블록체인일 수 있으며, 그 종류는 제한되지 않는다.

[0039] 실시 예에 따라, 블록체인 네트워크(NET_BC)는 BFT(Byzantine Fault Tolerance) 계열의 합의 프로토콜을 사용할 수 있다.

[0040] 본 명세서에서 "노드(node)"는 네트워크의 적어도 일부를 구성하는 장치를 의미할 수 있으며, "노드 장치"라고 일컬어질 수도 있다.

[0042] 도 2는 도 1에 도시된 블록체인 네트워크에서 리더 블록체인 노드의 일 실시 예에 따른 블록도이다.

[0043] 도 1과 도 2를 참조하면, 도 2에 도시된 리더 블록체인 노드(100)는 블록체인 네트워크(NET_BC)에 포함된 블록체인 노드들(NODE1~NODE7) 중에서 리더 블록체인 노드로 동작하는 어느 하나의 블록체인 노드(예컨대, NODE1)를 의미할 수 있다.

[0044] 리더 블록체인 노드(100)는 통신 인터페이스(110), 메모리(120), 및 프로세서(130)를 포함할 수 있다.

[0045] 통신 인터페이스(110)는 리더 블록체인 노드(100)와 참여 블록체인 노드들(예컨대, NODE2~NODE7)과의 통신을 인터페이싱할 수 있으며, 인터페이싱 과정에서 송수신되는 데이터 또는 신호를 처리할 수 있다.

[0046] 실시 예에 따라, 통신 인터페이스(110)는 참여 블록체인 노드들(예컨대, NODE2~NODE7)과 송수신하는 메시지(예컨대, 합의 요청 메시지 또는 투표 메시지)를 인터페이싱할 수 있다.

[0047] 메모리(120)는 리더 블록체인 노드(100)가 가변 정족수 기반의 블록 체인 합의 방법을 수행하는 데에 필요한 데이터와 프로세서(130)의 처리 과정에서 필요한 데이터, 프로세서(130)의 처리 과정 중 또는 처리 완료 후에 생성된 데이터를 저장할 수 있다.

[0048] 실시 예에 따라, 메모리(120)는 본 발명의 실시 예에 따른 가변 정족수 기반의 블록 체인 합의 방법을 수행하기 위한 프로그램을 저장할 수 있으며, 메모리(120)는 프로세서(130)와 결합되어 상기 프로그램을 실행시킬 수 있

다.

[0049] 프로세서(130)는 합의 요청 메시지 생성 모듈(132), 정족수 변경 모듈(134), 및 합의 결과 처리 모듈(136)을 포함할 수 있다.

[0050] 합의 요청 메시지 생성 모듈(132)은 신규 생성 블록에 대한 합의 과정을 시작하기 위하여 참여 블록체인 노드들(예컨대, NODE2~NODE7)에게 합의 과정의 수행을 요청하는 합의 요청 메시지를 생성할 수 있다.

[0051] 정족수 변경 모듈(134)은 참여 블록체인 노드들(예컨대, NODE2~NODE7) 중에서 비잔틴 오류(Byzantine Fault)가 발생한 참여 블록체인 노드들의 수와 무효의 투표 메시지를 브로드캐스트한 참여 블록체인 노드의 수를 이용하여, 정족수를 변경할 수 있다.

[0052] 정족수는 합의 과정 상의 투표에서 합의가 된 것으로 판단하기 위한 기준이 되는 값이며, "동의","거절", 및 "무효"의 투표 메시지 중에서 "동의"의 투표 메시지의 수가 정족수 이상인 경우에 합의된 것으로 판단할 수 있다.

[0053] 합의 결과 처리 모듈(136)은 블록체인 노드들(예컨대, NODE1~NODE7) 의 투표 메시지들 중에서, "동의"의 투표 메시지의 수가 정족수 변경 모듈(134)에 의해 변경된 정족수 이상인지에 따라 합의 여부를 결정할 수 있다.

[0054] 가변 정족수 기반의 블록 체인 합의 방법의 세부적인 수행 과정은 도 3 내지 도 6을 참조하여 후술한다.

[0056] 도 3은 도 1에 도시된 블록체인 네트워크에서 수행되는 합의 과정의 일 실시 예에 따른 플로우차트이다.

[0057] 도 1 내지 도 3을 참조하면, 리더 블록체인 노드(예컨대, NODE1)는 최초에 제안 단계(S300)를 수행할 수 있다.

[0058] 제안 단계(S300)에서, 리더 블록체인 노드(예컨대, NODE1)는 신규 생성 블록과 신규 생성 블록에 대한 합의 요청 메시지를 참여 블록체인 노드들(예컨대, NODE2~NODE7)로 전송할 수 있다.

[0059] 실시 예에 따라, 리더 블록체인 노드(예컨대, NODE1)는 신규 생성 블록의 블록 생성자와 동일할 수도 있고 다를 수도 있다.

[0060] 실시 예에 따라, 신규 생성 블록과 합의 요청 메시지는 서로 분리되어 전송될 수 있다.

[0061] 제안 단계(S300)에서 리더 블록체인 노드(예컨대, NODE1)의 합의 요청 메시지가 정해진 시간 내에 전송되지 않는 경우(S301), 리더 블록체인 노드(예컨대, NODE1)는 참여 블록체인 노드들(예컨대, NODE2~NODE7) 중의 어느 하나로 교체될 수 있다(S340).

[0062] 제안 단계(S300)에서 리더 블록체인 노드(예컨대, NODE1)의 합의 요청 메시지가 정해진 시간 내에 전송된 경우(S302), 리더 블록체인 노드(예컨대, NODE1)와 참여 블록체인 노드들(예컨대, NODE2~NODE7)은 투표 단계(S310)를 수행할 수 있다.

[0063] 투표 단계(S310)에서, 리더 블록체인 노드(예컨대, NODE1)와 참여 블록체인 노드들(예컨대, NODE2~NODE7)은 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트할 수 있다.

[0064] 실시 예에 따라, 리더 블록체인 노드(예컨대, NODE1)와 참여 블록체인 노드들(예컨대, NODE2~NODE7)은 신규 생성 블록에 대한 합의에 동의하는 경우에는 동의의 투표 메시지를, 신규 생성 블록에 대한 합의에 부동의하는 경우에는 거절의 투표 메시지를, 정해진 시간 내에 신규 생성 블록과 합의 요청 메시지를 수신하지 못한 경우에는 무효의 투표 메시지를 브로드캐스트할 수 있다.

[0065] 투표 단계(S310)에서 정해진 시간(예컨대, view change timer) 내에 투표가 이루어지지 않는 경우(S311), 리더 블록체인 노드(예컨대, NODE1)는 참여 블록체인 노드들(예컨대, NODE2~NODE7) 중의 어느 하나로 교체될 수 있다(S340).

[0066] 투표 단계(S310)에서 동의의 투표 메시지 수가 정족수 이상인 것으로 판단되는 경우(S312), 합의 완료 단계(S330)로 넘어갈 수 있다.

[0067] 투표 단계(S310)에서는 참여 블록체인 노드들(예컨대, NODE2~NODE7)이 비정상적인 메시지를 전송한 경우 또는 정해진 시간 내에 메시지를 전송하지 않은 경우의 비잔틴 오류를 검출할 수 있다. 리더 블록체인 노드(예컨대, NODE1)는 검출된 비잔틴 오류에 따라, 비잔틴 오류가 발생한 참여 블록체인 노드의 수와 무효의 투표 메시지를 발행한 참여 블록체인 노드의 수에 기초하여, 정족수를 변경하고 변경된 정족수에 따라 합의 여부를 판단할 수 있다.

[0068] 실시 예에 따라, 비정상적인 메시지를 전송하는 경우는 블록체인의 프로토콜(protocol)에 어긋나는 메시지를 전송한 경우일 수 있다.

[0069] 투표 단계(S310)에서 정해진 시간(예컨대, vote timer) 내에 합의가 이루어지지 않는 경우(S313), 리더 블록체인 노드(예컨대, NODE1)는 수집 단계(S320)를 수행할 수 있다.

[0070] 수집 단계(S320)에서, 리더 블록체인 노드(예컨대, NODE1)와 참여 블록체인 노드들(예컨대, NODE2~NODE7) 각각은 수신한 모든 투표 메시지와 자신이 전송한 투표 메시지를 모아서 브로드캐스트할 수 있다.

[0071] 수집 단계(S320)에서는 참여 블록체인 노드들(예컨대, NODE2~NODE7)이 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우의 비잔틴 오류를 검출할 수 있다. 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우의 비잔틴 오류는, 정상적인 메시지들 각각이 블록체인 프로토콜에 맞게 작성되었으나, 이중으로 투표한 경우에 발생하는 비잔틴 오류일 수 있다. 리더 블록체인 노드(예컨대, NODE1)는 검출된 비잔틴 오류에 따라, 정족수를 추가적으로 변경할 수 있다.

[0072] 실시 예에 따라, 수집 단계(S320)에서 리더 블록체인 노드(예컨대, NODE1)는 네트워크 오류에 의하여 투표에 참여하지 못하였던 참여 블록체인 노드를 포함시켜서 정족수를 추가적으로 변경할 수 있다.

[0073] 수집 단계(S320)에서 정해진 시간(예컨대, view change timer) 내에 합의가 되지 않는 경우(S321), 리더 블록체인 노드(예컨대, NODE1)는 참여 블록체인 노드들(예컨대, NODE2~NODE7) 중의 어느 하나로 교체될 수 있다(S340).

[0074] 수집 단계(S320)에서 동의의 투표 메시지의 수가 추가적으로 변경된 정족수 이상인 경우(S322), 합의 완료 단계(S330)로 넘어갈 수 있다.

[0076] 도 4는 도 3의 합의 과정의 구체적인 예시를 나타낸 도면이다.

[0077] 도 1 내지 도 4를 참조하면, 제1블록체인 노드(NODE1(101))가 리더 블록체인 노드로 동작하고, 나머지 블록체인 노드들(NODE2(102)~NODE7(107))이 참여 블록체인 노드로 동작할 수 있다.

[0078] 제안단계(Propose)에서 리더 블록체인 노드(101)는 참여 블록체인 노드들(102~107)로 신규 생성 블록과 신규 생성 블록에 대한 합의 요청 메시지를 브로드캐스트할 수 있다(S401).

[0079] 리더 블록체인 노드(101)와 참여 블록체인 노드들(102~107)은 신규 생성 블록에 대한 투표를 진행할 수 있다.

[0080] 리더 블록체인 노드(101)와 일부 참여 블록체인 노드들(104, 105)은 동의의 투표 메시지를 브로드캐스트 할 수 있다(S411, S413, S414).

[0081] 일부 참여 블록체인 노드(107)는 거절의 투표를 하고자 하였으나 투표 메시지가 프로토콜에 맞지 않아서 비잔틴 오류를 가질 수 있다(S415).

[0082] 일부 참여 블록체인 노드(102)는 리더 블록체인 노드(101)로부터 신규 생성 블록과 합의 요청 메시지를 수신하지 못하여, 무효의 투표 메시지를 브로드캐스트 할 수 있다(S412).

[0083] 일부 참여 블록체인 노드(103, 106)는 리더 블록체인 노드(101)로부터 신규 생성 블록과 합의 요청 메시지는 수신하였으나, 네트워크 문제로 정해진 시간 내에 투표 메시지를 전송하지 못할 수 있다.

[0084] 이 때, 프로토콜에 맞지 않는 투표 메시지를 전송한 참여 블록체인 노드(107) 또는 정해진 시간 내에 투표 메시지를 전송하지 못한 참여 블록체인 노드(103, 106)는 비잔틴 오류를 가지므로 이후의 투표단계(Vote)의 정족수에서 빠지며, 무효의 투표 메시지를 브로드캐스트한 참여 블록체인 노드(102)는 정족수에서 빠지지 않을 수 있다.

[0085] 리더 블록체인 노드(101)는 비잔틴 오류가 발생한 블록체인 노드의 수와 무효의 투표 메시지를 브로드캐스트한 블록체인의 노드 수에 기초하여 기 설정된 정족수를 변경할 수 있다(S430).

[0086] 실시 예에 따라, 본 발명의 실시 예에 따른 블록체인은 BTF(Byzantine Fault Tolerance) 계열의 프로토콜을 따를 수 있으며, 합의에 필요한 최소 블록체인 노드의 수를 3f+1(f는 허용 가능한 최대 비잔틴 오류를 가지는 블록체인 노드의 수)라고 할 때, 정족수는 2f+1을 기준으로 설정할 수 있다.

[0087] 이 경우, 도 4에서는 3f+1이 7의 값을 가지므로, f는 2이고, 정족수는 5로 기설정될 수 있다. S430 단계에서는 기 설정된 정족수 5에서, 무효의 투표 메시지를 브로드캐스트한 참여 블록체인 노드(102)의 수(1개)는 빼지 않

고, 비잔틴 오류가 발생한 블록체인 노드(103, 106, 107)의 수(3개)는 뺀 값인 2로 정족수를 변경할 수 있다.

[0088] 투표에 참여한 제1그룹(GR_COM1)의 참여 블록체인 노드들(101, 102, 104, 105) 중에서, 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수는 3개로써, 정족수 이상이므로, 신규 생성 블록에 대하여 합의가 완료된 것으로 판단할 수 있다.

[0089] 일부 블록체인 노드(103)는 네트워크 오류로 인하여 투표단계에서 참여하지 못하였으나 네트워크 오류가 투표단계 이후에 해소될 수 있다. 이 경우에는 수집 단계(Collate)에서 다시 한번 합의 과정에 참여할 수 있다(S441).

[0090] 도 4의 경우에는 투표 단계에서 합의가 이루어질 수 있으나, 투표 단계에서 합의가 이루어지지 않은 경우를 가정하면, 수집 단계에서는 네트워크 오류가 해소된 일부 블록체인 노드(103)을 포함하여 리더 블록체인 노드와 참여 블록체인 노드들 각각이 수신한 모든 투표 메시지와 자신이 전송한 투표 메시지를 모아서 추가적으로 브로드캐스트할 수 있다(S451).

[0091] 이에 따라, 수집 단계에서는 두 개 이상의 서로 상충하는 정상적인 메시지를 전송한 경우의 비잔틴 오류를 추가적으로 검출할 수 있다.

[0092] 또한, 수집 단계에서 리더 블록체인 노드(101)는 네트워크 오류가 해소된 일부 블록체인 노드(103)의 수(1개)를 추가하고, 두 개 이상의 서로 상충하는 정상적인 메시지를 전송한 경우의 비잔틴 오류가 발생한 블록체인 노드의 수(이 경우, 없는 것으로 가정)를 차감하여, S430 단계에서 변경되었던 정족수를 추가적으로 변경(예컨대, 3으로 변경)할 수 있다.

[0093] 합의된 결과는 수집 단계가 진행될 때까지 네트워크 오류가 해결된 블록체인 노드(예컨대, 103, 106)에까지 추가적으로 브로드캐스트될 수 있다.

[0094] 리더 블록체인 노드(101)와 합의 결과를 브로드캐스트 받은 블록체인 노드들(102~106)은 최종적으로 합의 상태로 변경되며, 비잔틴 오류가 해소되지 않은 블록체인 노드(107)는 합의 상태에서 제외될 수 있다.

[0096] 도 5는 본 발명의 실시 예에 따라 설정될 수 있는 타이머의 예시를 나타낸 도면이다.

[0097] 도 5를 참조하면, 제안 단계(Propose), 투표 단계(Vote), 수집 단계(Collate)는 순차적으로 수행될 수 있으며, 제안 단계, 투표 단계, 및 수집 단계로 구성된 하나의 라운드(Round1)가 종료되면, 다음 라운드(Round2)의 신규 생성 블록(B2)에 대한 합의 과정이 수행될 수 있다.

[0098] 최초 라운드(Round1)의 합의 과정에서는 각 단계에서의 타이머, 예컨대 제안 타이머(propose timer, TP-11~TP-14), 투표 타이머(vote timer, TV-11~TV-14), 수집 타이머(collate timer, TC-11~TC-14)는 일괄적으로 설정될 수 있다.

[0099] 하지만, 각 블록체인 노드들(111~114)에서의 투표 단계와 수집 단계가 완료되는 시점이 다르기 때문에, 다음 라운드(Round2)의 합의 과정에서는 블록체인 노드들(111~114) 마다 타이머가 각자 개별적으로 설정될 수 있다.

[0101] 도 6은 본 발명의 실시 예에 따른 가변 정족수 기반의 블록 체인 합의 방법의 플로우차트이다.

[0102] 도 1 내지 도 6을 참조하면, 리더 블록체인 노드(예컨대, 101)는 신규 생성 블록과 신규 생성 블록에 대한 합의 요청 메시지를 다른 블록체인 노드들(예컨대, 102~107)로 전송할 수 있다(S610).

[0103] 참여 블록체인 노드들(예컨대, 102~107)은 신규 생성 블록의 합의 요청에 대한 투표 메시지를 브로드 캐스트할 수 있다(S620).

[0104] 실시 예에 따라, 투표 메시지는, 동의, 거절, 또는 무효의 투표메시지일 수 있다.

[0105] 리더 블록체인 노드(예컨대, 101)는 참여 블록체인 노드들 중에서 비잔틴 오류가 발생한 블록체인 노드의 수와 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경할 수 있다(S630).

[0106] 실시 예에 따라, 비잔틴 오류가 발생한 경우는, 비정상적인 메시지를 전송한 경우, 정해진 시간 내에 메시지를 전송하지 않은 경우, 또는 두 개 이상의 서로 상충하는 정상적인 메시지들을 전송한 경우일 수 있다.

[0107] 실시 예에 따라, 정족수를 변경하는 S630 단계는 비정상적인 메시지를 전송한 경우 또는 정해진 시간 내에 메시지를 전송하지 않은 경우의 비잔틴 오류가 발생한 블록체인 노드의 수와 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여 정족수를 변경하는 단계와, 두 개 이상의 서로 상충하는 정상적인 메시지들을

전송한 경우의 비잔틴 오류가 발생한 블록체인 노드의 수에 기초하여 정족수를 추가적으로 변경하는 단계로 구분될 수도 있다.

[0108] 리더 블록체인 노드(예컨대, 101)는 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 정족수 이상인지에 따라 합의 여부를 결정할 수 있다(S640).

[0109] 실시 예에 따라, S630 단계에서 정족수가 추가적으로 변경된 경우에는, 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 추가적으로 변경된 정족수 이상인지에 따라 합의 여부를 결정할 수 있다

[0111] 이상, 본 발명의 기술적 사상을 다양한 실시 예들을 들어 상세하게 설명하였으나, 본 발명의 기술적 사상은 상기 실시 예들에 한정되지 않고, 본 발명의 기술적 사상의 범위 내에서 당 분야에서 통상의 지식을 가진 자에 의하여 여러가지 변형 및 변경이 가능하다.

부호의 설명

[0112] 100, 101~107, 111~114 : 블록체인 노드

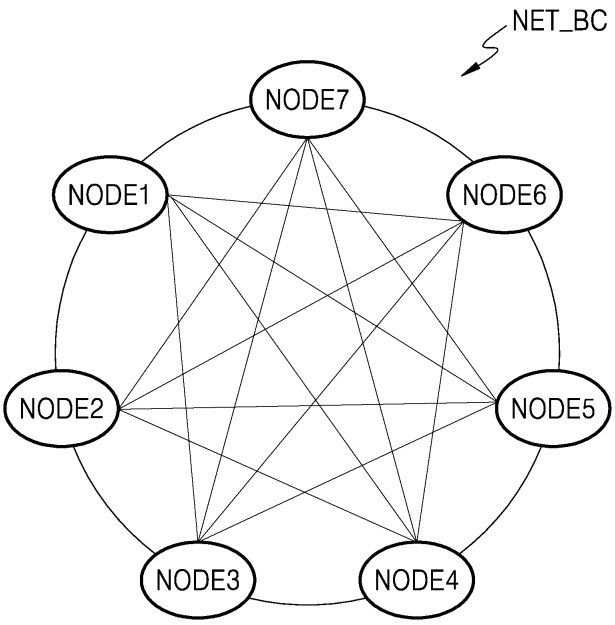
110 : 통신 인터페이스

120 : 메모리

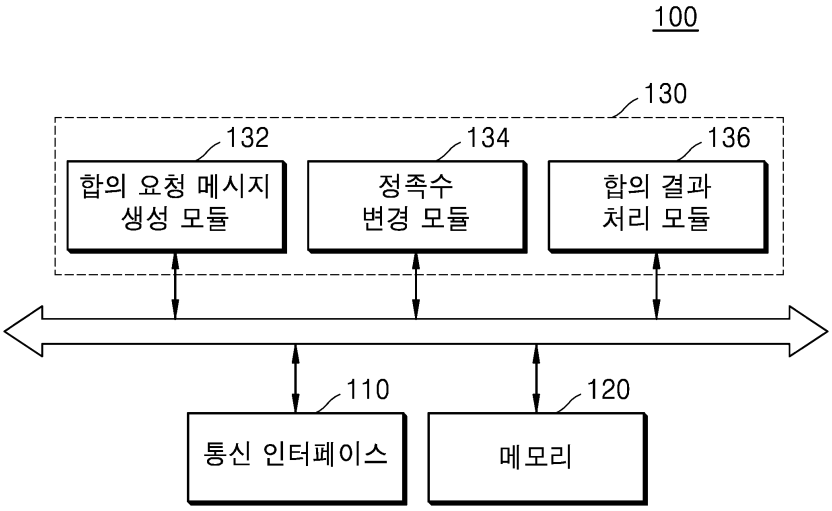
130 : 프로세서

도면

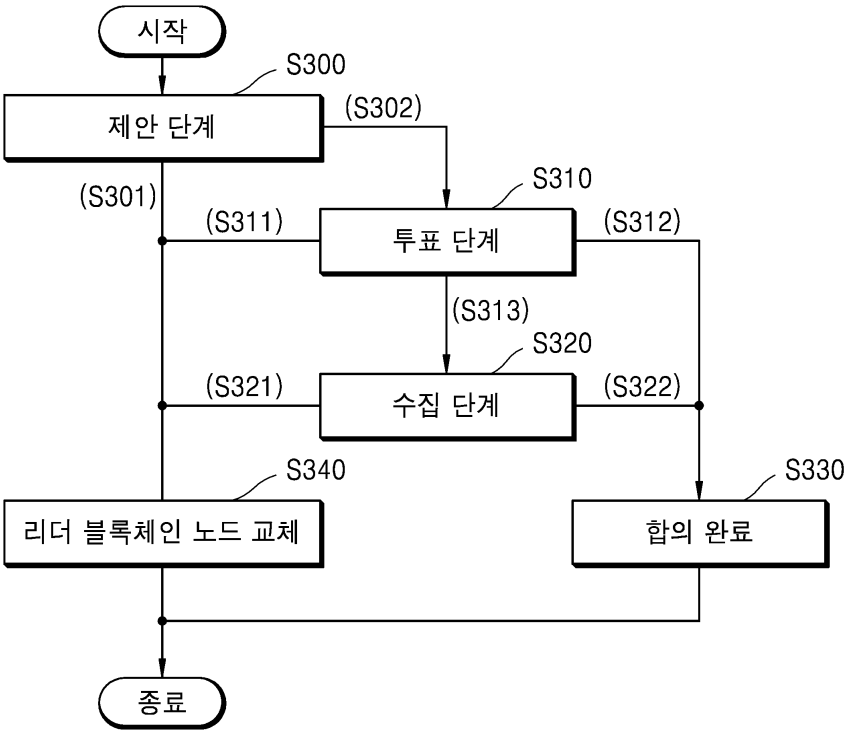
도면1



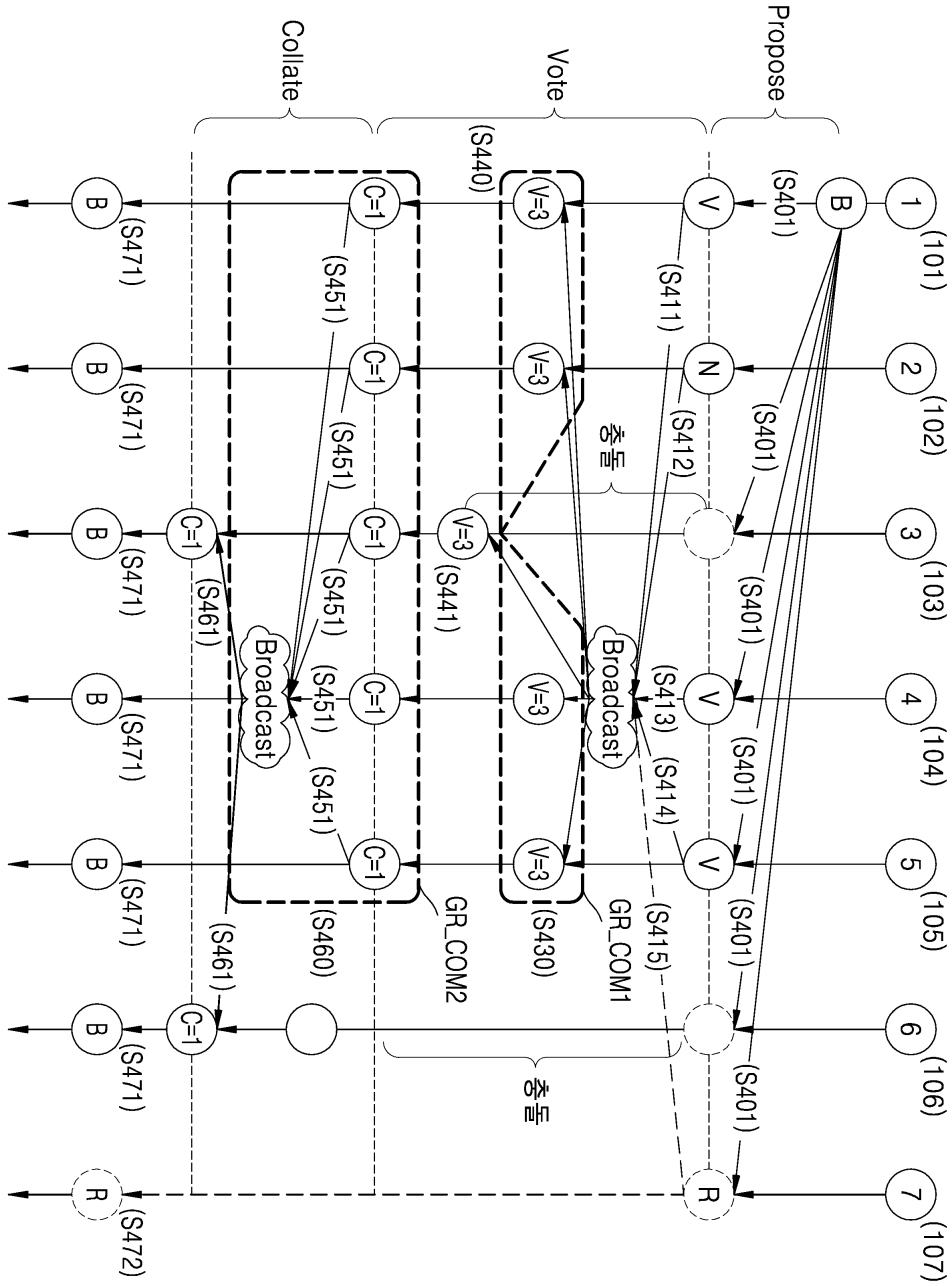
도면2


100
130
132
합의 요청 메시지 생성 모듈
134
정족수 변경 모듈
136
합의 결과 처리 모듈
110
통신 인터페이스
120
메모리

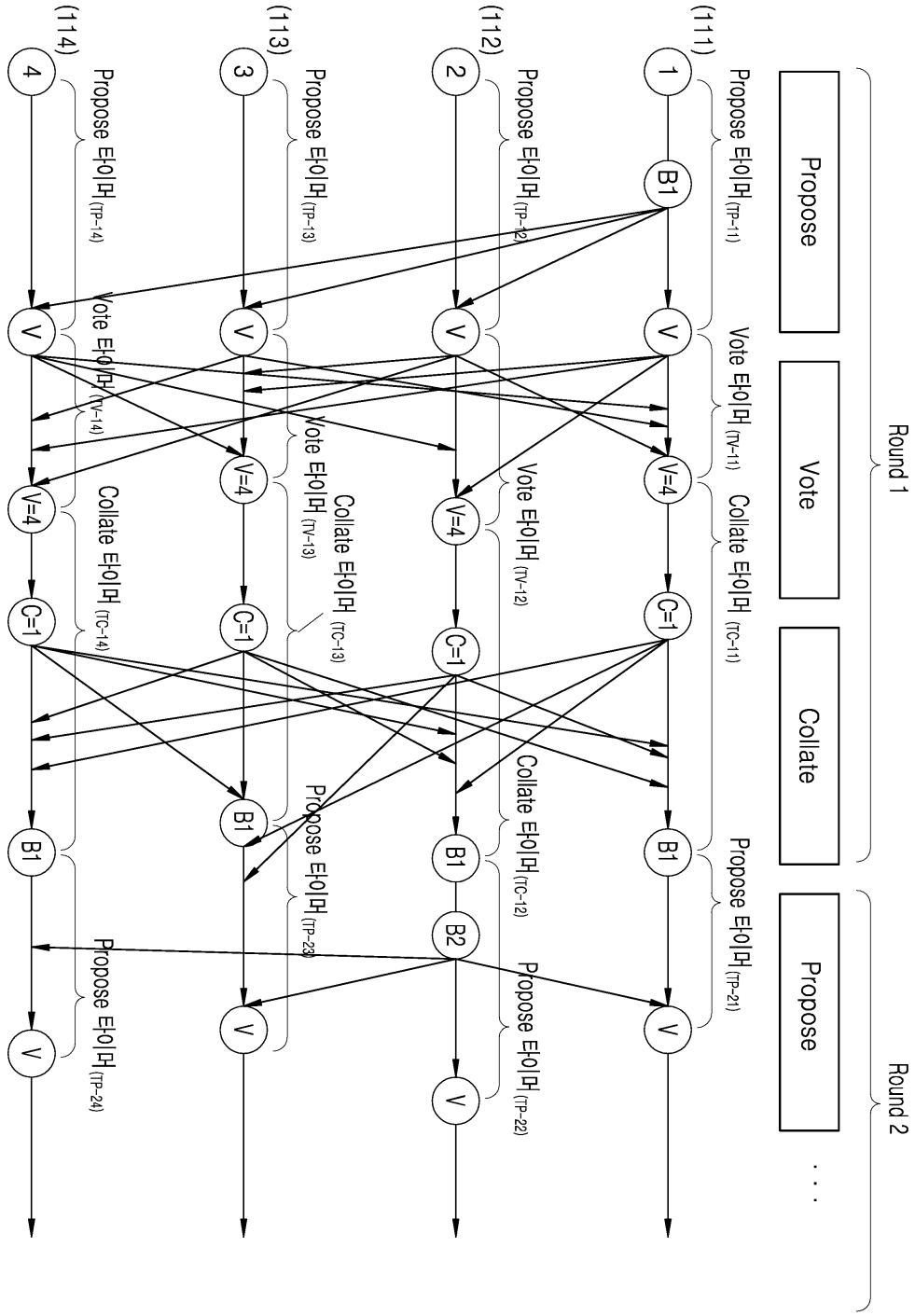
도면3


시작
S300
제안 단계
(S302)
(S301)
S310
(S311)
투표 단계
(S312)
(S313)
S320
(S321)
수집 단계
(S322)
S340
리더 블록체인 노드 교체
S330
합의 완료
종료

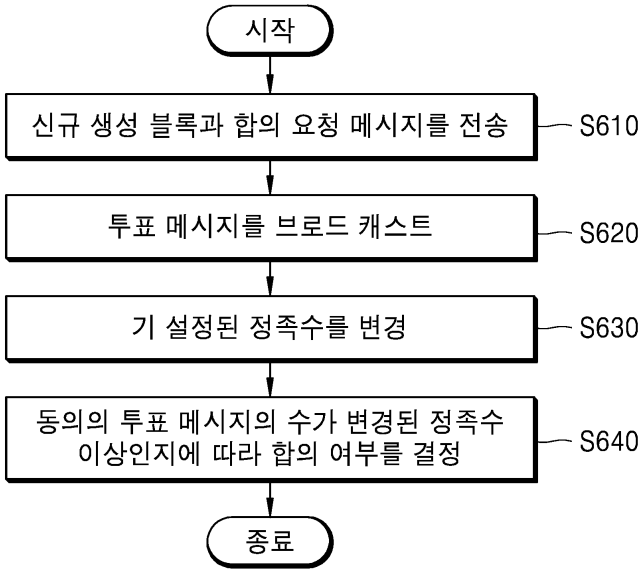
도면4


Propose
Vote
Collate
(S401)
(S440)
(S411)
(S412)
충돌
(S441)
(S451)
(S461)
Broadcast
(S413)
(S414)
(S415)
(S460)
(S430)
GR_COM1
GR_COM2
충돌
(S471)
(S472)
1
2
3
4
5
6
7
(101)
(102)
(103)
(104)
(105)
(106)
(107)
B
V
N
V=3
C=1
R

도면5


Propose
Vote
Collate
Propose
Round 1
Round 2
(111)
(112)
(113)
(114)
1
2
3
4
B1
V
V=4
C=1
B2
Propose 타이머 (TP-11)
Vote 타이머 (TV-11)
Collate 타이머 (TC-11)
Propose 타이머 (TP-21)
Propose 타이머 (TP-12)
Vote 타이머 (TV-12)
Collate 타이머 (TC-12)
Propose 타이머 (TP-22)
Propose 타이머 (TP-13)
Vote 타이머 (TV-13)
Collate 타이머 (TC-13)
Propose 타이머 (TP-23)
Propose 타이머 (TP-14)
Vote 타이머 (TV-14)
Collate 타이머 (TC-14)
Propose 타이머 (TP-24)

도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 15

【변경전】

프로세서(processor)와 결합되어 가변 정족수 기반의 블록체인 합의 방법을 수행하기 위한 매체에 저장된 프로그램으로서,

리더 블록체인 노드로부터 전송된 신규 생성 블록과 상기 신규 생성 블록에 대한 합의 요청 메시지에 따라, 상기 리더 블록체인 노드와 참여 블록체인 노드들이 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트(broadcast)하는 단계;

상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 단계; 및

상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 단계를 수행하는, 매체에 저장된 프로그램.

【변경후】

프로세서(processor)와 결합되어 가변 정족수 기반의 블록체인 합의 방법을 수행하기 위한 컴퓨터 기록 매체에 저장된 프로그램으로서,

리더 블록체인 노드로부터 전송된 신규 생성 블록과 상기 신규 생성 블록에 대한 합의 요청 메시지에 따라, 상기 리더 블록체인 노드와 참여 블록체인 노드들이 동의, 거절, 또는 무효의 투표 메시지를 브로드캐스트(broadcast)하는 단계;

상기 참여 블록체인 노드들 중에서 비잔틴 오류(Byzantine Fault)가 발생한 블록체인 노드의 수와 상기 무효의 투표 메시지를 브로드캐스트한 블록체인 노드의 수에 기초하여, 기 설정된 정족수를 변경하는 단계; 및

상기 동의의 투표 메시지를 브로드캐스트한 블록체인 노드의 수가 변경된 상기 정족수 이상인지에 따라 합의 여부를 결정하는 단계를 수행하는, 컴퓨터 기록 매체에 저장된 프로그램.