(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년06월02일
(11) 등록번호 10-2260093
(24) 등록일자 2021년05월28일

(51) 국제특허분류(Int. Cl.)
G06F 16/27 (2019.01) *G06F 16/23* (2019.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
G06F 16/278 (2019.01)
G06F 16/2365 (2019.01)
(21) 출원번호 10-2019-0107485
(22) 출원일자 2019년08월30일
심사청구일자 2019년08월30일
(65) 공개번호 10-2021-0026545
(43) 공개일자 2021년03월10일
(56) 선행기술조사문헌
Hyunkyung Yoo et al., The Blockchain for Domain based Static Sharding, 2018.08.01. 1689-1692pages. <DOI: 10.1109/TrustCom/BigDataSE.2018.00252> 1부.*
(뒷면에 계속)

(73) 특허권자
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
정종문
서울특별시 용산구 이촌로 181, 104동 101호(이촌동, 한강대우아파트)
윤주식
서울특별시 서대문구 신촌로7길 49-6, 202호(창천동, 청송빌)
고윤영
서울특별시 서대문구 신촌로7길 49-15(창천동)
(74) 대리인
민영준

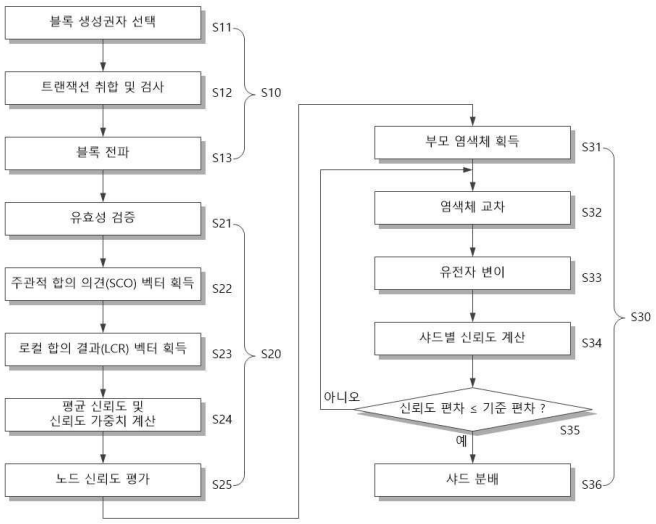
전체 청구항 수 : 총 12 항 심사관 : 최재귀

(54) 발명의 명칭 **내결함성 블록체인 네트워크의 신뢰도 기반 샤드 분배 장치 및 방법**

(57) 요 약

본 발명은 블록체인 네트워크의 다수의 노드 각각으로부터 블록에 대해 유효성을 검증한 결과와 다른 노드들에서 검증한 유효성 검증 결과와 취합하여 획득한 합의 결과를 인가받아 다수의 노드 각각에 대한 신뢰도를 획득하는 신뢰도 계산부 및 다수의 노드를 기지정된 다수의 샤드로 분배하되, 다수의 샤드 각각에 분배되는 노드의 신뢰도의 합으로 나타나는 샤드 신뢰도를 계산하고, 계산된 다수의 샤드 신뢰도 사이의 편차가 최소가 되도록 다수의 노드를 분배하는 샤드 분배부를 포함하여, 악성 노드가 특정 샤드에 집중되는 것을 방지할 수 있으므로 각 샤드에서 악성 노드들의 담합을 억제하여 비정상 합의 공격뿐만 아니라 합의를 정상적으로 하면서 다른 노드의 의견 변조하는 패시브 공격을 방지할 수 있는 블록체인 네트워크의 샤드 분배 장치 및 방법을 제공할 수 있다.

대 표 도 - 도6



(52) CPC특허분류
H04L 63/0815 (2013.01)
H04L 63/0869 (2013.01)
H04L 67/1097 (2013.01)
H04L 2209/38 (2013.01)

(56) 선행기술조사문헌
Sunho Seo et al., Reconfiguration time and complexity minimized trust-based clustering scheme for MANETs, 2017.09.18. <DOI: 10.1186/s13638-017-0938-8> 1부.*
Xin Chen et al., GlobalTrust: An attack-resilient reputation system for tactical networks, 2014 IEEE SECON, 2014.06.30, 275-283pages. 1부.*
WO2017109140 A1
US20180089436A1
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093476
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터지원사업
연구과제명	블록체인 비즈니스 서비스 기술 개발 및 인력양성
기 여 율	1/1
과제수행기관명	연세대학교 산학협력단
연구기간	2019.04.01 ~ 2019.12.31

명 세 서

청구범위

청구항 1

블록체인 네트워크의 다수의 노드 각각으로부터 블록에 대해 유효성을 검증한 결과와 다른 노드들에서 검증한 유효성 검증 결과와 취합하여 획득한 합의 결과를 인가받아 다수의 노드 각각에 대한 신뢰도를 획득하는 신뢰도 계산부; 및

상기 다수의 노드를 기지정된 다수의 샤드로 분배하되, 다수의 샤드 각각에 분배되는 노드의 신뢰도의 합으로 나타나는 샤드 신뢰도를 계산하고, 계산된 다수의 샤드 신뢰도 사이의 편차가 최소가 되도록 상기 다수의 노드를 분배하는 샤드 분배부를 포함하되,

상기 샤드 분배부는

동일한 신뢰도를 갖는 노드가 동일한 샤드에 분배되지 않도록 분산하여 분배하는 샤드 분배 장치.

청구항 2

삭제

청구항 3

제1 항에 있어서, 상기 샤드 분배부는

상기 다수의 노드를 랜덤하게 다수의 샤드로 분배하고, 상기 다수의 노드가 분배된 샤드의 인덱스를 유전자로서 나열하여 다수의 부모 염색체를 획득하고,

상기 다수의 부모 염색체에서 한쌍으로 선택되는 부모 염색체의 유전자 중 적어도 하나의 유전자 선택하여, 대응하는 유전자를 상호 교환하여 자식 염색체를 획득하며,

획득된 상기 자식 염색체에서 적어도 하나의 유전자를 선택하여 다른 샤드 인덱스로 변이시킨 후, 변이된 자식 염색체에 나열된 유전자인 샤드 인덱스를 기반으로 다수의 샤드 각각에 대해 획득된 신뢰도 사이의 편차를 누적하고,

누적된 신뢰도 편차가 기지정된 기준 편차 이하이면, 상기 다수의 노드를 변이된 자식 염색체에 나열된 유전자인 샤드 인덱스를 기반으로 분배하며,

상기 누적된 신뢰도 편차가 상기 기준 편차를 초과하면, 상기 자식 염색체를 부모 염색체로하여 다시 자식 염색체를 획득하고 변이시키는 샤드 분배 장치.

청구항 4

제3 항에 있어서, 상기 샤드 분배부는

상기 자식 염색체에서 적어도 하나의 유전자를 선택하고, 선택된 유전자에 대응하는 노드의 신뢰도와 동일한 신뢰도를 갖는 노드를 판별하고, 선택된 유전자에 대한 샤드 인덱스가 동일한 신뢰도를 갖는 것으로 판별된 노드와 다른 샤드 인덱스를 갖도록 변이시키는 샤드 분배 장치.

청구항 5

제1 항에 있어서, 상기 신뢰도 계산부는

블록체인 네트워크의 다수의 노드 각각이 블록에 대한 유효성을 검증하고, 유효성 검증 결과를 다른 노드들에서 검증한 유효성 검증 결과와 취합하여 획득한 주관적 합의 의견(이하 SCO) 벡터를 인가받아 결합하여 로컬 합의 결과(이하 LCR) 벡터를 획득하며, 상기 LCR 벡터를 이용하여 다수의 노드 각각에 대한 신뢰도를 계산하는 샤드 분배 장치.

청구항 6

제5 항에 있어서, 상기 신뢰도 계산부는

상기 다수의 노드 각각이 다수의 노드에서 블록에 대해 수행한 유효성 검증 결과로 판별된 승인 또는 비승인을 개별적으로 취합하여 획득한 다수의 SCO 벡터를 인가받고, 다수의 SCO 벡터 각각에서 승인 및 비승인을 승인 개수 및 비승인 개수의 비율에 따라 수치로 변환하고, 결합하여 상기 LCR 벡터를 획득하며,

상기 LCR 벡터의 수치를 기반으로 다수의 노드 각각에 대한 다른 노드의 평가인 평균 신뢰도를 계산하고,

상기 LCR 벡터의 수치를 기반으로 다수의 SCO 벡터 사이의 유사도를 나타내는 신뢰도 가중치를 계산하며,

계산된 평균 신뢰도와 신뢰도 가중치를 곱하여 다수의 노드 각각에 대한 신뢰도를 계산하는 샤드 분배 장치.

청구항 7

블록체인 네트워크의 다수의 노드 각각으로부터 블록에 대해 유효성을 검증한 결과와 다른 노드들에서 검증한 유효성 검증 결과와 취합하여 획득한 합의 결과를 인가받아 다수의 노드 각각에 대한 신뢰도를 획득하는 단계; 및

상기 다수의 노드를 기지정된 다수의 샤드로 분배하되, 다수의 샤드 각각에 분배되는 노드의 신뢰도의 합으로 나타나는 샤드 신뢰도를 계산하고, 계산된 다수의 샤드 신뢰도 사이의 편차가 최소가 되도록 상기 다수의 노드를 분배하는 단계를 포함하되,

상기 다수의 노드를 분배하는 단계는

동일한 신뢰도를 갖는 노드가 동일한 샤드에 분배되지 않도록 분산하여 분배하는 샤드 분배 방법.

청구항 8

삭제

청구항 9

제7 항에 있어서, 상기 다수의 노드를 분배하는 단계는

상기 다수의 노드를 랜덤하게 다수의 샤드로 분배하고, 상기 다수의 노드가 분배된 샤드의 인덱스를 유전자로서 나열하여 다수의 부모 염색체를 획득하는 단계;

상기 다수의 부모 염색체에서 한쌍으로 선택되는 부모 염색체의 유전자 중 적어도 하나의 유전자 선택하여, 대응하는 유전자를 상호 교환하여 자식 염색체를 획득하는 단계;

획득된 상기 자식 염색체에서 적어도 하나의 유전자를 선택하여 다른 샤드 인덱스로 변이시키는 단계; 및

변이된 자식 염색체에 나열된 유전자인 샤드 인덱스를 기반으로 다수의 샤드 각각에 포함되는 노드별 신뢰도의 합을 계산하여 샤드 신뢰도를 획득하는 단계;

다수의 샤드 각각에 대해 획득된 신뢰도 사이의 편차를 누적하고, 누적된 신뢰도 편차가 기지정된 기준 편차 이하이면, 상기 다수의 노드를 변이된 자식 염색체에 나열된 유전자인 샤드 인덱스를 기반으로 분배하는 단계; 및

상기 누적된 신뢰도 편차가 상기 기준 편차를 초과하면, 상기 자식 염색체를 부모 염색체로하여 다시 자식 염색체를 획득하고 변이시키는 단계를 포함하는 샤드 분배 방법.

청구항 10

제9 항에 있어서, 상기 다른 샤드 인덱스로 변이시키는 단계는

상기 자식 염색체에서 적어도 하나의 유전자를 선택하는 단계;

선택된 유전자에 대응하는 노드의 신뢰도와 동일한 신뢰도를 갖는 노드를 판별하는 단계; 및

동일한 신뢰도를 갖는 노드가 판별되면, 선택된 유전자에 대한 샤드 인덱스가 동일한 신뢰도를 갖는 것으로 판

별된 노드와 다른 샤드 인덱스를 갖도록 변이시키는 단계를 포함하는 샤드 분배 방법.

청구항 11

제7 항에 있어서, 상기 신뢰도를 획득하는 단계는

블록체인 네트워크의 다수의 노드 각각이 블록에 대해 검증한 유효성 검증 결과를 다른 노드들에서 검증된 유효성 검증 결과와 취합하여 획득한 주관적 합의 의견(이하 SCO) 벡터를 인가받는 단계;

상기 다수의 노드 각각에서 인가된 다수의 SCO 벡터를 기지정된 방식으로 변환하고 결합하여 로컬 합의 결과(이하 LCR) 벡터를 획득하는 단계; 및

상기 LCR 벡터를 이용하여 다수의 노드 각각에 대한 신뢰도를 계산하는 단계를 포함하는 샤드 분배 방법.

청구항 12

제11 항에 있어서, 상기 신뢰도를 계산하는 단계는

상기 LCR 벡터의 수치를 기반으로 다수의 노드 각각에 대한 다른 노드의 평가인 평균 신뢰도를 계산하는 단계;

상기 LCR 벡터의 수치를 기반으로 다수의 SCO 벡터 사이의 유사도를 나타내는 신뢰도 가중치를 계산하는 단계; 및

계산된 평균 신뢰도와 신뢰도 가중치를 곱하여 다수의 노드 각각에 대한 신뢰도를 계산하는 단계를 포함하는 샤드 분배 방법.

청구항 13

제11 항에 있어서, 상기 LCR 벡터를 획득하는 단계는

다수의 SCO 벡터 각각에서 승인 및 비승인을 승인 개수 및 비승인 개수의 비율에 따라 수치로 변환하고, 결합하여 상기 LCR 벡터를 획득하는 샤드 분배 방법.

청구항 14

제7 항에 따른 샤드 분배 방법을 수행시키기 위한 프로그램 명령어가 기록된 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 네트워크에 관한 것으로, 내결함성 블록체인 네트워크의 신뢰도 기반 샤드 분배 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 블록체인은 기존의 중앙화된 기관이 거래 내용을 단일 위치(single point)에 저장하는 중앙화된 방식을 탈피하고자 등장한 탈중앙화 분산 트랜잭션 관리 기술이다. 블록체인에서는 거래내역 및 장부에 대한 트랜잭션들을 모든 검증인 노드들이 P2P (Peer to Peer) 방식으로 검사하고, 과반수 노드들에 의해 합의를 얻은 경우 각 검증 노드들은 해당 거래내역모음을 해시 체인(Hash-chain)형태로 저장한다. 이는 분산데이터 저장의 한 기술로서 악의적인 운영자에 의한 데이터, 거래내역 조작이 불가능하도록 고안되었다. 블록체인 기술은 현재 암호화폐에서 주로 사용되고 있다. 블록체인에서 데이터를 조작하려면, 검증인으로 참여하는 다수의 노드의 과반수 이상의 블록들 모두를 제한된 시간 내에 수정해야 하므로, 실질적으로 데이터 조작이 불가능한 데이터 구조로 알려져 있다.

[0003] 다만 블록체인에서는 다수의 노드 각각이 블록을 검증함에 따라 트랜잭션에 대한 낮은 처리량(transactions per second)으로 인해 실시간 서비스에 적용하기 어렵다는 문제가 있다. 이러한 문제를 해결하기 위해 최근 블록체인 기법에서는 다수의 노드를 다수의 샤드(shard group)에 분배하고, 분배된 각 샤드에 다수의 트랜잭션을 분할하여 병렬로 처리하도록 하는 샤딩(sharding) 기법이 도입되었다. 샤딩 기법에서 병렬 처리된 트랜잭션들은 샤드 내에서 블록에 연결되는 사이드 체인(side chain) 구조를 갖는다.

[0004] 그러나 샤딩 기법을 도입함에 따라 트랜잭션을 검증하기 위한 노드의 개수는 샤드의 수에 대응하여 줄어들게 되고, 이로 인해 악의적 노드들의 합의 공격에 의해 데이터가 조작될 위험성이 높아지게 되는 문제가 있다. 합의 공격은 블록체인에 대한 공격 유형 중 가장 위험한 공격이다. 블록 체인에서 다수의 노드를 포함하는 검증 집단은 기본적으로 과반수의 합의를 통해 블록을 검증하며, 과반수의 합의에 도달하지 못한 블록은 폐기되어 체인에 연결될 수 없다. 그러나 악의적인 노드들이 검증집단의 과반수 이상을 차지하게 되는 경우, 거짓 블록이 체인에 연결될 수 있게 된다.

[0005] 일반적으로 블록체인에서는 수만 내지 수십만의 노드가 검증 집단에 포함되므로 악의적 노드의 수가 과반수 이상을 차지하는 것은 현실적으로 불가능하다. 그러나 샤딩 기법이 도입되면, 샤드의 개수가 증가함에 따라 각 샤드내에서 노드의 개수가 줄어 들게 되어 악의적 노드의 수가 과반수 이상을 차지하게 되는 경우가 발생될 수 있다. 즉 공격자가 포섭해야 하는 노드의 개수가 줄어들어 거짓 블록이 체인에 연결될 가능성이 있다. 특히 악의적 노드가 특정 샤드에 집중되어 배치되는 경우, 잘못된 검증을 수행할 가능성이 크게 높아진다.

[0006] 이러한 취약점을 보완하기 위하여, 현재 샤딩 기법에서는 다수의 노드들을 다수의 샤드에 랜덤하게 분배하되, 보안성을 유지하기 위해 각 샤드당 노드의 개수는 수백 내지 수천개 이상으로 확보되어야 함을 전제로 하고 있다. 그러나 단순히 샤드당 노드의 개수를 증가시키는 것은 효율적이지 않으므로 블록체인 서비스를 확장시키는데 장애가 되고 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국 공개 특허 제10-2019-0067581호 (2019.06.17 공개)

발명의 내용

해결하려는 과제

[0008] 본 발명의 목적은 다수의 노드 각각의 신뢰도를 계산하고, 다수의 샤드 각각에 포함되는 노드들의 신뢰도의 합이 유사하도록 샤드에 다수의 노드를 분배하는 샤드 분배 장치 및 방법을 제공하는데 있다.

[0009] 본 발명의 다른 목적은 각 샤드간 신뢰도 편차가 최소화되도록 유전 알고리즘을 기반으로 다수의 노드를 다수의 샤드에 분배하는 샤드 분배 장치 및 방법을 제공하는데 있다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 샤드 분배 장치는 블록체인 네트워크의 다수의 노드 각각으로부터 블록에 대해 유효성을 검증한 결과와 다른 노드들에서 검증한 유효성 검증 결과와 취합하여 획득한 합의 결과를 인가받아 다수의 노드 각각에 대한 신뢰도를 획득하는 신뢰도 계산부; 및 상기 다수의 노드를 기지정된 다수의 샤드로 분배하되, 다수의 샤드 각각에 분배되는 노드의 신뢰도의 합으로 나타나는 샤드 신뢰도를 계산하고, 계산된 다수의 샤드 신뢰도 사이의 편차가 최소가 되도록 상기 다수의 노드를 분배하는 샤드 분배부를 포함한다.

[0011] 상기 샤드 분배부는 동일한 신뢰도를 갖는 노드가 동일한 샤드에 분배되지 않도록 분산하여 분배할 수 있다.

[0012] 상기 샤드 분배부는 상기 다수의 노드를 랜덤하게 다수의 샤드로 분배하고, 상기 다수의 노드가 분배된 샤드의 인덱스를 유전자로서 나열하여 다수의 부모 염색체를 획득하고, 상기 다수의 부모 염색체에서 한쌍으로 선택되는 부모 염색체의 유전자 중 적어도 하나의 유전자 선택하여, 대응하는 유전자를 상호 교환하여 자식 염색체를 획득하며, 획득된 상기 자식 염색체에서 적어도 하나의 유전자를 선택하여 다른 샤드 인덱스로 변이시킨 후, 변이된 자식 염색체에 나열된 유전자인 샤드 인덱스를 기반으로 다수의 샤드 각각에 대해 획득된 신뢰도 사이의 편차를 누적하고, 누적된 신뢰도 편차가 기지정된 기준 편차 이하이면, 상기 다수의 노드를 변이된 자식 염색체에 나열된 유전자인 샤드 인덱스를 기반으로 분배하며, 상기 누적된 신뢰도 편차가 상기 기준 편차를 초과하면, 상기 자식 염색체를 부모 염색체로하여 다시 자식 염색체를 획득하고 변이시킬 수 있다.

[0013] 상기 샤드 분배부는 상기 자식 염색체에서 적어도 하나의 유전자를 선택하고, 선택된 유전자에 대응하는 노드의 신뢰도와 동일한 신뢰도를 갖는 노드를 판별하고, 선택된 유전자에 대한 샤드 인덱스가 동일한 신뢰도를 갖는

것으로 판별된 노드와 다른 샤드 인덱스를 갖도록 변이시킬 수 있다.

[0014] 상기 신뢰도 계산부는 블록체인 네트워크의 다수의 노드 각각이 블록에 대한 유효성을 검증하고, 유효성 검증 결과를 다른 노드들에서 검증한 유효성 검증 결과와 취합하여 획득한 주관적 합의 의견(이하 SCO) 벡터를 인가받아 결합하여 로컬 합의 결과(이하 LCR) 벡터를 획득하며, 상기 LCR 벡터를 이용하여 다수의 노드 각각에 대한 신뢰도를 계산할 수 있다.

[0015] 상기 신뢰도 계산부는 상기 다수의 노드 각각이 다수의 노드에서 블록에 대해 수행한 유효성 검증 결과로 판별된 승인 또는 비승인을 개별적으로 취합하여 획득한 다수의 SCO 벡터를 인가받고, 다수의 SCO 벡터 각각에서 승인 및 비승인을 승인 개수 및 비승인 개수의 비율에 따라 수치로 변환하고, 결합하여 상기 LCR 벡터를 획득하며, 상기 LCR 벡터의 수치를 기반으로 다수의 노드 각각에 대한 다른 노드의 평가인 평균 신뢰도를 계산하고, 상기 LCR 벡터의 수치를 기반으로 다수의 SCO 벡터 사이의 유사도를 나타내는 신뢰도 가중치를 계산하며, 계산된 평균 신뢰도와 신뢰도 가중치를 곱하여 다수의 노드 각각에 대한 신뢰도를 계산할 수 있다.

[0016] 상기 목적을 달성하기 위한 본 발명의 다른 실시예에 따른 샤드 분배 방법은 블록체인 네트워크의 다수의 노드 각각으로부터 블록에 대해 유효성을 검증한 결과와 다른 노드들에서 검증한 유효성 검증 결과와 취합하여 획득한 합의 결과를 인가받아 다수의 노드 각각에 대한 신뢰도를 획득하는 단계; 및 상기 다수의 노드를 기지정된 다수의 샤드로 분배하되, 다수의 샤드 각각에 분배되는 노드의 신뢰도의 합으로 나타나는 샤드 신뢰도를 계산하고, 계산된 다수의 샤드 신뢰도 사이의 편차가 최소가 되도록 상기 다수의 노드를 분배하는 단계를 포함한다.

발명의 효과

[0017] 따라서, 본 발명의 실시예에 따른 샤드 분배 장치 및 방법은 합의를 방해하는 악성 노드가 존재하는 블록체인 네트워크에서 다수의 노드에 대한 신뢰도를 계산하고, 계산된 각 노드의 신뢰도를 기반으로 다수의 샤드 사이의 신뢰도 편차가 최소화되도록 다수의 노드를 분배함으로써, 악성 노드가 특정 샤드에 집중되는 것을 방지할 수 있다. 그러므로 각 샤드에서 악성 노드들의 담합을 억제하여 비정상 합의 공격뿐만 아니라 합의를 정상적으로 하면서 다른 노드의 의견 변조하는 패시브 공격을 방지할 수 있다. 즉 블록체인 네트워크의 신뢰도를 향상시킬 수 있으며, 샤드에 포함되는 검증 노드의 개수가 적은 경우에도 신뢰성 있는 블록체인 네트워크를 제공하여 블록체인 네트워크의 적용 분야를 효율적으로 확장할 수 있도록 한다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시예에 따른 블록체인 네트워크에서 다수의 노드의 개략적 구조를 나타낸다.

도 2는 도 1의 신뢰도 계산부가 다수의 노드 각각에 대한 신뢰도를 계산하는 과정을 설명하기 위한 도면이다.

도 3 내지 도 5는 도 1의 샤드 분배부가 유전 알고리즘을 기반으로 다수의 노드를 다수의 샤드에 분배하는 과정을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 블록체인 네트워크의 샤드 분배 방법을 나타낸다.

도 7은 블록체인 네트워크의 노드 사이에 교환되는 메시지의 구조를 나타낸다.

도 8은 본 실시예에 따른 블록체인 네트워크에서 블록의 구조를 나타낸다.

도 9는 본 실시예에 따른 신뢰도 기반 샤드 분배 장치 및 방법의 성능을 시뮬레이션한 결과를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시예를 예시하는 첨부 도면 및 첨부 도면에 기재된 내용을 참조하여야만 한다.

[0020] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 설명함으로써, 본 발명을 상세히 설명한다. 그러나, 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 설명하는 실시예에 한정되는 것이 아니다. 그리고, 본 발명을 명확하게 설명하기 위하여 설명과 관계없는 부분은 생략되며, 도면의 동일한 참조부호는 동일한 부재임을 나타낸다.

[0021] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈", "블록" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를

의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0022] 도 1은 본 발명의 일 실시예에 따른 블록체인 네트워크에서 다수의 노드의 개략적 구조를 나타내고, 도 2는 도 1의 신뢰도 계산부가 다수의 노드 각각에 대한 신뢰도를 계산하는 과정을 설명하기 위한 도면이며, 도 3 내지 도 5는 도 1의 샤드 분배부가 유전 알고리즘을 기반으로 다수의 노드를 다수의 샤드에 분배하는 과정을 설명하기 위한 도면이다.

[0023] 블록체인 네트워크의 다수의 노드는 기본적으로 블록의 유효성을 검증하는 검증 노드로서 기능하며, 다수의 노드 중 적어도 하나의 노드는 블록체인 네트워크 상의 다수의 노드를 다수의 샤드에 분배하는 샤드 매니저, 즉 샤드 분배 장치로 기능한다.

[0024] 이하에서는 우선 검증 노드에 대한 구성을 설명하고, 추가적으로 샤드 매니저의 구성을 설명한다.

[0025] 도 1을 참조하면, 블록체인 네트워크의 다수의 검증 노드 각각은 통신부(110), 제어부(120), 블록 생성부(130), 신뢰도 계산부(140) 및 블록 저장부(150)를 포함할 수 있다.

[0026] 통신부(110)는 다수의 노드 각각이 블록체인 네트워크 상의 다른 노드와 통신을 수행할 수 있도록 하고, 제어부(120)는 노드의 각 구성요소를 제어하여 내부에서 각 구성 요소 사이의 데이터를 전달할 뿐만 아니라 통신부(110)를 제어하여 다른 노드와 데이터를 송수신한다.

[0027] 블록 생성부(130)는 노드가 블록 생성권자로 선택되면, 처리해야할 트랜잭션을 수집하고 기록 및 검증하여 블록을 생성한다. 여기서 블록 생성부(130)는 다수의 노드가 이미 다수의 샤드에 분배된 상태라면, 블록 생성부(130)는 해당 노드가 포함된 샤드에서 처리해야할 트랜잭션을 수집하여 블록을 생성할 수 있다. 그리고 생성된 블록을 통신부(110)를 통해 블록체인 네트워크에 전파한다.

[0028] 블록 생성권자는 작업 증명(Proof of Work: PoW) 또는 지분 증명(Proof of Stake: PoS) 기법에 따라 선택될 수 있다. 작업 증명(PoW) 기법에서는 매번 블록을 생성하기에 앞서 모든 검증 노드들은 특정 난이도 미만의 해시(hash)값을 찾는 작업을 수행하고, 특정 난이도 미만의 해시값 중 가장 낮은 해시값을 제안한 노드에게 블록 생성권자로 선택된다. 여기서 생성된 블록은 블록체인 네트워크의 다수의 노드에 의한 합의 과정을 거쳐 과반수 이상의 동의를 받게 되면 최종 블록으로 선언되어 각 노드에 이전 저장된 블록체인에 연결된다.

[0029] 한편 지분 증명(PoS) 기법은 작업 증명(PoW) 기법에서의 과도한 해시 연산 부담을 줄이기 위해 제안된 기법으로 각 노드가 보유한 지분(Stake) 및 지분의 보유기간에 따라 블록 생성권자가 확률적으로 선택된다. 만약 모든 노드들의 지분과 보유기간이 동일하다면, 블록 생성권자는 다수의 노드가 동일 확률로 랜덤하게 선택될 수 있다.

[0030] 본 실시예에서는 일예로 블록 생성권자가 지분 증명(PoS) 기법에 따라 선택되고, 다수의 노드는 동일 확률로 랜덤하게 블록 생성권자로 선택되는 것으로 가정한다.

[0031] 신뢰도 계산부(140)는 블록 생성권자로 선택된 노드에서 생성되어 전파된 블록의 유효성을 검증하고, 다른 노드들의 블록 검증 결과를 함께 고려하여 블록합의 결과를 판별하여 승인 여부를 결정한다. 이때 신뢰도 계산부(140)는 노드가 특정 샤드에 포함된 상태이면 해당 샤드 내의 블록 생성권자에서 생성된 블록과 다른 노드들의 블록 검증 결과를 인가받을 수 있다.

[0032] 신뢰도 계산부(140)는 블록 생성권자에서 제안된 블록의 유효성을 검증하여 유효한 블록으로 판별되면, 승인을 의미하는 "Y"로 표기하고 무효한 블록으로 판별되면 비승인을 의미하는 "N"를 표기한다. 이때 신뢰도 계산부(140)는 자신의 유효성 검증 결과를 다른 노드들로 전송하고, 다른 노드들의 유효성 검증 결과를 인가받아 함께 분석하여 제안된 블록의 유효성을 블록합의 결과로 검증한다.

[0033] 즉 블록체인 네트워크에 n개의 노드가 존재하는 경우, 다수의 노드 각각에서 신뢰도 계산부(140)는 제안된 블록별로 1 × n 크기의 벡터를 생성하고, 생성된 벡터에 n개의 노드 각각에서 판별된 유효성 검증 결과인 승인(Y) 또는 비승인(N)을 기록한다. 그리고 승인(Y)의 개수가 n/2 이상이면, 블록합의 결과로 제안된 블록이 유효한 것으로 판정한다.

[0034] 여기서 신뢰도 계산부(140)에서 판별된 블록합의 결과는 비록 다수의 노드의 유효성 검증 의견을 취합한 것이지만, 다수의 노드 각각이 주관적으로 유효성 검증 의견을 취합하여 획득한 주관적 합의 의견(Subjective Consensus Opinion: 이하 SCO) 벡터로 볼 수 있다. 이하에서는 n개의 노드 중 i번째 노드에서 획득된 SCO 벡터는 S_i로 표기한다. 즉 n개의 노드 각각은 1 × n 크기의 벡터인 SCO 벡터(S_i)를 획득한다.

[0035] 한편, 신뢰도 계산부(140)는 다수의 노드 중 과반수 이상의 노드들이 유효한 블록으로 판별하였으면, 해당 블록을 블록 저장부(150)에 이전 저장된 블록체인에 연결하여 저장한다. 그리고 신뢰도 계산부(140)는 주관적 합의 의견(S_i)을 블록체인 네트워크의 샤드 매니저로 전달한다.

[0036] 블록 저장부(150)는 신뢰도 계산부(140)에서 유효한 것으로 판별된 블록을 인가받아 저장한다. 이때 블록 저장부(150)는 이전 저장된 블록체인에 인가된 블록을 연결하여 저장한다. 그리고 저장된 블록체인을 블록체인 네트워크의 다른 노드들로 전파할 수 있다.

[0037] 상기에서는 노드가 블록체인 네트워크에서 제안된 블록의 유효성을 검증하는 검증 노드로 기능을 수행하는 경우의 구성을 설명하였다. 그러나 상기한 바와 같이 블록체인 네트워크의 다수의 노드 중 적어도 하나의 노드는 샤드 매니저로도 기능할 수 있다.

[0038] 노드가 샤드 매니저인 경우, 신뢰도 계산부(140)는 다수의 노드에서 획득된 SCO 벡터(S_i)를 인가받아 로컬 합의 결과(Local Consensus Result: 이하 LCR) 벡터를 획득하고, 획득된 LCR 벡터(L)에 기반하여 각 노드에 대한 평균 신뢰도(Average trust) 및 신뢰도 가중치(trust weight)(W)를 계산하여 각 노드별 신뢰도를 획득한다.

[0039] 도 2를 참조하여 샤드 매니저의 신뢰도 계산부(140)가 노드별 신뢰도를 획득하는 과정을 설명하면, 신뢰도 계산부(140)는 우선 다수의 노드 각각에서 획득된 SCO 벡터(S_i)를 취합하여 (a)와 같은 LCR 벡터(L)를 획득한다.

[0040] 신뢰도 계산부(140)는 n개의 노드 각각에서 인가되는 n개의 1 × n 크기의 SCO 벡터(S_i)에서 승인(Y)과 비승인(N)을 수학식 1과 같이 승인(Y)의 개수(n(Y))와 비승인(N)의 개수(n(N))에 대한 비율로 각각 변환한다.

수학식 1

[0041] $$\frac{n(Y)}{n(Y)+n(N)'}\quad\frac{n(N)}{n(Y)+n(N)}$$

[0042] 일예로 3개의 노드를 갖는 블록체인 네트워크에서 각각의 노드가 SCO 벡터(S_i)로 (Y, Y, N)를 획득하여 샤드 매니저로 전송한 경우, 샤드 매니저의 신뢰도 계산부(140)는 각 노드에 대한 SCO 벡터(S_i) 각각을 (2/3, 2/3, 1/3)으로 변환할 수 있다. 그러나 만일 3개의 노드 중 제3 노드가 악의적 노드로서 SCO 벡터(S_3)를 (N, Y, N)으로 변경하여 전송한 경우, 샤드 매니저의 신뢰도 계산부(140)는 제3 노드의 SCO 벡터(S_3)를 (2/3, 1/3, 2/3)로 변환할 수 있다.

[0043] 그리고 변환된 SCO 벡터(S_i)들을 합하여 n × n 크기의 벡터인 LCR 벡터(L)를 획득한다. n × n 크기의 벡터인 LCR 벡터(L)에서 각 원소는 $L_{i,j}$로 표현될 수 있으며, 이는 i번째 노드가 평가한 j번째 노드의 신뢰도가 된다.

[0044] LCR 벡터(L)가 획득되면, 샤드 매니저의 신뢰도 계산부(140)는 (b)와 같이 LCR 벡터(L)를 기반으로 특정 노드(여기서는 일예로 j번째 노드)에 대한 다른 노드들의 평가를 반영한 객관적 지표로서 평균 신뢰도(u_j)를 수학식 2에 따라 계산할 수 있다.

수학식 2

[0045] $$\sum_{i=1}^{n}\frac{L_{i,j}}{n}=u_j$$

[0046] 즉 LCR 벡터(L)에서 열단위의 평균값을 획득하여 n개의 노드별 평균 신뢰도를 계산한다. 여기서 평균 신뢰도(u_j)는 악의적 노드의 비정상적 합의 행위에 대한 패널티를 부가하기 위해 계산된다.

[0047] 블록체인 네트워크 내의 모든 노드가 정상인 경우, 다수의 노드 각각에서 전송된 SCO 벡터(S_i)는 모두 동일한

값을 가져야 한다. 그러나 악의적인 노드는 SCO 벡터(S_i)를 거짓으로 작성하여 전송할 수 있다. LCR 벡터(L)에서 i번째 행 벡터를 £$_i$로 표기하고, i번째 행 벡터(£$_i$)는 i번째 노드의 신뢰도 보고 행위를 나타낸다.

[0048] 이에 각 노드 사이의 신뢰도 유사도를 (c)와 같이 분석하여 노드별 신뢰도 가중치(W_i)를 계산한다. 여기서 i번째 노드와 j번째 노드 사이의 신뢰도 유사도는 i번째 행 벡터(£$_i$)와 j번째 행 벡터(£$_j$) 사이의 코사인 유사도(cosine similarity)를 이용하여 수학식 3과 같이 계산될 수 있다.

수학식 3

[0049] $$W_{i,j} = cos(£_i, £_j)$$

[0050] 수학식 3으로부터 i번째 노드의 신뢰도 가중치(W_i)는 해당 노드와 다른 모든 노드 사이의 벡터간 유사도의 평균으로 수학식 4로 계산될 수 있다.

수학식 4

[0051] $$W_i = \sum_{j=1}^{n} \frac{W_{i,j}}{n}$$

[0052] 이후 신뢰도 계산부(140)는 (d)에 도시된 바와 같이, 수학식 2로 계산되는 각 노드별 평균 신뢰도(u_i)와 수학식 3으로 계산되는 신뢰도 가중치(W_i)를 곱하여 수학식 5와 같이 다수의 노드 각각에 대한 신뢰도(t_i)를 계산할 수 있다.

수학식 5

[0053] $$t_i = W_i u_i$$

[0054] 여기서 각 노드별 신뢰도(t_i)를 평균 신뢰도(u_i)와 신뢰도 가중치(W_i)의 곱으로 계산하는 것은 악의적 노드의 비정상적인 합의뿐만 아니라 비정상적 신뢰도 보고 행위에 대해서도 패널티를 부가하여 악의적 노드의 신뢰도를 낮추기 위함이다.

[0055] 코사인 유사도의 경우, 두 입력이 양의 실수이면 결과값이 [0, 1]의 범위 내에서 수렴하므로, 평균 신뢰도(u_i)와 신뢰도 가중치(W_i) 및 신뢰도(t_i) 또한 [0, 1]의 범위에서 수렴한다.

[0056] 한편 노드가 사드 매니져로 기능하는 경우, 해당 노드는 신뢰도 저장부(160) 및 샤드 분배부(170)를 더 포함할 수 있다.

[0057] 신뢰도 저장부(160)는 신뢰도 계산부(140)에서 계산된 다수의 노드 각각에 대한 신뢰도(t_i)를 저장한다. 그리고 샤드 분배부(170)는 다수의 노드를 기지정된 K개의 샤드로 분배한다. 이때 샤드 분배부(170)는 신뢰도 저장부(160)에 저장된 다수의 노드 각각에 대한 신뢰도(t_i)를 기반으로 K개의 샤드 사이의 샤드 신뢰도 편차가 최소가 되도록 다수의 노드를 분배한다.

[0058] 즉 샤드 분배부(170)는 K개의 샤드 각각에 포함되는 노드들의 신뢰도(t_i)의 총합을 샤드 신뢰도(S_{gk})(여기서 k = 1, …, K) 라 할 때, 다수의 샤드 사이의 샤드 신뢰도 편차를 나타내는 수학식 6의 함수가 최소가 되도록 다수의 노드를 K 개의 샤드에 분배한다.

수학식 6

[0059] $$\sum_{i=1}^{K}\sum_{j=1}^{K}\sqrt{\frac{(S_{gi}-S_{gj})^2}{K}} \quad (i,j \in \mathrm{K})$$

[0060] 특히 본 실시예에서 샤드 분배부(170)는 수학식 6의 함수가 최소가 되도록 유전 알고리즘(Genetic algorithm)을 적용하여 다수의 노드를 다수의 샤드에 분배할 수 있다.

[0061] 유전 알고리즘은 자연의 진화과정에 기초한 진화 알고리즘(evolutionary algorithm)의 한 분야로 개발된 전역 최적화 기법 중 하나이다. 유전 알고리즘은 교차(crossover) 및 변이(Mutation)의 2가지 프로세스를 통해 적자생존에 기반한 접근 법으로 최적해를 탐색하는 기법이다. 유전 알고리즘에서는 해결하고자 하는 최적화 문제가 존재할 때, 가능한 해(Solution)의 집합을 나타내는 자료구조를 염색체(Chromosome)라고 표현하고, 염색체들에 대한 교차 및 변이 과정을 진행하면서 특정 목적 함수를 만족하는 최적해를 탐색하는 기법이다.

[0062] 도 3 내지 도 5는 샤드 분배부(170)가 유전 알고리즘을 기반으로 다수의 노드를 다수의 샤드에 분배하는 과정을 시각적으로 나타낸다. 일예로 샤드 분배부(170)가 블록체인 네트워크의 6개의 노드(N_1 ~ N_6)를 3개의 샤드(S_1, S_2, S_3)에 분배하는 경우를 도시하였다.

[0063] 도 3은 유전 알고리즘을 적용하기 이전 초기 분배 과정을 나타낸다. 도3을 참조하면, 초기 분배 과정에서 샤드 분배부(170)는 (a)와 같이, 블록체인 네트워크에 포함된 6개의 노드(N_1 ~ N_6)를 (b)에 도시된 바와 같이, 임의로 3개의 샤드(S_1, S_2, S_3)에 랜덤하게 분배할 수 있다. 그리고 (c)와 같이 분배된 6개의 노드(N_1 ~ N_6) 순서에 따라 분배된 샤드의 인덱스(S_1, S_2, S_3)를 배열하여 염색체를 획득한다. 여기서 획득된 염색체 각각에 배열된 샤드 인덱스를 유전자라고 할 수 있다. 이때 샤드 분배부(170)는 하나의 염색체만을 획득하는 것이 아니라, 6개의 노드(N_1 ~ N_6)를 다양한 조합으로 분배하여 다수의 염색체를 획득할 수 있다. 이렇게 다수의 노드(N_1 ~ N_6)를 다수의 샤드(S_1, S_2, S_3)에 랜덤하게 분배하여 획득되는 다수의 염색체는 부모 염색체(Parent Chromosom)로 이용된다. 샤드 분배부(170)는 다수의 부모 염색체를 초기 부모 염색체 집합(P)으로 획득할 수 있다. 그리고 초기 부모 염색체 집합(P)에서 교차 및 변이에 이용할 M개의 부모 염색체를 선택한다.

[0064] 이후 샤드 분배부(170)는 M(일예로 50)개의 부모 염색체 중 서로 유전자를 교차시킬 쌍을 선택하여 유전자를 교차시킨다. 샤드 분배부(170)는 유전자를 교차시킬 ${}_{M}C_2$개의 순서쌍을 생성하고, 생성된 순서쌍에 따라 2개의 부모 염색체를 선택한다. 그리고 선택된 2개의 부모 염색체에서 적어도 하나의 유전자를 교환한다.

[0065] 도 4를 참조하면, 샤드 분배부(170)는 (a)에 도시된 바와 같이, 생성된 순서쌍에 따라 선택된 2개의 부모 염색체 각각에서 서로 대응하는 적어도 하나의 노드를 교차 유전자로 선택(여기서는 일예로 제2 노드(N_2) 및 제5 노드(N_5))하고, 선택된 교차 유전자의 노드가 분배된 샤드를 서로 교차(crossover)시켜 (b)와 같은 자식 염색체(Offspring Chromosom)를 획득한다. 도 4의 (b)에 도시된 자식 염색체는 (a)에 도시된 부모 염색체에 비해 제2 노드(N_2) 및 제5 노드(N_5)의 샤드가 서로 변경되었음을 알 수 있다. 여기서 샤드 분배부(170)는 부모 염색체에서 노드를 기지정된 개수(N)로 선택하며, 교차시킬 노드를 기지정된 교차 확률(P_c)(일예로 0.8)에 따라 선택할 수 있다.

[0066] 한편, 샤드 분배부(170)는 자식 염색체가 획득되면, 획득된 자식 염색체 중 적어도 하나의 염색체를 변이 유전자로 선택하여 변이시킨다.

[0067] 도 5를 참조하면, 샤드 분배부(170)는 도 4의 (b)와 같이 획득된 자식 염색체에서 기지정된 개수(N) 및 기지정된 변이 확률(P_m)(일예로 0.1)에 따라 변이시킬 노드를 선택(여기서는 일예로 제5 노드(N_5))할 수 있다. 그리고 선택된 노드를 현재 분배된 샤드(S_1)가 아닌 다른 샤드(S_3)로 분배한다. 즉 선택된 변이 유전자를 변경한다.

[0068] 특히 본 실시예에서 샤드 분배부(170)는 변이 과정에서 신뢰도 중복 방지라는 추가적인 진화의 방향성을 설정하여 유전자를 변이시킬 수 있다. 이를 위해 샤드 분배부(170)는 변이 유전자를 변경함에 있어, 동일한 신뢰도를

갖는 노드가 분배되지 않은 샤드를 탐색하여 해당 노드를 분배하는 방식으로 유전자를 변이시킨다.

[0069] 도 5에 도시된 바와 같이, (S_1, S_2, S_1, S_3, S_1, S_2)의 자식 유전자가 획득되고 제5 노드(N_5)에 대응하는 유전자(S_1)에 대한 변이를 진행할 때, 현재 분배된 샤드(S_1)는 제외되어야 하므로, 제2 및 제3 샤드(S_2, S_3) 중 하나로 변이되어야 한다. 이때 만약 제5 노드(N_5)의 신뢰도(t_5)와 제2 노드(N_2)의 신뢰도(t_3)가 동일하다면, 제5 노드(N_5)에 대응하는 유전자(S_1)는 제2 노드(N_2)에 대응하는 유전자(S_2)와 다른 유전자로 변이되어야 한다. 즉 제5 노드(N_5)에 대응하는 유전자(S_1)는 제3 샤드(S_3)로 변이되어야 한다.

[0070] 이는 신뢰도가 유사한 노드들이 서로 다른 샤드에 분배되도록 함으로써, 기존에 다수의 노드를 단순히 랜덤하게 분배하여 다수의 샤드를 구성하는 경우에 비해, 다수의 노드가 특정 샤드에 집중되지 않고 강제로 서로 다른 샤드에 분리되어 분배되도록 하여 악의적 노드에 의해 블록이 변조되는 것을 방지한다.

[0071] 샤드 분배부(170)는 변이 과정이 수행되면 자손 염색체 집합(O)을 생성하고, 생성된 자손 염색체 집합(O)에 대해 수학식 6의 함수를 최소화하는 최적의 값을 갖는 염색체를 다시 M개 추출하여 교차 및 변이 과정을 반복한다. 그리고 수학식 6의 다수의 샤드간 신뢰도 편차가 기지정된 기준 편차 이하가 되거나 기지정된 횟수만큼 반복하여 획득되는 자손 염색체를 기반으로 다수의 노드를 다수의 샤드에 분배한다.

[0072] 도 6은 본 발명의 일 실시예에 따른 블록체인 네트워크의 샤드 분배 방법을 나타낸다.

[0073] 도 1 내지 도 5를 참조하여, 도 6의 샤드 분배 방법을 설명하면, 샤드 분배 방법은 크게 블록을 생성하는 블록 생성 단계(S10), 각 노드별로 획득된 블록 합의 결과에 기반하여 다수의 노드 각각에 대한 신뢰도를 획득하는 신뢰도 계산 단계(S20) 및 획득된 노드별 신뢰도를 기반으로 다수의 샤드 사이의 샤드 신뢰도 편차가 최소화되도록 다수의 노드를 분배하는 노드 분배 단계(S30)를 포함할 수 있다.

[0074] 블록 생성 단계(S10)에서는 우선 블록체인 네트워크의 다수의 노드 중에서 블록 생성권자가 선택된다(S11). 블록 생성권자는 일예로 작업 증명(PoW) 또는 지분 증명(PoS) 기법에 의해 선택될 수 있다. 블록 생성권자로 선택된 노드는 처리해야할 트랜잭션을 수집하고 기록 및 검증하여 블록을 생성한다(S12). 그리고 생성된 블록을 다른 노드들로 전파한다(S13).

[0075] 신뢰도 계산 단계(S20)에서 블록을 인가받은 다수의 노드 각각은 인가된 블록에 대한 유효성을 검증하여 해당 블록의 승인(Y) 또는 비승인(N)을 판별한다(S21). 그리고 다수의 노드 각각은 자신의 유효성 검증 결과와 다른 노드들의 유효성 검증 결과를 취합하여 SCO 벡터(S_i)를 획득하고, 획득된 SCO 벡터(S_i)를 다수의 노드 중 기지정된 샤드 매니저, 즉 샤드 분배 장치로 전파한다(S22). 이때 다수의 노드 각각은 획득된 SCO 벡터(S_i)를 기반으로 다수의 노드 중 과반수 이상의 노드가 생성된 블록에 대해 승인한 것으로 판별되면, 해당 블록을 유효한 블록으로 판정하고, 기저장된 블록체인에 연결하여 저장한다. 그리고 저장된 블록체인을 다른 노드로 전파할 수 있다.

[0076] 한편, 샤드 매니저는 다수의 노드 각각에서 전송된 SCO 벡터(S_i)를 취합하여 LCR 벡터(L)를 획득한다(S23). 이때 샤드 매니저는 다수의 노드에서 전송된 다수의 SCO 벡터(S_i) 각각에서 승인(Y)과 비승인(N) 내역을 승인(Y) 및 비승인(N) 개수에 대한 비율로 변환하고 결합하여 LCR 벡터(L)를 획득할 수 있다.

[0077] LCR 벡터(L)가 획득되면, LCR 벡터(L)를 이용하여, 다수의 노드 각각에 대해 다른 노드들이 평가한 신뢰도인 평균 신뢰도(u_i)와 다수의 노드에서 획득된 SCO 벡터(S_i) 사이의 유사도를 기반으로 신뢰도 가중치(W_i)를 계산한다(S24).

[0078] 그리고 계산된 다수의 노드 각각에 대한 평균 신뢰도(u_i)와 신뢰도 가중치(W_i)를 곱하여 각 노드에 대한 신뢰도(t_i)를 평가한다(S25).

[0079] 다수의 노드 각각에 대해 평가된 신뢰도(t_i)가 획득되면, 노드 분배 단계(S30)에서는 획득된 신뢰도(t_i)를 기반으로 다수의 노드를 다수의 샤드에 분배한다. 이때, 샤드 매니저는 유전 알고리즘을 기반으로 다수의 노드를 다수의 샤드에 분배할 수 있다.

[0080] 노드 분배 단계(S30)에서 샤드 매니저는 우선 다수의 노드를 기지정된 개수의 샤드에 랜덤하게 분배하고, 다수의 노드가 분배된 샤드의 인덱스를 유전자로서 나열하여 다수의 부모 염색체를 획득한다(S31). 그리고 획득된

부모 염색체 중 서로 유전자를 교차시킬 부모 염색체를 2개씩 선택하고, 선택된 2개의 부모 염색체에서 기지정된 개수의 서로 대응하는 유전자를 기저정된 확률(P_c)에 따라 선택하여 교환한다. 즉 부모 염색체의 일부 유전자인 샤드 인덱스(S_i)를 서로 교차시켜 자식 염색체를 획득한다(S32).

[0081] 이후 획득된 자식 염색체에서 기지정된 개수의 유전자를 기지정된 확률(P_m)에 따라 선택하고, 선택된 유전자인 샤드 인덱스를 다른 샤드 인덱스로 변경함으로써 유전자를 변이시킨다(S33). 이때, 샤드 매니저는 변이를 위해 선택된 변이 유전자에 대응하는 노드의 신뢰도(t_i)와 동일한 신뢰도를 갖는 노드에 대응하는 유전자가 자식 염색체에 존재하는지 판별하고, 만일 동일한 신뢰도를 갖는 유전자가 존재하면, 해당 유전자의 샤드 인덱스가 아닌 다른 샤드 인덱스로 유전자를 변이시킨다.

[0082] 그리고 변이된 자식 염색체를 분석하여 다수의 샤드 각각에 대한 샤드 신뢰도(S_g)를 각 샤드에 포함되는 노드별 신뢰도(t_i)의 합으로 계산한다(S34). 다수의 샤드 각각에 대한 샤드 신뢰도가 계산되면, 계산된 샤드 신뢰도(S_g) 사이의 편차를 누적한 샤드 신뢰도 편차가 기지정된 기준 편차 이하인지 판별한다(S35). 만일 샤드 신뢰도 편차가 기준 편차 이하이면, 현재 획득된 자식 염색체를 기반으로 다수의 노드를 다수의 샤드에 분배한다(S36). 그러나 샤드 신뢰도 편차가 기준 편차를 초과하면, 자식 염색체를 교차하여 다시 유전자를 교환함으로써 추가적인 자손 염색체를 획득한다(S32).

[0083] 도 7은 블록체인 네트워크의 노드 사이에 교환되는 메시지의 구조를 나타낸다.

[0084] 도 7에서 길이 필드(Length)(701)는 전송하는 프레임의 길이를 나타내고, 노드 식별자 필드(Node Identifier)(702)는 메시지를 전송하는 노드의 주소를 나타내며, 타입 필드(Type)(703)는 메시지의 종류를 나타낸다. 여기서 메시지의 종류에는 블록 제안을 위한 용도, SCO보고를 위한 용도, 수신한 블록에 대한 유효성 검사여부, 합의된 블록전파를 위한 용도 등으로 구분될 수 있다. 플래그 필드(Flag)(704)는 메시지의 기타 정보로써 일예로 해당 블록의 라운드 수를 나타낼 수 있다. 페이로드 필드(payload)(705)는 메시지 타입에 따라 용도가 가변되는 데이터로서, 생성된 블록을 제안하는 경우, 샤드에서 이번 라운드에 할당된 처리해야하는 트랜잭션이 포함될 수 있다. 그러나 수신 블록에 대한 유효성 검사 결과인 경우, 해당 블록에 대한 승인 또는 비승인 나타내는 이진 데이터가 포함될 수 있다. 또한 메시지 타입이 샤드 매니저에게 전송하는 주관적 합의 의견(SCO)인 경우, SCO 벡터가 포함될 수 있다. 한편 전송 데이터가 합의된 블록인 경우, 해당 블록에 대한 데이터가 포함될 수 있다.

[0085] 도 8은 본 실시예에 따른 블록체인 네트워크에서 블록의 구조를 나타낸다.

[0086] 샤드 분배된 블록체인 네트워크에서 블록은 (a)에 도시된 사이드 블록와 (b)에 도시된 메인 블록의 두 종류로 구분될 수 있다.

[0087] 사이드 블록은 각 샤드에 저장되는 블록으로 메인 블록을 생성하기 위해 임시 저장되는 블록이며, 메인 블록은 각 샤드에 저장된 사이드 블록을 참고하여 최종 결정되는 블록이다.

[0088] (a) 및 (b)에 도시된 바와 같이 블록은 다시 블록 헤더(810, 830)과 블록 바디(820, 840)로 구성될 수 있다.

[0089] (a)의 사이드 블록에서 블록 헤더(810)에는 제안자 ID(811), 이전 블록 해시(812), 머클 루트 해시(merkle root hash)(813), 샤드 정보(Shard Info)(814)를 포함할 수 있다. 제안자 ID(811)는 해당 샤드에서 블록 생성 권자의 주소를 나타내고, 이전 블록 해시(812)는 이전 샤드 블록의 전체 해시값을 나타내며, 머클 루트 해시(813)는 트랜잭션에 대한 머클 루트 해시(Merkle root hash)를 나타낸다. 그리고 샤드 정보(814)는 해당 블록이 몇 번째 샤드 소속인지, 몇 번째 라운드인지를 나타내는 용도로 사용될 수 있다. 블록 바디(820)에서 트랜잭션(Transactions)(821)은 해당 샤드에서 처리한 트랜잭션의 모음을 나타낸다.

[0090] 한편, (b)의 메인 블록은 각 샤드 블록 데이터를 기반으로 생성된다. 메인 블록은 블록체인 네트워크의 모든 검증 노드가 필수적으로 저장해야 하는 블록으로 기존의 비트코인 블록과는 다른 구조를 갖는다. 기존의 비트코인의 블록구조에 사용되는 Nonce, Difficulty 영역은 자격 증명 기법(PoW)을 사용하기 위한 필드이므로 제거되었다.

[0091] 메인 블록의 블록 헤더(830)에서 라운드 플래그(Round flag)(831)는 해당 블록이 몇 번째 블록인지 나타내는 필드로서 블록 버전, 타임 스탬프(time stamp) 등이 추가될 수 있다. 이전 블록 해시(832)는 이전 블록의 해시값을 나타내며, 머클 루트 해시(833)는 전체 샤드에서 처리된 트랜잭션의 목록에 대한 머클 루트 해시를

나타낸다. 제안자 플래그(Proposer flags)(834)는 블록 제안자의 식별자에 대한 플래그 필드로, 각 샤드의 블록제안자에 대한 주소가 포함된다.

[0092] 한편 블록 바디(840)에는 트랜잭션 필드(841)와 샤드 분산 맵 필드(Shard distribution map)(842)가 포함된다. 트랜잭션 필드(841)는 각 샤드의 트랜잭션 필드(821)의 데이터를 모두 포함하는 필드로써, 전체 네트워크의 트랜잭션에 대한 정보가 포함될 수 있다. 그리고 샤드 분산 맵 필드(842)는 샤드 매니저에 의해 분배된 샤드 분포를 나타내는 필드로, 샤드 번호 확인 및 샤드 분포 위조를 방지하기 위해 사용될 수 있다.

[0093] 도 9는 본 실시예에 따른 신뢰도 기반 샤드 분배 장치 및 방법의 성능을 시뮬레이션한 결과를 나타낸다.

[0094] 도 9에서는 블록체인 네트워크 내의 검증 노드의 개수가 400개이고, 샤드의 개수(K)가 10개이며, 교차 확률(P_c)과 변이 확률(P_m)은 각각 0.8과 0.1 로 설정하였다. 그리고 교차 및 변이에 이용할 부모 염색체의 개수(M)를 50으로 설정하였다.

[0095] 여기서는 성능지표로 정확도(Accuracy, ACC) 및 거짓 합의 확률(False Consensus Probability, FCP)의 두가지를 이용하였다. 정확도는 정상적인 블록을 정상적인 다수의 노드에 의해 유효판정을 받는 경우와, 비정상적인 블록이 정상적인 다수의 노드에 의해 무효합의를 받는 두가지 경우를 계산하였다. 거짓 합의 확률 (FCP)는 정상 블록이 다수의 악성노드에 의해 무효판정을 받거나, 비정상 블록이 다수의 악성 노드들에 의해 유효판정을 받아 체인에 연결되는 경우를 계산하였다.

[0096] 또한 네트워크 공격 유형은 Selective Consensus Attack(SCA)와 Compromised Selective Consensus Attack(CSCA)의 두가지 상황을 가정하였다. SCA에서는 악의적인 노드가 정상블록을 항상 무효로 판정하며, 비정상 블록이 생성되면 정상블록으로 판정한다. 악성 노드는 제안자가 될 경우 항상 잘못된 블록을 생성한다고 가정하였다. 그러나 이 공격에서 악의적인 노드는 합의만 비정상으로 수행하고, 샤드 매니저에게 신뢰 보고행위를 거짓으로 보고하지 않는다. CSCA는 SCA공격유형에 신뢰보고 변조행위를 포함한 공격유형으로, SCA의 공격을 포함하여 신뢰행위를 반대로 보고한다. 예를 들어, 만약 3노드가 제안된 블록에 대해 (Y,Y,N)의 평가를 내린 경우, CSCA 공격자는 샤드 매니저에게 (N,N,Y)로 보고한다. CSCA의 경우 샤드 메니저에게 신뢰보고행위를 거짓 보고하여, 신뢰도 계산에 어려움을 준다.

[0097] 도 9에서 (a)는 세대수 대비 오차(E(RMS error))값이 어떻게 변화하는지 나타낸 결과이다. 세대를 거쳐 신뢰도 RMS 오차값이 낮아져 대략 300세대가 지난 후 오차(E)가 수렴하는 모습을 확인할 수 있었다. 따라서, 본 실시예에서는 라운드별 유전알고리즘의 반복횟수를 300세대로 제한하였다.

[0098] (b)의 경우 라운드에 따른 정확도 성능변화를 기존 샤드 기반 블록체인 기술인 ELASTICO와 비교한 그래프이다. 제안된 알고리즘 TBSD는 악의적인 노드의 비율 30%, 40%에서 모두 ELASTICO보다 높은 합의 정확도정 갖는 것을 알 수 있으며, (b)에서 우측의 오차 경계 또한 훨씬 더 수렴 특성이 높은 것을 알 수 있다. 이는 ELASTICO가 매 라운드마다 랜덤하게 샤드를 결정하는것과 대비하여, 제안된 기술은 신뢰도값을 기반으로 샤드당 신뢰오차를 최소화하기 때문에 훨씬 더 안정된 합의 성공률 특징을 갖음을 보여준다.

[0099] (c)와 (d)는 각 기술의 정확도 및 거짓 합의 확률을 SCA, CSCA 공격 하에서 나타낸 것이다. ELASTICO의 경우 신뢰도 기반 시스템이 아니므로 SCA, CSCA 둘다 동일한 결과를 제공한다. (c)에서 ELASTICO의 경우 악의적 노드 비율(malicious ratio)이 대략 20% 가 넘은 경우부터 합의성공률이 떨어지게 된다. 이는 기존 PBFT 기술이 1/3 미만의 악의적 유저에게 저항성이 있음과 대비되는데, 이는 샤딩의 효과에 의해 특정 샤드에서 블록검증에 필요한 노드들 중 이미 과반수가 악의적 유저에게 점거 당했기 때문에 발생한다. TBSD의 경우 ACC, FCP 모두 ELOASTICO보다 우수하며, CSCA의 경우는 신뢰보고 행위가 포함되어 SCA보다 근소한 차이로 성능하락이 있음을 확인할 수 있다. 이는 신뢰도를 변조하는 CSCA의 경우, 신뢰도 계산부의 신뢰보고 유사도 검사에 의해 거짓보고에 의한 페널티효과에 의해 전반적인 공격효과가 약화되기 때문이다. 전체 네트워크의 악의적인 노드의 비율이 절반을 넘는 상황은 현실적으로 일어나기 힘든 상황이므로, 제안하는 TBSD 기술이 샤드기반 블록체인의 malicious 공격에 대해 더욱 더 높은 합의성공률을 보장한다고 할 수 있다.

[0100] 본 발명에 따른 방법은 컴퓨터에서 실행시키기 위한 매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다. 여기서 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스 될 수 있는 임의의 가용 매체일 수 있고, 또한 컴퓨터 저장 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함하며, ROM(판독 전용 메모리), RAM(랜덤 액세스 메모리), CD(컴팩트 디스크)-ROM, DVD(디

지털 비디오 디스크)-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등을 포함할 수 있다.

[0101] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다.

[0102] 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0103] 110: 통신부 120: 제어부

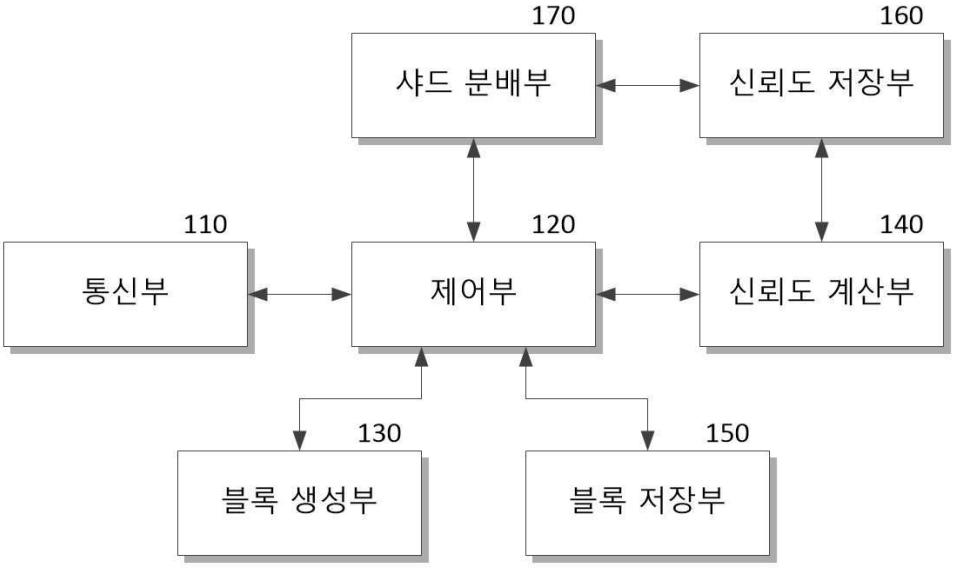
130: 블록 생성부 140: 신뢰도 계산부

150: 블록 저장부 160: 신뢰도 저장부

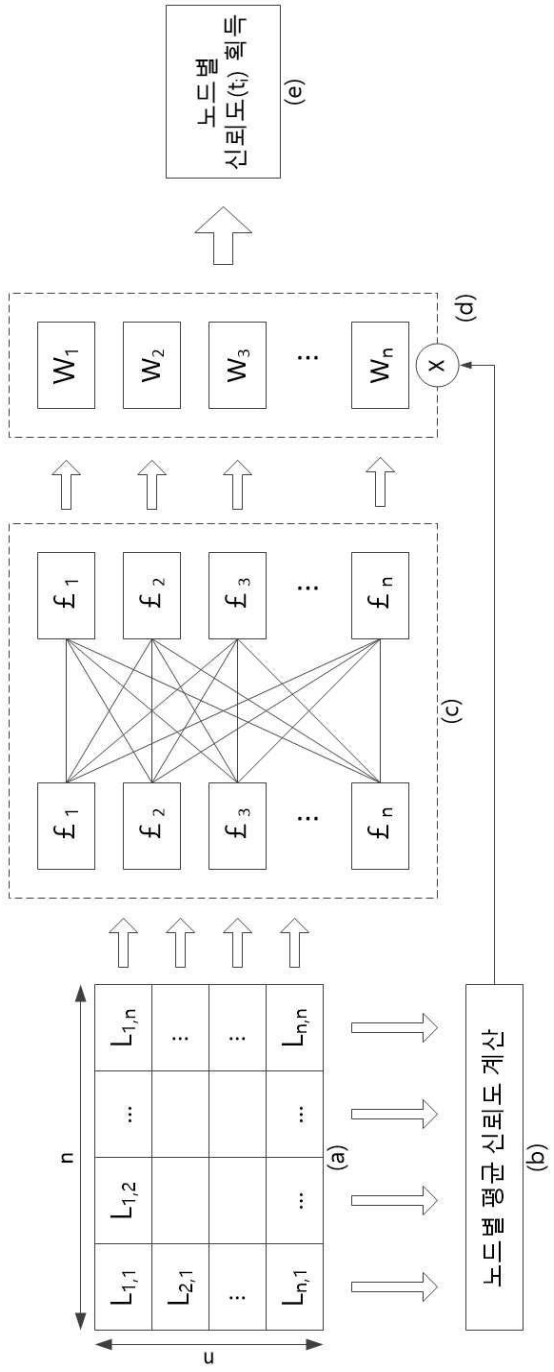
170: 샤드 분배부

도면

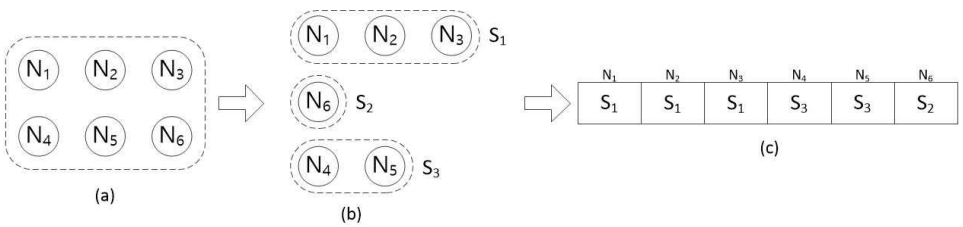
도면1



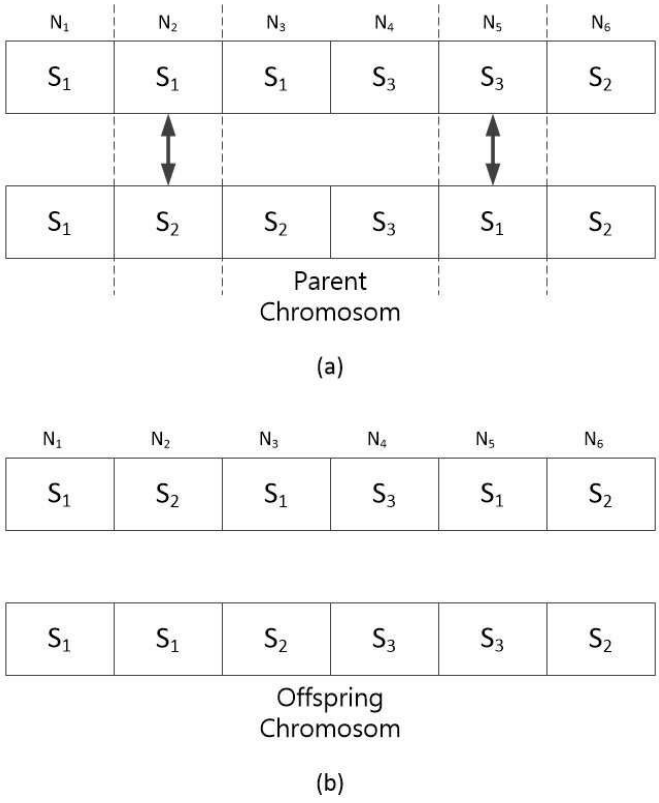
도면2


노드별
신뢰도(ti) 획득
(e)
W1
W2
W3
Wn
(d)
£1
£2
£3
£n
(c)
L1,n
Ln,n
L1,2
L1,1
L2,1
Ln,1
n
u
(a)
노드별 평균 신뢰도 계산
(b)

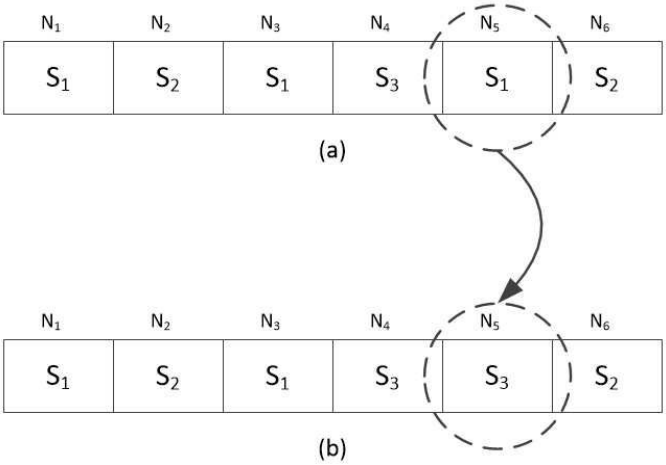
도면3


N1
N2
N3
N4
N5
N6
(a)
S1
S2
S3
(b)
S1
S1
S1
S3
S3
S2
(c)

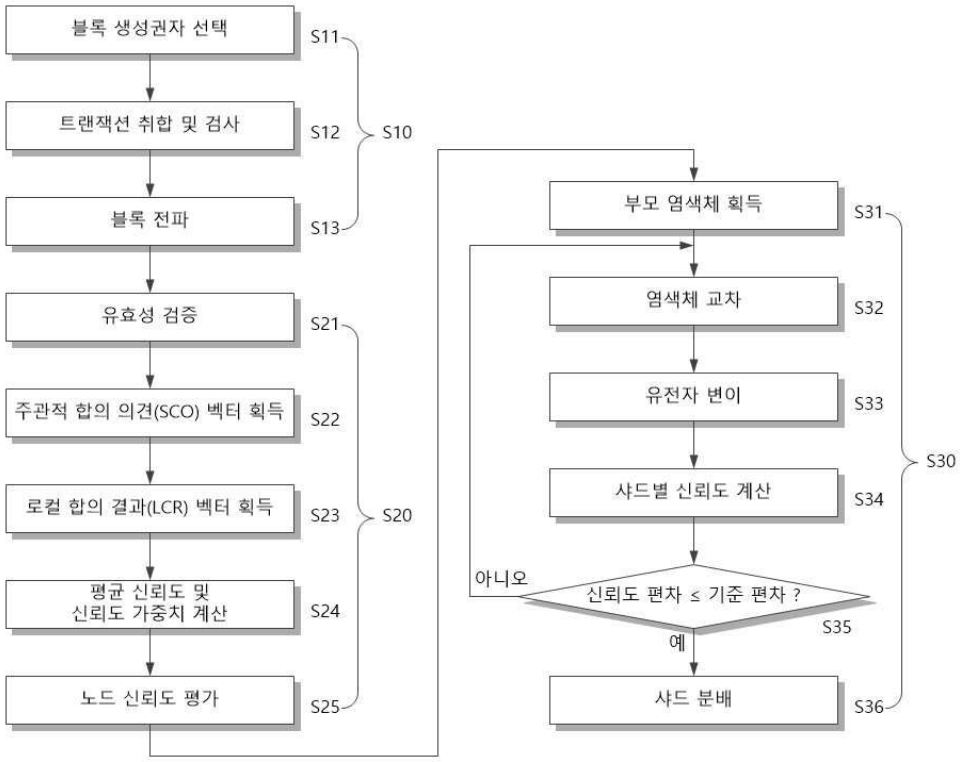
도면4


N1 N2 N3 N4 N5 N6
S1 S1 S1 S3 S3 S2
S1 S2 S2 S3 S1 S2
Parent Chromosom
(a)
N1 N2 N3 N4 N5 N6
S1 S2 S1 S3 S1 S2
S1 S1 S2 S3 S3 S2
Offspring Chromosom
(b)

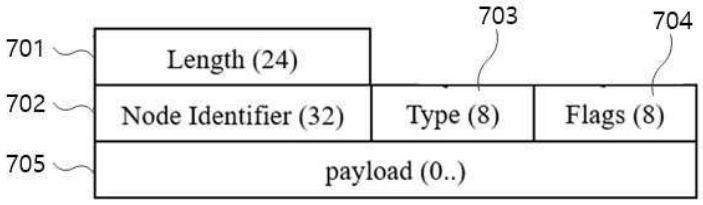
도면5


N1 N2 N3 N4 N5 N6
S1 S2 S1 S3 S1 S2
(a)
N1 N2 N3 N4 N5 N6
S1 S2 S1 S3 S3 S2
(b)

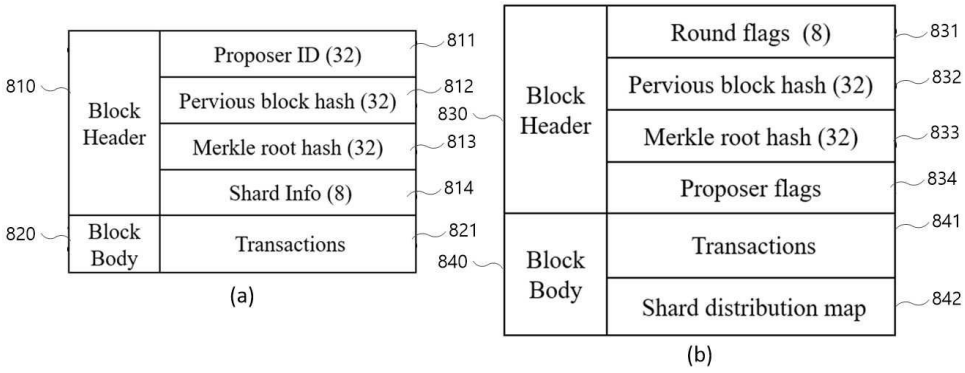
도면6


블록 생성권자 선택
S11
트랜잭션 취합 및 검사
S12
S10
블록 전파
S13
유효성 검증
S21
주관적 합의 의견(SCO) 벡터 획득
S22
로컬 합의 결과(LCR) 벡터 획득
S23
S20
평균 신뢰도 및
신뢰도 가중치 계산
S24
노드 신뢰도 평가
S25
부모 염색체 획득
S31
염색체 교차
S32
유전자 변이
S33
샤드별 신뢰도 계산
S34
S30
아니오
신뢰도 편차 ≤ 기준 편차 ?
S35
예
샤드 분배
S36

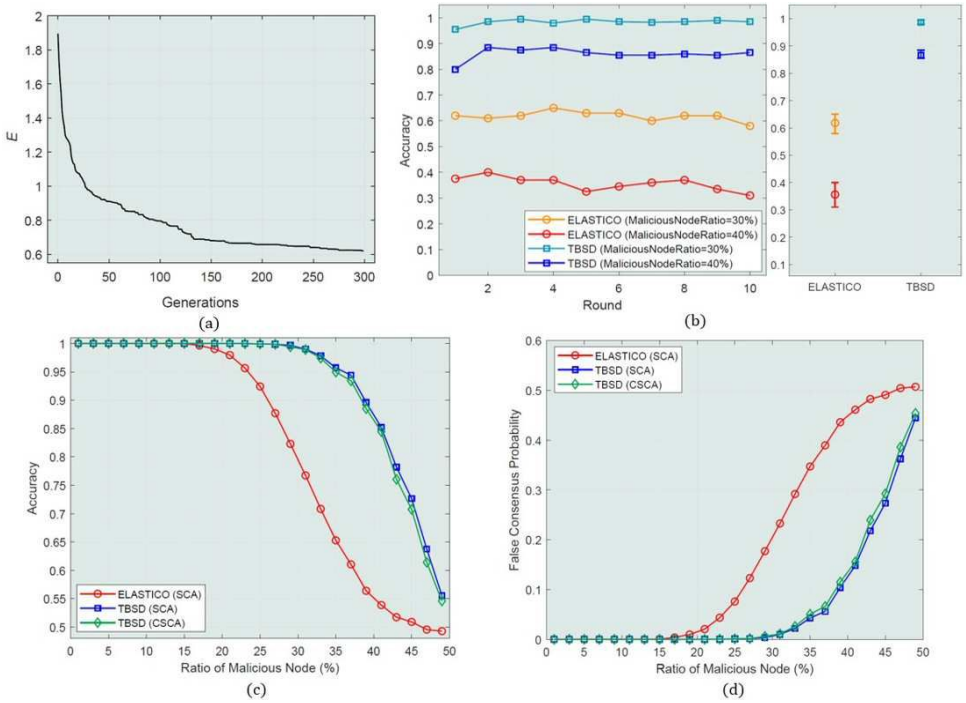
도면7


701
Length (24)
703
704
702
Node Identifier (32)
Type (8)
Flags (8)
705
payload (0..)

도면8


810
Block Header
Proposer ID (32)
811
Pervious block hash (32)
812
Merkle root hash (32)
813
Shard Info (8)
814
820
Block Body
Transactions
821
(a)
830
Block Header
Round flags (8)
831
Pervious block hash (32)
832
Merkle root hash (32)
833
Proposer flags
834
840
Block Body
Transactions
841
Shard distribution map
842
(b)

도면9



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 14

【변경전】

제7 항에 따른 샤드 분배 방법을 수행하기 위한 프로그램 명령어가 기록된 기록매체.

【변경후】

제7 항에 따른 샤드 분배 방법을 수행시키기 위한 프로그램 명령어가 기록된 컴퓨터로 읽을 수 있는 기록매체.