(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0100733
(43) 공개일자 2019년08월29일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 40/00* (2006.01)
H04L 29/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
G06Q 20/3827 (2013.01)
G06Q 40/00 (2013.01)
(21) 출원번호 10-2018-0020661
(22) 출원일자 2018년02월21일
심사청구일자 2018년02월21일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호 (더샵센트럴파크2단지아파트)
채기준
서울특별시 강남구 강남대로136길 34, 402호(논현동,월드노블레스빌)
전솔
경기도 시흥시 미산로100번길 11, 101동 1705호(미산동해가든더클래식아파트)
(74) 대리인
윤귀상

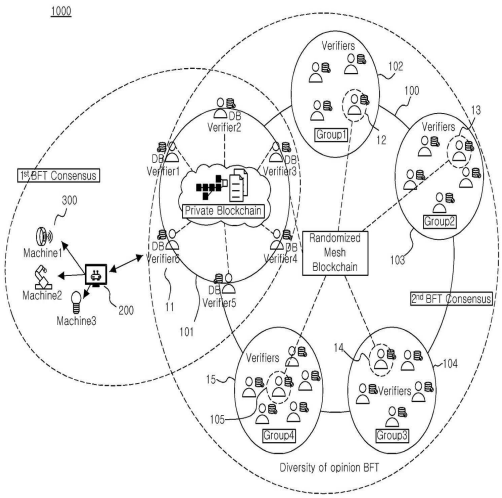
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **그룹기반의 랜덤화 된 메시 블록체인 시스템 및 이의 무결성 확인 방법**

(57) 요 약

그룹기반의 랜덤화 된 메시 블록체인 시스템 및 그의 무결성 확인 방법이 개시된다. 그룹기반의 랜덤화 된 메시 블록체인 시스템은 복수의 검증자로 구성되며, 트랜잭션을 요청 받는 경우, 상기 복수의 검증자를 그룹화하여 상기 트랜잭션을 요청한 사용자가 속하는 그룹에서 제1 합의 알고리즘을 진행하고, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하는 블록체인 및 상기 트랜잭션의 실행을 관리하는 스마트 매니저를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 67/1044 (2013.01)
H04L 9/321 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2016R1A2B4015899
부처명 과학기술정보통신부
연구관리전문기관 한국연구재단
연구사업명 기초연구사업(학술진흥)-중견연구자지원사업
연구과제명 CPS환경에서의 신뢰성있는 서비스 제공을 위한 보안기법 및 공격 대응 방안
기 여 율 1/1
주관기관 이화여자대학교 산학협력단
연구기간 2016.06.01 ~ 2019.05.31

명 세 서

청구범위

청구항 1

복수의 검증자로 구성되며, 트랜잭션을 요청 받는 경우, 상기 복수의 검증자를 그룹화하여 상기 트랜잭션을 요청한 사용자가 속하는 그룹에서 제1 합의 알고리즘을 진행하고, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하는 블록체인; 및

상기 트랜잭션의 실행을 관리하는 스마트 매니저를 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템.

청구항 2

제1항에 있어서,

상기 블록체인은,

BFT(Byzantine Fault Tolerance) 합의 알고리즘인 상기 제1 합의 알고리즘 및 상기 제2 알고리즘을 진행하는 그룹기반의 랜덤화 된 메시 블록체인 시스템.

청구항 3

제1항에 있어서,

상기 블록체인은,

상기 제2 합의 알고리즘 진행 시, 각 그룹에 속하는 검증자의 수에 비례하여 각 그룹에서 적어도 하나의 검증자를 랜덤으로 선출하는 그룹기반의 랜덤화 된 메시 블록체인 시스템.

청구항 4

제1항에 있어서,

상기 블록체인은,

상기 복수의 검증자 각각의 관련 분야에 따라 상기 복수의 검증자를 그룹화하는 그룹기반의 랜덤화 된 메시 블록체인 시스템.

청구항 5

제1항에 있어서,

상기 스마트 매니저는,

상기 블록체인에서 상기 트랜잭션에 대한 합의가 완료되면, 상기 트랜잭션이 스마트 컨트랙트(Smart Contract)를 만족하는지 여부를 검증하는 것을 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템.

청구항 6

제5항에 있어서,

상기 스마트 매니저는,

상기 스마트 컨트랙트에 따라 실행되는 디바이스가 승인된 디바이스인지를 확인하고, 상기 디바이스가 승인된 디바이스로 확인되면, 상기 디바이스로 상기 스마트 컨트랙트에 따른 제어를 요청하는 것을 더 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템.

청구항 7

복수의 검증자로 구성되어 트랜잭션에 대한 합의를 수행하는 블록체인 및 상기 트랜잭션의 실행을 관리하는 스

마트 매니저를 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법에 있어서,

상기 블록체인에서 상기 복수의 검증자를 그룹화하여 상기 트랜잭션을 요청한 사용자가 속하는 그룹에서 제1 합의 알고리즘을 진행하고, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하며,

상기 제1 합의 알고리즘 및 상기 제2 합의 알고리즘에 따라 상기 트랜잭션에 대한 합의가 완료되면, 상기 스마트 매니저에서 상기 트랜잭션의 무결성을 확인하여 상기 트랜잭션이 실행되도록 제어하는 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법.

청구항 8

제7항에 있어서,

상기 블록체인에서 상기 복수의 검증자를 그룹화하여 상기 트랜잭션을 요청한 사용자가 속하는 그룹에서 제1 합의 알고리즘을 진행하고, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하는 것은,

BFT(Byzantine Fault Tolerance) 합의 알고리즘인 상기 제1 합의 알고리즘 및 상기 제2 알고리즘을 진행하는 것인 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법.

청구항 9

제7항에 있어서,

상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하는 것은,

각 그룹에 속하는 검증자의 수에 비례하여 각 그룹에서 적어도 하나의 검증자를 랜덤으로 선출하는 것을 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법.

청구항 10

제7항에 있어서,

상기 복수의 검증자를 그룹화하는 것은,

상기 복수의 검증자 각각의 관련 분야에 따라 상기 복수의 검증자를 그룹화하는 것인 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법.

청구항 11

제7항에 있어서,

상기 스마트 매니저에서 상기 트랜잭션의 무결성을 확인하여 상기 트랜잭션이 실행되도록 제어하는 것은,

상기 트랜잭션이 스마트 컨트랙트(Smart Contract)를 만족하는지 여부를 검증하는 것을 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법.

청구항 12

제11항에 있어서,

상기 스마트 매니저에서 상기 트랜잭션의 무결성을 확인하여 상기 트랜잭션이 실행되도록 제어하는 것은,

상기 스마트 컨트랙트에 따라 실행되는 디바이스가 승인된 디바이스인지를 확인하고, 상기 디바이스가 승인된 디바이스로 확인되면, 상기 디바이스로 상기 스마트 컨트랙트에 따른 제어를 요청하는 것을 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 그룹기반의 랜덤화 된 메시 블록체인 시스템 및 이의 무결성 확인 방법에 관한 것으로서, 더욱 상세하게는 BFT(Byzantine Fault Tolerance) 합의 알고리즘을 적용한 그룹기반의 랜덤화 된 메시 블록체인 시스템 및 이의 무결성 확인 방법에 관한 것이다.

배 경 기 술

[0002] 최근 블록체인 기술이 다양한 분야에 적용되고 있다. 블록체인은 공공 블록체인 및 프라이빗 블록체인으로 나뉠 수 있다.

[0003] 공공 블록체인은 누구나 네트워크에 참여 가능하고 트랜잭션을 생성할 수 있다. 공공 블록체인에서 생성되는 트랜잭션의 합의 알고리즘으로는 PoW(Proof of Work) 알고리즘이 널리 사용되고 있다.

[0004] 프라이빗 블록체인은 인증된 사용자만이 네트워크에 참여할 수 있으며, 트랜잭션 생성 또한 마찬가지이다. 프라이빗 블록체인에서 생성되는 트랜잭션은 네트워크 참여자의 과반 이상이 합의하면 승인될 수 있는데 이를 위한 합의 알고리즘으로는 BFT(Byzantine Fault Tolerance) 알고리즘이 적용될 수 있다.

[0005] 한편, 프라이빗 블록체인 네트워크 참여자 수가 제한되므로, 악의적인 사용자가 과반 이상인 경우 트랜잭션에 대한 올바른 합의를 도출할 수 없다. 아울러, 프라이빗 블록체인은 기업 내의 소규모의 그룹으로 구성되는 경우가 대부분인데, 이에 따라 사용자들 간에 악의적인 담합이 존재할 가능성이 매우 높다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 일측면은 트랜잭션을 요청한 사용자가 속하는 그룹에서 제1 합의 알고리즘을 진행하고, 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 랜덤으로 선출한 검증자에 의해 제2 합의 알고리즘을 진행하는 블록체인 및 트랜잭션의 실행을 관리하는 스마트 매니저를 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템 및 이의 무결성 확인 방법을 제공한다.

[0007] 본 발명의 다른 측면은 블록체인에서 트랜잭션에 대한 이중 합의를 진행하고, 스마트 매니저에서 스마트 컨트랙트에 기반하여 트랜잭션 합의에 대해 검증하는 그룹기반의 랜덤화 된 메시 블록체인 시스템 및 이의 무결성 확인 방법을 제공한다.

과제의 해결 수단

[0008] 상기 과제를 해결하기 위한 본 발명의 일 측면에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템은 복수의 검증자로 구성되며, 트랜잭션을 요청 받는 경우, 상기 복수의 검증자를 그룹화하여 상기 트랜잭션을 요청한 사용자가 속하는 그룹에서 제1 합의 알고리즘을 진행하고, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하는 블록체인 및 상기 트랜잭션의 실행을 관리하는 스마트 매니저를 포함한다.

[0009] 한편, 상기 블록체인은, BFT(Byzantine Fault Tolerance) 합의 알고리즘인 상기 제1 합의 알고리즘 및 상기 제2 알고리즘을 진행할 수 있다.

[0010] 또한, 상기 블록체인은, 상기 제2 합의 알고리즘 진행 시, 각 그룹에 속하는 검증자의 수에 비례하여 각 그룹에서 적어도 하나의 검증자를 랜덤으로 선출할 수 있다.

[0011] 또한, 상기 블록체인은, 상기 복수의 검증자 각각의 관련 분야에 따라 상기 복수의 검증자를 그룹화할 수 있다.

[0012] 또한, 상기 스마트 매니저는, 상기 블록체인에서 상기 트랜잭션에 대한 합의가 완료되면, 상기 트랜잭션이 스마트 컨트랙트(Smart Contract)를 만족하는지 여부를 검증하는 것을 포함할 수 있다.

[0013] 또한, 상기 스마트 매니저는, 상기 스마트 컨트랙트에 따라 실행되는 디바이스가 승인된 디바이스인지를 확인하고, 상기 디바이스가 승인된 디바이스로 확인되면, 상기 디바이스로 상기 스마트 컨트랙트에 따른 제어를 요청하는 것을 더 포함할 수 있다.

[0014] 한편, 본 발명의 다른 측면은 복수의 검증자로 구성되어 트랜잭션에 대한 합의를 수행하는 블록체인 및 상기 트랜잭션의 실행을 관리하는 스마트 매니저를 포함하는 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법에 있어서, 상기 블록체인에서 상기 복수의 검증자를 그룹화하여 상기 트랜잭션을 요청한 사용자가 속하

는 그룹에서 제1 합의 알고리즘을 진행하고, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하며, 상기 제1 합의 알고리즘 및 상기 제2 합의 알고리즘에 따라 상기 트랜잭션에 대한 합의가 완료되면, 상기 스마트 매니저에서 상기 트랜잭션의 무결성을 확인하여 상기 트랜잭션이 실행되도록 제어한다.

[0015] 한편, 상기 블록체인에서 상기 복수의 검증자를 그룹화하여 상기 트랜잭션을 요청한 사용자가 속하는 그룹에서 제1 합의 알고리즘을 진행하고, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하는 것은, BFT(Byzantine Fault Tolerance) 합의 알고리즘인 상기 제1 합의 알고리즘 및 상기 제2 알고리즘을 진행하는 것일 수 있다.

[0016] 또한, 상기 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하여 제2 합의 알고리즘을 진행하는 것은, 각 그룹에 속하는 검증자의 수에 비례하여 각 그룹에서 적어도 하나의 검증자를 랜덤으로 선출하는 것을 포함할 수 있다.

[0017] 또한, 상기 복수의 검증자를 그룹화하는 것은, 상기 복수의 검증자 각각의 관련 분야에 따라 상기 복수의 검증자를 그룹화하는 것일 수 있다.

[0018] 또한, 상기 스마트 매니저에서 상기 트랜잭션의 무결성을 확인하여 상기 트랜잭션이 실행되도록 제어하는 것은, 상기 트랜잭션이 스마트 컨트랙트(Smart Contract)를 만족하는지 여부를 검증하는 것을 포함할 수 있다.

[0019] 또한, 상기 스마트 매니저에서 상기 트랜잭션의 무결성을 확인하여 상기 트랜잭션이 실행되도록 제어하는 것은, 상기 스마트 컨트랙트에 따라 실행되는 디바이스가 승인된 디바이스인지를 확인하고, 상기 디바이스가 승인된 디바이스로 확인되면, 상기 디바이스로 상기 스마트 컨트랙트에 따른 제어를 요청하는 것을 포함할 수 있다.

발명의 효과

[0020] 본 발명에 따르면, 트랜잭션을 요청한 사용자가 속한 그룹을 제외한 나머지 그룹에서 합의 알고리즘을 진행할 검증자를 랜덤으로 선출함으로써, 검증자 수가 제한되는 프라이빗 블록체인에 있어서 검증자의 담합으로 잘못된 트랜잭션 합의가 도출될 가능성을 낮출 수 있다. 또한, 제3자의 입장에서의 객관적인 합의 결과를 기대할 수 있으며, 실제 합의에 참여하는 검증자는 소수로 선출되므로 그 속도가 느려지는 것을 방지할 수 있다.

[0021] 또한, 블록체인에서 수행되어야 하는 트랜잭션 합의에 대한 검증 부분을 스마트 매니저에서 담당함으로써 그 과정에서 발생하는 비용을 없애고 블록체인의 오버헤드를 감소시킬 수 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 개념도이다.

도 2는 도 1에 도시된 블록체인에서 진행하는 트랜잭션 합의 알고리즘을 설명하기 위한 도면이다.

도 3은 도 1에 도시된 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법의 순서도이다.

도 4는 종래의 한 차례의 BFT 합의 알고리즘에 따른 악의적 담합 가능성과, 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법에 따른 악의적 담합 가능성을 산출하여 비교한 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0023] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0024] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0025] 도 1은 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 개념도이고, 도 2는 도 1에 도시된 블록체인에서 진행하는 트랜잭션 합의 알고리즘을 설명하기 위한 도면이다.

[0026] 도 1을 참조하면, 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템(1000)은 복수의 검증자(Verifier)(10)가 참여하여 트랜잭션(transaction)을 합의 및 기록하는 블록체인(100) 및 블록체인(100)에서의 트랜잭션 합의를 검증하여 디바이스(300)로 트랜잭션 실행을 요청하는 스마트 매니저(200)를 포함할 수 있다.

[0027] 블록체인(100)은 일반적인 블록체인 네트워크로, 일정 시간(일예로, 10분)동안 발생하는 트랜잭션을 모아 블록(block)을 생성하고, 트랜잭션에 대한 합의를 진행한 뒤 그 결과에 따라 트랜잭션이 포함되는 블록을 기존에 생성된 블록과 연결하여 트랜잭션을 기록할 수 있다.

[0028] 블록체인(100)은 중앙 관리자에 의해 검증된 검증자(10)로만 구성되는 프라이빗 블록체인 네트워크를 구축할 수 있다. 중앙 관리자에 의해 사전에 검증된 검증자(10)는 자신의 데이터베이스에 기초하여 블록체인(100)에 참여를 요청할 수 있다.

[0029] 블록체인(100)은 트랜잭션 발생 시 복수의 검증자(10)에 의하여 트랜잭션의 허용에 대한 합의를 수행할 수 있다. 블록체인(100)은 BFT(Byzantine Fault Tolerance) 합의 알고리즘을 진행하여 트랜잭션의 허용에 대한 합의를 수행할 수 있다. BFT 합의 알고리즘에 대해 간략히 설명하면, 블록체인 네트워크에 참여하는 과반 이상의 사용자가 트랜잭션을 합의하면 해당 트랜잭션을 허용하는 합의 알고리즘이다. BFT 합의 알고리즘은 사용자 수가 제한되는 프라이빗 블록체인 네트워크에 적용 시, 과반 이상의 사용자가 악의적 사용자로 변질되어 담합하는 경우 트랜잭션에 대한 잘못된 합의가 이루어질 수 있다. 이러한 문제점을 해결하기 위해 블록체인(100)은 두 차례의 BFT 합의 알고리즘을 진행할 수 있다. 이와 관련하여 도 2를 참조하여 구체적으로 설명하기로 한다.

[0030] 도 2를 참조하면, 블록체인(100)은 복수의 검증자를 그룹화할 수 있다. 블록체인(100)은 복수의 검증자 각각의 관련 분야에 따라 제1 그룹(101) 내지 제5 그룹(105)으로 그룹화할 수 있다.

[0031] 블록체인(100)은 트랜잭션을 요청한 사용자(11)가 속하는 그룹에서 제1 합의 알고리즘을 진행할 수 있다. 제1 합의 알고리즘은 BFT 합의 알고리즘일 수 있다. 블록체인(100)은 프라이빗 블록체인 네트워크이므로, 트랜잭션을 요청한 사용자(11)는 블록체인(100)을 구성하는 복수의 검증자 중 하나일 수 있다.

[0032] 예를 들면, 블록체인(100)은 트랜잭션을 요청한 사용자(11)가 속하는 그룹인 제1 그룹(101)에서 BFT 합의 알고리즘을 진행할 수 있다. 블록체인(100)은 제1 그룹(101)에 속하는 과반 이상의 검증자가 트랜잭션을 합의하면 제1 합의 알고리즘 진행 결과를 허용으로 도출할 수 있다.

[0033] 블록체인(100)은 제1 합의 알고리즘 진행 결과가 트랜잭션 허용이면, 제2 합의 알고리즘을 진행할 수 있다. 그 반대의 경우 블록체인(100)은 트랜잭션을 거절할 수 있다.

[0034] 블록체인(100)은 트랜잭션을 요청한 사용자(11)가 속하는 그룹을 제외한 나머지 그룹에서 각각 적어도 하나의 검증자를 랜덤으로 선출하고, 선출된 검증자에 의한 제2 합의 알고리즘을 진행할 수 있다. 제2 합의 알고리즘은 BFT 합의 알고리즘일 수 있다. 블록체인(100)은 제2 합의 알고리즘에 참여하는 검증자를 사용자(11)가 속하는 그룹을 제외한 나머지 그룹에서 랜덤으로 선출함으로써 제3자의 입장에서의 객관적인 합의 결과를 기대할 수 있다. 또한, 제2 합의 알고리즘은 랜덤으로 소수의 검증자를 선출하고, 선출된 검증자에 의해 진행됨으로써, 그 속도가 느려지는 것을 방지할 수 있다.

[0035] 예를 들면, 블록체인(100)은 트랜잭션을 요청한 사용자(11)가 속하는 제1 그룹(101)을 제외한 나머지 그룹인 제2 그룹(102) 내지 제5 그룹(105)에서 각각 적어도 하나의 검증자(12, 13, 14, 15)를 랜덤으로 선출하고, 선출된 검증자(12, 13, 14, 15)에 의한 BFT 합의 알고리즘을 진행할 수 있다. 블록체인(100)은 랜덤으로 선출된 검증자(12, 13, 14, 15) 중 과반 이상의 검증자가 트랜잭션을 합의하면 제2 합의 알고리즘 진행 결과를 허용으로 도출할 수 있다.

[0036] 한편, 블록체인(100)은 각 그룹에서 제2 합의 알고리즘에 참여할 검증자를 랜덤으로 선출 시, 각 그룹에 속하는 전체 검증자의 수에 비례하여 각 그룹에서 적어도 하나의 검증자를 랜덤으로 선출할 수 있다.

[0037] 예를 들면, 블록체인(100)은 그룹에 속하는 전체 검증자(10) 수의 50%의 검증자를 랜덤으로 선출하는 경우, 제2 그룹(102)에서는 전체 검증자(10) 수 '4'에 비례하여 2 명의 검증자를 랜덤으로 선출하고, 나머지 그룹 또한 각 그룹의 전체 검증자(10) 수의 50%의 검증자를 랜덤으로 선출할 수 있다.

[0038] 블록체인(100)은 이와 같이 트랜잭션에 대하여 해당 트랜잭션을 요청한 사용자가 속한 그룹의 검증자들 및 그 외의 그룹에서 랜덤으로 선출한 검증자들에 의한 두 차례의 BFT 합의 알고리즘을 수행할 수 있다. 본 실시예에서 이러한 합의 알고리즘을 DBFT(Diversity of opinion Byzantine Fault Tolerance) 합의 알고리즘이라 정의하기로 한다. 블록체인(100)은 DBFT 합의 알고리즘을 진행함으로써 검증자의 수가 제한됨에도 불구하고 검증자의 담합으로 잘못된 트랜잭션 합의가 도출될 가능성을 낮출 수 있다.

[0039] 블록체인(100)은 DBFT 합의 알고리즘에 따라 트랜잭션에 대한 합의를 완료하면, 해당 트랜잭션을 포함하는 블록을 기존에 생성된 블록과 연결하여 트랜잭션을 기록할 수 있으며, 블록 업데이트 사실을 복수의 검증자에게 알릴 수 있다.

[0040] 한편, 스마트 매니저(200)는 블록체인(100)에서 합의가 완료된 트랜잭션에 대하여 무결성을 확인하고, 트랜잭션이 실행되도록 디바이스(300)에 제어 명령을 전달할 수 있다.

[0041] 구체적으로는, 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템(1000)에는 공지된 기술인 스마트 컨트랙트(Smart Contract)가 적용될 수 있다. 스마트 컨트랙트에 대하여 간략히 설명하면, 특정 액션의 실행에 대한 규칙이 명시된 컨트랙트라 할 수 있다. 이러한 스마트 컨트랙트에 명시된 액션은 디바이스(300)에서 실행될 수 있다. 디바이스(300)는 IoT 디바이스, 저전력 디바이스, 저용량 디바이스, 간단한 기능을 수행하는 저장 공간을 갖는 디바이스 등을 의미한다.

[0042] 스마트 매니저(200)는 블록체인(100)에서 합의가 완료된 트랜잭션이 스마트 컨트랙트를 만족하는지 여부를 검증할 수 있다. 이로부터 스마트 매니저(200)는 안전한 트랜잭션을 가능하게 하고 데이터의 무결성을 보장할 수 있다.

[0043] 스마트 매니저(200)는 스마트 컨트랙트에 따라 실행되는 디바이스(300)가 관리자에 의해 사전에 승인된 디바이스(300)인지를 확인할 수 있다. 스마트 매니저(200)는 블록체인(100)에서 합의가 완료된 트랜잭션이 스마트 컨트랙트를 만족하고, 디바이스(300)의 승인을 확인하면, 스마트 컨트랙트에 따른 제어를 디바이스(300)로 요청할 수 있다.

[0044] 스마트 매니저(200)는 이와 같이 블록체인(100)에서 수행되어야 하는 트랜잭션 합의에 대한 검증 부분을 담당함으로써 그 과정에서 발생하는 보상을 없애고 블록체인(100)의 오버헤드를 감소시킬 수 있다.

[0045] 이하에서는, 도 3을 참조하여, 도 1에 도시된 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법에 대하여 설명하기로 한다.

[0046] 도 3은 도 1에 도시된 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법의 순서도이다.

[0047] 도 3을 참조하면, 사용자에 의해 스마트 컨트랙트가 생성되면(500), 블록체인(100)은 트랜잭션을 복수의 검증자로 전파하고, 블록을 생성할 수 있다(510). 사용자는 스마트 컨트랙트를 생성하면, 그룹기반의 랜덤화 된 메시 블록체인 시스템(1000)으로 스마트 컨트랙트에 대한 합의 진행을 요청할 수 있다. 블록체인(100)은 이에 대응하여 트랜잭션을 복수의 검증자로 전파하고, 미리 정해진 시간동안 발생하는 트랜잭션을 모아 블록을 생성할 수 있다.

[0048] 블록체인(100)은 트랜잭션에 대한 제1 합의 알고리즘을 진행할 수 있다(520). 블록체인(100)은 블록체인(100)에 참여하는 복수의 검증자를 그룹화하여, 트랜잭션을 요청한 사용자가 속하는 그룹에서 BFT 합의 알고리즘을 진행할 수 있다.

[0049] 블록체인(100)은 트랜잭션에 대한 제1 합의 알고리즘 진행 결과, 트랜잭션이 합의되면(530), 제2 합의 알고리즘을 진행할 수 있다(540). 블록체인(100)은 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 나머지 그룹에서 적어도 하나의 검증자를 랜덤으로 선출할 수 있다. 블록체인(100)은 각 그룹에 속하는 검증자의 수에 비례하여 각 그룹에서 적어도 하나의 검증자를 랜덤으로 선출할 수 있다. 블록체인(100)은 선출된 검증자에 의한 BFT 합의 알고리즘을 진행할 수 있다.

[0050] 블록체인(100)에서의 트랜잭션에 대한 제2 합의 알고리즘 진행 결과, 트랜잭션이 합의되면(550), 스마트 매니저(200)는 트랜잭션이 스마트 컨트랙트를 만족하는지를 검증하고(560), 스마트 컨트랙트에 따라 실행되는 디바이스(300)가 인증된 디바이스(300)인지를 확인할 수 있다(570).

[0051] 스마트 매니저(200)는 트랜잭션이 스마트 컨트랙트를 만족하고(560), 디바이스(300)가 인증된 디바이스(300)이면(570), 해당 디바이스(300)로 스마트 컨트랙트에 따른 제어를 요청할 수 있다(580).

[0052] 블록체인(100)은 생성한 블록을 연결하고, 블록 업데이트 결과를 복수의 검증자로 전파할 수 있다(590).

[0053] 이하에서는, 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법의 유리한 효과에 대하여 설명한다.

[0054] 도 4는 종래의 한 차례의 BFT 합의 알고리즘에 따른 악의적 담합 가능성과, 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법에 따른 악의적 담합 가능성을 산출하여 비교한 그래프이다.

[0055] 종래의 방식에 따르면, 트랜잭션 합의를 위해 한 차례의 BFT 합의 알고리즘을 진행할 수 있다. 그러나, 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템(1000)에서는 트랜잭션을 요청한 사용자가 속하는 그룹에서 1차 BFT 합의 알고리즘을 진행하고, 그 외의 그룹에서 검증자를 랜덤으로 선출하여 2차 BFT 합의 알고리즘을 진행할 수 있다.

[0056] 도 4를 참조하면, 종래의 한 차례의 BFT 합의 알고리즘에 따른 악의적 담합 방지 가능성에 비해 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법에 따른 악의적 담합 가능성이 현저히 낮음을 확인할 수 있다. 악의적 담합 가능성은 아래의 수학식 1로부터 산출될 수 있다.

수학식 1

[0057]
$$P_{a_i}(\%) = \frac{degree\ of\ closeness((R_{IE_i} \times R_{p_i} \times R_{ac_i})/node_{c_i})}{\sum_{i=1}^{n}((R_{IE_i} \times R_{p_i} \times R_{ac_i})/node_{c_i})} \times 100$$

[0058] 수학식 1의 각 파라미터는 아래의 표 1과 같이 정의될 수 있다.

표 1

[0059]

R_{IE_i}	R_{p_i}	R_{ac_i}
Relation (Internal/External)	*Relation (Position)*	*Relation (acquaintance)*
Level 1-10	*Level1-10*	*Level1-10*

[0060] 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법에 따르면, 제2 합의 알고리즘 진행을 위해 선출되는 검증자는 트랜잭션을 요청한 사용자가 속하는 그룹을 제외한 그룹에서 랜덤으로 선출되므로, 트랜잭션을 요청한 사용자와의 관련도가 낮아 제3자 입장에서의 객관적인 판단이 가능하다. 따라서, 본 발명의 일 실시예에 따른 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법은 트랜잭션 합의 검증에 필요한 별도의 비용 지불이 요구되지 않음에도 불구하고, 낮은 담합 가능성을 갖는다.

[0061] 이와 같은, 그룹기반의 랜덤화 된 메시 블록체인 시스템의 무결성 확인 방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0062] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0063] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical

media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0064] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0065] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0066] 1000: 그룹기반의 랜덤화 된 메시 블록체인 시스템

10: 검증자

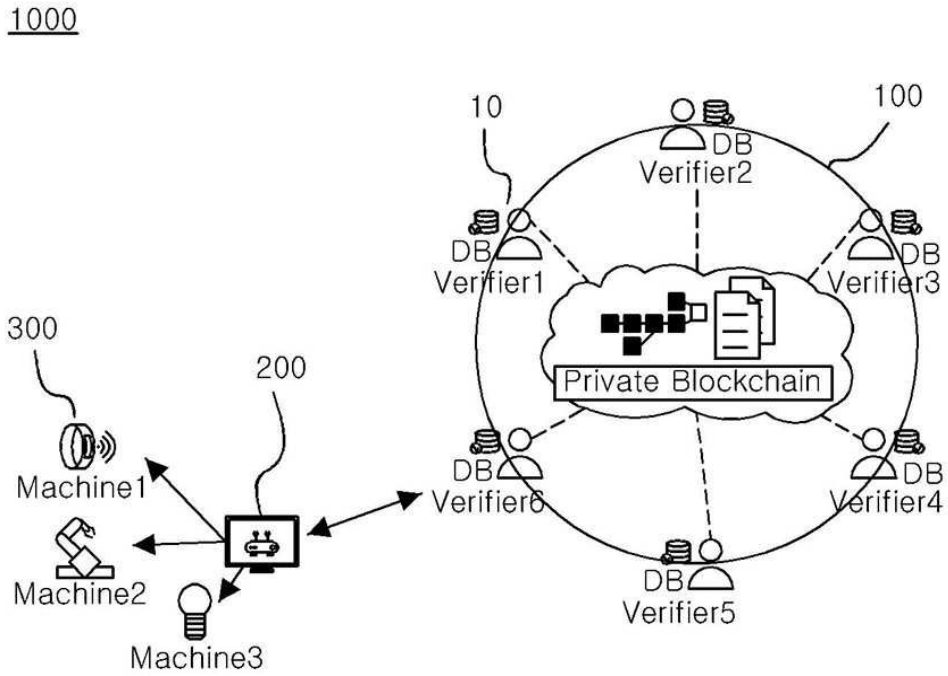
100: 블록체인

200: 스마트 매니저

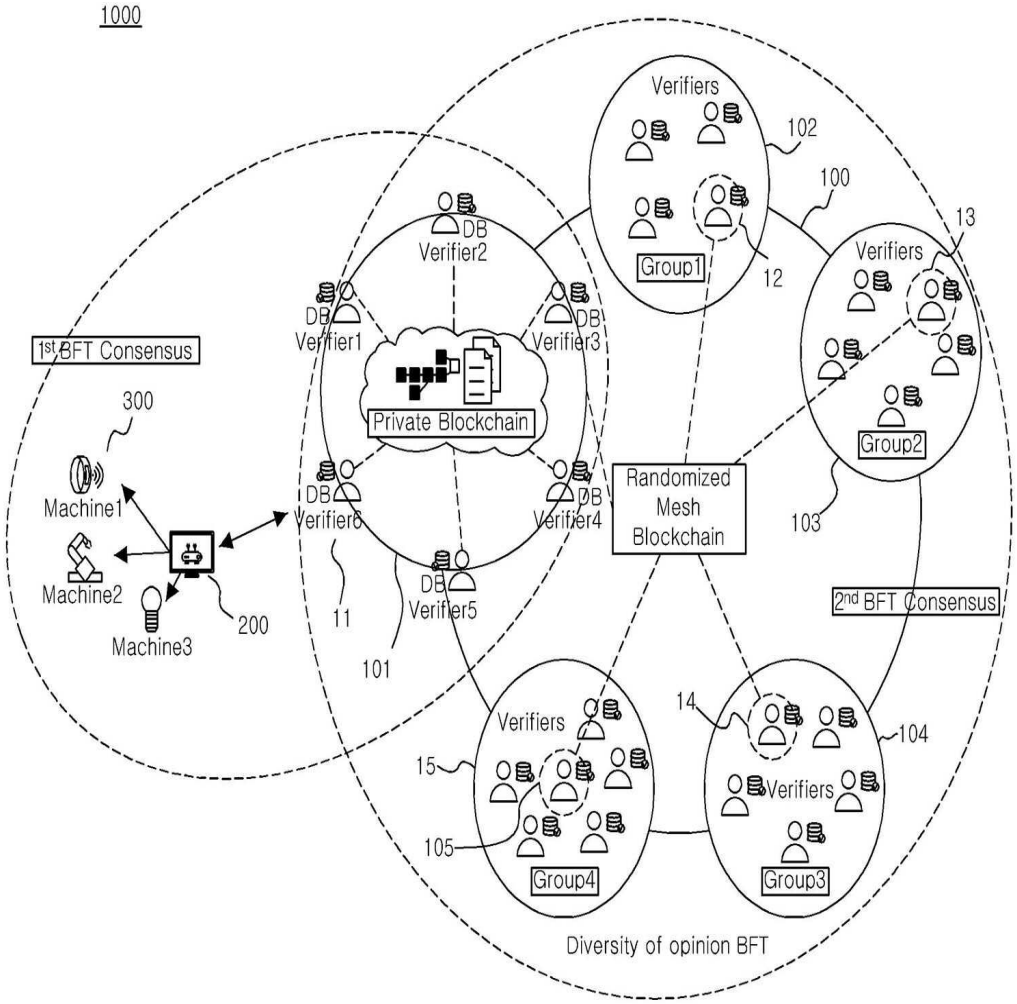
300: 디바이스

도면

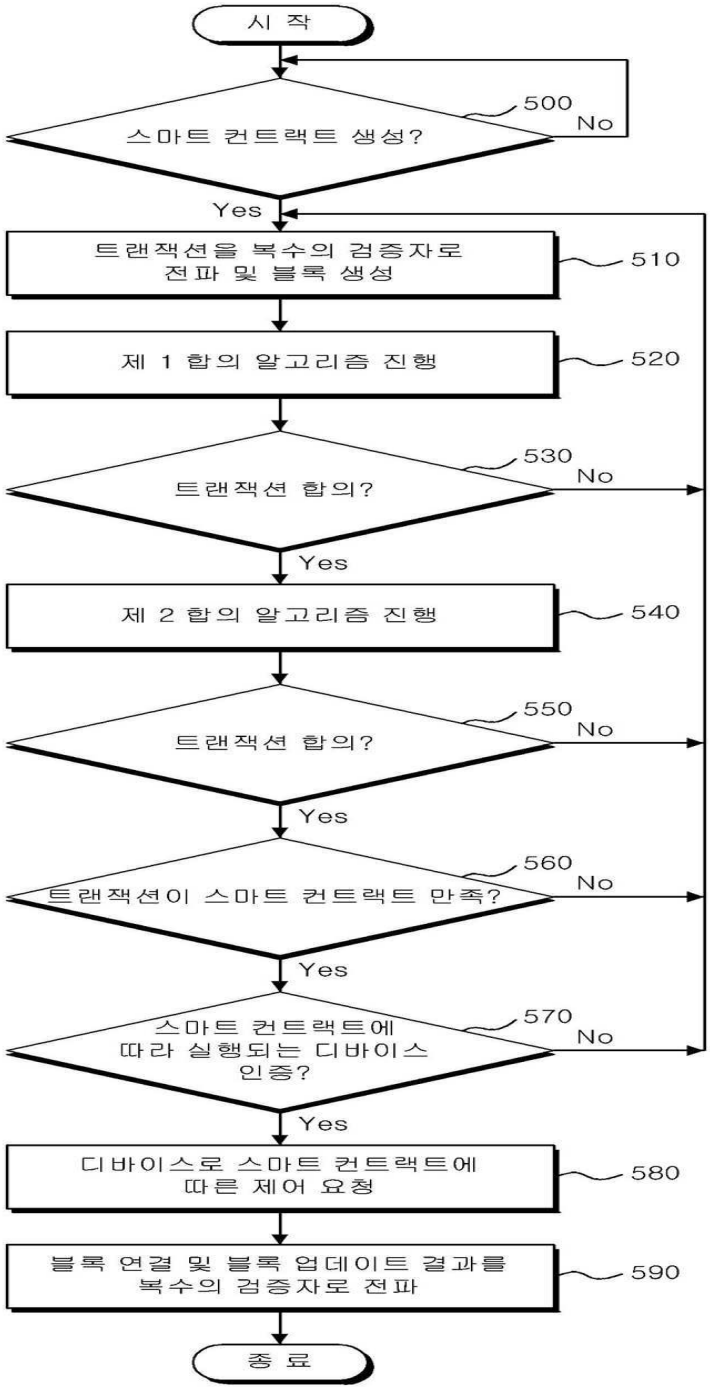
도면1



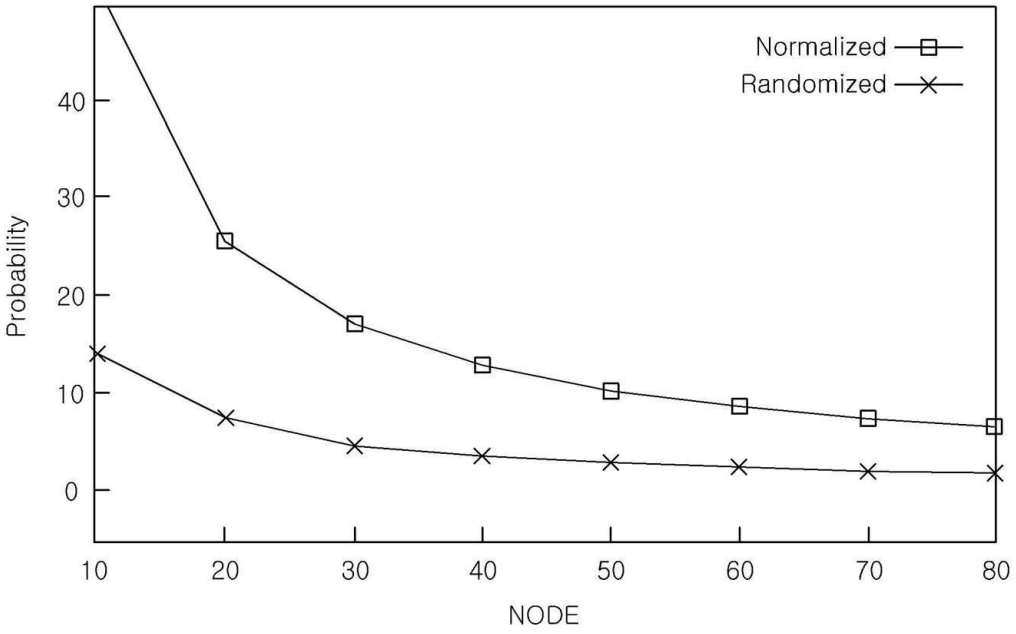
도면2


1000
Verifiers
102
100
13
DB
Verifier2
Group1
12
Verifiers
DB
Verifier1
DB
Verifier3
1st BFT Consensus
300
Private Blockchain
Group2
Machine1
Randomized
Mesh
Blockchain
DB
Verifier6
DB
Verifier4
103
Machine2
DB
Verifier5
2nd BFT Consensus
200
11
101
Machine3
Verifiers
14
104
15
Verifiers
105
Group4
Group3
Diversity of opinion BFT

도면3


시 작
스마트 컨트랙트 생성?
500
No
Yes
트랜잭션을 복수의 검증자로 전파 및 블록 생성
510
제 1 합의 알고리즘 진행
520
트랜잭션 합의?
530
No
Yes
제 2 합의 알고리즘 진행
540
트랜잭션 합의?
550
No
Yes
트랜잭션이 스마트 컨트랙트 만족?
560
No
Yes
스마트 컨트랙트에 따라 실행되는 디바이스 인증?
570
No
Yes
디바이스로 스마트 컨트랙트에 따른 제어 요청
580
블록 연결 및 블록 업데이트 결과를 복수의 검증자로 전파
590
종 료

도면4


Normalized
Randomized
Probability
40
30
20
10
0
10
20
30
40
50
60
70
80
NODE