(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0072794
(43) 공개일자 2021년06월17일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 16/27* (2019.01)
G06F 16/28 (2019.01) *H04L 29/06* (2006.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/3239 (2013.01)
G06F 16/27 (2019.01)
(21) 출원번호 10-2021-7013393
(22) 출원일자(국제) 2019년10월02일
심사청구일자 없음
(85) 번역문제출일자 2021년05월03일
(86) 국제출원번호 PCT/US2019/054311
(87) 국제공개번호 WO 2020/072659
국제공개일자 2020년04월09일
(30) 우선권주장
62/740,020 2018년10월02일 미국(US)

(71) 출원인
뮤츄얼링크, 인크.
미국 코네티컷 06492 월링포드 사우쓰 브로드 스트리트 1269
(72) 발명자
마차렐라 조셉 알
미국 코네티컷주 06084 톨랜드 도일 로드 110
(74) 대리인
김태홍, 김진희

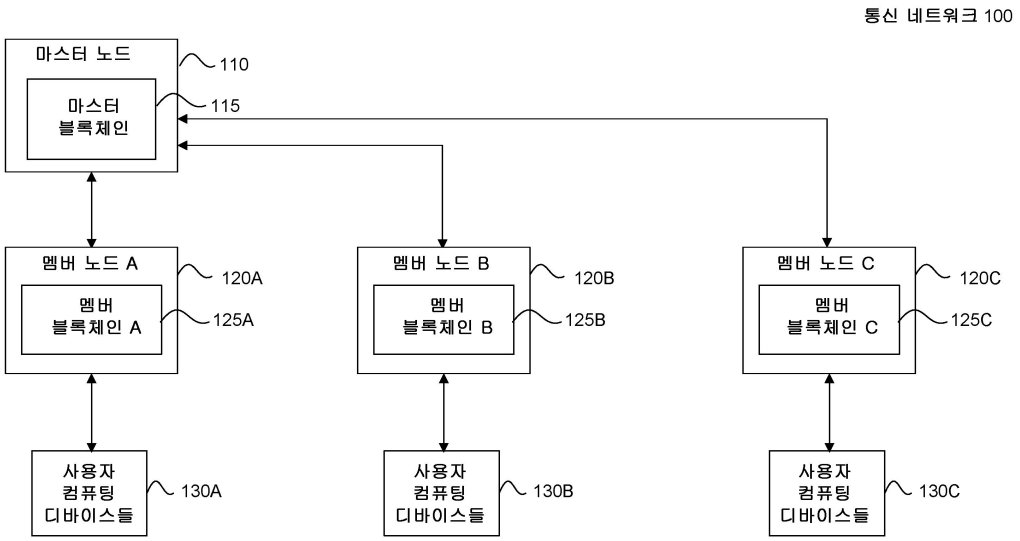
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **블록체인 기반의 신원 서명 메커니즘을 채택한 네트워크 멤버 식별을 위한 합의 기반 투표**

(57) 요 약

통신 방법 및 통신 네트워크를 동작시키기 위한 방법이 개시된다. 방법은 통신 네트워크의 제1 멤버에 대한 네트워크 식별자(NI)를 획득하는 단계 - 제1 멤버는 미검증되고 제1 사용자와 연관됨 -; 통신 네트워크에서 제2 멤버의 제2 사용자로부터 제1 사용자에 관한 표결 값을 획득하는 단계 - 제2 멤버는 검증됨 -; 표결 값에 기초하여 NI에 대한 신뢰 스코어를 생성하는 단계; 및 신뢰 스코어가 신뢰 스코어 임계치를 충족시키는 것에 응답하여, NI에 기초하여 제1 검증된 멤버 아이덴티티 해시 블록(MIHB)을 통신 네트워크에 대한 마스터 블록체인 원장에 삽입함으로써 제1 멤버를 검증하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
G06F 16/285 (2019.01)
H04L 63/08 (2013.01)
H04L 63/123 (2013.01)
H04L 9/0637 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/3255 (2013.01)
H04L 9/3297 (2013.01)
H04L 2209/463 (2013.01)

명 세 서

청구범위

청구항 1

통신 네트워크를 동작시키기 위한 방법에 있어서,

통신 네트워크의 제1 멤버에 대한 네트워크 식별자(network identifier; NI)를 획득하는 단계 - 상기 제1 멤버는 미검증되고 제1 사용자와 연관됨 -;

상기 통신 네트워크에서 제2 멤버의 제2 사용자로부터 상기 제1 사용자에 관한 표결 값을 획득하는 단계 - 상기 제2 멤버는 검증됨 -;

상기 표결 값에 기초하여 상기 NI에 대한 신뢰 스코어를 생성하는 단계; 및

상기 신뢰 스코어가 신뢰 스코어 임계치를 충족시키는 것에 응답하여, 상기 NI에 기초하여 제1 검증된 멤버 아이덴티티 해시 블록(member identity hash block; MIHB)을 상기 통신 네트워크에 대한 마스터 블록체인 원장에 삽입함으로써 상기 제1 멤버를 검증하는 단계를 포함하는, 방법.

청구항 2

제1항에 있어서,

상기 신뢰 스코어를 생성하기 전에 관계형 원장에, 상기 NI를 포함하는 미검증된 MIHB를 저장하는 단계 - 상기 제1 검증된 MIHB는 상기 미검증된 MIHB에 기초하여 생성됨 -; 및

상기 제1 멤버를 검증한 후에, 상기 미검증된 MIHB를 상기 관계형 원장으로부터 제거하는 단계를 더 포함하는, 방법.

청구항 3

제1항에 있어서,

상기 신뢰 스코어를 생성하는 단계는 상기 통신 네트워크에서 상기 제2 멤버의 검증 타임스탬프에 기초하여 상기 표결 값에 가중치를 할당하는 단계를 포함하고;

상기 표결 값은 상기 제1 사용자와 상기 제2 사용자 사이의 통신 세션에 기초하는, 방법.

청구항 4

제3항에 있어서,

상기 제2 멤버는 정부 기관이고, 상기 제2 사용자는 상기 정부 기관의 직원인, 방법.

청구항 5

제1항에 있어서,

상기 NI에 대한 개정(revision)을 획득하는 단계;

상기 개정에 대한 개정 스코어를 결정하는 단계;

상기 개정 스코어를 주요 개정 임계치(major revision threshold)와 비교하는 단계; 및

상기 개정 스코어가 상기 주요 개정 임계치 미만으로 떨어지는 것에 응답하여, 상기 개정에 기초한 제2 검증된 MIHB를 상기 마스터 블록체인 원장에 삽입함으로써 상기 제1 멤버를 재검증하는 단계를 더 포함하는, 방법.

청구항 6

통신 네트워크를 동작시키기 위한 방법에 있어서,

통신 네트워크에서 의심 사용자의 아이덴티티 속성을 획득하는 단계;

상기 의심 사용자와 연관된 의심 멤버의 식별 속성을 획득하는 단계;

상기 통신 네트워크에 대한 마스터 블록체인 원장 및 상기 식별 속성에 기초하여 상기 의심 멤버가 검증되었다고 결정하는 단계;

상기 의심 멤버가 검증되었다고 결정하는 것에 응답하여, 상기 의심 멤버의 멤버 블록체인 원장을 획득하는 단계;

제1 멤버와 연관된 제1 멤버 노드에 의해, 상기 멤버 블록체인 원장이 상기 의심 사용자의 아이덴티티 속성을 포함한다고 결정하는 단계; 및

상기 멤버 블록체인 원장이 상기 아이덴티티 속성을 포함한다고 결정하는 것에 응답하여, 상기 의심 사용자를 신뢰되는 것으로 분류하는 단계를 포함하는, 방법.

청구항 7

제6항에 있어서,

NI가 상기 의심 멤버에 대한 연락처 정보를 포함하고;

상기 제1 멤버 노드는 상기 연락처 정보를 사용하여 상기 의심 멤버로부터 상기 멤버 블록체인 원장을 요청하는, 방법.

청구항 8

제6항에 있어서,

상기 통신 네트워크 내의 상기 제1 멤버의 제1 사용자로부터, 상기 통신 네트워크 내의 제2 멤버의 제2 사용자에 관한 표결 값을 획득하는 단계 - 상기 제1 멤버는 검증되고 상기 제2 멤버는 미검증됨 -; 및

상기 마스터 블록체인 원장을 포함하는 상기 통신 네트워크의 마스터 노드에 상기 표결 값을 포워딩하는 단계를 더 포함하고,

상기 마스터 노드는 상기 제2 멤버의 NI에 기초하여 검증된 멤버 아이덴티티 해시 블록을 상기 마스터 블록체인 원장에 삽입함으로써 상기 표결 값에 기초하여 상기 제2 멤버를 검증하는, 방법.

청구항 9

제6항에 있어서,

상기 제1 멤버의 새로운 사용자에 기초한 멤버 블록을 상기 제1 멤버의 멤버 블록체인 원장에 삽입하는 단계;

상기 통신 네트워크에서 상기 제1 멤버에 대한 개정된 NI를 생성하는 단계;

상기 개정된 NI에 기초한 멤버 블록을 상기 멤버 블록체인 원장에 삽입하는 단계; 및

상기 마스터 블록체인 원장을 포함하는 상기 통신 네트워크의 마스터 노드에 상기 개정된 NI를 포워딩하는 단계를 더 포함하고,

상기 마스터 노드는, 상기 개정된 NI에 기초하여 검증된 멤버 아이덴티티 해시 블록을 상기 마스터 블록체인 원장에 삽입함으로써 상기 제1 멤버를 재검증하는, 방법.

청구항 10

제6항에 있어서,

상기 통신 네트워크에서 상기 제1 멤버에 대한 개정된 NI를 생성하는 단계;

상기 개정된 NI를 포함하는 루트(root) 노드를 포함하는 멤버 블록체인 원장을 생성하는 단계; 및

상기 개정된 NI를 마스터 노드에 포워딩하는 단계를 더 포함하고,

상기 마스터 노드는, 상기 개정된 NI에 기초하여 검증된 멤버 아이덴티티 해시 블록을 상기 마스터 블록체인 원

장에 삽입함으로써 상기 제1 멤버를 재검증하는, 방법.

청구항 11

시스템에 있어서,

통신 네트워크와 연관된 마스터 블록체인 원장;

상기 통신 네트워크의 제1 멤버에 대한 네트워크 식별자(NI)를 포함하는 미검증된 멤버 아이덴티티 해시 블록(MIHB)을 저장하도록 구성된 관계형 원장 - 상기 제1 멤버는 미검증되고 제1 사용자와 연관됨 -;

신뢰 집계 엔진(trust tabulation engin) - 상기 신뢰 집계 엔진은,

상기 통신 네트워크에서 제2 멤버의 제2 사용자로부터 상기 제1 사용자에 관한 표결 값을 획득하고;

상기 표결 값에 기초하여 상기 NI에 대한 신뢰 스코어를 생성하도록 구성되며, 상기 제2 멤버는 검증됨 -; 및

마스터 블록체인 제어기를 포함하고, 상기 마스터 블록체인 제어기는,

상기 신뢰 스코어를 신뢰 임계 값과 비교하고;

상기 신뢰 스코어가 상기 신뢰 임계 값을 충족시키는 것에 응답하여, 상기 미검증된 MIHB에 기초하여 검증된 MIHB를 상기 마스터 블록체인 원장에 삽입함으로써 상기 제1 멤버를 검증하도록 구성되는, 시스템.

청구항 12

제11항에 있어서,

상기 NI는 상기 제1 멤버의 물리적 어드레스 및 상기 제1 멤버의 공개 IP 어드레스를 포함하는, 시스템.

청구항 13

제11항에 있어서,

상기 신뢰 스코어를 생성하는 것은 상기 통신 네트워크에서 상기 제2 멤버의 검증 날짜에 기초하여 상기 표결 값에 가중치를 할당하는 것을 포함하고;

상기 표결 값은 상기 제1 사용자와 상기 제2 사용자 사이의 통신 세션에 기초하는, 시스템.

청구항 14

제11항에 있어서,

상기 검증된 MIHB는 상기 미검증된 MIHB의 해시 및 상기 신뢰 스코어를 포함하는, 시스템.

청구항 15

제11항에 있어서,

상기 제1 멤버와 연관된 제1 멤버 노드; 및

상기 제2 멤버와 연관된 제2 멤버 노드를 더 포함하고,

상기 마스터 블록체인 원장 및 상기 마스터 블록체인 제어기는 마스터 노드에 위치하는, 시스템.

청구항 16

제15항에 있어서, 상기 제1 멤버 노드는,

멤버 블록체인 원장; 및

멤버 블록체인 제어기를 포함하고,

상기 멤버 블록체인 제어기는,

상기 제1 멤버의 새로운 사용자에 기초한 멤버 블록을 상기 멤버 블록체인 원장에 삽입하고;

상기 제1 멤버에 대한 개정된 NI를 획득하고;

상기 개정된 NI에 기초한 멤버 블록을 상기 멤버 블록체인 원장에 삽입하고;

상기 개정된 NI를 상기 마스터 노드에 포워딩하도록 구성되고,

상기 마스터 블록체인 제어기는, 상기 개정된 NI에 기초하여 검증된 MIHB를 상기 마스터 블록체인 원장에 삽입함으로써 상기 제1 멤버를 재검증하는, 시스템.

청구항 17

제15항에 있어서, 상기 제1 멤버 노드는,

제1 멤버 블록체인 원장; 및

멤버 블록체인 제어기를 포함하고,

상기 멤버 블록체인 제어기는,

상기 제1 멤버에 대한 개정된 NI를 획득하고;

상기 개정된 NI를 포함하는 루트 노드를 포함하는 제2 멤버 블록체인 원장을 생성하고;

상기 개정된 NI를 상기 마스터 노드에 포워딩하도록 구성되고,

상기 마스터 노드는, 상기 개정된 NI에 기초하여 검증된 MIHB를 상기 마스터 블록체인 원장에 삽입함으로써 상기 제1 멤버를 재검증하는, 시스템.

청구항 18

제15항에 있어서, 상기 제2 멤버 노드는,

멤버 블록체인 제어기를 포함하고,

상기 멤버 블록체인 제어기는,

통신 네트워크에서 의심 사용자의 아이덴티티 속성을 획득하고;

상기 의심 사용자와 연관된 의심 멤버의 식별 속성을 획득하고;

상기 마스터 블록체인 원장이 상기 의심 멤버의 식별 속성을 포함하는 NI를 포함한다고 결정하고;

상기 마스터 블록체인 원장이 상기 식별 속성을 포함하는 NI를 포함한다고 결정하는 것에 응답하여, 상기 의심 멤버의 멤버 블록체인 원장을 획득하고;

상기 멤버 블록체인 원장이 상기 의심 사용자의 아이덴티티 속성을 포함한다고 결정하고;

상기 멤버 블록체인 원장이 상기 아이덴티티 속성을 포함하는 것에 응답하여, 상기 의심 사용자를 신뢰되는 것으로 분류하도록 구성되는, 시스템.

청구항 19

제18항에 있어서,

상기 식별 속성을 포함하는 NI는 상기 의심 멤버에 대한 연락처 정보를 더 포함하고;

상기 멤버 블록체인 제어기는 또한, 상기 연락처 정보를 사용하여 상기 의심 멤버로부터 상기 멤버 블록체인 원장을 요청하도록 구성되는, 시스템.

청구항 20

제11항에 있어서,

상기 제2 멤버는 정부 기관이고, 상기 제2 사용자는 상기 정부 기관의 직원인, 시스템.

발명의 설명

기 술 분 야

[0001] 합의 기반 표결을 사용하고 블록체인 기반 아이덴티티 서명 메커니즘을 채택하여, 네트워크 내의 멤버들의 아이덴티티를 인증 및 검증하기 위한, 그리고 네트워크 디렉토리-관련 아이덴티티 속성들의 변경들을 인증 및 검증하기 위한 시스템 및 방법이 본 명세서에 개시된다.

배 경 기 술

[0002] 임의의 폐쇄형 멤버쉽 네트워크에서, 새로운 멤버는, 멤버가 자격들을 만족하고 그리고/또는 멤버쉽의 조건들을 충족시키는 경우에만 네트워크에 가입할 수 있다. 이러한 자격들은 멤버의 일부이거나 멤버와 연관된 특정 특성 또는 속성들에 기초할 수 있다.

[0003] 엔드포인트 멤버들이 네트워크 내의 다른 엔드포인트 멤버들과 통신하도록 허용되거나 인에이블되는 통신 네트워크들에서, 폐쇄형 네트워크 도메인 속성들은 마찬가지로, 네트워크 액세스 및 멤버십 자격을 통해 엔드포인트 멤버쉽에 대한 제한들에 의해 부과될 수 있다. 선험적으로 제한될 때 통신 네트워크의 멤버쉽, 액세스 및 사용은 일반적으로, 다른 이름들 중에서도, "사설 네트워크들", "폐쇄형 네트워크들", "제한된 액세스 네트워크들", "특권 액세스 네트워크들", "인클레이브된(enclaved) 네트워크들"을 포함하는 많은 이름들로 지칭된다. 추가적으로, 사설 네트워크를 이용하더라도, 특정 멤버들은 일반적으로 다른 멤버들에게 이용가능하지 않은 특수한 상태 또는 특권들을 가져서, 서브네트워크들, 서브도메인들 또는 특수한 액세스 영역들을 생성할 수 있다. 이는 네트워크 사용자들의 더 큰 세트의 서브세트를 효과적으로 표현하고, 멤버들의 서브세트는 서브세트 멤버쉽에 대해 이들을 적격성 심사하는 하나 이상의 다른 공유 특성들 또는 속성들을 소유할 수 있다.

[0004] 임의의 네트워크의 경우, 엔티티가 네트워크에서 멤버로서 적격성 심사되는지 여부를 결정하는 것과 연관된 문제들은 다중적이다. 첫 번째 문제는, 제안된 새로운 멤버가 자격을 위해 필요한 속성들 또는 멤버쉽의 속성들을 소유해야 한다는 것이다. 이러한 적격성 심사 속성들은 종종, 네트워크 멤버쉽 가입자뿐만 아니라, 네트워크의 액세스 또는 사용에 대한 멤버쉽 상태 및 특권의 지속적인 검증을 위해 요구된다. 일반적으로, 자격 증명은 자격 증명을 주장하는 규정된 정보의 제시를 요구한다. 이들 술어 증명(predicate proof)들은 신뢰성을 갖는 것으로 간주되거나 가정되는 다른 기존의 조직들, 시스템들 또는 이벤트들로부터 발생되거나 생성된 문서화일 수 있다. 각각의 술어 증명은 그 자체로 또는 다른 문서 증명들과 조합하여 그리고 다른 확인 프로세스들 또는 액션들과 함께 또는 없이 신뢰되는 것으로 추정된다. 일반적인 예는 운전 면허증의 발행에 요구되는 문서들이다. 운전 면허증에 대한 신청자의 공통적인 문서 증명 요건은 출생 증명서의 인증 사본, 거주지 어드레스가 있는 청구서의 현재 사본, 및 사진 식별 문서, 이를테면 유효한 여권을 포함할 수 있다. 제시될 때, 증명들은 그들의 유효성을 결정하기 위해 인증되어야 한다. 임의의 증명 주장의 유효성은 일반적으로 적어도 2배이다. 먼저, 정보를 포함하는 문서 또는 다른 매체는 진품인 것으로(즉, 위조되거나 변경되지 않은 것으로) 결정되어야 한다. 둘째로, 얼굴 진품 문서인 경우, 그 문서가 사기 없이 발행 또는 획득되었는지 여부가 결정되어야 한다. 충분한 검증 증명들이 제시되고 확인될 때, 증명서 형태, 이를 테면, 멤버쉽 및 멤버쉽 아이덴티티를 표시하는 고유하게 대표적인 증서, 문서, 토큰, 심볼, 또는 정보의 세트일 수 있는 운전 면허증이 발행될 것이다.

[0005] 두 번째 문제는 증명서가 제시될 때 진본으로서 검증되어야 한다는 것이다. 다시 말해서, 증명서들은 조건부 기반인 경우, 이를 테면 일정 시간 기간 동안 유효한 경우, 유효성의 조건들에 대해 검증되어야 하며, 이들은 위조될 수 없다.

[0006] 세 번째 문제는, 증명서들이 연관되어 증명서들이 사람 또는 사물과 연관되는 경우, 그 연관성은 유효해야 한다는 것이다.

[0007] 통신 네트워크들에서, 멤버 엔드포인트의 진본성은 여러 수단을 통해 검증될 수 있다. 이들은, 주장된 아이덴티티를 입력하고 아이덴티티와 연관된 유효한 패스코드를 입력함으로써, 엔드포인트가 네트워크에 대한 액세스를 허용받을 때의 검증을 포함한다. 입력될 때, 증명서들은, 네트워크에 대한 액세스를 허용하거나 네트워크 상에서 허용된 기능들을 수행하기 위한 목적들을 위해 증명서들의 유효성을 결정하기 위해 데이터 저장소에 대해 검증 기능을 수행하는 에이전트, 통상적으로 서버 또는 다른 컴퓨팅 디바이스에 전송된다. 종종, 종래의 통신 네트워크들에서, 사용자 패스워드들 및 로그인 증명서들은, 멤버의 엔드포인트 네트워크 어드레스 및 공개가능 또는 발견가능 아이덴티티 정보를 저장하는 디렉토리와 관계적으로 연관된다. 이 정보는 수신자 멤버에게 통신들을 전송하기 위해 다른 네트워크 멤버들에 의해 액세스될 수 있다. 마찬가지로, 엔드포인트 멤버가 의도된 수신자에게 메시지를 전송할 때, 전송 멤버의 아이덴티티는 또한, 디렉토리를 사용하여 송신될 수 있다.

[0008] 위의 인증 및 검증 프로세스는 인증 기관(CA)으로서 동작하는 에이전트와 함께 잘 알려져 있고 이해되는 개인-공개 키 또는 대칭적 키 암호화 방식들을 이용함으로써 보안이 이루어질 수 있다.

[0009] 자격 파라미터들의 부과에 의해 멤버쉽이 제한되고 아이덴티티가 명시적 또는 묵시적 조건부 구성인 임의의 폐쇄형 네트워크에서, 네트워크의 목적, 신뢰성, 비밀성 및/또는 취약성이 손상될 수 있고, 여기서, 멤버쉽 자격, 증명서들, 및/또는 멤버와 연관된 아이덴티티는 위조되거나 남용된다. 이는 증명서 및 아이덴티티 인증 및 검증의 루트 체인에서 발생할 수 있다. 오용 및 위조는 다양한 사회 공학 기법들 및 디지털 스푸핑 기법들을 이용하는 것을 포함하는 임의의 수의 방식들로 발생할 수 있다. 개인들에 대한 아이덴티티 검증의 경우, 검증은 독립적인 아이덴티티 데이터의 상호 참조 체크들을 통해 달성될 수 있다. 이는 식별 이미지에 대한 대상의 시각적 검증을 위해 운전 면허증 또는 다른 사진 식별의 물리적 제시를 요구하는 것을 포함한다. 지문, 홍채 스캔들, 음성 인증, 얼굴 인식, 및 기존의 데이터 저장소에 대한 DNA 샘플링 비교를 포함하는 다른 생체인식 검증 프로세스들이 이용될 수 있다.

[0010] 폐쇄형 네트워크에서 제시되는 고유한 난제들은 네트워크에 가입할 때 그리고 네트워크의 멤버인 동안, 증명서들 및 아이덴티티의 진본성이 보장될 수 있는 시스템을 고안하고, 위조 또는 남용을 검출하고, 관련 디렉토리 정보의 변경들을 검증한다. 다중 기관 공공 안전 및 비상 통신 네트워크들의 경우, 교환되는 정보의 성질이 민감하고 인가되지 않은 당사자들이 유효한 통신들에 액세스, 송신 또는 간섭하는 것으로 인해 네트워크 통신들을 손상시킬 수 있기 때문에, 멤버쉽 자격을 인증하고 보장하는 능력은 매우 중요하다.

[0011] 사용자들 또는 엔드포인트들이 연관되거나 또는 기업 네트워크 에이전트의 관리 제어 하에 있는 기업 네트워크들에서, 클라이언트-서버 기반 디렉토리 시스템들, 이를 테면, 경량 디렉토리 액세스 프로토콜(Lightweight Directory Access Protocol; LDAP) 또는 RADIUS 기반 인증 및 계정 프로토콜들, 이를 테면 암호 인증 프로토콜(Password Authentication Protocol; PAP), 챌린지 핸드셰이크 인증 프로토콜(challenge handshake authentication protocol; CHAP) 및 확장가능한 인증 프로토콜(extensible authentication protocol; EAP)이 사용되고, 기업은 인증 정책에서 확립된 속성 팩터들 또는 기준들에 기초하여 검증 및 인증할 수 있다. 그러나, 초기 멤버쉽 자격과 연관된 초기 인증은 일반적으로, 아이덴티티를 확인하기 위해 사용자 및/또는 연관된 검증 문서의 어떤 형태의 물리적 또는 시각적 검사에 의해 확립된다. 일단 아이덴티티가 주장되고 검증되면, 고유한 식별 또는 증명서들이 발행되거나 생성될 수 있다. 종종, 이는 사용자 사진들과 함께 기업 발행 식별 카드들의 사용을 수반한다. 이러한 식별 카드들은 또한 전자 키 카드 액세스와 같은 다른 기능들을 제공할 수 있고, 컴퓨터 또는 디바이스 액세스를 위한 단일 또는 다중-팩터 인증의 일부로서 사용될 수 있다.

[0012] 그러나, 서로 상호작용하는 공공 안전 기관들 또는 서로 상호작용하는 다른 기업들의 경우, 반드시 동일한 레벨의 조사 또는 증명 표준을 보장하는 공통 또는 공유된 검증 방법 및 인증 방식이 존재하는 것은 아니다. 통상적으로, 크로스-기관 인증은 주장된 아이덴티티에 의해 추정되고, 기관과 연관된 사용자들은 이들이 연관되는 기관의 신뢰되는 체인의 일부인 것으로 가정된다. 예를 들어, 법 집행 기관 멤버들만의 네트워크에서, 경찰서 B가 네트워크("멤버십 자격 검증" 또는 "MQF")에 가입했을 때 호출된 추정 멤버십 자격 검증 기능에 기초하여 경찰서 B가 자신이 누구인지를 주장하는 네트워크 디렉토리 기반 주장에 기초하여 경찰서 A는 경찰서 B의 아이덴티티를 신뢰할 것이다. 더욱이, 경찰서 B의 연관된 엔드포인트들 또는 사용자들은, 경찰서 B의 네트워크 또는 보안 도메인 내의 사용자 또는 엔드포인트인 것으로 경찰서 B에 의해 부과된 추정된 인증 기준들로부터 발생하는 추론에 의해 진본인 것으로 가정된다. 따라서, 자신을 경찰서 B의 John Doe로서 식별하는 사용자는 경찰서 B의 사용자의 유효한 아이덴티티인 것으로 간주된다.

발명의 내용

[0013] 하나 이상의 실시예들은 통신 네트워크를 동작시키기 위한 방법에 관한 것이다. 방법은 통신 네트워크의 제1 멤버에 대한 네트워크 식별자(NI)를 획득하는 단계 - 제1 멤버는 미검증되고 제1 사용자와 연관됨 -; 통신 네트워크에서 제2 멤버의 제2 사용자로부터 제1 사용자에 관한 표결 값을 획득하는 단계 - 제2 멤버는 검증됨 -; 표결 값에 기초하여 NI에 대한 신뢰 스코어를 생성하는 단계; 및 신뢰 스코어가 신뢰 스코어 임계치를 충족시키는 것에 응답하여, NI에 기초하여 제1 검증된 멤버 아이덴티티 해시 블록(MIHB)을 통신 네트워크에 대한 마스터 블록체인 원장에 삽입함으로써 제1 멤버를 검증하는 단계를 포함한다.

[0014] 하나 이상의 실시예들은 통신 네트워크를 동작시키기 위한 방법에 관한 것이다. 방법은, 통신 네트워크에서 의심 사용자의 아이덴티티 속성을 획득하는 단계; 의심 사용자와 연관된 의심 멤버의 식별 속성을 획득하는 단계; 통신 네트워크에 대한 마스터 블록체인 원장 및 식별 속성에 기초하여 의심 멤버가 검증되었다고 결정하는

단계; 의심 멤버가 검증되었다고 결정하는 것에 응답하여, 의심 멤버의 멤버 블록체인 원장을 획득하는 단계; 제1 멤버와 연관된 제1 멤버 노드에 의해, 멤버 블록체인 원장이 의심 사용자의 아이덴티티 속성을 포함한다고 결정하는 단계; 및 멤버 블록체인 원장이 아이덴티티 속성을 포함한다고 결정하는 것에 응답하여, 의심 사용자를 신뢰되는 것으로 분류하는 단계를 포함한다.

[0015] 하나 이상의 실시예들은 시스템과 관련된다. 시스템은, 통신 네트워크와 연관된 마스터 블록체인 원장; 통신 네트워크의 제1 멤버에 대한 네트워크 식별자(NI)를 포함하는 미검증된 멤버 아이덴티티 해시 블록(MIHB)을 저장하도록 구성된 관계형 원장 - 제1 멤버는 미검증되고 제1 사용자와 연관됨 -; 통신 네트워크에서 제2 멤버의 제2 사용자로부터 제1 사용자에 관한 표결 값을 획득하고 - 제2 멤버는 검증됨 -; 표결 값에 기초하여 NI에 대한 신뢰 스코어를 생성하도록 구성된 신뢰 집계 엔진; 및 마스터 블록체인 제어기를 포함하고, 마스터 블록체인 제어기는, 신뢰 스코어를 신뢰 임계 값과 비교하고; 신뢰 스코어가 신뢰 임계 값을 충족시키는 것에 응답하여, 미검증된 MIHB에 기초하여 검증된 MIHB를 마스터 블록체인 원장에 삽입함으로써 제1 멤버를 검증하도록 구성된다.

도면의 간단한 설명

[0016] 도 1은 하나 이상의 실시예들에 따른 통신 네트워크를 도시한다.

도 2는 하나 이상의 실시예들에 따른 마스터 노드를 도시한다.

도 3은 하나 이상의 실시예들에 따른 멤버 노드를 도시한다.

도 4 내지 도 7은 하나 이상의 실시예들에 따른 흐름도들을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0017] 네트워크 내의 멤버들의 아이덴티티를 인증 및 검증하기 위한, 그리고 네트워크 디렉토리-관련 아이덴티티 속성들의 변경들을 인증 및 검증하기 위한 시스템 및 방법이 본 명세서에 개시된다. 기존의 네트워크들은 멤버들을 인증 및 검증하기 위해 잘 알려진 기술들을 이용하기 때문에, 네트워크 보안 조치들은 종종 우회되고 네트워크 보안이 손상될 수 있다. 개시된 시스템 및 방법은 암호화, 블록체인 또는 분산형 원장 기술, 및 합의 표결의 특정 양상들을 통합하고 이용하여, 기존 네트워크들에 비해, 멤버십(네트워크의 새로운 및 기존 멤버들 또는 노드들 둘 모두의 멤버쉽)을 인증하고 네트워크 디렉토리-관련 아이덴티티 속성들의 변화들을 검증하는 정확도를 개선하며, 이는 네트워크 보안을 증가시킨다. 일 실시예에서, 다중-기관 공공 안전 및 비상 통신 네트워크들은, 네트워크의 새로운 멤버들 또는 노드들을 인증 및 검증하기 위해 암호화, 블록체인 기술, 및 합의 표결을 이용하여, 새로운 멤버들 또는 노드들이 네트워크에 참여하고 다른 멤버들 또는 노드들과 상호작용할 수 있게 한다. 이 실시예에서, 네트워크는 추가로, 기존의 멤버들 또는 노드들의 멤버쉽을 인증 및 검증하고, 네트워크 디렉토리-관련 식별 속성들의 임의의 변경들을 인증 및 검증할 수 있다. 본 명세서에 설명된 기술들은, 네트워크 보안을 증가시키고 피어 네트워크들에서 아이덴티티를 보장하기 위해 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 조합으로 구현될 수 있다.

[0018] 개방형 원장, 블록체인-기반 시스템들은 블록 프로세싱 및 기록을 포함하는 안전하고 공개적으로 인증가능한 블록 트랜잭션들을 허용한다. 이러한 시스템들은 불변의 트랜잭션 기록들을 생성한다. 이러한 시스템들은 단방향 암호화 기법들 및 방법들을 이용하는 다양한 작업 증명 알고리즘들에 결합될 때 가상 또는 디지털 화폐 및 고유한 토큰 아이덴티티에 대해 이용되었다. 블록체인들은 작업 증명 이외의 합의 알고리즘들, 이를 테면, 이해 관계 증명을 이용할 수 있다. 일반적으로, 증명-기반, 블록체인 개방 원장 시스템들이 넌스(nonce)를 "마이닝"하기 위해 요구되는 속도 및 프로세싱 능력으로부터 발생하는 트랜잭션 프로세싱 레이트 제한들을 갖고 넌스와 연관된 연관 정보 블록이 커뮤니티 블록체인 소프트웨어에 의해 규정된다는 것은 잘 알려져 있고 인식된 문제이다. 추가적으로, 블록 내에 기록된 트랜잭션들은 순서, 크기, 또는 다른 실세계 서수 고려사항들과 관련되지 않고 블록 프로모터의 재량으로 채워진다. 더욱이, 네트워크 상의 멤버의 온라인 존재 또는 상태, 이들의 현재 네트워크 어드레스(직접적으로 또는 프록시를 통한) 및/또는 위치가 발견가능해야 하는 실시간 네트워크들의 경우, 종래의 블록 체인 구현들은 멤버의 상태를 캡처하고 도모하는 데 필요한 속도가 부족하고, 게다가, 종래의 분산형 공유 원장에서, 원장들의 업데이트 사본들을 발행함으로써 다른 멤버들에게 상태의 변화들을 통신하는 것에 대한 통신 오버헤드는 비효율적이다. 그 결과, 현재 생각되는 바와 같은 현재의 블록체인 및 개방형 원장 시스템들의 사용은 실시간 통신 네트워크들에 대해 쉽게 명백한 적용가능성을 갖지 않는 것으로 간주된다. 블록체인 구현은 공개일 수 있으며, 여기서 공개의 임의의 멤버는 마이닝 및 공개 원장에 블록들을 추가하는 것에 참여할 수 있다. 다른 블록체인 구현들이 허용가능할 수 있으며, 여기서, 특정 참여자들만이 마이닝하고 원

장에 블록들을 추가하도록 허용(허가)되며, 이는 공개일 수 있거나 또한 특정 뷰잉 제한들을 가질 수 있다. 본 명세서에서 설명된 시스템 및 방법은 공개 또는 허용 블록체인들을 사용하여 구현될 수 있다.

[0019] 일 실시예에 따른, 블록체인-기반 식별 서명 메커니즘들을 이용하는 네트워크 멤버 식별을 위한 합의-기반 표결이 아래에서 설명된다. 본 명세서에서 개시되는 시스템 및 방법은 작업 증명 및 이해 관계 증명을 포함하지만 이에 제한되지 않는 임의의 합의 알고리즘을 이용할 수 있다. 본 명세서에 개시된 멤버 식별 기술들은 다중-기관 공공 안전 및 비상 통신 네트워크들, 또는 네트워크 보안을 증가시키기 위해 멤버쉽 자격 또는 아이덴티티가 요구되는 임의의 다른 네트워크에서 구현될 수 있다.

[0020] 네트워크 멤버 식별을 위한 합의-기반 표결의 본 개시에 따른 예시적인 시스템은 하나 이상의 컴퓨터들, 이를테면 하나 이상의 서버들을 포함할 수 있다. 시스템은 컴퓨터 판독가능 메모리를 포함한다. 시스템은 관계형 데이터베이스(관계형 데이터 구조 또는 관계형 원장을 포함함), 블록체인 데이터베이스(블록체인 데이터 구조 또는 블록체인 원장을 포함함), 인증 모듈(Authentication Module; "AM"), 신뢰 메시징 모듈(Trust Messaging Module; "TMM"), 및 신뢰 집계 모듈(Trust Tabulation Module; "TTM")을 포함한다. AM, TMM 및 TTM은 소프트웨어, 또는 하드웨어 또는 하드웨어와 소프트웨어의 조합으로 구현될 수 있다.

[0021] 블록체인 원장은 다음 기술을 사용하여 통신 네트워크에 대해 개시될 수 있다. 제1 네트워크 서명 인스턴스화를 표현하는 루트 암호화 해시가 생성될 수 있다. 이러한 루트 암호화 해시는, "제네시스 블록(Genesis Block)"으로 알려진 규정된 크기의 네트워크 식별 스트링과 결합된 규정된 크기의 임의의 넌스로부터 도출될 수 있다. 네트워크 식별 스트링은 네트워크 이름 공간, 네트워크인스턴스화의 날짜 및 시간, 위치, 제1 생성자 아이덴티티, 네트워크 내의 하나 이상의 라우팅 또는 다른 머신 엘리먼트들의 MAC 어드레스, 네트워크의 제1 멤버 또는 멤버들 ID들 등을 포함하는 임의의 상대적 데이터로부터 형성될 수 있다. 제네시스 블록은 블록체인 원장 상의 제1 엔트리이다.

[0022] 제네시스 블록에 후속하여, 블록체인 원장은 검증된 멤버 아이덴티티 해시 블록들("검증된 MIHB")을 데이터 기록들로서 기록한다. 즉, 블록체인 원장에 추가된 각각의 연속적인 블록은 검증된 MIHB이며, 이는, 아래에서 더 상세히 논의되는 바와 같이, 블록이 검증된 MIHB로 간주되는 데 필요한 신뢰 검증 레벨을 달성하면, 순서대로 기록 및 저장된다.

[0023] 관계형 원장은 미검증된 멤버 아이덴티티 해시 블록들("미검증된 MIHB")을 저장한다. 미검증된 MIHB들은 순서대로 관계형 원장에 기록 및 저장된다. 아래에서 더 상세히 논의되는 바와 같이, MIHB의 필수 신뢰 검증 레벨이 미리 결정된 레벨을 달성하면, 미검증된 MIHB들은 관계형 원장으로부터 제거될 수 있고, 이 때, 미검증된 MIHB가 검증된 MIHB가 된다.

[0024] 다음으로, 본 개시에 따른 통신 네트워크에 가입하기 위한 기법이 설명된다. 네트워크에 가입할 때 각각의 새로운 멤버에는 고유한 네트워크 아이덴티티("NI")가 할당될 수 있으며, 이는 다음 중 하나 이상으로 구성될 수 있다: (a) 사용자 이름, 네트워크 디렉토리 이름, 기관 또는 조직 이름, 네트워크 어드레스, 지리적 위치, 전화번호, 이메일 어드레스, 또는 그 자체로 또는 엔드포인트 멤버 아이덴티티와 관련하여 다른 데이터와 조합되어 연관되어 구별되는 임의의 다른 데이터; 및 (b) 사용자 또는 랜덤으로 생성되는 패스코드일 수 있는 고유한 검증 속성 또는 속성들, 단독으로 또는 머신 액세스 코드 어드레스와 조합될 수 있는 영숫자 스트링 또는 일련의 스트링들로 구성되는 챌린지 및 답신 프로토콜에 대한 어구 또는 일련의 응답 입력들, 사용자 생체인식 서명 디지털 입력, 엔드포인트의 호스트 디바이스와 연관된 암호화된 개인 또는 공개 키 또는 펌웨어 기반 암호화 키, 위치 또는 다른 유사한 정보 또는 데이터; (c) 고유의 식별 속성들은 멤버로서 네트워크에 가입하기 위한 조건으로서 요구되는 하나 이상의 속성들일 수 있고, 하나 이상의 요구된 검증 속성들일 수 있다.

[0025] 네트워크 아이덴티티는 암호화된 해시 함수에 입력되어 아이덴티티를 표현하는 해시 스트링을 출력할 수 있으며, 이는 멤버 아이덴티티 해시 블록("MIHB")으로 지칭될 수 있다. 암호화된 해시 함수는 SHA3 해시 암호화 함수와 같은 단방향 해싱 암호화 함수일 수 있다.

[0026] 새로운 MIHB는 네트워크의 컴퓨터 또는 서버 상에 상주하는 소프트웨어 모듈일 수 있는 인증 모듈에 송신될 수 있다. 인증 모듈은 새로운 MIHB를 수신하고, 적어도 다음을 입력으로서 사용하여 해시 동작을 수행한다: (i) 블록체인 원장에 첨부된 가장 최근 블록의 해시 값(이는 검증된 MIHB임) 및 (ii) MIHB 값. 새로운 MIHB가 네트워크의 첫 번째 멤버인 경우, 블록체인 원장의 가장 최근 블록은 제네시스 블록이고, 인증 모듈은 제네시스 블록의 해시 값을 사용한다. 이 해시 동작의 출력은 미검증된 MIHB로 지칭될 수 있으며, 이는 적어도 미검증된 MIHB 해시 값, 즉, 블록체인 원장에 첨부된 가장 최근 블록의 해시 값(즉, 해시 동작에 대한 입력으로서 사용되는 검

증된 MIHB의 해시 값), 및 MIHB를 포함한다.

[0027] 이 시점에서, 미검증된 MIHB는 신뢰되지 않는 것으로 간주된다. 미검증된 MIHB들은 관계형 원장에 송신될 수 있으며, 여기서, 그것은 순서대로 기록 및 저장될 수 있다. 미검증된 MIHB가 관계형 원장에 송신될 때, 이는 새로운 멤버에게 할당된 네트워크 아이덴티티와 연관될 수 있다.

[0028] 미검증된 MIHB를 갖는 제안된 네트워크 멤버는, 미검증된 MIHB를 검증된 MIHB로 변환하고 이를 네트워크의 블록체인 원장에 추가함으로써 관리 기능을 통해 네트워크 소유자에 의해 인증된 멤버로서 승인될 수 있거나, 또는 미검증된 멤버로서 네트워크 기능들에 대한 액세스를 갖는 네트워크의 멤버로서 승인될 수 있다.

[0029] 미검증된 MIHB를 갖는 네트워크의 새로운 멤버가 네트워크의 임의의 다른 멤버와의 제1 통신 세션 또는 네트워크 상의 임의의 다른 세션 이벤트에 진입할 때, 신뢰 메시지는 새로운 멤버의 엔드포인트로부터 직접적으로 또는 네트워크 내의 컴퓨터 또는 서버 상에 상주하는 소프트웨어 모듈일 수 있는 신뢰 메시징 모듈("TMM")을 통해 간접적으로 전송될 수 있다. TMM은 통신 세션의 당사자들인 하나 이상의 다른 수신 엔드포인트들에 의해 수신될 수 있다. TMM은 전송 엔드포인트의 신뢰 상태를 표시하는 수신자 엔드포인트 사용자 인터페이스 내에서 청가각 또는 시각적 방식으로 디스플레이될 수 있다. 예컨대, 전송 및 수신 엔드포인트들은 스마트폰들일 수 있고, TMM은 수신 스마트폰들의 스크린 상에 전송 스마트폰과 연관된 당사자의 신뢰 상태를 디스플레이할 수 있다.

[0030] 멤버 엔드포인트의 신뢰 상태는 신뢰 집계 모듈("TTM, Trust Tabulation module")에 의해 계산되고, 임계 레벨 또는 신뢰 레벨들에 대응하는 일련의 값들 또는 스칼라 값으로서 표현될 수 있다. TTM은 상대적인 신뢰 상태를 나타내도록 의도된 하나 이상의 타입들의 스칼라 데이터, 팩터들 및 연관된 계산 방법들을 활용하는 네트워크의 컴퓨터 또는 서버 상에 상주하는 소프트웨어일 수 있다. 계산들은 단일 변수 또는 다변량 알고리즘들, 정적 또는 동적 통계 모델들 및 분산 분석, 휴리스틱 간섭 모델들, 확률적 분석, 고유 분해, 또는 통신 주파수를 포함하는 임의의 정량화가능한 데이터 또는 정보를 활용하는 신경망 기반 인공 지능 평가들, 별개의 다른 멤버들 또는 멤버들의 그룹들 사이의 통신들에서의 주파수, 위치, 네트워크 조직, MAC 어드레스, 셀 타워 또는 중계 위치, 지연 시간, IP 헤더 메타 데이터, 인코딩 방식, 클라이언트 로그인 또는 패스워드 시도들, 파일 또는 데이터 손상 이벤트들 또는 레이트들, 바이러스 서명들, 코드 주입 이벤트들, 및 다른 멤버 신뢰 등급 또는 표결들에 기초하여 다양한 기능들로 구성된다. 일 실시예에서, 하나 이상의 임계 값들이 설정되는 대응하는 스칼라 범위가 신뢰 범위에 할당된다. 다른 멤버들은 신뢰 값들의 선택들 또는 등급들에 기초하여 표결할 수 있고, 선택들 또는 등급들은 정의된 범위 내의 일련의 심볼 디스크립터들 또는 숫자 값들과 상관될 수 있다. 예를 들어, 최소로 신뢰되는 1의 값 내지 최대로 신뢰되는 5의 값을 갖는 대응하는 신뢰 평가를 선택 및 송신함으로써 하나의 멤버가 다른 멤버의 주장된 아이덴티티의 신뢰도에 대해 표결할 수 있는 5-단계 신뢰 스케일이 이용될 수 있다. 멤버에 관한 표결들의 충분한 수집이 수신될 때, 송신된 표결 값들의 평균 값은 에이전트에 의해 계산되고, 평균 값은 네트워크 내의 멤버 신뢰 레벨을 확인하는 데 사용된다. 이 프로세스는 네트워크 트랜잭션 맥락에서 발생할 수 있다.

[0031] 예를 들어, 세션의 종료 또는 세션에서의 네트워크 멤버의 참여의 종료 시에, 엔드포인트의 아이덴티티를 확인하거나 질문하는 일련의 표결 선택들일 수 있는 표결 입력을 요청하는 대화형 메시지가 엔드포인트 멤버의 사용자 인터페이스에 디스플레이될 수 있다. 선택이 선택될 때, 표결 값 및 MIHB가 전송된다. TTM은 세션 거래와 관련하여 참가자 멤버들로부터 수신된 총 표결 값들을 계산할 수 있다. 그 다음, 표결 값이 기록되고, 표결들이 캐스팅된 신뢰되지 않거나 미검증된 멤버의 MIHB 또는 NI와 연관된 관계형 원장에 저장되며, TMM은 대상 멤버에 대해 캐스팅된 표결들의 누적 값을 업데이트한다.

[0032] 네트워크 또는 그의 서브세트들에, 네트워크 멤버의 누적 표결 값이 적용될 수 있는 신뢰 스케일이 할당될 수 있다. 확립된 검증된 신뢰에 대한 임계 값이 있을 수 있으며, 이는 멤버의 누적 표결 값이 신뢰 임계 값과 동일하거나 이를 초과할 때, 멤버의 MIHB가 신뢰되고 검증된 것으로 간주되고, 상태가 미검증된 MIHB로부터 검증된 MIHB로 변환된다. 이는, TMM이 대상 멤버에 대해 캐스트된 표결들의 누적 값을 업데이트하고 표결들의 누적 값을 임계 값과 비교할 때 발생할 수 있고, 값과 동일하거나 또는 그 값을 초과하면 메시지에 대한 명령을 TTM에 전송한다. 검증된 MIHB는 블록체인 원장에 첨부될 수 있다.

[0033] 멤버의 디렉토리 정보가 변경되거나 수정되면, 변경에 대해 트리거링되고 디렉토리에 대한 변경들의 타입에 기초하여 멤버의 누적 표결 값을 리셋 또는 조정하는 알고리즘 기능 모듈이 존재할 수 있다. 변경 시에, 새로운 MIHB가 생성되어 관계형 원장에 전송된다. 새로운 MIHB 해시는 블록체인 원장에 위치한 변경 전의 멤버의 MIHB로부터 재계산되고 도출된다. 그 다음, 새로운 MIHB는 미검증된 MIHB로서 분류되고, 위의 표결 프로세스를 사용하여 재검증된다.

[0034] 본 명세서에서 설명되는 시스템은, (a) 네트워크 내의 표결 멤버들의 상대적인 신뢰 값들; (b) 별개의 멤버들에 의한 상이한 표결들의 수; (c) 검증된 멤버 해시 블록들이 유효한 네트워크 멤버쉽의 지속기간; (d) 세션들의 수, 세션들의 지속기간 또는 유사한 메트릭들에 의해 측정되는 네트워크의 사용 빈도; (e) 클라이언트 엔드포인트 디바이스가 네트워크에 대한 액세스를 등록하거나 네트워크를 사용한 시간의 지속기간; (f) 최종 사용자 아이덴티티의 위치, 랭킹 또는 특권 레벨; (g) 표결시에 또는 다른 관련 멤버들과 관련하여 멤버의 근접 위치; (h) 표결할 때 또는 세션에서 멤버에 의해 송신된 네트워크 어드레스에 기초하는 것을 포함하여, 하나 이상의 파라미터들에 기초하여 임의의 수의 알고리즘 가중 표결 방식들 및 투표 값 계산들을 이용할 수 있다.

[0035] 도 1은 하나 이상의 실시예들에 따른 통신 네트워크(100)를 도시한다. 도 1에 도시된 바와 같이, 통신 네트워크(100)는 마스터 노드(110) 및 다수의 멤버 노드들(예컨대, 멤버 노드 A(120A), 멤버 노드 B(120B), 멤버 노드 C(120C))을 포함하는 다수의 노드들을 갖는다. 각각의 노드(예컨대, 110, 120A, 120B, 120C)는 유선 및/또는 무선 채널들을 사용하여 데이터를 교환하는 하나 이상의 컴퓨팅 디바이스들(예컨대, 메인프레임들, 서버들, 라우터들, PC(personal computers), 태블릿 PC, 스마트 폰들, 컴퓨팅 디바이스들의 네트워크 등)에 대응할 수 있다. 더욱이, 각각의 노드(110, 120A, 120B, 120C)는 유선 및/또는 무선 채널들을 사용하여 다른 노드들(110, 120A, 120B, 120C)과 데이터를 교환할 수 있다. 데이터는 다른 노드(110, 120A, 120B, 120C)에 송신되기 전에 암호화될 수 있다.

[0036] 하나 이상의 실시예들에서, 각각의 멤버 노드(120A, 120B, 120C)는 멤버(예컨대, 비즈니스 엔티티, 정부 기관 또는 부서, 군사 기관, 자선 단체, 교육 기관, 공공 안전 기관, 경찰서, 소방서, 응급 의료 서비스 제공자 등)에 대응한다. 예컨대, 멤버 노드 A(120A), 멤버 노드 B(120B), 및 멤버 노드 C(120C)는 각각 멤버 A, 멤버 B 및 멤버 C에 대응한다. 각각의 멤버는 하나 이상의 사용자들 또는 최종 사용자들(예컨대, 직원들, 계약자들, 자원 봉사자들, 학생들 등)을 가질 수 있다. 최종 사용자들은 노드들(110, 120A, 120B, 120C)과 데이터를 교환하기 위해 그리고/또는 동일한 멤버 또는 상이한 멤버에 속하는 다른 사용자들과 통신하기 위해 사용자 컴퓨팅 디바이스들을 동작시킬 수 있다. 예를 들어, 멤버 A의 최종 사용자들은 일 세트의 사용자 컴퓨팅 디바이스들(130A)을 동작시킬 수 있고, 멤버 B의 최종 사용자들은 다른 세트의 사용자 컴퓨팅 디바이스들(130B)을 동작시킬 수 있고, 멤버 C의 최종 사용자들은 또 다른 세트의 사용자 컴퓨팅 디바이스들(130C)을 동작시킬 수 있다.

[0037] 하나 이상의 실시예들에서, 위에서 논의된 바와 같이, 각각의 멤버에는 네트워크 아이덴티티("NI")가 할당된다. 개정된 NI는 NI 내의 하나 이상의 속성들이 추가, 제거, 수정될 때 생성될 수 있다. NI 또는 개정된 NI의 하나 이상의 속성들은 해싱될 수 있다.

[0038] 도 1을 계속 참조하면, 마스터 노드(110)는 마스터 블록체인(115)을 포함한다. 마스터 블록체인(115)의 하나 이상의 블록들은 멤버의 NI뿐만 아니라 멤버에 관한 임의의 추가적인 정보를 포함할 수 있다. 마스터 블록체인(115)은 아래에서 논의되는 검증된 또는 신뢰되는 멤버들의 기록을 유지한다. 멤버가 자신의 NI를 변경하고 수정하는 경우, 그 멤버는 아래에서 논의되는 바와 같이, 재검증될 때까지 마스터 블록체인으로부터 제거될 수 있다. 검증되지 않은 당사자들, 예컨대 미검증된 당사자들은 이들이 검증 프로세스를 통과할 때까지 마스터 블록체인에 기록되지 않는다.

[0039] 도 1에 또한 도시된 바와 같이, 각각의 멤버 노드(120A, 120B, 120C)는 멤버 블록체인(예컨대, 멤버 블록체인 A(125A), 멤버 블록체인 B(125B), 멤버 블록체인 C(125C))을 포함한다. 하나 이상의 실시예들에서, 멤버 블록체인(125A, 125B, 125C)은 멤버에 대한 NI를 저장한다. 멤버 블록체인은 최소의 루트 블록으로 구성되며, 이는 NI(또는 NI의 해시)로부터 도출될 수 있다. 하나 이상의 실시예들에서, 멤버 블록체인(125A, 125B, 125C)은 멤버에 속하는 각각의 사용자에 대한 아이덴티티 정보(예컨대, 이름, 이메일 어드레스, 전화 번호, MAC 어드레스, IP 어드레스 등)를 저장한다. 하나 이상의 실시예들에서, 멤버 블록체인 원장(125A, 125B, 125C)은 또한, 멤버의 이전 사용자들(예컨대, 퇴직한 직원들, 해고된 직원들, 졸업생들 등)에 대한 아이덴티티 정보를 저장한다.

[0040] 비-제한적인 예로서, 멤버 노드 A는 워싱톤 카운티 경찰국에 의해 동작된다. 워싱톤 카운티 경찰국의 네트워크 관리자는 블록체인에 추가 또는 새로운 간부들 또는 직원들과 같은 멤버 블록체인 A를 유지할 수 있다. 네트워크 관리자는 또한, 직원이 더 이상 워싱톤 카운티 경찰국에 의해 고용되지 않는다는 표시를 블록에 포함시킴으로써 과거의 직원들, 이를 테면, 퇴직했거나 해고된 직원들을 제거할 수 있다.

[0041] 마스터 블록체인(115) 및 하나 이상의 멤버 블록체인들, 예컨대, 멤버 블록체인(120A)은 통신 세션 동안, 서로를 알지 못할 수 있는 최종 사용자들(이를 테면, 한번도 만난 적이 없는 상이한 경찰서들로부터의 간부들) 사이의 신뢰를 평가하기 위해 사용될 수 있다. 알려지지 않은 최종 사용자와의 통신 세션(예컨대, 이메일, 인스턴트 메시징, 전화 호출, 문자 메시지, 파일 전송 등) 전에 또는 그 동안, 알려지지 않은 최종 사용자를 "신뢰되는"

또는 "신뢰되지 않는" 것으로 분류하는 것이 바람직하다. "신뢰되는" 사용자는 또한 인증된 사용자로 지칭될 수 있다. 이러한 분류/인증은 마스터 블록체인(115) 및 멤버 블록체인(120A, 120B, 120C) 둘 모두를 사용하여 달성될 수 있다. 구체적으로, 미지의 최종 사용자가 검증된 멤버(즉, 마스터 블록체인(115)이 멤버의 NI를 포함함)에 속하고, 미지의 최종 사용자의 아이덴티티 정보가 검증된 멤버의 멤버 블록체인(125A, 125B, 125C)에 저장되는 경우, 미지의 최종 사용자는, 검증된 멤버와 연관되지 않은 미지의 최종 사용자보다 신뢰될 수 있거나 적어도 더 높은 신뢰 레벨을 가질 수 있다.

[0042] 도 2는 도 1의 마스터 노드(110)와 같은 예시적인 마스터 노드를 도시한다. 도 2에 도시된 바와 같이, 마스터 노드(110)는 마스터 블록체인(115), 관계형 원장(240), 마스터 블록체인 제어기(260), 인증 모듈(299) 및 신뢰되는 집계 모듈(270)을 포함하는 다수의 컴포넌트들을 갖는다. 이러한 컴포넌트들 각각은 동일한 컴퓨팅 디바이스(예컨대, 서버, 메인프레임, PC(personal computer), 태블릿 PC, 스마트 폰 등) 상에서 또는 유선 및/또는 무선 채널들에 의해 연결된 다수의 컴퓨팅 디바이스들 상에서 구현될 수 있다.

[0043] 관계형 원장(240)은 관계형 데이터베이스로서 또는 그 자신의 블록체인 원장을 포함하는 임의의 다른 타입의 데이터 구조로서 구현될 수 있다. 도 2에 도시된 바와 같이, 관계형 원장(240)은 하나 이상의 미검증된 MIHB(예컨대, 미검증된 MIHB 1(242), 미검증된 MIHB 2(252))를 저장한다. 각각의 미검증된 MIHB(242, 252)는 검증을 추구하는 멤버의 NI 또는 재검증을 추구하는 멤버의 개정된 NI를 포함한다. 예컨대, 멤버 C가 검증을 추구하는 새로운 멤버라고 가정한다. 따라서, 미검증된 MIHB 1(242)은 멤버 C(244)의 NI를 포함한다. 다른 예로서, 이미 검증된 멤버 B가 자신의 물리적 어드레스를 변경한 것과 같이 자신의 NI를 수정했다고 가정한다. 따라서, 미검증된 MIHB 2(252)는 멤버 B(254)의 개정된 NI를 포함한다.

[0044] 하나 이상의 실시예들에서, 각각의 미검증된 MIHB는 인증 모듈(299)에 의해 생성된다. 따라서, 인증 모듈(299)은 미검증된 MIHB들(242, 252)을 생성하는 데 요구되는 동작들, 예컨대 해싱을 수행한다.

[0045] 하나 이상의 실시예들에서, 관계형 원장(240)은 또한, 미검증된 MIHB들(242, 252) 각각에 대한 표결 수집들(예컨대, 표결 수집 1(248), 표결 수집 2(258))을 저장한다. 표결 수집(248, 258)의 표결 값들은 검증된 멤버들의 사용자들에 의해 생성되며, 이들 사용자들이 미검증된 멤버(또는 재검증을 추구하는 멤버)의 사용자들의 아이덴티티들에 대해 갖는 신뢰도/신뢰를 표현할 수 있다. 따라서, 이들 표결 값들은 또한, 적어도 간접적으로, 이들 사용자가 대응하는 미검증된 MIHB에서 NI 또는 개정된 NI의 정확성 및 적법성에 대해 갖는 신뢰도/신뢰를 표현할 수 있다. 예를 들어, 표결 수집 1(248)은 검증된 멤버들의 다양한 최종 사용자들로부터의 표결 값들을 포함하며, 여기서 표결 값들은 미검증된 멤버 C의 하나 이상의 최종 사용자들이 신뢰될 수 있는지 여부를 표시한다. 이 예에서, 미검증된 멤버 C의 최종 사용자들은 그들이 신뢰할 수 있는 것으로 표시된 충분한 수의 표결들을 누적했으며, 멤버 C는 검증된 멤버로서 마스터 블록체인(115)에 추가될 수 있다. 대안적으로, 검증된 멤버들의 최종 사용자들은 미검증된 멤버의 최종 사용자에 대한 표결에 추가하여 또는 그 대신에 미검증된 멤버(예컨대, 멤버 C)에 대해 표결할 수 있다. 하나 이상의 실시예들에서, 검증된 멤버들의 사용자들은 미검증된 멤버(예컨대, 멤버 C) 또는 재검증을 추구하는 검증된 멤버(예컨대, 멤버 B)의 사용자들과의 통신 세션들 전에, 그 동안 또는 그 후에 표결한다.

[0046] 하나 이상의 실시예들에서, 신뢰 집계 모듈(TTM)(270)은 대응하는 표결 수집들(248, 258) 내의 표결 값들에 기초하여 미검증된 MIHB 블록들(242, 252)에서 각각의 NI 또는 개정된 NI에 대한 신뢰 스코어를 계산하도록 구성된다. 신뢰 스코어는 표결 수집에서 표결 값들을 합산 또는 평균함으로써 계산될 수 있다. 더욱이, 상이한 사용자들의 표결 값들에 상이한 가중치들이 할당될 수 있다. 가중치들은: 사용자가 멤버에 얼마나 오래 속하는지 및 멤버가 얼마나 오래 검증되었는지(즉, 검증 타임스탬프), 검증된 멤버의 사용자와 검증 또는 재검증을 추구하는 멤버의 사용자 사이의 통신 세션의 지속기간, 통신 세션의 타입, 검증된 멤버의 사용자와 검증 또는 재검증을 추구하는 멤버의 사용자 사이의 거리, 검증된 멤버의 사용자가 얼마나 자주 표결하는지, 검증된 멤버의 사용자가 얼마자 자주 통신 세션들을 개시하거나 참여하는지, 표결할 때 사용자의 네트워크 어드레스 등 중 하나 이상에 기초하여 결정될 수 있다. 신뢰 스코어는 추가적인 표결 값들이 수신될 때 업데이트될 수 있다. 더욱이, 검증 또는 재검증을 추구하는 멤버의 사용자와의 통신 세션 이전에, 그 동안 및/또는 그 후에 현재 신뢰 스코어가 검증된 멤버의 사용자에게 송신 및 디스플레이될 수 있다.

[0047] 하나 이상의 실시예들에서, TTM(270)은 또한 계산된 신뢰 스코어와 신뢰 임계 값 사이의 비교를 실행하도록 구성된다. 하나 이상의 실시예들에서, 신뢰 스코어가 신뢰 임계 값을 충족(예컨대, 동일하거나 초과)하면, 미검증된 MIHB에 대응하는 멤버는 각각 검증을 위해 승인되거나 또는 새로운 멤버 또는 개정된 NI를 갖는 검증된 멤버의 경우에 재검증을 위해 승인된다.

[0048] 도 2에 도시된 바와 같이, 마스터 블록체인(115)은 제네시스 블록(205) 및 다수의 검증된 MIHB들(예컨대, 검증된 MIHB 1(210), 검증된 MIHB 2(220), 검증된 MIHB 3(230))을 포함하는 다수의 블록들을 갖는다. 각각의 검증된 MIHB(210, 220, 230)는 검증된 또는 재검증된 멤버에 대응할 수 있다. 각각의 검증된 MIHB(210, 220, 230)는 검증된 멤버의 NI(예컨대, 멤버 A NI(212), 멤버 B NI(222)) 또는 재검증된 멤버의 개정된 NI(예컨대, 멤버 D의 개정된 NI(232))를 포함할 수 있다. 추가로, 각각의 검증된 MIHB(210, 220, 230)는 미검증된 MIHB 해시(219, 229, 239)를 포함할 수 있다. 미검증된 MIHB 해시(219, 229, 239)는 TTM에 의해 생성된 대응하는 신뢰 스코어로부터 생성된 해시, 및/또는 미검증된 블록이 저장된 미검증된 MIHB 블록체인 또는 고유한 데이터베이스 로케이터로부터의 연관된 블록 해시일 수 있다. 또한 추가로, 각각의 검증된 멤버 블록(210, 220, 230)은 또한 이전(즉, 바로 이전) 블록의 해시를 포함할 수 있다. 다시 말해서, 이전 블록 해시(216)는 제네시스 블록(205)의 해시이다. 유사하게, 이전 블록 해시(226)는 검증된 멤버 블록 1(210)의 해시이다. 또한, 이전 블록 해시(236)는 검증된 멤버 블록 3(230) 직전에 검증된 멤버 블록(미도시)의 해시이다. 도 2의 마스터 블록체인(115)은 각각의 블록이 단일 검증된 멤버를 기록하는 것을 예시하지만, 마스터 블록체인(115)은 그렇게 제한되지 않는다(예컨대, 각각의 블록은 하나보다 많은 검증된 멤버를 기록할 수 있음). 마스터 블록체인(115)의 블록들은 또한, 검증된 멤버들과 연관된 다른 정보, 이를 테면, 마스터 블록체인(115)에 추가될 때 멤버가 수신한 표결들과 연관된 정보를 기록할 수 있다.

[0049] 하나 이상의 실시예들에서, 제네시스 블록(205)은 통신 네트워크(100)의 이름 공간, 네트워크 인스턴스화의 날짜 및 시간, 통신 네트워크(100)의 위치, 제1 생성자 아이덴티티, 통신 네트워크(100)의 하나 이상의 라우팅 또는 다른 머신 요소들의 MAC 어드레스, 통신 네트워크(100)의 제1 멤버 또는 멤버들 ID 등을 포함하는 임의의 관련 데이터로부터 형성된 식별 스트링(도시되지 않음)을 포함한다. 제네시스 블록(205)은 또한 넌스를 포함할 수 있다.

[0050] 하나 이상의 실시예들에서, 마스터 블록 제어기(260)는 멤버에 대응하는 새로운 검증된 MIHB를 마스터 블록체인(115)에 삽입함으로써 멤버를 검증하거나 재검증하도록 구성된다. 새로운 검증된 MIHB는 멤버에 대응하는 미검증된 MIHB에 기초하여 생성된다. 다시 말해서, 새로운 검증된 MIHB는 대응하는 미검증된 MIHB로부터의 NI 또는 개정된 NI를 포함하고, 이러한 미검증된 블록이 저장된 미검증된 MIHB 블록체인 또는 고유한 데이터베이스 로케이터로부터의 연관된 블록 해시 및 TTM에 의해 생성된 대응하는 신뢰 스코어를 그의 해싱 입력에 포함할 수 있다. 새로운 검증된 MIHB는 또한 대응하는 미검증된 MIHB에 마지막 검증된 블록 해시를 포함할 수 있다.

[0051] 하나 이상의 실시예들에서, 마스터 블록 제어기(260)는 멤버가 미검증된 것을 나타내는 블록을 마스터 블록체인(115)에 추가함으로써, 마스터 블록체인으로부터 멤버를 효과적으로 제거하도록 구성된다(멤버가 검증된 것에서 미검증된 것으로 변환됨). 마스터 블록 제어기(260)는 다양한 이유들로 멤버를 미검증할 수 있다. 그 이유들은, 검증된 MIHB를 유지하기 위해, 멤버의 계산된 신뢰 스코어가 확립된 신뢰 값 임계치 미만으로 떨어진 것을 포함할 수 있다. 이는, 예컨대, 네트워크 사용 비활동, 멤버의 NI 정보의 과도한 또는 실질적인 변화들, 또는 대상 멤버가 사기에 관여하고 있다는 하나 이상의 다른 멤버 사용자들로부터의 확인을 수신하는 것과 같은 그러나 이에 제한되지 않는 다른 이벤트 트리거들로부터 발생할 수 있다. 따라서, 마스터 블록체인은, 멤버들의 불변성 또는 변조 방지 레코드 기록, 및 멤버들이 커뮤니티/산업에서 어떻게 지각되는지를 포함할 수 있다.

[0052] 도 3은 하나 이상의 실시예들에 따른 멤버 노드 B(120B)를 도시한다. 도 3에 도시된 바와 같이, 멤버 노드 B(120B)는 멤버 블록체인 B(125B) 및 멤버 블록체인 제어기(350)를 포함하는 다수의 컴포넌트들을 갖는다. 이러한 컴포넌트들 각각은 동일한 컴퓨팅 디바이스(예컨대, 서버, 메인프레임, PC(personal computer), 태블릿 PC, 스마트 폰 등) 상에서 또는 유선 및/또는 무선 채널들에 의해 연결된 다수의 컴퓨팅 디바이스들 상에서 구현될 수 있다.

[0053] 도 3에 도시된 바와 같이, 멤버 블록체인 B(125B)는 루트 블록(305) 및 다수의 멤버 블록들(예컨대, 멤버 블록 1(310), 멤버 블록 2(320), 멤버 블록 3(330))을 포함한다. 루트 블록(305)은 멤버 B(222)에 대한 NI(또는 멤버 B(222)에 대한 NI의 해시 값) 및 넌스(도시되지 않음)를 포함할 수 있다. 각각의 멤버 블록(310, 320, 330)은 현재 또는 이전에 멤버 B에 속하는 사용자 및/또는 멤버 B의 NI에 대한 개정에 대응할 수 있다. 예컨대, 멤버 블록 1(310) 및 멤버 블록 2(320)는 멤버 B에 속하는 사용자들(예컨대, 사용자 1, 사용자 2)에 대응한다. 대조적으로, 멤버 블록 3(330)은 멤버 B에 대한 NI에 대한 개정에 대응한다. 도 2의 멤버 블록체인(125B)은 각각의 블록이 단일 최종 사용자를 기록하는 것을 예시하지만, 멤버 블록체인(125B)은 그렇게 제한되지 않는다(예컨대, 각각의 블록은 최종 사용자보다 더 많은 것을 기록할 수 있고, 각각의 블록은 최종 사용자들 또는 멤버 B에 관한 추가 정보를 기록할 수 있는 등등이다).

[0054] 하나 이상의 실시예들에서, 사용자에 대응하는 멤버 블록들은 사용자의 하나 이상의 아이덴티티 속성들(예컨대, 이름, 이메일 어드레스, 전화 번호, 물리적 어드레스, 사용자에 의해 동작되는 컴퓨팅 디바이스의 MAC 어드레스, 사용자의 IP 어드레스 등)을 포함한다. 따라서, 멤버 블록 1(310) 및 멤버 블록 2(320)는 사용자 1(312)의 아이덴티티 속성들 및 사용자 2(322)의 아이덴티티 속성들을 각각 포함한다. 하나 이상의 실시예들에서, 개정된 NI에 대응하는 멤버 블록들은 개정된 NI를 포함한다. 따라서, 멤버 블록 3(330)은 멤버 B(254)에 대한 개정된 NI를 포함한다. 도 3에 도시된 바와 같이, 각각의 멤버 블록(310, 320, 330)은 또한 이전(즉, 바로 이전) 블록의 해시를 포함할 수 있다. 다시 말해서, 이전 블록 해시(314)는 루트 블록(305)의 해시이다. 유사하게, 이전 블록 해시(324)는 멤버 블록 1(310)의 해시이다. 또한, 이전 블록 해시(334)는 멤버 블록 3(230) 직전의 멤버 블록(미도시)의 해시이다.

[0055] 하나 이상의 실시예들에서, 멤버 블록체인 제어기(350)는 멤버 블록들(310, 320, 330)을 생성하여 멤버 블록체인 B(125B)에 추가하도록 구성된다. 추가로, 멤버 블록체인 제어기(350)는 루트 노드(305)를 생성하고 멤버 블록체인 B(125B)를 시작하도록 구성될 수 있다. 하나 이상의 실시예들에서, 멤버 블록체인 제어기(350)는 아래에서 논의되는 바와 같이, 다른 멤버들의 최종 사용자들을 식별하기 위해 다른 멤버들의 블록체인들을 검사하도록 구성된다.

[0056] 도 3은 멤버 노드 B(120B)만을 도시하지만, 모든 멤버 노드들(120A, 120C)은 도 3에 도시된 것들과 유사한 컴포넌트들을 가질 수 있다. 추가로, 도 3은 단지 하나의 멤버 블록체인만을 갖는 멤버 노드 B(120B)를 도시하지만, 다른 실시예들에서, 멤버 노드는 (아래에서 논의되는) 다수의 멤버 블록체인들을 가질 수 있다.

[0057] 도 4는 하나 이상의 실시예들에 따른 흐름도를 도시한다. 도 4의 흐름도는 통신 네트워크를 관리하고 그리고/또는 통신 네트워크의 멤버들을 검증하기 위한 프로세스를 도시한다. 프로세스는 도 1 및 도 2를 참조하여 위에서 논의된 마스터 노드(110)의 하나 이상의 컴포넌트들에 의해 수행될 수 있다. 하나 이상의 실시예들에서, 도 4에 도시된 단계들 중 하나 이상은 생략, 반복 및/또는 도 4에 도시된 순서와는 상이한 순서로 수행될 수 있다. 따라서, 범위는 도 4에 도시된 단계들의 특정 배열로 제한되는 것으로 간주되지 않아야 한다. 도 4에 도시된 단계들은, 명령어들이 실행될 때, 프로세서로 하여금 도 4의 프로세스를 수행하게 하는 컴퓨터-판독가능 매체들 상에 저장된 컴퓨터-판독가능 명령어들로서 구현될 수 있다.

[0058] 초기에, 통신 네트워크에서 멤버의 네트워크 아이덴티티(NI)가 획득된다(단계(405)). 멤버는 미검증되고 검증을 추구할 수 있다. 위에서 논의된 바와 같이, NI는 멤버의 하나 이상의 식별 속성들 또는 연락처 정보, 멤버의 하나 이상의 고유한 검증 속성들, 및/또는 멤버가 통신 네트워크의 일부가 되는 데 필요한 하나 이상의 속성들을 포함할 수 있다.

[0059] 단계(410)에서, 미검증된 MIHB가 멤버에 대해 생성된다. 미검증된 MIHB는 멤버의 NI를 포함할 수 있다. 미검증된 MIHB는 또한 통신 네트워크에 대한 마스터 블록체인에 가장 최근에 첨부된 블록의 해시를 포함할 수 있다. 미검증된 MIHB는 관계형 원장에 저장될 수 있다.

[0060] 단계(415)에서, 표결 값들이 획득된다. 하나 이상의 실시예들에서, 표결 값들은 검증된 멤버들에 속하는 사용자들에 의해 생성되고, 이러한 사용자들이 미검증된 멤버의 사용자들의 아이덴티티들에 대해 갖는 신뢰/신뢰도를 나타낸다. 따라서, 이들 표결 값들은 또한, 적어도 간접적으로, 이들 사용자가 NI의 정확성 및 적법성에 관해 갖는 신뢰도/신뢰를 표현할 수 있다. 검증된 멤버들에 속하는 최종 사용자들은 NI를 갖는 미검증된 멤버의 최종 사용자들과의 통신 세션들(예컨대, 이메일, 전화 호출들, 인스턴트 메시징, 문자 메시지, 파일 전송들 등) 전에, 그 동안 또는 후에 표결 값들을 캐스팅할 수 있다. 표결 값들은 관계형 저장소에 저장되고 미검증된 MIHB에 링크될 수 있다.

[0061] 단계(420)에서, 표결 값들에 기초하여 미검증된 멤버에 대한 신뢰 스코어가 생성된다. 인증 스코어는 표결 값들을 합산 또는 평균함으로써 생성될 수 있다. 하나 이상의 실시예들에서, 상이한 최종 사용자들로부터의 표결 값들에 상이한 가중치들이 할당될 수 있다(위에서 논의됨).

[0062] 단계(425)에서, 신뢰 스코어가 신뢰 임계 값을 충족시키는지(예컨대, 초과하거나 동일한지) 여부가 결정된다. 신뢰 스코어가 신뢰 임계 값을 충족시키는 것으로 결정될 때, 미검증된 멤버는 검증을 위해 승인되고, 프로세스는 단계(430)로 진행한다. 신뢰 스코어가 신뢰 임계 값을 충족시키지 않는 것으로 결정될 때, 미검증된 멤버는 검증을 위해 승인되는 것으로 간주되지 않고, 프로세스는 단계(435)로 진행한다.

[0063] 단계(430)에서, 미검증된 멤버가 검증된다. 멤버를 검증하는 것은 검증된 MIHB를 생성하는 것 및 검증된 MIHB를 통신 네트워크에 대한 마스터 블록체인 원장에 삽입하는 것을 포함할 수 있다. 검증된 MIHB는 미검증된 MIHB(예

컨대, 네트워크의 NI)의 모든 콘텐츠를 포함할 수 있다. 검증된 MIHB는 또한 미검증된 MIHB 및/또는 신뢰 스코어로부터 생성된 해시를 포함할 수 있다. 검증된 MIHB는 또한 마스터 블록체인 원장 내의 이전(즉, 바로 선행하는) 블록의 해시를 포함할 수 있다.

[0064] 단계(435)에 도달할 때, 미검증된 멤버가 검증되거나 미검증된 멤버가 검증을 위해 승인되지 않았다. 따라서, 단계(435)에서, 미검증된 MIHB 및 미검증된 MIHB 내의 NI에 대한 임의의 저장된 표결들은 관계형 원장으로부터 제거된다. 대안적으로, 미검증된 MIHB는, 신뢰되는 것으로 간주되고 마스터 블록체인에 추가되기에 충분한 표결들을 수신할 때까지 관계형 원장에 남아있을 수 있다. 추가로, 미검증된 MIHB는 미리 정의된 기간 동안 관계형 원장에 남아있을 수 있고, 만약 멤버가 미리 정의된 기간 내에 신뢰되는 것으로 간주되기에 충분한 표결들을 수신하지 못하면 제거될 수 있다.

[0065] 하나 이상의 실시예들에서, 도 4에 도시된 프로세스는 검증을 추구하는 각각의 부재에 대해 반복될 수 있다. 추가로, 이러한 상세한 설명의 이익을 갖는 당업자들은, 다른 검증된 멤버들의 사용자들로부터의 표결 값들 및 신뢰 스코어가 악의적인 또는 사기성 멤버가 부주의하게 검증될 가능성을 감소시킨다는 것을 인식할 것이다. 이는 적어도 네트워크 액세스 제어 및 온라인 인증의 기술 분야들에 대한 개선이다.

[0066] 도 5는 하나 이상의 실시예들에 따른 흐름도를 도시한다. 도 5의 흐름도는 통신 네트워크를 관리하고 그리고/또는 통신 네트워크의 멤버들을 재검증하기 위한 프로세스를 도시한다. 프로세스는 도 1 및 도 2를 참조하여 위에서 논의된 마스터 노드(110)의 하나 이상의 컴포넌트들에 의해 수행될 수 있다. 하나 이상의 실시예들에서, 도 5에 도시된 단계들 중 하나 이상은 생략, 반복 및/또는 도 5에 도시된 순서와는 상이한 순서로 수행될 수 있다. 따라서, 범위는 도 5에 도시된 단계들의 특정 배열로 제한되는 것으로 간주되지 않아야 한다. 더욱이, 도 5의 하나 이상의 단계들은 도 4에 도시된 프로세스 이전 또는 이후에 실행될 수 있다. 도 5에 도시된 단계들은, 명령어들이 실행될 때, 프로세서로 하여금 도 5의 프로세스를 수행하게 하는 컴퓨터-판독가능 매체들 상에 저장된 컴퓨터-판독가능 명령어들로서 구현될 수 있다.

[0067] 단계(505)에서, 개정된 NI가 획득된다. 개정된 NI는 재검증을 추구하는 검증된 멤버로부터 획득될 수 있다. 개정된 NI는 멤버의 오리지널 NI의 속성들(예컨대, 멤버의 물리적 어드레스의 변경)과 상이한 하나 이상의 속성들을 가질 수 있다.

[0068] 단계(510)에서, 개정된 NI에 대한 개정 스코어가 생성된다. 개정 스코어는 (마스터 블록체인에 저장된) 멤버에 대한 오리지널 NI와 멤버에 대한 개정된 NI 사이의 변화들의 크기를 반영할 수 있다. 개정 스코어는 오리지널 NI와 개정된 NI 사이에서 변화된 속성들의 수를 카운팅함으로써 계산될 수 있다. 더욱이, 가중치들은 속성들 중 하나 이상에 할당될 수 있다. 다시 말해서, 일부 속성들은 다른 속성들보다 더 중요하며, 이러한 중요한 속성들이 변경될 때, 이는 더 높은 개정 스코어를 초래한다.

[0069] 단계(515)에서, 개정 스코어가 주요 개정 임계치를 충족시키는지 여부가 결정된다. 개정 스코어가 주요 개정 임계치를 충족시키지 않는다고(예컨대, 그 미만인 것으로) 결정될 때, 개정된 NI는 사소한 개정들을 갖는 것으로 간주되고, 프로세스는 단계(540)로 진행한다. 개정 스코어가 주요 개정 임계치를 충족한다고(예컨대, 동일하거나 초과하는 것으로) 결정될 때, 개정된 NI는 주요 개정들을 갖는 것으로 간주되고, 프로세스는 단계(520)로 진행한다.

[0070] 단계(520)에서, 미검증된 MIHB가 멤버에 대해 생성된다. 미검증된 MIHB는 개정된 NI를 포함할 수 있다. 미검증된 MIHB는 또한 통신 네트워크에 대한 마스터 블록체인 원장에 첨부된 가장 최근 블록의 해시를 포함할 수 있다. 미검증된 MIHB는 관계형 원장에 저장될 수 있다.

[0071] 단계(525)에서, 표결 값들이 획득된다. 하나 이상의 실시예들에서, 표결 값들은 검증된 멤버들에 속하는 사용자들에 의해 생성되고, 이러한 사용자들이 재검증을 추구하는 멤버의 사용자들의 아이덴티티들에 대해 갖는 신뢰/신뢰도를 나타낸다. 따라서, 이들 표결 값들은 또한, 적어도 간접적으로, 이들 사용자가 개정된 NI의 정확성 및 적법성에 관해 갖는 신뢰도/신뢰를 표현할 수 있다. 다른 검증된 멤버들에 속하는 사용자들은 개정된 NI를 갖는 멤버의 사용자들과의 통신 세션들(예컨대, 이메일, 전화 호출들, 인스턴트 메시징, 문자 메시지, 파일 전송들 등) 전에, 그 동안 또는 후에 표결 값들을 캐스팅할 수 있다. 이들 표결 값들은 검증된 멤버들에 대응하는 멤버 노드들에 의해 사용자들의 컴퓨팅 디바이스들로부터 통신 네트워크의 마스터 노드로 중계될 수 있다. 표결들은 관계형 원장에 저장되고 미검증된 MIHB에 링크될 수 있다.

[0072] 단계(530)에서, 표결 값들에 기초하여 재검증을 추구하는 멤버에 대한 신뢰 스코어가 생성된다. 신뢰 스코어는 표결 값들을 합산 또는 평균함으로써 생성될 수 있다. 하나 이상의 실시예들에서, 상이한 사용자들로부터의 표

결 값들에 상이한 가중치들이 할당될 수 있다.

[0073] 단계(535)에서, 신뢰 스코어가 신뢰 임계 값을 충족시키는지(예컨대, 초과하거나 동일한지) 여부가 결정된다. 신뢰 스코어가 신뢰 임계 값을 충족시키는 것으로 결정될 때, 멤버는 재검증을 위해 승인되고, 프로세스는 단계(540)로 진행한다. 신뢰 스코어가 신뢰 임계 값을 충족시키지 않는 것으로 결정될 때, 멤버는 재검증을 위해 승인되는 것으로 간주되지 않고, 프로세스는 종료될 수 있다.

[0074] 단계(540)에서, 멤버가 재검증된다. 멤버를 재검증하는 것은 검증된 MIHB를 생성하는 것 및 검증된 MIHB를 통신 네트워크에 대한 마스터 블록체인 원장에 삽입하는 것을 포함할 수 있다. 검증된 MIHB는 적어도 개정된 NI를 포함한다. 검증된 MIHB는 또한 미검증된 MIHB 및/또는 신뢰 스코어로부터 생성된 해시를 포함할 수 있다. 검증된 MIHB는 또한 마스터 블록체인 원장 내의 이전(즉, 바로 선행하는) 블록의 해시를 포함할 수 있다.

[0075] 이러한 상세한 설명의 이익을 갖는 당업자들은, NI에 대한 개정들이 사소한 경우, 도 5에 도시된 프로세스가 표결 프로세스에 대한 필요성 없이 멤버가 재검증될 수 있게 한다는 것을 인식할 것이다. 다시 말해서, NI에 대한 변화들이 사소한 경우 가속된 재검증 경로가 제공된다. 이러한 가속된 재검증 경로는 정규 검증 프로세스보다 더 적은 통신 네트워크 자원들을 소비하고, 그렇지 않으면 사용자들로부터 표결 값들을 송신함으로써 소비될 통신 네트워크 상의 트래픽을 제거한다(즉, 대역폭을 증가시킨다).

[0076] 도 6은 하나 이상의 실시예들에 따른 흐름도를 도시한다. 도 6의 흐름도는 통신 네트워크를 관리하고 그리고/또는 통신 네트워크에서 의심 최종 사용자(예컨대, 미지의 최종 사용자)를 분류/인증하기 위한 프로세스를 도시한다. 프로세스는 도 1, 도 2 및 도 3를 참조하여 위에서 논의된 마스터 노드(110) 및/또는 멤버 노드(120A, 120B, 120C)의 하나 이상의 컴포넌트들에 의해 수행될 수 있다. 하나 이상의 실시예들에서, 도 6에 도시된 단계들 중 하나 이상은 생략, 반복 및/또는 도 6에 도시된 순서와는 상이한 순서로 수행될 수 있다. 따라서, 범위는 도 6에 도시된 단계들의 특정 배열로 제한되는 것으로 간주되지 않아야 한다. 더욱이, 도 6의 하나 이상의 단계들은 도 4 또는 도 5에 도시된 프로세스 이전 또는 이후에 실행될 수 있다. 도 6에 도시된 단계들은, 명령어들이 실행될 때, 프로세서로 하여금 도 6의 프로세스를 수행하게 하는 컴퓨터-판독가능 매체들 상에 저장된 컴퓨터-판독가능 명령어들로서 구현될 수 있다.

[0077] 하나 이상의 실시예들에서, 최종 사용자가 다른 최종 사용자와의 통신 세션(예컨대, 이메일, 전화 통화, 문자 메시지, 인스턴트 메시징, 파일 전송 등)을 개시하려고 시도(또는 성공적으로 개시)할 때, 통신 세션을 개시한 사용자는 의심 사용자(또는 미지의 최종 사용자)로 지칭될 수 있다. 다른 최종 사용자는 비-의심 사용자(또는 검증된 멤버에 의해 고용된 최종 사용자와 같은 알려진 최종 사용자)로 지칭될 수 있다. 추가적으로 또는 대안적으로, 제1 최종 사용자는 제2 최종 사용자와의 통신 세션을 개시하거나 이에 동의하기 전에 제2 최종 사용자를 인증하기를 원할 수 있다. 그러한 시나리오들에서, 제1 최종 사용자 및 제2 최종 사용자는 또한, 비-의심 최종 사용자 및 의심 최종 사용자로 각각 지칭될 수 있다. 더욱이, 의심 최종 사용자가 속하는(또는 속한 것으로 추정되는) 멤버는 의심 멤버로 지칭될 수 있는 한편, 비-의심 최종 사용자가 속하는 멤버는 비-의심 멤버로 지칭될 수 있다.

[0078] 초기에, 의심 최종 사용자의 아이덴티티 속성(예컨대, 이름, 사용자 이름, 이메일 어드레스, 전화 번호, 물리적 어드레스, 의심 사용자에 의해 동작되는 컴퓨팅 디바이스의 MAC 어드레스, 의심 사용자의 IP 어드레스 등)이 획득된다(단계(605)). 의심 최종 사용자의 아이덴티티 속성은 의심 최종 사용자와의 통신(예컨대, 이메일 헤더들, 네트워크 패킷들, 전화 통화들, 텍스트 메시지들, 인스턴트 메시지들 등)로부터 추출될 수 있다. 추출은 비-의심 최종 사용자에 의해 동작되는 컴퓨팅 디바이스에 의해 그리고/또는 비-의심 멤버에 대응하는 멤버 노드에 의해 실행될 수 있다.

[0079] 단계(610)에서, 의심 멤버의 NI에 있을 가능성이 있는 하나 이상의 식별 속성들이 획득된다. 의심 사용자의 아이덴티티 속성과 같이, 의심 멤버에 대한 아이덴티티 속성(들)은 의심 사용자로부터의 통신으로부터 추출될 수 있다. 추가적으로 또는 대안적으로, 아이덴티티 속성(들)은 의심 멤버로부터 직접 요청될 수 있다.

[0080] 단계(615)에서, 의심 멤버의 식별 속성들에 기초하여, 의심 멤버가 검증된 멤버인지 여부가 결정된다. 다시 말해서, 마스터 블록체인 원장이 의심 멤버의 식별 속성들을 갖는 NI를 저장하는 검증된 MIHB를 포함하는지 여부가 결정된다. 하나 이상의 실시예들에서, 이러한 결정은 매칭되는 NI(즉, 의심 멤버의 식별 속성들을 갖는 NI)의 검색에서 마스터 블록체인을 횡단하는 것을 포함한다. 마스터 노드는 비-의심 최종 사용자 및/또는 비-의심 멤버로부터의 요청 시에 마스터 블록체인을 횡단할 수 있다. 추가적으로 또는 대안적으로, 비-의심 멤버에 대응하는 멤버 노드는 마스터 블록체인 원장의 사본을 획득하고 횡단을 실행할 수 있다. 의심 멤버가 검증된 멤버인

것으로 결정될 때, 프로세스는 단계(620)로 진행한다. 의심 멤버가 미검증된 멤버인 것으로 결정될 때, 프로세스는 단계(640)로 진행한다.

[0081] 단계(620)에서, 의심 멤버의 멤버 블록체인 원장이 획득된다. 하나 이상의 실시예들에서, 비-의심 사용자 및/또는 비-의심 멤버는 의심 멤버로부터 직접 멤버 블록체인 원장을 요청할 수 있다. 비-의심 최종 사용자 및/또는 비-의심 멤버는 매칭되는 NI로부터의 연락처 정보를 활용하여 의심 멤버에게 접촉하고 멤버 블록체인을 요청할 수 있다.

[0082] 단계(630)에서, 멤버 블록체인 원장이 의심 최종 사용자의 아이덴티티 속성을 포함하는지 여부가 결정된다. 다시 말해서, 의심 최종 사용자가 현재 의심 멤버에 속하는 사용자인지 여부가 결정된다. 이러한 결정은, 비-의심 최종 사용자 또는 비-의심 멤버의 멤버 노드가 현재 사용자에 대응하고 의심 최종 사용자의 아이덴티티 속성을 갖는 블록을 검색하여 멤버 블록체인을 횡단하는 것을 수반할 수 있다. 의심 사용자가 의심 멤버에 속하는 현재 최종 사용자인 것으로 결정될 때, 프로세스는 단계(635)로 진행한다. 의심 사용자가 현재 최종 사용자가 아니라고 결정될 때(즉, 의심 사용자의 아이덴티티 속성이 멤버 블록체인에서 누락됨), 프로세스는 단계(640)로 진행할 수 있다. 멤버 블록체인을 횡단하는 동안, 아이덴티티 속성이 의심 멤버에 속하는 이전 최종 사용자(예컨대, 해고된 직원, 졸업생 등)에 대응하는 블록에서 발견되면, 의심 최종 사용자는 유효하거나 신뢰되는 최종 사용자가 아닌 것으로 간주된다.

[0083] 단계(635)에서, 의심 최종 사용자는 (마스터 블록체인 원장을 횡단함으로써 검증된) 검증된 멤버에 속하고, 검증된 멤버에 대한 멤버 블록체인 원장이 의심 사용자의 아이덴티티 속성을 포함하기 때문에, 의심 최종 사용자는 신뢰되는 것으로 분류된다. 이러한 분류는 비-의심 최종 사용자에게 보고(예컨대, 디스플레이)될 수 있다. 비-의심 최종 사용자는 이제, 의심 최종 사용자가 인증되었기 때문에, 의심 최종 사용자와의 통신 세션을 개시/참여할 수 있다.

[0084] 단계(640)에서, 의심 멤버가 미검증되고 그리고/또는 멤버 블록체인 원장이 의심 멤버의 아이덴티티 속성(들)을 갖지 않았기 때문에, 의심 최종 사용자는 위협으로서 또는 신뢰되지 않는 것으로 분류된다. 이러한 분류는 비-의심 최종 사용자에게 보고(예컨대, 디스플레이)될 수 있다. 비-의심 최종 사용자는 의심 최종 사용자와의 통신 세션을 거부 또는 종료할 수 있고 그리고/또는 의심 사용자가 인증될 수 있을 때까지 기밀 정보를 의심 최종 사용자와 공유하지 않도록 주의해야 한다.

[0085] 이러한 상세한 설명의 이익을 갖는 당업자들은, 개별적인 블록체인의 불변의 특성들과 함께 다수의 레벨들/계층들의 블록체인들을 사용함으로써, 더 안전한 사용자 인증/분류가 실행될 수 있다는 것을 인식할 것이다. 이는 적어도 네트워크 액세스 제어 및 온라인 인증 분야들에 대한 기술적 개선이다.

[0086] 도 7은 하나 이상의 실시예들에 따른 흐름도를 도시한다. 도 7의 흐름도는 통신 네트워크를 관리하고 그리고/또는 통신 네트워크에서 멤버의 NI를 개정하기 위한 프로세스를 도시한다. 프로세스는 도 1 및 도 3을 참조하여 위에서 논의된 멤버 노드(120A, 120B, 120C)의 하나 이상의 컴포넌트들에 의해 수행될 수 있다. 하나 이상의 실시예들에서, 도 7에 도시된 단계들 중 하나 이상은 생략, 반복 및/또는 도 7에 도시된 순서와는 상이한 순서로 수행될 수 있다. 따라서, 범위는 도 5에 도시된 단계들의 특정 배열로 제한되는 것으로 간주되지 않아야 한다. 더욱이, 도 7의 하나 이상의 단계들은 도 4 내지 도 6에 도시된 프로세스들 이전 또는 이후에 실행될 수 있다. 도 7에 도시된 단계들은, 명령어들이 실행될 때, 프로세서로 하여금 도 7의 프로세스를 수행하게 하는 컴퓨터-판독가능 매체들 상에 저장된 컴퓨터-판독가능 명령어들로서 구현될 수 있다.

[0087] 초기에, 멤버의 개정된 NI가 획득된다(단계(705)). 멤버는 멤버의 하나 이상의 속성들이 변경되었기 때문에 자신의 NI를 수정할 수 있다. 예컨대, 멤버는 이름들을 변경했을 수 있고, 멤버는 구성들(buildings)을 변경했을 수 있고, 멤버는 이메일 어드레스 또는 공개 IP 어드레스 등을 변경했을 수 있다.

[0088] 단계(710)에서, 새로운 블록이 멤버에 대한 멤버 블록체인 원장에 삽입된다. 새로운 블록은 개정된 NI를 포함한다. 위에서 논의된 바와 같이, 멤버 블록체인 원장은 또한 멤버에 속하는 현재 및 이전 사용자들에 대응하는 멤버 블록들을 가질 수 있다. 더욱이, 멤버 블록체인 원장의 루트 블록은 멤버에 대한 오리지널 NI를 포함할 수 있다.

[0089] 단계(720)에서, 도 5를 참조하여 위에서 논의된 바와 같이, 멤버를 재검증하기 위해, 개정된 NI가 마스터 노드에 전송된다. 재검증은 NI 블록에서 하나 이상의 미리 정의된 데이터 위치 또는 유의도(significance) 필드 값들이 변경될 때 발생할 수 있다. 개정된 NI를 갖는 전체 새로운 블록은 마스터 노드에 전송될 수 있다. 추가적으로 또는 대안적으로, 개정된 NI만이 마스터 노드에 전송될 수 있다. 마스터 노드에 전송된 데이터는 암호화될

수 있다. 마스터 노드는 NI를 포함하는 개정된 블록을 암호해독하고, 임의의 하나 이상의 유의도 변경들이 이루어졌는지 여부를 결정한다. 마스터 제어기(260)는, 멤버가 미검증된 것을 표시하는 블록을 마스터 블록체인(115)에 추가함으로써, 개정된 NI에 응답하여 멤버를 미검증할 수 있다.

[0090] 하나 이상의 실시예들에서, 단계(710) 대신에 단계(715)가 실행될 수 있다. 단계(715)에서, 멤버에 대한 새로운 멤버 블록체인 원장이 생성된다. 새로운 멤버 블록체인 원장에 대한 루트 블록은, 제1 인스턴스화에서, 마스터 네트워크 블록체인의 마지막 블록의 해시 값 및 개정된 NI를 포함한다. 추가적으로 또는 대안적으로, 새로운 멤버 블록체인에서 루트 블록 다음의 제1 블록은 기존의 멤버 블록체인 원장의 마지막 블록의 복제물(또는 그에 대한 포인터를 포함함)일 수 있다. 하나 이상의 실시예들에서, 새로운 블록들의 세트가 새로운 멤버 블록체인 원장에 추가될 수 있다. 기존의 멤버 블록체인의 블록들에 저장된 사용자 아이덴티티 정보는 새로운 블록들에 복사될 수 있다.

[0091] 본 명세서, 예컨대, 도 1에 개시된 병렬 블록체인 아키텍처는, 멤버에 의해 제어 및 인증되고 루트 멤버 네트워크 아이덴티티 하의 통신 네트워크에 대한 액세스를 갖는 관련 서브-사용자들 또는 멤버 엔드포인트들의 불변의 기록을 보장함으로써 통신 네트워크의 보안을 증가시킨다. 그 다음, 멤버 네트워크 아이덴티티는 마스터 블록체인 원장에 논리적으로 링크된다. 이는, 네트워크의 임의의 다른 멤버가 먼저 멤버의 아이덴티티를 검증할 수 있고, 이어서 마스터 네트워크 블록체인 원장을 통해 임의의 서브-사용자 또는 엔드포인트 엔티티를 조사하고 검증할 수 있고, 이어서 멤버 블록체인 블록 검증을 추구할 수 있다는 것을 보장한다.

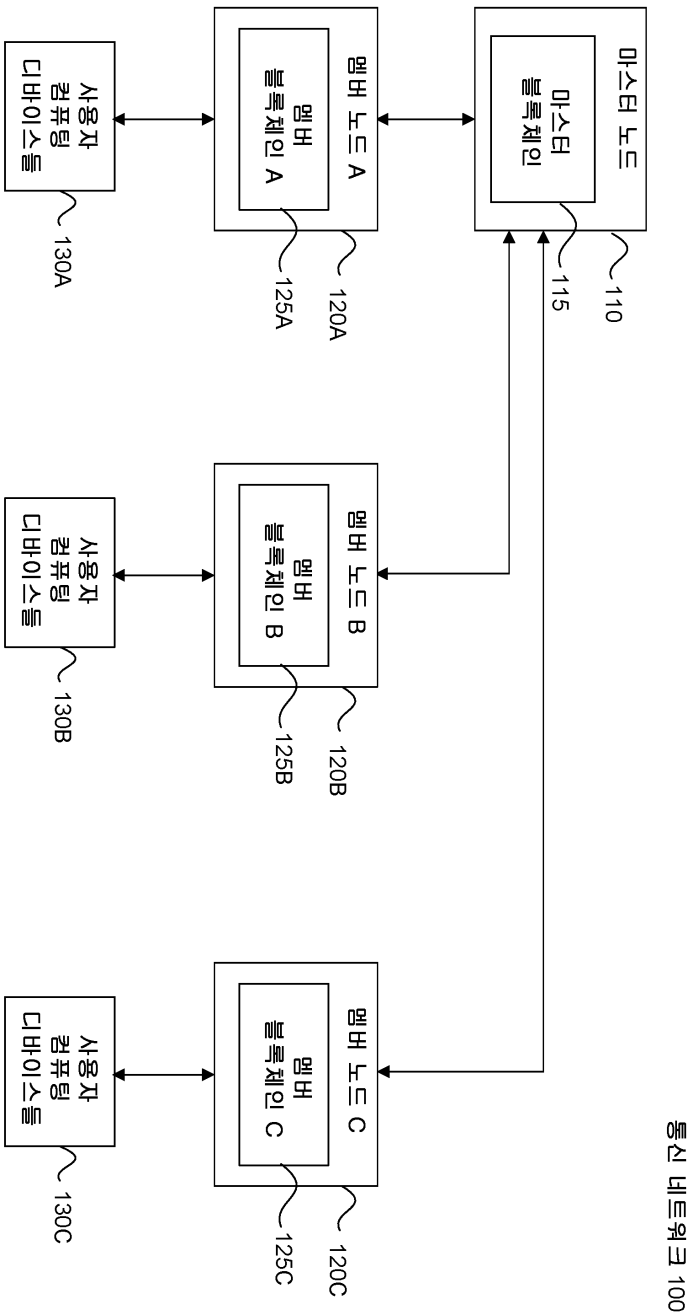
[0092] 개요 및 요약 섹션들이 아니라 상세한 설명 섹션이 청구범위를 해석하는 데 사용되도록 의도된다는 것을 인식해야 한다. 개요 및 요약 섹션들은 본 발명자(들)에 의해 고려되는 바와 같은 본 발명의 하나 이상의, 그러나 전부가 아닌 예시적인 실시예들을 제시할 수 있고, 따라서, 본 발명 및 첨부된 청구범위를 어떠한 방식으로도 제한하도록 의도되지 않는다.

[0093] 본 발명은 특정된 기능들 및 이들의 관계들의 구현을 예시하는 기능적 구축 블록들의 도움으로 위에서 설명되었다. 이들 기능적 구축 블록들의 경계들은 설명의 편의를 위해 본 명세서에서 임의적으로 정의되었다. 특정된 기능들 및 이들의 관계들이 적절하게 수행되는 한, 대안적인 경계들이 정의될 수 있다.

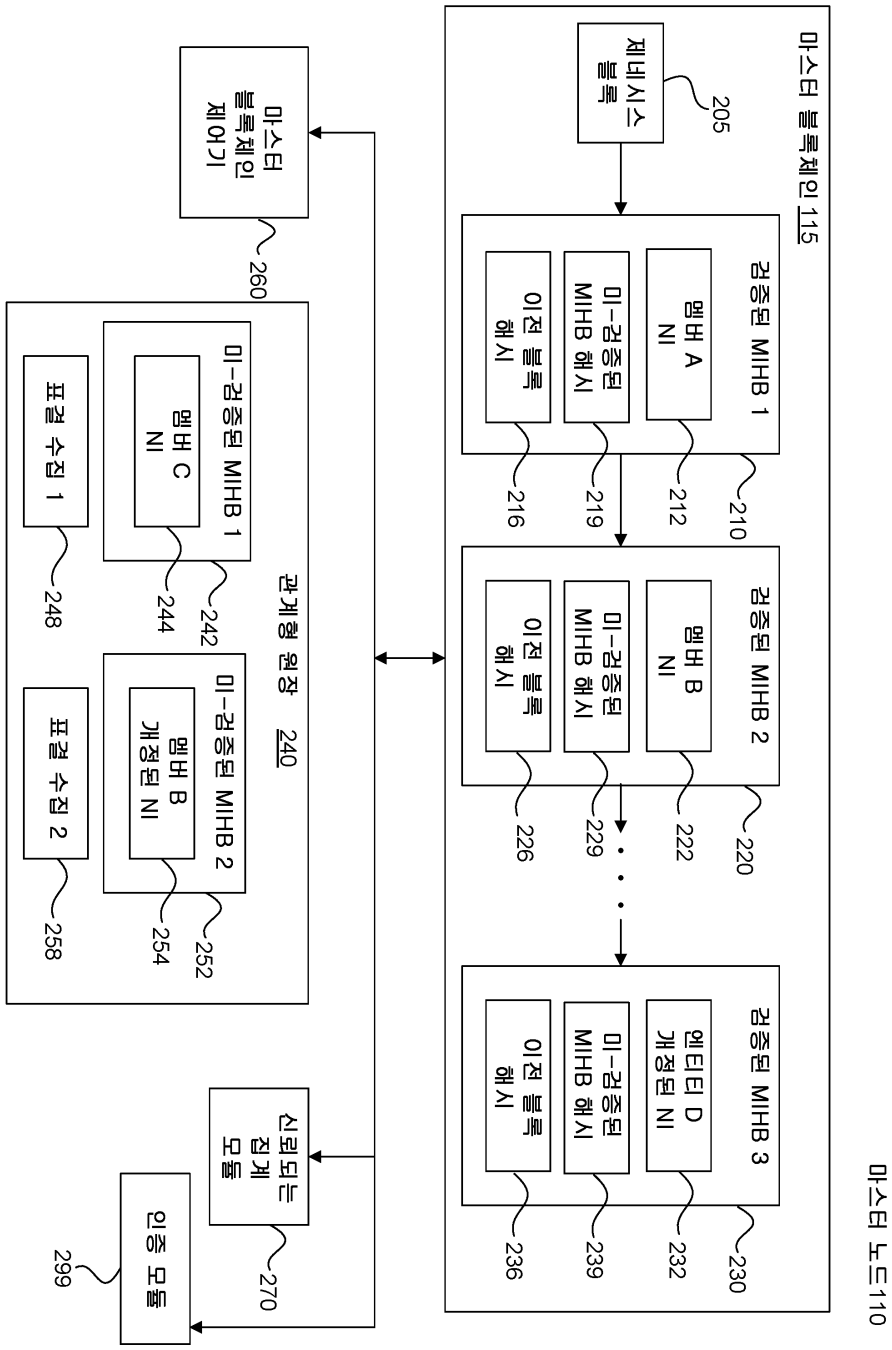
[0094] 특정 실시예들의 전술한 설명은, 본 발명의 일반적 개념을 벗어남이 없이, 과도한 실험 없이, 본 기술분야 내의 지식을 적용함으로써 다른 사람들이 이러한 특정 실시예들의 다양한 적용들을 용이하게 수정 및/또는 적응시킬 수 있도록 본 발명의 일반적 성질을 완전히 드러낼 것이다. 따라서, 그러한 적응들 및 수정들은 본 명세서에서 제시된 교시 및 안내에 기초하여, 개시된 실시예들의 등가물들의 의미 및 범위 내에 있는 것으로 의도된다. 본 명세서의 어구 또는 용어는 제한이 아니라 설명의 목적을 위한 것이며, 따라서 본 명세서의 용어 또는 어구는 교시들 및 안내의 관점에서 당업자에 의해 해석되어야 한다는 것이 이해되어야 한다.

도면

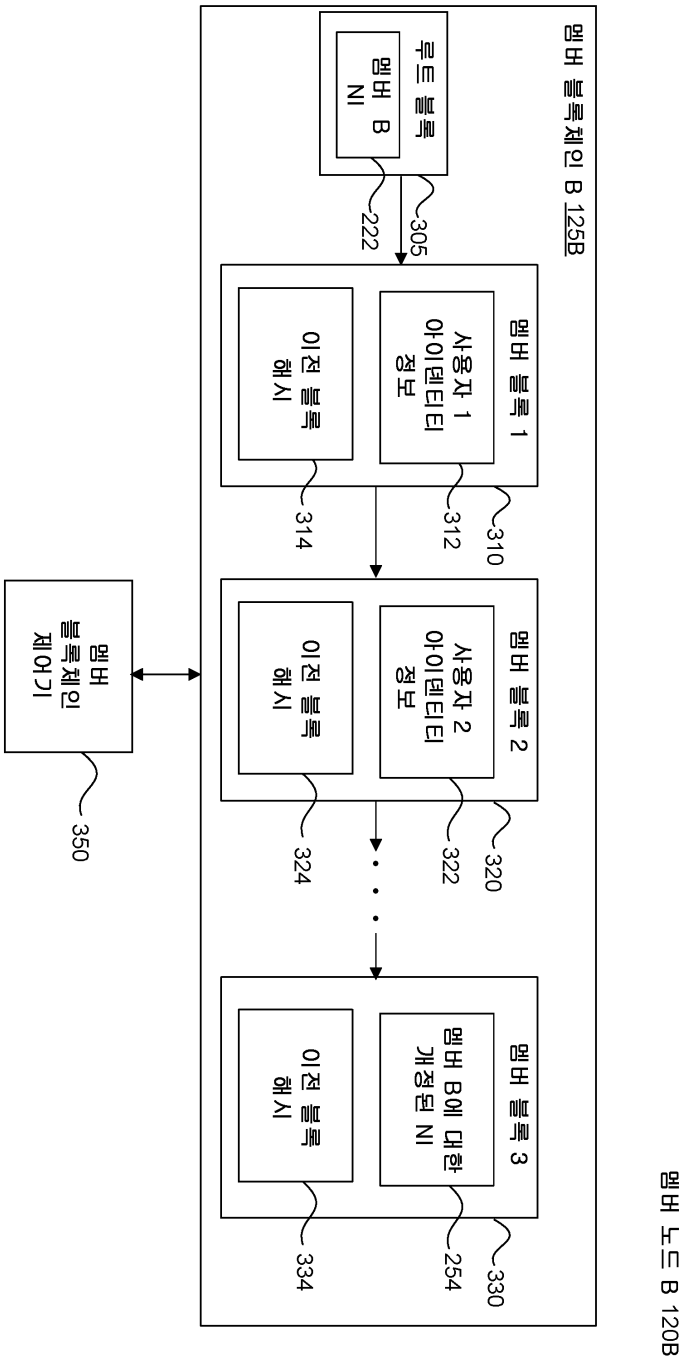
도면1


마스터 노드
마스터 블록체인
110
115
멤버 노드 A
멤버 블록체인 A
120A
125A
멤버 노드 B
멤버 블록체인 B
120B
125B
멤버 노드 C
멤버 블록체인 C
120C
125C
사용자 컴퓨팅 디바이스들
130A
130B
130C
통신 네트워크 100

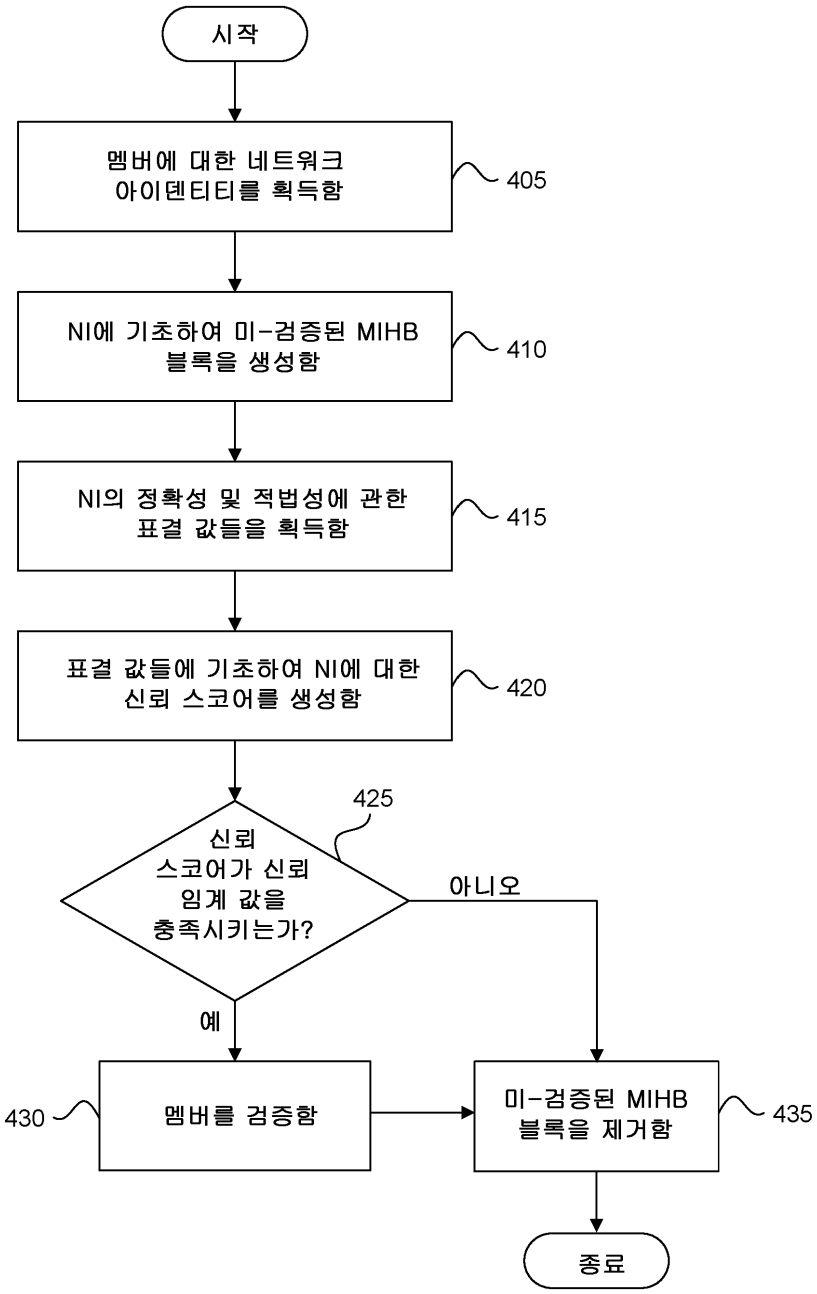
도면2


마스터 노드110
마스터 블록체인 115
제네시스 블록
205
검증된 MIHB 1
멤버 A NI
미-검증된 MIHB 해시
이전 블록 해시
210
212
219
216
검증된 MIHB 2
멤버 B NI
미-검증된 MIHB 해시
이전 블록 해시
220
222
229
226
검증된 MIHB 3
엔티티 D 개정된 NI
미-검증된 MIHB 해시
이전 블록 해시
230
232
239
236
마스터 블록체인 제어기
260
관계형 원장 240
미-검증된 MIHB 1
멤버 C NI
242
244
표결 수집 1
248
미-검증된 MIHB 2
멤버 B 개정된 NI
252
254
표결 수집 2
258
신뢰되는 집계 모듈
270
인증 모듈
299

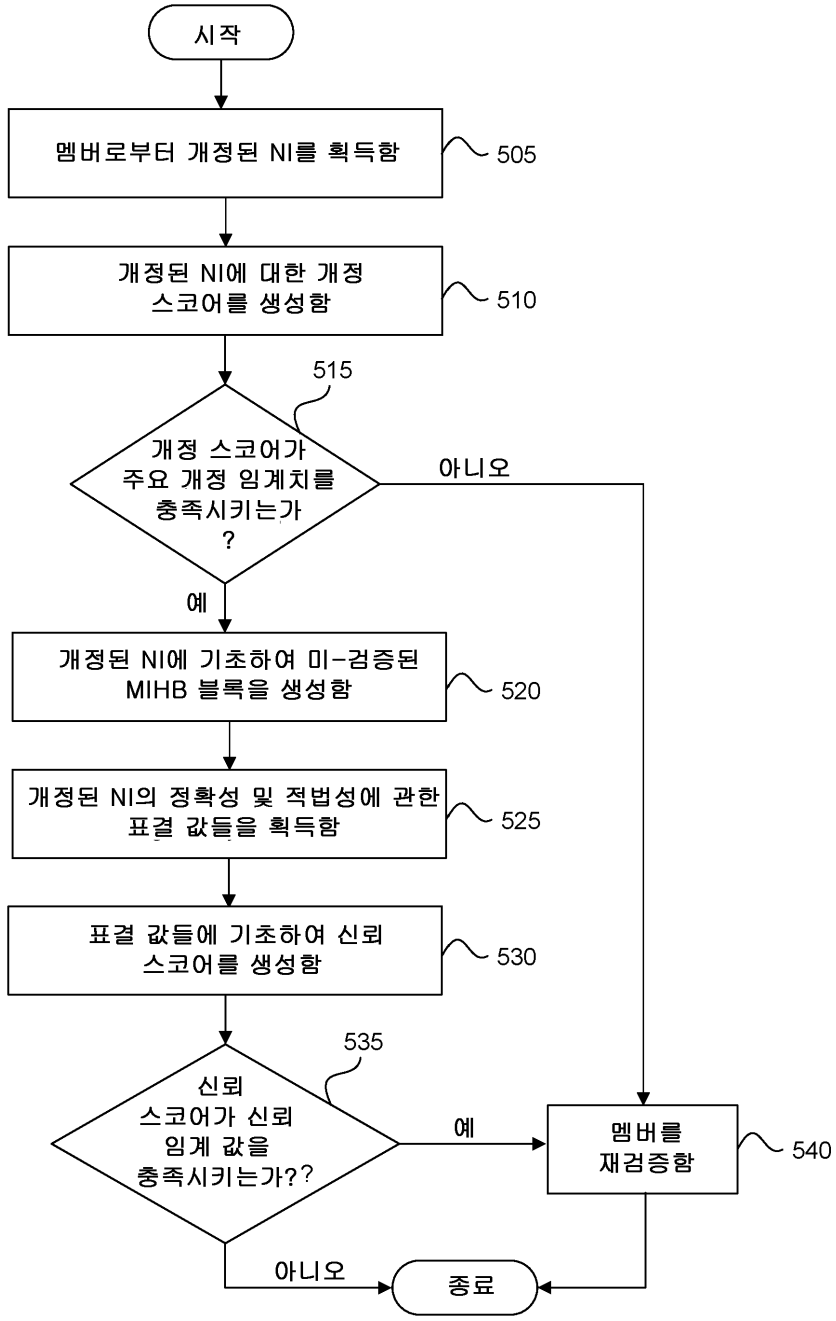
도면3


멤버 블록체인 B 125B
루트 블록
멤버 B NI
222
305
멤버 블록 1
사용자 1 아이덴티티 정보
이전 블록 해시
310
312
314
멤버 블록 2
사용자 2 아이덴티티 정보
이전 블록 해시
320
322
324
멤버 블록 3
멤버 B에 대한 개정된 NI
이전 블록 해시
330
254
334
멤버 블록체인 제어기
350
멤버 노드 B 120B

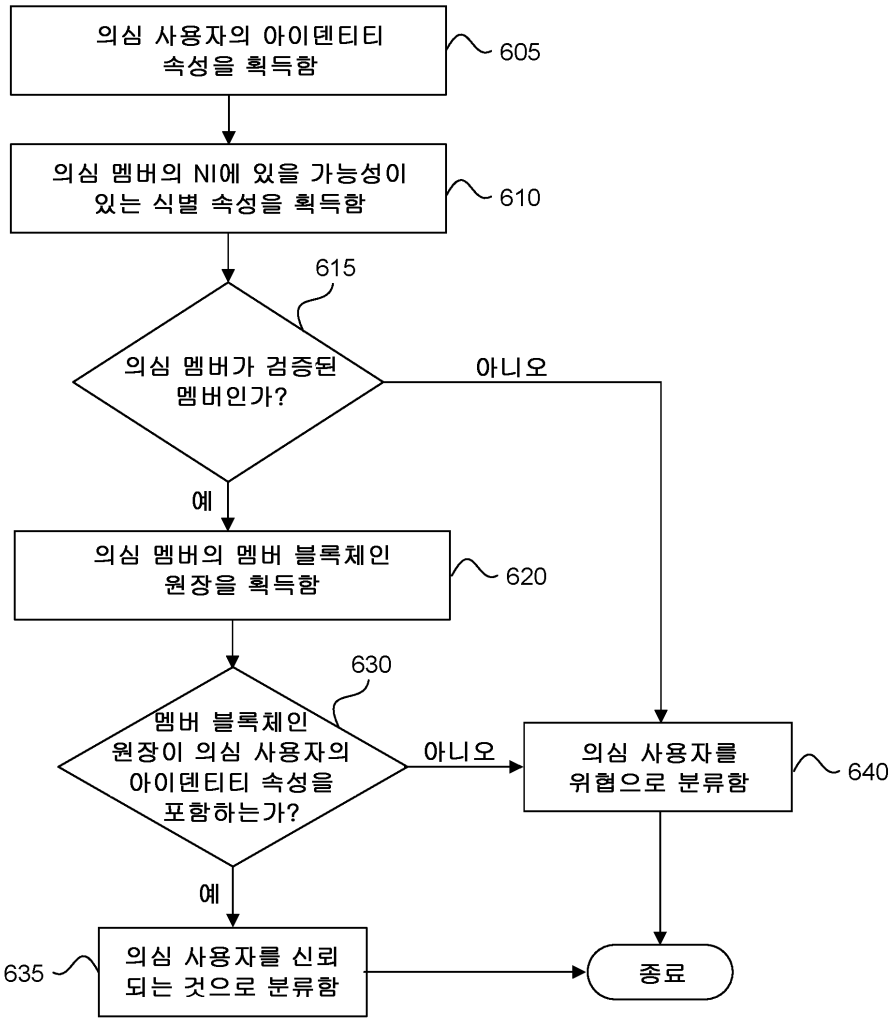
도면4


시작
멤버에 대한 네트워크 아이덴티티를 획득함
405
NI에 기초하여 미-검증된 MIHB 블록을 생성함
410
NI의 정확성 및 적법성에 관한 표결 값들을 획득함
415
표결 값들에 기초하여 NI에 대한 신뢰 스코어를 생성함
420
425
신뢰 스코어가 신뢰 임계 값을 충족시키는가?
아니오
예
430
멤버를 검증함
미-검증된 MIHB 블록을 제거함
435
종료

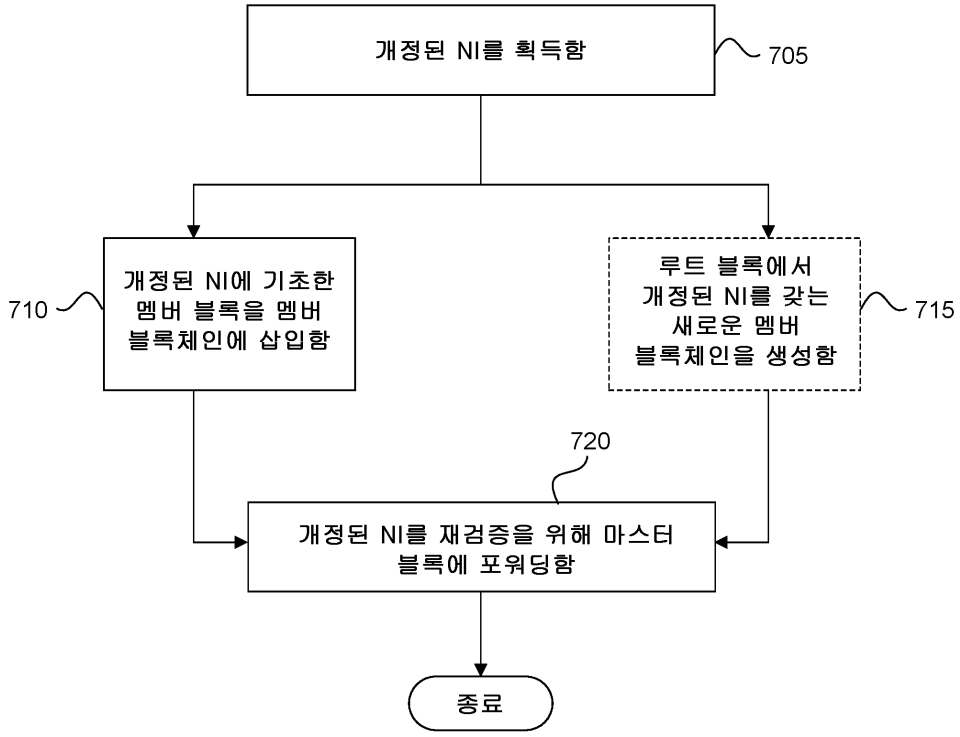
도면5


시작
멤버로부터 개정된 NI를 획득함
505
개정된 NI에 대한 개정 스코어를 생성함
510
515
개정 스코어가 주요 개정 임계치를 충족시키는가 ?
아니오
예
개정된 NI에 기초하여 미-검증된 MIHB 블록을 생성함
520
개정된 NI의 정확성 및 적법성에 관한 표결 값들을 획득함
525
표결 값들에 기초하여 신뢰 스코어를 생성함
530
535
신뢰 스코어가 신뢰 임계 값을 충족시키는가??
예
멤버를 재검증함
540
아니오
종료

도면6


의심 사용자의 아이덴티티 속성을 획득함
605
의심 멤버의 NI에 있을 가능성이 있는 식별 속성을 획득함
610
615
의심 멤버가 검증된 멤버인가?
아니오
예
의심 멤버의 멤버 블록체인 원장을 획득함
620
630
멤버 블록체인 원장이 의심 사용자의 아이덴티티 속성을 포함하는가?
아니오
의심 사용자를 위협으로 분류함
640
예
635
의심 사용자를 신뢰되는 것으로 분류함
종료

도면7


개정된 NI를 획득함
705
개정된 NI에 기초한 멤버 블록을 멤버 블록체인에 삽입함
710
루트 블록에서 개정된 NI를 갖는 새로운 멤버 블록체인을 생성함
715
720
개정된 NI를 재검증을 위해 마스터 블록에 포워딩함
종료