(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년07월20일
(11) 등록번호 10-2135856
(24) 등록일자 2020년07월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3263 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2018-0076061
(22) 출원일자 2018년06월29일
심사청구일자 2018년06월29일
(65) 공개번호 10-2020-0002501
(43) 공개일자 2020년01월08일
(56) 선행기술조사문헌
KR100941321 B1*
KR101849917 B1*
KR101851261 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
부산대학교 산학협력단
부산광역시 금정구 부산대학로63번길 2 (장전동, 부산대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호 (신천동, 파크리오)
남일구
서울특별시 송파구 올림픽로 435, 311동 2001호 (신천동, 파크리오)
(74) 대리인
두호특허법인

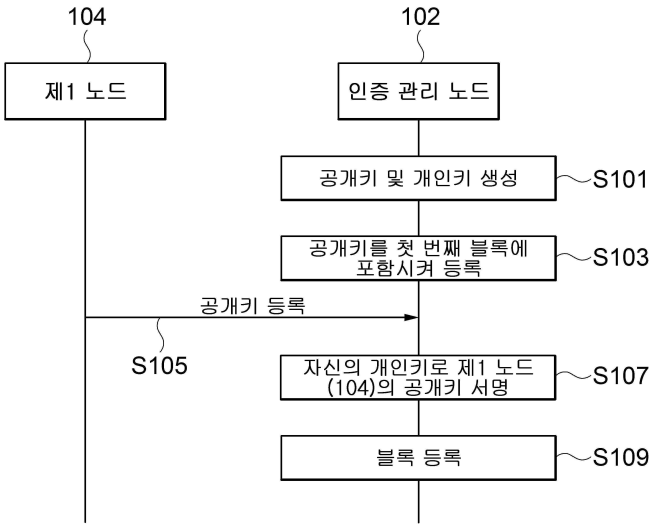
전체 청구항 수 : 총 14 항 심사관 : 문형섭

(54) 발명의 명칭 **퍼블릭 블록체인의 노드 인증 방법과 이를 수행하기 위한 장치 및 시스템**

(57) 요 약

퍼블릭 블록체인의 노드 인증 방법과 이를 수행하기 위한 장치 및 시스템 이 개시된다. 개시되는 일 실시예에 따르면, 퍼블릭 블록체인 시스템으로서, 공개키 및 상기 공개키에 대응되는 개인키를 생성하고, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 인증 관리 노드; 및 상기 인증 관리 노드로 자신의 공개키를 전송하는 제1 노드를 포함하고, 상기 인증 관리 노드는, 상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 서명값을 생성하고, 상기 제1 노드의 공개키 및 상기 서명값을 포함하는 블록을 생성하며, 생성된 상기 블록을 상기 블록체인에 등록하는, 퍼블릭 블록체인 시스템이 제공된다.

대 표 도 - 도3



(52) CPC특허분류
H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711058858
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발
연구과제명 (함수암호 3세부) 함수서명 설계기법 및 응용기술 연구
기 여 율 8/10
주관기관 고려대학교산학협력단
연구기간 2017.08.01 ~ 2018.05.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711070434
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학 ICT 연구센터육성지원사업
연구과제명 자가충전형 초소형 전국단위 위치추적 시스템 원천기술 개발
기 여 율 2/10
주관기관 울산과학기술원
연구기간 2017.06.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

퍼블릭 블록체인 시스템으로서,

공개키 및 상기 공개키에 대응되는 개인키를 생성하고, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 인증 관리 노드; 및

상기 인증 관리 노드로 자신의 공개키를 전송하는 제1 노드를 포함하고,

상기 인증 관리 노드는, 상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 서명값을 생성하고, 상기 제1 노드의 공개키 및 상기 서명값을 포함하는 블록을 생성하며, 생성된 상기 블록을 상기 블록체인에 등록하는,

상기 인증 관리 노드는, 상기 퍼블릭 블록체인 시스템을 구성하는 하나의 노드로서, 상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성되는, 퍼블릭 블록체인 시스템.

청구항 2

삭제

청구항 3

청구항 1에 있어서,

상기 블록체인으로부터 상기 제1 노드의 공개키, 상기 서명값 및 상기 상기 인증 관리 노드의 공개키를 획득하고,

상기 서명값을 상기 인증 관리 노드의 공개키로 복호화하며,

획득된 상기 제1 노드의 공개키 및 복호화된 상기 서명값의 일치 여부에 따라 상기 제1 노드를 인증하는 제2 노드를 더 포함하는, 퍼블릭 블록체인 시스템.

청구항 4

퍼블릭 블록체인 시스템으로서,

공개키 및 상기 공개키에 대응되는 개인키를 생성하고, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하며, 외부 인증 서버로부터 상기 외부 인증 서버의 공개키를 수신하는 인증 관리 노드; 및

자신의 공개키를 상기 외부 인증 서버로 전송하며, 상기 외부 인증 서버로부터 상기 자신의 공개키를 상기 외부 인증 서버의 개인키로 암호화한 제1 서명값을 수신하고, 상기 자신의 공개키 및 상기 제1 서명값을 상기 인증 관리 노드로 전송하는 제1 노드를 포함하는, 퍼블릭 블록체인 시스템.

청구항 5

청구항 4에 있어서,

상기 인증 관리 노드는,

상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of

Stake) 없이 상기 블록체인에 블록을 등록하도록 구성되는, 퍼블릭 블록체인 시스템.

청구항 6

청구항 4에 있어서,

상기 인증 관리 노드는,

상기 제1 노드로부터 수신한 상기 제1 서명값을 상기 외부 인증 서버의 공개키로 복호화하고, 상기 제1 노드로부터 수신한 공개키 및 복호화된 상기 제1 서명값의 일치 여부에 따라 상기 제1 노드를 인증하는, 퍼블릭 블록체인 시스템.

청구항 7

청구항 6에 있어서,

상기 인증 관리 노드는,

상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 제2 서명값을 생성하고, 상기 제1 노드의 공개키 및 제2 서명값을 포함하는 블록을 생성하며, 생성된 블록을 상기 블록체인에 등록하는, 퍼블릭 블록체인 시스템.

청구항 8

청구항 4에 있어서,

상기 제1 노드는,

상기 제1 서명값에서 상기 제1 노드와 관련된 사적 정보가 포함되어 있는 경우, 상기 사적 정보를 삭제한 후 상기 인증 관리 노드로 전송하는, 퍼블릭 블록체인 시스템.

청구항 9

인증 관리 노드에서, 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계;

상기 인증 관리 노드에서, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계;

상기 인증 관리 노드에서, 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터 상기 제1 노드의 공개키를 수신하는 단계;

상기 인증 관리 노드에서, 상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 서명값을 생성하는 단계; 및

상기 인증 관리 노드에서, 상기 제1 노드의 공개키 및 상기 서명값을 포함하는 블록을 생성하고, 생성된 블록을 상기 블록체인에 등록하는 단계를 포함하고,

상기 인증 관리 노드는, 상기 퍼블릭 블록체인 시스템을 구성하는 하나의 노드로서, 상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성되는, 퍼블릭 블록체인의 노드 인증 방법.

청구항 10

삭제

청구항 11

청구항 9에 있어서,

상기 퍼블릭 블록체인 시스템에 참여중인 제2 노드에서, 상기 블록체인으로부터 상기 제1 노드의 공개키, 상기 서명값 및 상기 상기 인증 관리 노드의 공개키를 획득하고, 상기 서명값을 상기 인증 관리 노드의 공개키로 복호화 하는 단계; 및

상기 제2 노드에서, 획득된 상기 제1 노드의 공개키 및 복호화된 상기 서명값의 일치 여부에 따라 상기 제1 노드를 인증하는 단계를 더 포함하는, 퍼블릭 블록체인의 노드 인증 방법.

청구항 12

퍼블릭 블록체인의 노드 인증 방법으로서,

인증 관리 노드에서, 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계;

상기 인증 관리 노드에서, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계;

상기 인증 관리 노드에서, 외부 인증 서버로부터 상기 외부 인증 서버의 공개키를 수신하는 단계;

상기 인증 관리 노드에서, 상기 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터, 상기 제1 노드의 공개키 및 상기 제1 노드의 공개키를 상기 외부 인증 서버의 개인키로 암호화한 제1 서명값을 수신하는 단계;

상기 인증 관리 노드에서, 상기 제1 서명값을 상기 외부 인증 서버의 공개키로 복호화 하는 단계; 및

상기 인증 관리 노드에서, 복호화된 상기 제1 서명값과 상기 제1 노드로부터 수신한 상기 제1 노드의 공개키의 일치 여부에 따라 상기 제1 노드를 인증하는 단계를 포함하는, 퍼블릭 블록체인의 노드 인증 방법.

청구항 13

청구항 12에 있어서,

상기 인증 관리 노드는,

상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성되는, 퍼블릭 블록체인의 노드 인증 방법.

청구항 14

청구항 12에 있어서,

상기 제1 노드를 인증하는 단계 이후에,

상기 인증 관리 노드에서,

상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 제2 서명값을 생성하는 단계; 및

상기 인증 관리 노드에서, 상기 제1 노드의 공개키 및 상기 제2 서명값을 포함하는 블록을 생성하며, 생성된 블록을 상기 블록체인에 등록하는 단계를 더 포함하는, 퍼블릭 블록체인의 노드 인증 방법.

청구항 15

하나 이상의 프로세서들;

메모리; 및

하나 이상의 프로그램들을 포함하고,

상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되는 컴퓨팅 장치로서,

상기 컴퓨팅 장치는, 퍼블릭 블록체인 시스템의 노드 인증을 위한 장치이고,

상기 하나 이상의 프로그램들은,

상기 컴퓨팅 장치의 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계;

상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계;

상기 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터 상기 제1 노드의 공개키를 수신하는 단계;

상기 컴퓨팅 장치의 개인키로 상기 제1 노드의 공개키를 암호화하여 서명값을 생성하는 단계; 및

상기 제1 노드의 공개키 및 상기 서명값을 포함하는 블록을 생성하고, 생성된 블록을 상기 블록체인에 등록하는 단계를 수행하기 위한 명령을 포함하고,

상기 컴퓨팅 장치는, 상기 퍼블릭 블록체인 시스템을 구성하는 하나의 노드로서, 상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성되는, 컴퓨팅 장치.

청구항 16

하나 이상의 프로세서들;

메모리; 및

하나 이상의 프로그램들을 포함하고,

상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되는 컴퓨팅 장치로서,

상기 컴퓨팅 장치는, 퍼블릭 블록체인 시스템의 노드 인증을 위한 장치이고,

상기 하나 이상의 프로그램들은,

상기 컴퓨팅 장치의 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계;

상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계;

외부 인증 서버로부터 상기 외부 인증 서버의 공개키를 수신하는 단계;

상기 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터, 상기 제1 노드의 공개키 및 상기 제1 노드의 공개키를 상기 외부 인증 서버의 개인키로 암호화한 제1 서명값을 수신하는 단계;

상기 제1 서명값을 상기 외부 인증 서버의 공개키로 복호화 하는 단계; 및

복호화된 상기 제1 서명값과 상기 제1 노드로부터 수신한 상기 제1 노드의 공개키의 일치 여부에 따라 상기 제1 노드를 인증하는 단계를 수행하기 위한 명령을 포함하는, 컴퓨팅 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예는 퍼블릭 블록체인 기술과 관련된다.

배 경 기 술

[0003] 최근, 다양한 형태의 암호 체계를 이용한 디지털 화폐(암호화 화폐)가 등장하면서 많은 관심을 끌고 있다. 이러한 암호화 화폐를 온라인 상에서 처리하는 과정에서 블록체인(Block Chain) 기술이 핵심적인 역할을 한다. 블록

체인은 트랜잭션(Transaction) 정보를 담은 하나의 블록이 이전의 블록과 다음의 블록을 고유 값으로 상호 참조하도록 하여 체인처럼 연결된 구조를 갖게 된다.

[0004] 블록체인은 참여자 범위에 따라 퍼블릭(Public) 블록체인, 프라이빗(Private) 블록체인, 및 하이브리드(Hybrid) 블록체인으로 분류할 수 있다. 이 중 퍼블릭 블록체인은 참여자 모두에게 정보가 공개되는 블록체인으로, 누구나 자유롭게 참여하여 트랜잭션을 생성 및 검증할 수 있다는 점에서 가장 광범위하게 사용되고 있다.

[0005] 퍼블릭 블록체인에 참여중인 소정 노드는 트랜잭션을 자신의 개인키(Private Key)로 암호화하여 전송하고, 이를 수신한 다른 노드는 상기 소정 노드의 공개키(Public Key)로 암호화된 트랜잭션을 복호화하여 트랜잭션을 검증하게 된다.

[0006] 일반적으로, 공개키(Public Key)를 올바르게 사용하기 위해서는 공개키에 대한 인증서가 필요하고 이를 위해서 PKI(Public Key Infrastructure)가 구축되어야 하다. 퍼블릭 블록체인에서는 PKI 구축의 문제를 극복하기 위해, 공개키를 블록에 등록시켜 공개키의 무결성(Integrity)를 보장하는 방법을 사용한다.

[0007] 그러나, 실제 응용에서는 이러한 방식으로 안전성을 보장하기에는 한계가 있으며, 많은 경우 퍼블릭 블록체인 내의 노드에 대한 확실한 인증을 필요로 한다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국등록특허공보 제10-1799343호(2017.11.22)

발명의 내용

해결하려는 과제

[0010] 본 발명의 실시예는 퍼블릭 블록체인의 비중심화의 장점을 살리면서 노드를 인증할 수 있는 퍼블릭 블록체인의 노드 인증 방법과 이를 수행하기 위한 장치 및 시스템을 제공하기 위한 것이다.

과제의 해결 수단

[0012] 개시되는 일 실시예에 따르면, 퍼블릭 블록체인 시스템으로서, 공개키 및 상기 공개키에 대응되는 개인키를 생성하고, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 인증 관리 노드; 및 상기 인증 관리 노드로 자신의 공개키를 전송하는 제1 노드를 포함하고, 상기 인증 관리 노드는, 상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 서명값을 생성하고, 상기 제1 노드의 공개키 및 상기 서명값을 포함하는 블록을 생성하며, 생성된 상기 블록을 상기 블록체인에 등록하는, 퍼블릭 블록체인 시스템이 제공된다.

[0013] 상기 인증 관리 노드는, 상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성될 수 있다.

[0014] 상기 시스템은, 상기 블록체인으로부터 상기 제1 노드의 공개키, 상기 서명값 및 상기 상기 인증 관리 노드의 공개키를 획득하고, 상기 서명값을 상기 인증 관리 노드의 공개키로 복호화하며, 획득된 상기 제1 노드의 공개키 및 복호화된 상기 서명값의 일치 여부에 따라 상기 제1 노드를 인증하는 제2 노드를 더 포함할 수 있다.

[0015] 다른 예시적인 실시예에 따르면, 퍼블릭 블록체인 시스템으로서, 공개키 및 상기 공개키에 대응되는 개인키를 생성하고, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하며, 외부 인증 서버로부터 상기 외부 인증 서버의 공개키를 수신하는 인증 관리 노드; 및 자신의 공개키를 상기 외부 인증 서버로 전송하며, 상기 외부 인증 서버로부터 상기 자신의 공개키를 상기 외부 인증 서버의 개인키로 암호화한 제1 서명값을 수신하고, 상기 자신의 공개키 및 상기 제1 서명값을 상기 인증 관리 노드로 전송하는 제1 노드를 포함하는, 퍼블릭 블록체인 시스템이 제공된다.

[0016] 상기 인증 관리 노드는, 상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성될 수 있다.

[0017] 상기 인증 관리 노드는, 상기 제1 노드로부터 수신한 상기 제1 서명값을 상기 외부 인증 서버의 공개키로 복호화하고, 상기 제1 노드로부터 수신한 공개키 및 복호화된 상기 제1 서명값의 일치 여부에 따라 상기 제1 노드를 인증할 수 있다.

[0018] 상기 인증 관리 노드는, 상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 제2 서명값을 생성하고, 상기 제1 노드의 공개키 및 제2 서명값을 포함하는 블록을 생성하며, 생성된 블록을 상기 블록체인에 등록할 수 있다.

[0019] 상기 제1 노드는, 상기 제1 서명값에서 상기 제1 노드와 관련된 사적 정보가 포함되어 있는 경우, 상기 사적 정보를 삭제한 후 상기 인증 관리 노드로 전송할 수 있다.

[0020] 다른 예시적인 실시예에 따르면, 인증 관리 노드에서, 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계; 상기 인증 관리 노드에서, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계; 상기 인증 관리 노드에서, 상기 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터 상기 제1 노드의 공개키를 수신하는 단계; 상기 인증 관리 노드에서, 상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 서명값을 생성하는 단계; 및 상기 인증 관리 노드에서, 상기 제1 노드의 공개키 및 상기 서명값을 포함하는 블록을 생성하고, 생성된 블록을 상기 블록체인에 등록하는 단계를 포함하는, 퍼블릭 블록체인의 노드 인증 방법이 제공된다.

[0021] 상기 인증 관리 노드는, 상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성될 수 있다.

[0022] 상기 방법은, 상기 퍼블릭 블록체인 시스템에 참여중인 제2 노드에서, 상기 블록체인으로부터 상기 제1 노드의 공개키, 상기 서명값 및 상기 상기 인증 관리 노드의 공개키를 획득하고, 상기 서명값을 상기 인증 관리 노드의 공개키로 복호화 하는 단계; 및 상기 제2 노드에서, 획득된 상기 제1 노드의 공개키 및 복호화된 상기 서명값의 일치 여부에 따라 상기 제1 노드를 인증하는 단계를 더 포함할 수 있다.

[0023] 다른 예시적인 실시예에 따르면, 퍼블릭 블록체인의 노드 인증 방법으로서, 인증 관리 노드에서, 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계; 상기 인증 관리 노드에서, 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계; 상기 인증 관리 노드에서, 외부 인증 서버로부터 상기 외부 인증 서버의 공개키를 수신하는 단계; 상기 인증 관리 노드에서, 상기 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터, 상기 제1 노드의 공개키 및 상기 제1 노드의 공개키를 상기 외부 인증 서버의 개인키로 암호화한 제1 서명값을 수신하는 단계; 상기 인증 관리 노드에서, 상기 제1 서명값을 상기 외부 인증 서버의 공개키로 복호화하는 단계; 및 상기 인증 관리 노드에서, 복호화된 상기 제1 서명값과 상기 제1 노드로부터 수신한 상기 제1 노드의 공개키의 일치 여부에 따라 상기 제1 노드를 인증하는 단계를 포함하는, 퍼블릭 블록체인의 노드 인증 방법이 제공된다.

[0024] 상기 인증 관리 노드는, 상기 퍼블릭 블록체인 시스템에 참여중인 타 노드에 의한 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 상기 블록체인에 블록을 등록하도록 구성될 수 있다.

[0025] 상기 방법은, 상기 제1 노드를 인증하는 단계 이후에, 상기 인증 관리 노드에서, 상기 인증 관리 노드의 개인키로 상기 제1 노드의 공개키를 암호화하여 제2 서명값을 생성하는 단계; 및 상기 인증 관리 노드에서, 상기 제1 노드의 공개키 및 상기 제2 서명값을 포함하는 블록을 생성하며, 생성된 블록을 상기 블록체인에 등록하는 단계를 더 포함할 수 있다.

[0026] 다른 예시적인 실시예에 따르면, 하나 이상의 프로세서들; 메모리; 및 하나 이상의 프로그램들을 포함하고, 상기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되는 컴퓨팅 장치로서, 상기 컴퓨팅 장치는, 퍼블릭 블록체인 시스템의 노드 인증을 위한 장치이고, 상기 하나 이상의 프로그램들은, 상기 컴퓨팅 장치의 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계; 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계; 상기 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터 상기 제1 노드의 공개키를 수신하는 단계; 상기 컴퓨팅 장치의 개인키로 상기 제1 노드의 공개키를 암호화하여 서명값을 생성하는 단계; 및 상기 제1 노드의 공개키 및 상기 서명값을 포함하는 블록을 생성하고, 생성된 블록을 상기 블록체인에 등록하는 단계를 수행하기 위한 명령을 포함하는, 컴퓨팅 장치가 제공된다.

[0027] 다른 예시적인 실시예에 따르면, 하나 이상의 프로세서들; 메모리; 및 하나 이상의 프로그램들을 포함하고, 상

기 하나 이상의 프로그램들은 상기 메모리에 저장되고, 상기 하나 이상의 프로세서들에 의해 실행되도록 구성되는 컴퓨팅 장치로서, 상기 컴퓨팅 장치는, 퍼블릭 블록체인 시스템의 노드 인증을 위한 장치이고, 상기 하나 이상의 프로그램들은, 상기 컴퓨팅 장치의 공개키 및 상기 공개키에 대응되는 개인키를 생성하는 단계; 상기 공개키를 포함하는 블록을 블록체인의 첫 번째 블록으로 등록하는 단계; 외부 인증 서버로부터 상기 외부 인증 서버의 공개키를 수신하는 단계; 상기 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드로부터, 상기 제1 노드의 공개키 및 상기 제1 노드의 공개키를 상기 외부 인증 서버의 개인키로 암호화한 제1 서명값을 수신하는 단계; 상기 제1 서명값을 상기 외부 인증 서버의 공개키로 복호화 하는 단계; 및 복호화된 상기 제1 서명값과 상기 제1 노드로부터 수신한 상기 제1 노드의 공개키의 일치 여부에 따라 상기 제1 노드를 인증하는 단계를 수행하기 위한 명령을 포함하는, 컴퓨팅 장치가 제공된다.

발명의 효과

[0029] 개시되는 실시예에서는, 인증 관리 노드가 자신의 공개키를 블록체인의 첫 번째 블록에 포함시키고, 자신의 개인키로 해당 퍼블릭 블록체인 시스템에 참여하고자 하는 노드의 공개키를 암호화 함으로써, 해당 퍼블릭 블록체인 내의 다른 노드들이 인증 관리 노드의 공개키로 암호화된 노드의 공개키를 복호화하여 노드를 인증할 수 있게 된다. 이를 통해, 퍼블릭 블록체인의 장점은 그대로 유지하면서 퍼블릭 블록체인에 참여하는 노드들을 인증할 수 있어 안전성을 보장할 수 있게 된다.

[0030] 또한, 퍼블릭 블록체인에 참여하고자 하는 노드는 인증 관리 노드에 등록된 외부 인증 서버로부터 인증서(외부 인증 서버의 개인키로 서명된 해당 노드의 공개키)를 받은 후 편집 가능 전자서명(Redactable Signature, 또는 Sanitizable Signature) 기능을 통해 해당 노드의 사적 정보와 관련된 내용은 삭제하여 인증 관리 노드로 전송함으로써, 퍼블릭 블록체인에서 해당 노드의 익명성을 보장하면서도 해당 노드를 인증할 수 있게 된다.

도면의 간단한 설명

[0032] 도 1은 본 발명의 일 실시예에 따른 퍼블릭 블록체인 시스템의 구성을 나타낸 도면

도 2는 본 발명의 다른 실시예에 따른 퍼블릭 블록체인 시스템의 구성을 나타낸 도면

도 3은 본 발명의 일 실시예에 따른 퍼블릭 블록체인 시스템의 노드 인증 방법을 설명하기 위한 흐름도

도 4는 본 발명의 다른 실시예에 따른 퍼블릭 블록체인 시스템의 노드 인증 방법을 설명하기 위한 흐름도

도 5는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0033] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0034] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0035] 이하의 설명에 있어서, 신호 또는 정보의 "전송", "통신", "송신", "수신" 기타 이와 유사한 의미의 용어는 일 구성요소에서 다른 구성요소로 신호 또는 정보가 직접 전달되는 것뿐만이 아니라 다른 구성요소를 거쳐 전달되는 것도 포함한다. 특히 신호 또는 정보를 일 구성요소로 "전송" 또는 "송신"한다는 것은 그 신호 또는 정보의 최종 목적지를 지시하는 것이고 직접적인 목적지를 의미하는 것이 아니다. 이는 신호 또는 정보의 "수신"에 있어서도 동일하다. 또한 본 명세서에 있어서, 2 이상의 데이터 또는 정보가 "관련"된다는 것은 하나의 데이터(또

는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.

[0036] 또한, 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.

[0038] 도 1은 본 발명의 일 실시예에 따른 퍼블릭 블록체인 시스템의 구성을 나타낸 도면이다.

[0039] 도 1을 참조하면, 퍼블릭 블록체인 시스템(100)은 인증 관리 노드(102), 제1 노드(104), 및 제2 노드(106)를 포함할 수 있다. 인증 관리 노드(102), 제1 노드(104), 및 제2 노드(106)는 각각 통신 네트워크(130)를 통해 통신 가능하게 연결될 수 있다.

[0040] 여기서, 통신 네트워크(130)는 퍼블릭 블록체인에 참여중인 노드들 간의 통신을 위한 통신 네트워크를 의미한다. 몇몇 실시예들에서, 통신 네트워크(130)는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wire area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0041] 인증 관리 노드(102)는 퍼블릭 블록체인 시스템(100)에 참여하는 각 노드를 인증할 수 있다. 인증 관리 노드(102)는 별도의 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 블록체인 내에 블록을 등록할 수 있도록 마련될 수 있다.

[0042] 즉, 인증 관리 노드(102)는 퍼블릭 블록체인 시스템(100)을 구성하는 많은 노드들 중 하나의 노드이나, 별도의 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 블록체인 내에 블록을 등록할 수 있고, 퍼블릭 블록체인 시스템(100)에 참여하는 노드를 인증하는 기능을 가지는 특별한 노드일 수 있다.

[0043] 인증 관리 노드(102)는 인증 관리 노드(102)의 공개키를 퍼블릭 블록체인 시스템(100)의 첫 번째 블록에 포함시켜 등록시킬 수 있다. 인증 관리 노드(102)는 제1 노드(104)로부터 공개키를 수신하는 경우, 인증 관리 노드(102)의 개인키로 제1 노드(104)의 공개키를 암호화하여 서명할 수 있다. 인증 관리 노드(102)는 제1 노드(104)의 공개키 및 인증 관리 노드(102)의 개인키로 서명된 제1 노드(104)의 공개키(서명값)를 포함하는 블록을 블록체인에 등록할 수 있다.

[0044] 제1 노드(104)는 퍼블릭 블록체인 시스템(100)에 참여하고자 하는 노드일 수 있다. 제1 노드(104)는 자신의 공개키 및 개인키를 각각 생성할 수 있다. 제1 노드(104)는 자신의 공개키를 인증 관리 노드(102)로 전송하여 등록할 수 있다.

[0045] 제2 노드(106)는 퍼블릭 블록체인 시스템(100)에 참여중인 노드일 수 있다. 제2 노드(106)는 퍼블릭 블록체인 시스템(100) 내의 제1 노드(104)를 인증하고자 하는 경우, 블록체인으로부터 제1 노드(104)의 공개키, 상기 개인키의 서명값(즉, 제1 노드(104)의 공개키를 인증 관리 노드(102)의 개인키로 서명한 값) 및 인증 관리 노드(102)의 공개키를 획득할 수 있다. 이때 제1 노드(104)의 공개키 및 상기 개인키의 서명값은 동일한 블록에 포함되어 있으며, 인증 관리 노드(102)의 공개키는 해당 블록체인의 첫번째 블록에 포함되어 있다. 제2 노드(106)는 인증 관리 노드(102)의 공개키를 이용하여 상기 서명값을 복호화할 수 있다. 제2 노드(106)는 복호화된 상기 서명값이 제1 노드(104)의 공개키와 일치하는 지 여부를 확인하여 제1 노드(104)가 인증 관리 노드(102)에 등록된 노드인지를 확인할 수 있다.

[0047] 도 2는 본 발명의 다른 실시예에 따른 퍼블릭 블록체인 시스템의 구성을 나타낸 도면이다.

[0048] 도 2를 참조하면, 퍼블릭 블록체인 시스템(100)은 인증 관리 노드(102), 제1 노드(104), 제2 노드(106), 및 외부 인증 서버(150)를 포함할 수 있다. 인증 관리 노드(102), 제1 노드(104), 제2 노드(106), 및 외부 인증 서버(150)는 각각 통신 네트워크(130)를 통해 통신 가능하게 연결될 수 있다.

[0049] 여기서, 통신 네트워크(130)는 퍼블릭 블록체인에 참여중인 노드들 간의 통신을 위한 통신 네트워크를 의미한다. 몇몇 실시예들에서, 통신 네트워크(130)는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wire area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0050] 인증 관리 노드(102), 제1 노드(104), 및 제2 노드(106)들이 퍼블릭 블록체인을 구성하는 노드들이고, 외부 인증 서버(150)는 퍼블릭 블록체인에 참여하지 않는 서버 컴퓨팅 장치이다.

[0051] 인증 관리 노드(102)는 자신의 공개키 및 개인키를 각각 생성할 수 있다. 인증 관리 노드(102)는 인증 관리 노드(102)의 공개키를 퍼블릭 블록체인 시스템(100)의 첫 번째 블록에 포함시켜 등록시킬 수 있다.

[0052] 인증 관리 노드(102)는 외부 인증 서버(150)로부터 외부 인증 서버(150)의 공개키를 수신하여 외부 인증 서버(150)를 등록할 수 있다. 즉, 인증 관리 노드(102)는 제1 노드(104)를 인증하는데 사용되는 외부 인증 서버(150)를 등록할 수 있다.

[0053] 인증 관리 노드(102)는 제1 노드(104)로부터 제1 노드(104)의 공개키 및 외부 인증 서버(150)의 개인키로 서명된 제1 노드(104)의 공개키 서명값을 수신할 수 있다. 인증 관리 노드(102)는 수신된 서명값을 외부 인증 서버(150)의 공개키로 복호화 할 수 있다. 인증 관리 노드(102)는 복호화 된 값과 제1 노드(104)로부터 수신한 제1 노드(104)의 공개키의 일치 여부를 확인하여 제1 노드(104)를 인증할 수 있다.

[0054] 인증 관리 노드(102)는 인증 관리 노드(102)의 개인키로 제1 노드(104)의 공개키를 암호화하여 서명하고, 제1 노드(104)의 공개키, 및 제1 노드(104)의 공개키를 인증 관리 노드(102)의 개인키로 서명한 서명값을 포함하는 블록을 블록체인에 등록할 수 있다.

[0055] 외부 인증 서버(150)는 인증 관리 노드(102)가 속한 퍼블릭 블록체인에 속하지 않은 외부의 서버 컴퓨팅 장치일 수 있다. 외부 인증 서버(150)는 자신의 공개키 및 개인키를 각각 생성할 수 있다. 외부 인증 서버(150)는 자신의 공개키를 인증 관리 노드(102)로 전송하여 인증 관리 노드(102)에 자신을 등록할 수 있다.

[0056] 외부 인증 서버(150)는 제1 노드(104)로부터 제1 노드(104)의 공개키를 수신하는 경우, 외부 인증 서버(150)의 개인키로 제1 노드(104)의 공개키를 암호화하여 서명할 수 있다. 외부 인증 서버(150)는 제1 노드(104)의 공개키 서명한 서명값을 제1 노드(104)로 전송할 수 있다.

[0057] 제1 노드(104)는 자신의 공개키 및 상기 공개키에 대응되는 개인키를 각각 생성할 수 있다. 제1 노드(104)는 자신의 공개키를 외부 인증 서버(150)로 전송할 수 있다. 제1 노드(104)는 외부 인증 서버(150)로부터 자신의 공개키에 대응되는 서명값을 수신할 수 있다.

[0058] 제1 노드(104)는 편집 가능 전자서명(Redactable Signature, 또는 Sanitizable Signature) 기능을 이용하여 외부 인증 서버(150)의 개인키로 서명된 제1 노드(104)의 공개키에서 제1 노드(104)의 민감한 사적 정보(privacy information)와 관련된 내용(예를 들어, 제1 노드(104)의 아이디, 소속 또는 제1 노드(104)의 공개키의 생성 일시 등)을 삭제할 수 있다. 제1 노드(104)는 제1 노드(104)의 공개키 및 제1 노드(104)의 사적 정보와 관련된 내용이 삭제된 상기 서명된 제1 노드(104)의 공개키를 인증 관리 노드(102)로 전송할 수 있다.

[0059] 제2 노드(106)는 퍼블릭 블록체인 시스템(100)에 참여중인 노드일 수 있다. 제2 노드(106)는 퍼블릭 블록체인 시스템(100) 내의 제1 노드(104)를 인증하고자 하는 경우, 블록체인으로부터 제1 노드(104)의 공개키, 상기 개인키의 서명값(즉, 제1 노드(104)의 공개키를 인증 관리 노드(102)의 개인키로 서명한 값) 및 인증 관리 노드(102)의 공개키를 획득할 수 있다. 이때 제1 노드(104)의 공개키 및 상기 개인키의 서명값은 동일한 블록에 포함되어 있으며, 인증 관리 노드(102)의 공개키는 해당 블록체인의 첫번째 블록에 포함되어 있다. 제2 노드(106)는 인증 관리 노드(102)의 공개키를 이용하여 상기 서명값을 복호화할 수 있다. 제2 노드(106)는 복호화된 상기 서명값이 제1 노드(104)의 공개키와 일치하는 지 여부를 확인하여 제1 노드(104)가 인증 관리 노드(102)에 등록된 노드인지를 확인할 수 있다.

[0061] 도 3은 본 발명의 일 실시예에 따른 퍼블릭 블록체인 시스템의 노드 인증 방법을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0062] 도 3을 참조하면, 인증 관리 노드(102)는 자신의 공개키(Public Key) 및 상기 공개키에 대응되는 개인키(Private Key)를 각각 생성한다(S 101). 인증 관리 노드(102)는 생성한 개인키(Private Key)를 비밀로 보관한다.

[0063] 여기서, 인증 관리 노드(102)는 퍼블릭 블록체인 시스템 내에 마련되는 컴퓨팅 장치로서, 작업 증명(Proof of Work) 또는 지분 증명(Proof of Stake) 없이 블록을 등록할 수 있도록 마련될 수 있다. 인증 관리 노드(102)는 퍼블릭 블록체인 시스템 내에서 해당 퍼블릭 블록체인 시스템에 참여하는 각 노드를 인증하는 기능을 수행할 수 있다.

[0064] 다음으로, 인증 관리 노드(102)는 자신의 공개키를 해당 퍼블릭 블록체인 시스템의 첫 번째 블록에 포함시켜 첫

번째 블록을 등록한다(S 103). 즉, 인증 관리 노드(102)는 자신의 공개키를 포함하는 블록을 해당 퍼블릭 블록체인 시스템의 첫 번째 블록으로 등록하여 블록체인이 시작되도록 할 수 있다.

[0065] 다음으로, 해당 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드(104)는 자신의 공개키 및 개인키를 각각 생성하고, 생성한 자신의 공개키를 인증 관리 노드(102)에 등록한다(S 105). 제1 노드(104)는 생성한 자신의 개인키를 비밀로 보관한다.

[0066] 다음으로, 인증 관리 노드(102)는 제1 노드(104)의 공개키를 인증 관리 노드(102)의 개인키로 암호화하여 서명한다(S 107).

[0067] 다음으로, 인증 관리 노드(102)는 제1 노드(104)의 공개키 및 S 107 단계에서 이를 서명한 서명값을 포함하는 새로운 블록을 생성하고, 생성된 블록을 블록체인에 등록한다(S 109).

[0068] 한편, 해당 퍼블릭 블록체인 시스템에 참여하고 있는 다른 노드(예를 들어, 제2 노드(106))는 상기 블록 내에 포함된 서명값을 인증 관리 노드(102)의 공개키로 복호화 한다. 이때, 제1 노드(104)의 공개키는 인증 관리 노드(102)의 개인키로 암호화하여 서명되었으므로, 인증 관리 노드(102)의 공개키로 복호화 할 수 있게 된다. 이때, 다른 노드는 블록체인 내의 첫 번째 블록에서 인증 관리 노드(102)의 공개키를 추출하여 암호화된 제1 노드(104)의 공개키를 복호화 할 수 있다. 이후, 다른 노드는 S 111단계에서 복호화된 제1 노드(104)의 공개키가 상기 블록에 포함된 제1 노드(104)의 공개키와 일치하는지 여부를 확인하여 제1 노드(104)를 인증한다.

[0069] 개시되는 실시예에서는, 인증 관리 노드(102)가 자신의 공개키를 블록체인의 첫 번째 블록에 포함시키고, 자신의 개인키로 해당 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드(104)의 공개키를 암호화함으로써, 해당 퍼블릭 블록체인 내의 다른 노드들이 인증 관리 노드(102)의 공개키로 서명된 제1 노드(104)의 공개키를 복호화하여 제1 노드(104)를 인증할 수 있게 된다. 이를 통해, 퍼블릭 블록체인의 장점은 그대로 유지하면서 퍼블릭 블록체인에 참여하는 노드들을 인증할 수 있어 노드의 신뢰성을 보장할 수 있게 된다.

[0070] 즉, 인증 관리 노드(102)는 퍼블릭 블록체인 시스템에 참여하는 노드의 인증이라는 최소한의 역할을 하도록 함으로써, 비중심화라고 하는 퍼블릭 블록체인의 장점은 그대로 유지시키면서, 노드를 인증할 수 있어 보안성을 향상시킬 수 있게 된다.

[0072] 도 4는 본 발명의 다른 실시예에 따른 퍼블릭 블록체인 시스템의 노드 인증 방법을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0073] 도 4를 참조하면, 인증 관리 노드(102)는 자신의 공개키(Public Key) 및 개인키(Private Key)를 각각 생성한다(S 201). 인증 관리 노드(102)는 생성한 개인키(Private Key)를 비밀로 보관한다.

[0074] 다음으로, 인증 관리 노드(102)는 자신의 공개키를 해당 퍼블릭 블록체인 시스템의 첫 번째 블록에 포함시켜 첫 번째 블록을 등록한다(S 203). 즉, 인증 관리 노드(102)는 자신의 공개키를 포함하는 블록을 해당 퍼블릭 블록체인 시스템의 첫 번째 블록으로 등록하여 블록체인이 시작되도록 할 수 있다.

[0075] 다음으로, 인증 관리 노드(102)는 해당 퍼블릭 블록체인 시스템 외부에 존재하는 외부 인증 서버(150)로부터 공개키를 수신하고(S 205), 수신된 공개키를 이용하여 외부 인증 서버(150)를 등록한다(S 207). 여기서, 외부 인증 서버(150)는 인증 관리 노드(102)가 속한 퍼블릭 블록체인에 속하지 않은 외부의 서버 컴퓨팅 장치를 의미할 수 있다. 이때, 인증 관리 노드(102)는 외부 인증 서버(150)의 공개키를 저장할 수 있다.

[0076] 다음으로, 해당 퍼블릭 블록체인 시스템에 참여하고자 하는 제1 노드(104)는 자신의 공개키 및 개인키를 각각 생성하고, 생성한 자신의 공개키를 외부 인증 서버(150)로 전송한다(S 209). 제1 노드(104)는 생성한 자신의 개인키를 비밀로 보관한다.

[0077] 다음으로, 외부 인증 서버(150)는 제1 노드(104)의 공개키를 외부 인증 서버(150)의 개인키로 서명하고(S 211), 서명된 제1 노드(104)의 공개키를 제1 노드(104)로 전송한다(S 213).

[0078] 즉, 외부 인증 서버(150)는 제1 노드(104)의 공개키를 외부 인증 서버(150)의 개인키로 서명하고, 외부 인증 서버(150)의 개인키로 서명된 노드(104)의 공개키(서명값)를 제1 노드(104)로 전송할 수 있다.

[0079] 다음으로, 제1 노드(104)는 자신의 공개키 및 외부 인증 서버(150)로부터 수신한 서명값을 인증 관리 노드(102)로 전송한다(S 215). 일 실시예에서, 제1 노드(104)는 수신된 서명값에서 제1 노드(104)의 사적 정보와 관련

된 내용은 삭제하고 인증 관리 노드(102)로 전송할 수 있다.

[0080] 즉, 제1 노드(104)는 편집 가능 전자서명(Redactable Signature, 또는 Sanitizable Signature) 알고리즘을 이용하여 수신된 서명값에서 제1 노드(104)의 사적 정보와 관련된 내용(예를 들어, 제1 노드(104)의 아이디 및 제1 노드(104)의 공개키의 생성 일시 등)은 삭제하고 인증 관리 노드(102)로 전송할 수 있다.

[0081] 다음으로, 인증 관리 노드(102)는 수신된 서명값을 기 저장된 외부 인증 서버(150)의 공개키로 복호화 한다(S 217). 외부 인증 서버(150)의 공개키는 인증 관리 노드(102)에 등록되어 있고, 상기 서명된 제1 노드(104)의 공개키는 외부 인증 서버(150)의 개인키로 암호화 되어 있으므로, 인증 관리 노드(102)는 외부 인증 서버(150)의 공개키로 상기 서명된 제1 노드(104)의 공개키를 복호화 할 수 있다.

[0082] 다음으로, 인증 관리 노드(102)는 복호화 된 제1 노드(104)의 공개키가 제1 노드(104)로부터 수신한 제1 노드(104)의 공개키와 일치하는지 여부를 확인하여 제1 노드(104)를 인증한다(S 219).

[0083] 다음으로, 인증 관리 노드(102)는 제1 노드(104)의 공개키를 인증 관리 노드(102)의 개인키로 암호화하여 서명하고(S 221), 제1 노드(104)의 공개키 및 인증 관리 노드(102)의 개인키로 서명된 서명값을 포함하는 블록을 생성하여 블록체인 내 새로운 블록으로 등록한다(S 223).

[0084] 그러면, 해당 퍼블릭 블록체인 시스템에 참여하고 있는 다른 노드(예를 들어 제2 노드(106))는 해당 블록체인의 첫번째 블록에 포함된 인증 관리 노드(102)의 공개키를 이용하여 인증 관리 노드(102)의 개인키로 서명된 제1 노드(104)의 공개키를 복호화 함으로써 제1 노드(102)가 인증 관리 노드(102)에 등록된 노드인지의 여부를 인증할 수 있다.

[0085] 개시되는 실시예에 의하면, 제1 노드(104)는 인증 관리 노드(102)에 등록된 외부 인증 서버(150)로부터 인증서(외부 인증 서버(150)의 개인키로 서명된 제1 노드(104)의 공개키)를 받은 후 편집 가능 전자서명(Redactable Signature, 또는 Sanitizable Signature) 기능을 통해 제1 노드(104)의 사적 정보와 관련된 내용은 삭제하여 인증 관리 노드(102)로 전송함으로써, 퍼블릭 블록체인에서 제1 노드(104)의 익명성을 보장하면서도 제1 노드(104)를 인증할 수 있게 된다.

[0087] 도 5는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0088] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 인증 관리 노드(예를 들어, 인증 관리 노드(102))일 수 있다. 또한, 컴퓨팅 장치(12)는 외부 인증 서버(예를 들어, 외부 인증 서버(150))일 수 있다. 또한, 컴퓨팅 장치(12)는 노드 장치(예를 들어, 노드(102) 또는 노드(104))일 수 있다.

[0089] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0090] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0091] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0092] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅

장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0094] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0096] 100 : 퍼블릭 블록체인 시스템

102 : 인증 관리 노드

104 : 제1 노드

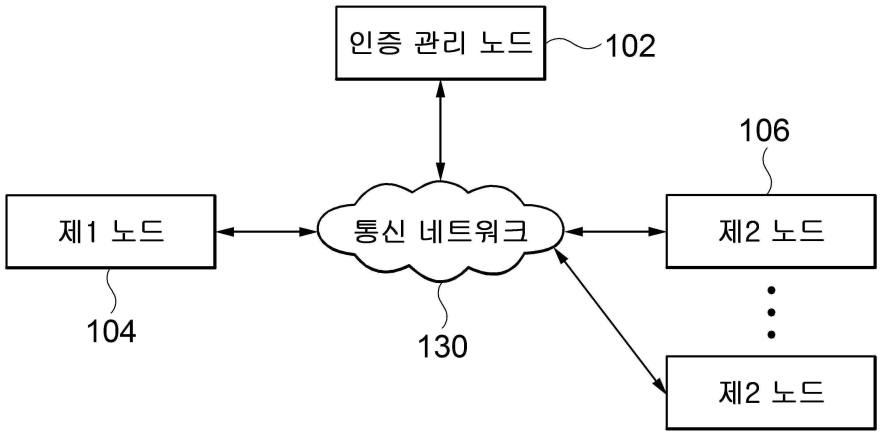
106 : 제2 노드

150 : 외부 인증 서버

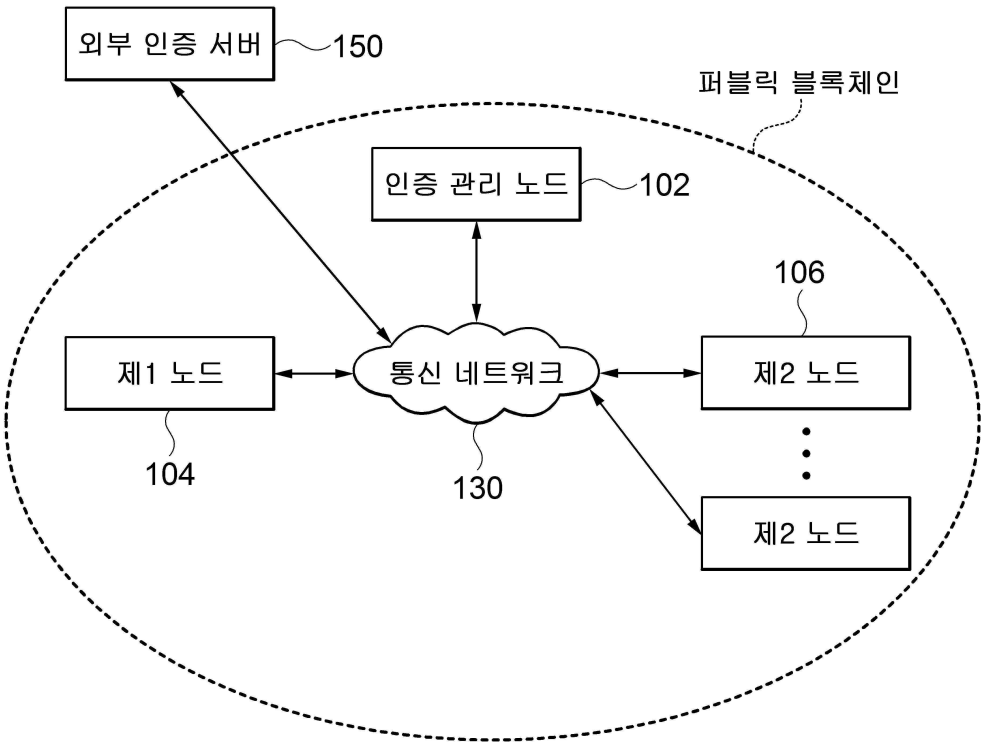
도면

도면1

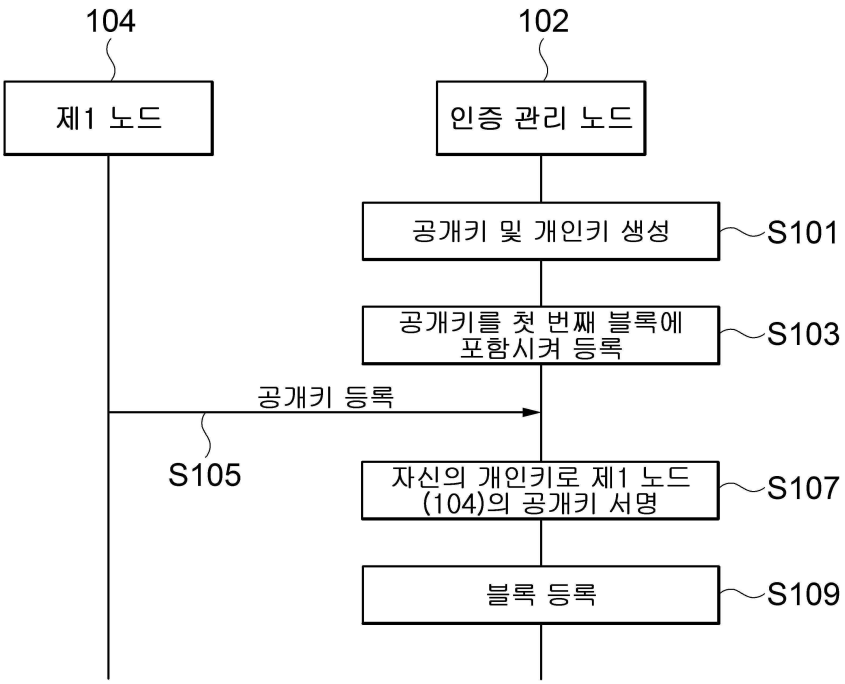
100



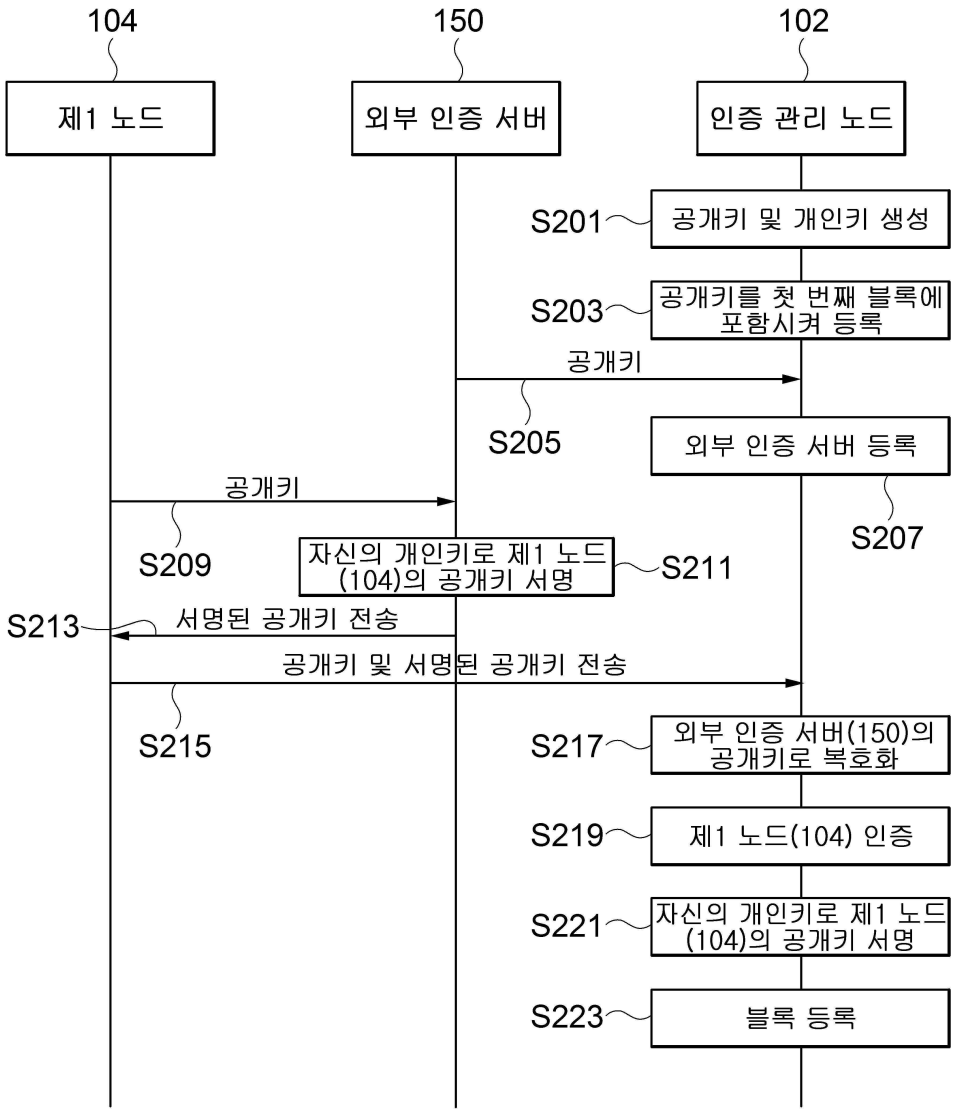
도면2


200
외부 인증 서버
150
퍼블릭 블록체인
인증 관리 노드
102
106
제1 노드
통신 네트워크
제2 노드
104
130
제2 노드

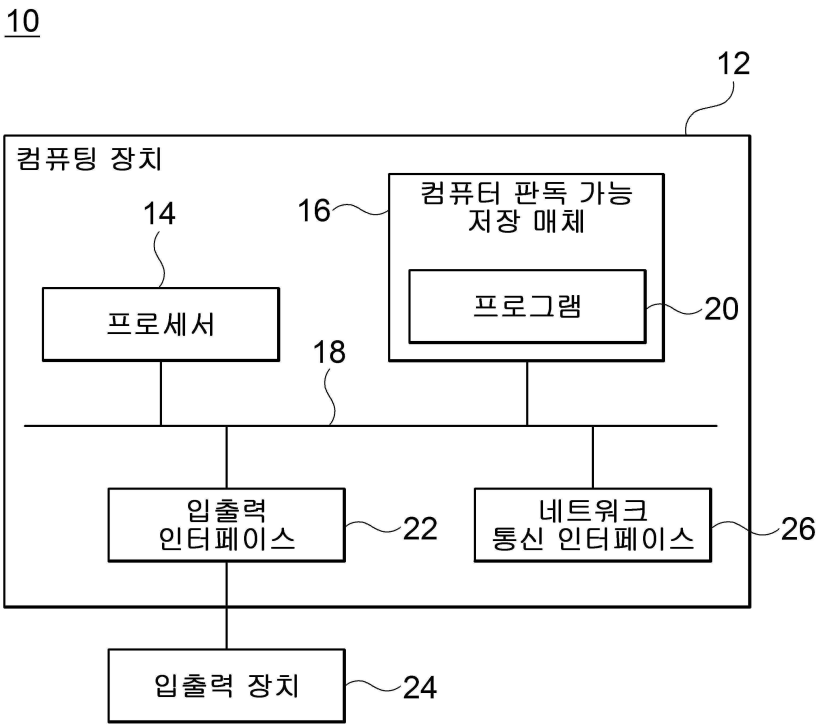
도면3


104
102
제1 노드
인증 관리 노드
공개키 및 개인키 생성
S101
공개키를 첫 번째 블록에 포함시켜 등록
S103
공개키 등록
S105
자신의 개인키로 제1 노드 (104)의 공개키 서명
S107
블록 등록
S109

도면4


104
150
102
제1 노드
외부 인증 서버
인증 관리 노드
S201
공개키 및 개인키 생성
S203
공개키를 첫 번째 블록에 포함시켜 등록
공개키
S205
외부 인증 서버 등록
S207
공개키
S209
자신의 개인키로 제1 노드(104)의 공개키 서명
S211
S213
서명된 공개키 전송
공개키 및 서명된 공개키 전송
S215
S217
외부 인증 서버(150)의 공개키로 복호화
S219
제1 노드(104) 인증
S221
자신의 개인키로 제1 노드(104)의 공개키 서명
S223
블록 등록

도면5


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24