(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년02월15일
(11) 등록번호 10-2500419
(24) 등록일자 2023년02월13일

(51) 국제특허분류(Int. Cl.)
G06F 21/33 (2013.01) *G06F 21/60* (2013.01)
G06F 21/62 (2013.01) *G06F 21/64* (2013.01)
G06F 21/79 (2013.01) *H04L 9/08* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/33 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2021-0047133
(22) 출원일자 2021년04월12일
심사청구일자 2021년04월12일
(65) 공개번호 10-2022-0141058
(43) 공개일자 2022년10월19일
(56) 선행기술조사문헌
KR101590076 B1*
KR1020180129027 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 광진구 능동로 209 세종대학교 대양AI센터 708호
(74) 대리인
두호특허법인

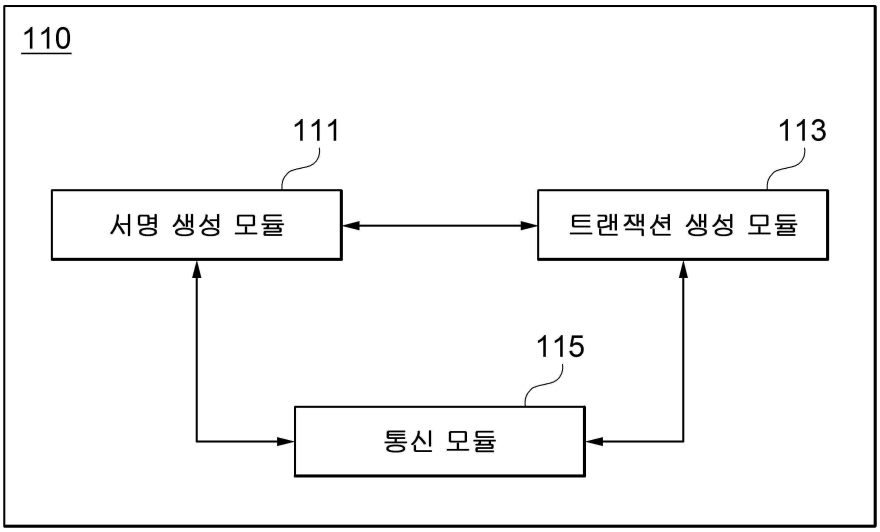
전체 청구항 수 : 총 16 항 심사관 : 문남두

(54) 발명의 명칭 **데이터 관리 방법과 이를 수행하기 위한 컴퓨팅 장치**

(57) 요 약

데이터 관리 방법과 이를 수행하기 위한 컴퓨팅 장치가 개시된다. 일 실시예에 따른 컴퓨팅 장치는 인증된 가명(Pseudonym)에 기초하여 사용자 관련 정보에 대한 서명을 생성하는 서명 생성 모듈; 가명, 사용자 관련 정보 및 서명을 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈; 및 생성된 트랜잭션을 블록체인 망에 게시하는 통신 모듈을 포함한다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/62 (2013.01)
G06F 21/64 (2013.01)
G06F 21/79 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/321 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/42 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711117818
과제번호	2020R1F1A1072275
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)(R&D)
연구과제명	무인항공기를 위한 블록체인 기반 보안 강화 기술 개발
기 여 율	1/1
과제수행기관명	세종대학교
연구기간	2020.06.01 ~ 2021.02.28

명 세 서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치로서,

블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 가명 검증 모듈; 및

검증된 가명에 기초하여 상기 마지막 블록 내 사용자 관련 정보의 유효성을 검증하는 사용자 관련 정보 검증 모듈을 포함하며,

상기 하나 이상의 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 각각 포함하고, 각 블록의 N번째 트랜잭션은 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 기반으로 생성된 블룸 필터(Bloom Filter)이며,

상기 마지막 블록의 블룸 필터는, 상기 블록체인 망의 블록체인을 구성하는 하나 이상의 블록의 각 블룸 필터에 상기 마지막 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 추가하여 생성되는, 컴퓨팅 장치.

청구항 5

청구항 4항에 있어서,

상기 가명 검증 모듈은,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 상기 가명에 대한 상기 블룸 필터의 조회 결과에 기초하여 상기 가명의 유효성을 검증하는, 컴퓨팅 장치.

청구항 6

청구항 4항에 있어서,

상기 가명 검증 모듈은,

상기 마지막 블록에서 상기 가명이 포함된 트랜잭션을 탐색하고, 상기 탐색된 트랜잭션에 포함된 상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증하는, 컴퓨팅 장치.

청구항 7

청구항 4항에 있어서,

상기 사용자 관련 정보는,

상기 검증된 가명에 대응되는 비밀키로 서명되고,

상기 사용자 관련 정보 검증 모듈은,

상기 검증된 가명을 이용하여 상기 마지막 블록 내 상기 사용자 관련 정보에 대한 서명을 검증함으로써 상기 사용자 관련 정보의 유효성을 검증하는, 컴퓨팅 장치.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치에서 수행되는 방법으로서,

블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 단계; 및

검증된 가명에 기초하여 상기 마지막 블록 내 사용자 관련 정보의 유효성을 검증하는 단계를 포함하며,

상기 하나 이상의 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 각각 포함하고, 각 블록의 N번째 트랜잭션은 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 기반으로 생성된 블룸 필터(Bloom Filter)이며,

상기 마지막 블록의 블룸 필터는, 상기 블록체인 망의 블록체인을 구성하는 하나 이상의 블록의 각 블룸 필터에 상기 마지막 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 추가하여 생성되는, 데이터 관리 방법.

청구항 12

청구항 11항에 있어서,

상기 가명의 유효성을 검증하는 단계는,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및

상기 가명에 대한 상기 블룸 필터의 조회 결과에 기초하여 상기 가명의 유효성을 검증하는 단계를 포함하는, 데이터 관리 방법.

청구항 13

청구항 11항에 있어서,

상기 가명의 유효성을 검증하는 단계는,

상기 마지막 블록에서 상기 가명이 포함된 트랜잭션을 탐색하는 단계; 및

상기 탐색된 트랜잭션에 포함된 상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증하는 단계

를 포함하는, 데이터 관리 방법.

청구항 14

청구항 11항에 있어서,

상기 사용자 관련 정보는,

상기 검증된 가명에 대응되는 비밀키로 서명되고,

상기 사용자 관련 정보의 유효성을 검증하는 단계는,

상기 검증된 가명을 이용하여 상기 마지막 블록 내 상기 사용자 관련 정보에 대한 서명을 검증함으로써 상기 사용자 관련 정보의 유효성을 검증하는, 데이터 관리 방법.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치로서,

블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 가명 검증 모듈;

검증된 가명에 기초하여 상기 마지막 블록 내 암호문의 유효성을 검증하는 암호문 검증 모듈; 및

상기 컴퓨팅 장치의 비밀키로 상기 검증된 암호문을 복호화하는 복호화 모듈을 포함하고,

상기 암호문은, 상기 컴퓨팅 장치의 공개키로 상기 마지막 블록 내 사용자 관련 정보를 암호화하여 생성된 후 상기 가명에 기초하여 서명되며,

상기 하나 이상의 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 각각 포함하고, 각 블록의 N번째 트랜잭션은 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 기반으로 생성된 블룸 필터(Bloom Filter)이며,

상기 마지막 블록의 블룸 필터는, 상기 블록체인 망의 블록체인을 구성하는 하나 이상의 블록의 각 블룸 필터에 상기 마지막 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 추가하여 생성되는, 컴퓨팅 장치.

청구항 19

청구항 18항에 있어서,

상기 가명 검증 모듈은,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 상기 가명에 대한 상기 블룸 필터의 조회 결과에 기초하여 상기 가명의 유효성을 검증하는, 컴퓨팅 장치.

청구항 20

청구항 18항에 있어서,

상기 가명 검증 모듈은,

상기 마지막 블록에서 상기 가명이 포함된 트랜잭션을 탐색하고, 상기 탐색된 트랜잭션에 포함된 상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증하는, 컴퓨팅 장치.

청구항 21

청구항 18항에 있어서,

상기 암호문은,

상기 검증된 가명에 대응되는 비밀키로 서명되고,

상기 암호문 검증 모듈은,

상기 검증된 가명을 이용하여 상기 마지막 블록 내 상기 암호문에 대한 서명을 검증함으로써 상기 암호문의 유효성을 검증하는, 컴퓨팅 장치.

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치에서 수행되는 방법으로서,

블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 단계;

검증된 가명에 기초하여 상기 마지막 블록 내 암호문의 유효성을 검증하는 단계; 및

상기 컴퓨팅 장치의 비밀키로 상기 검증된 암호문을 복호화하는 단계를 포함하고,

상기 암호문은, 상기 컴퓨팅 장치의 공개키로 상기 마지막 블록 내 사용자 관련 정보를 암호화하여 생성된 후 상기 가명에 기초하여 서명되며,

상기 하나 이상의 블록은, N(N은 2이상의 자연수)개의 트랜잭션을 각각 포함하고, 각 블록의 N번째 트랜잭션은 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 기반으로 생성된 블룸 필터(Bloom Filter)이며,

상기 마지막 블록의 블룸 필터는, 상기 블록체인 망의 블록체인을 구성하는 하나 이상의 블록의 각 블룸 필터에 상기 마지막 블록의 첫 번째 트랜잭션부터 N-1번째 트랜잭션에 포함된 가명을 추가하여 생성되는, 데이터 관리 방법.

청구항 26

청구항 25항에 있어서,

상기 가명의 유효성을 검증하는 단계는,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및

상기 가명에 대한 상기 블룸 필터의 조회 결과에 기초하여 상기 가명의 유효성을 검증하는 단계를 포함하는, 데이터 관리 방법.

청구항 27

청구항 25항에 있어서,

상기 가명의 유효성을 검증하는 단계는,

상기 마지막 블록에서 상기 가명이 포함된 트랜잭션을 탐색하는 단계; 및

상기 탐색된 트랜잭션에 포함된 상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증하는 단계를 포함하는, 데이터 관리 방법.

청구항 28

청구항 25항에 있어서,

상기 암호문은,

상기 검증된 가명에 대응되는 비밀키로 서명되고,

상기 암호문의 유효성을 검증하는 단계는,

상기 검증된 가명을 이용하여 상기 마지막 블록 내 상기 암호문에 대한 서명을 검증함으로써 상기 암호문의 유효성을 검증하는, 데이터 관리 방법.

발명의 설명

기 술 분 야

[0001] 개시되는 실시예들은 블록체인 기반의 데이터 관리 기술에 관한 것이다.

배 경 기 술

[0003] 날이 갈수록 여러 분야에서 방대한 양의 데이터가 축적됨에 따라, 데이터의 무결성(Integrity)을 보증하기 위해 탈중앙화(Decentralization) 기반의 데이터 관리 기법이 각광받고 있다.

[0004] 그러나, 데이터가 분산원장에 기록됨으로써 무결성은 담보된다 하더라도, 데이터의 기밀성(Confidentiality)까지 담보되는 것은 아니다. 데이터는 그 특성에 따라 접근 가능한 레벨이 다양하게 설정되어야 하기 때문에, 탈중앙화 기반의 데이터 관리에 있어서도 데이터의 무결성 뿐만 아니라 기밀성까지 달성할 수 있는 기법을 고려할 필요가 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 일본 공개특허공보 제2018-020944호(2018.02.01 공개)

발명의 내용

해결하려는 과제

[0007] 개시되는 실시예들은 블록체인을 기반으로 탈중앙화(Decentralization)된 데이터 관리 기법에 있어서, 데이터의 기밀성을 달성하기 위한 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 개시되는 일 실시예에 따른 사용자 단말로 동작되는 컴퓨팅 장치는, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치로서, 인증된 가명(Pseudonym)에 기초하여 사용자 관련 정보에 대한 서명을 생성하는 서명 생성 모듈; 가명, 사용자 관련 정보 및 서명을 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈; 및 생성된 트랜잭션을 블록체인 망에 게시하는 통신 모듈을 포함한다.

[0010] 서명 생성 모듈은, 가명 및 가명에 대응되는 비밀키를 생성하고, 비밀키를 이용하여 사용자 관련 정보에 대한 서명을 생성할 수 있고, 트랜잭션 생성 모듈은, 가명, 가명에 대한 인증서, 사용자 관련 정보 및 서명을 포함하는 트랜잭션을 생성할 수 있다.

[0011] 가명은, 컴퓨팅 장치의 공개키일 수 있고, 가명에 대한 인증서는, 블록체인 망에 포함된 인증 기관으로부터 컴퓨팅 장치로 발급될 수 있다.

[0012] 개시되는 일 실시예에 따른 서비스 서버로 동작되는 컴퓨팅 장치는, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치로서, 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 가명 검증 모듈; 및 검증된 가명에 기초하여 마지막 블록 내 사용자 관련 정보의 유효성을 검증하는 사용자 관련 정보 검증 모듈을 포함한다.

[0013] 가명 검증 모듈은, 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 가명에 대한 블룸 필터의 조회 결과에 기초하여 가명의 유효성을 검증할 수 있다.

[0014] 가명 검증 모듈은, 마지막 블록에서 가명이 포함된 트랜잭션을 탐색하고, 탐색된 트랜잭션에 포함된 가명에 대한 인증서를 검증함으로써 가명의 유효성을 검증할 수 있다.

[0015] 사용자 관련 정보는, 검증된 가명에 대응되는 비밀키로 서명될 수 있고, 사용자 관련 정보 검증 모듈은, 검증된 가명을 이용하여 마지막 블록 내 사용자 관련 정보에 대한 서명을 검증함으로써 사용자 관련 정보의 유효성을 검증할 수 있다.

[0016] 개시되는 일 실시예에 따라 사용자 단말에서 수행되는 데이터 관리 방법은, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치에서 수행되는 방법으로서, 인증된 가명(Pseudonym)에 기초하여 사용자 관련 정보에 대한 서명을 생성하는 단계; 가명, 사용자 관련 정보 및 서명을 포함하는 트랜잭션을 생성하는 단계; 및 생성된 트랜잭션을 블록체인 망에 게시하는 단계를 포함한다.

[0017] 서명을 생성하는 단계는, 가명 및 가명에 대응되는 비밀키를 생성하는 단계; 및 비밀키를 이용하여 사용자 관련 정보에 대한 서명을 생성하는 단계를 포함할 수 있고, 트랜잭션을 생성하는 단계는, 가명, 가명에 대한 인증서, 사용자 관련 정보 및 서명을 포함하는 트랜잭션을 생성할 수 있다.

[0018] 가명은, 컴퓨팅 장치의 공개키일 수 있고, 가명에 대한 인증서는, 블록체인 망에 포함된 인증 기관으로부터 컴퓨팅 장치로 발급될 수 있다.

[0019] 개시되는 일 실시예에 따라 서비스 서버에서 수행되는 데이터 관리 방법은, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치에서 수행되는 방법으로서, 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 단계; 및 검증된 가명에 기초하여 마지막 블록 내 사용자 관련 정보의 유효성을 검증하는 단계를 포함한다.

[0020] 가명의 유효성을 검증하는 단계는, 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및 가명에 대한 블룸 필터의 조회 결과에 기초하여 가명의 유효성을 검증하는 단계를 포함할 수 있다.

[0021] 가명의 유효성을 검증하는 단계는, 마지막 블록에서 가명이 포함된 트랜잭션을 탐색하는 단계; 및 탐색된 트랜

잭션에 포함된 가명에 대한 인증서를 검증함으로써 가명의 유효성을 검증하는 단계를 포함할 수 있다.

[0022] 사용자 관련 정보는, 검증된 가명에 대응되는 비밀키로 서명될 수 있고, 사용자 관련 정보의 유효성을 검증하는 단계는, 검증된 가명을 이용하여 마지막 블록 내 사용자 관련 정보에 대한 서명을 검증함으로써 사용자 관련 정보의 유효성을 검증할 수 있다.

[0023] 개시되는 다른 실시예에 따른 사용자 단말은, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치로서, 블록체인 망에 포함된 서비스 서버의 공개키를 이용하여 사용자 관련 정보에 대한 암호문을 생성하는 암호화 모듈; 인증된 가명(Pseudonym)에 기초하여 암호문에 대한 서명을 생성하는 서명 생성 모듈; 가명, 암호문 및 서명을 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈; 및 생성된 트랜잭션을 블록체인 망에 게시하는 통신 모듈을 포함한다.

[0024] 서명 생성 모듈은, 가명 및 가명에 대응되는 비밀키를 생성하고, 비밀키를 이용하여 암호문에 대한 서명을 생성할 수 있고, 트랜잭션 생성 모듈은, 가명, 가명에 대한 인증서, 암호문 및 서명을 포함하는 트랜잭션을 생성할 수 있다.

[0025] 가명은, 컴퓨팅 장치의 공개키일 수 있고, 가명에 대한 인증서는, 블록체인 망에 포함된 인증 기관으로부터 컴퓨팅 장치로 발급될 수 있다.

[0026] 개시되는 다른 실시예에 따른 서비스 서버는, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치로서, 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 가명 검증 모듈; 검증된 가명에 기초하여 마지막 블록 내 암호문의 유효성을 검증하는 암호문 검증 모듈; 및 컴퓨팅 장치의 비밀키로 검증된 암호문을 복호화하는 복호화 모듈을 포함하고, 암호문은, 컴퓨팅 장치의 공개키로 마지막 블록 내 사용자 관련 정보를 암호화하여 생성된 후 가명에 기초하여 서명된다.

[0027] 가명 검증 모듈은, 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 가명에 대한 블룸 필터의 조회 결과에 기초하여 가명의 유효성을 검증할 수 있다.

[0028] 가명 검증 모듈은, 마지막 블록에서 가명이 포함된 트랜잭션을 탐색하고, 탐색된 트랜잭션에 포함된 가명에 대한 인증서를 검증함으로써 가명의 유효성을 검증할 수 있다.

[0029] 암호문은, 검증된 가명에 대응되는 비밀키로 서명될 수 있고, 암호문 검증 모듈은, 검증된 가명을 이용하여 마지막 블록 내 암호문에 대한 서명을 검증함으로써 암호문의 유효성을 검증할 수 있다.

[0030] 개시되는 다른 실시예에 따라 사용자 단말에서 수행되는 데이터 관리 방법은, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치에서 수행되는 방법으로서, 블록체인 망에 포함된 서비스 서버의 공개키를 이용하여 사용자 관련 정보에 대한 암호문을 생성하는 단계; 인증된 가명(Pseudonym)에 기초하여 암호문에 대한 서명을 생성하는 단계; 가명, 암호문 및 서명을 포함하는 트랜잭션을 생성하는 단계; 및 생성된 트랜잭션을 블록체인 망에 게시하는 단계를 포함한다.

[0031] 서명을 생성하는 단계는, 가명 및 가명에 대응되는 비밀키를 생성하는 단계; 및 비밀키를 이용하여 암호문에 대한 서명을 생성하는 단계를 포함할 수 있고, 트랜잭션을 생성하는 단계는, 가명, 가명에 대한 인증서, 암호문 및 서명을 포함하는 트랜잭션을 생성할 수 있다.

[0032] 가명은, 컴퓨팅 장치의 공개키일 수 있고, 가명에 대한 인증서는, 블록체인 망에 포함된 인증 기관으로부터 컴퓨팅 장치로 발급될 수 있다.

[0033] 개시되는 다른 실시예에 따라 서비스 서버에서 수행되는 데이터 관리 방법은, 하나 이상의 프로세서들, 및 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하는 컴퓨팅 장치에서 수행되는 방법으로서, 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 단계; 검증된 가명에 기초하여 마지막 블록 내 암호문의 유효성을 검증하는 단계; 및 컴퓨팅 장치의 비밀키로 검증된 암호문을 복호화하는 단계를 포함하고, 암호문은, 컴퓨팅 장치의 공개키로 마지막 블록 내 사용자 관련 정보를 암호화하여 생성된 후 가명에 기초하여 서명된다.

[0034] 가명의 유효성을 검증하는 단계는, 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및 가명에 대한 블룸 필터의 조회 결과에 기초하여 가명의 유효성을 검증하는 단계를 포함할 수 있다.

[0035] 가명의 유효성을 검증하는 단계는, 마지막 블록에서 가명이 포함된 트랜잭션을 탐색하는 단계; 및 탐색된 트랜

잭션에 포함된 가명에 대한 인증서를 검증함으로써 가명의 유효성을 검증하는 단계를 포함할 수 있다.

[0036] 암호문은, 검증된 가명에 대응되는 비밀키로 서명되고, 암호문의 유효성을 검증하는 단계는, 검증된 가명을 이용하여 마지막 블록 내 암호문에 대한 서명을 검증함으로써 암호문의 유효성을 검증할 수 있다.

발명의 효과

[0038] 개시되는 실시예들에 따르면, 블록체인을 기반으로 사용자 단말의 가명(Pseudonym)을 이용하여 탈중앙화 방식의 데이터 서비스를 제공함으로써, 서비스에 관련된 데이터의 무결성(Integrity)과 더불어 기밀성(Confidentiality)을 보증할 수 있다.

도면의 간단한 설명

[0040] 도 1은 일 실시예에 따른 데이터 관리 시스템을 설명하기 위한 블록도

도 2는 제1 실시예에 따른 사용자 단말을 설명하기 위한 블록도

도 3은 제1 실시예에 따른 서비스 서버를 설명하기 위한 블록도

도 4는 제2 실시예에 따른 사용자 단말을 설명하기 위한 블록도

도 5는 제2 실시예에 따른 서비스 서버를 설명하기 위한 블록도

도 6은 제1 실시예에 따라 사용자 단말에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도

도 7은 제1 실시예에 따라 서비스 서버에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도

도 8은 일 실시예에서 블록에 블룸 필터를 생성하는 상태를 나타내는 도면

도 9는 제2 실시예에 따라 사용자 단말에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도

도 10은 제2 실시예에 따라 서비스 서버에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도

도 11은 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0041] 이하, 도면을 참조하여 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 개시되는 실시예들은 이에 제한되지 않는다.

[0042] 실시예들을 설명함에 있어서, 관련된 공지기술에 대한 구체적인 설명이 개시되는 실시예들의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 개시되는 실시예들에서의 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 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.

[0043] 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.

[0044] 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(또는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.

[0045] 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 목적으

로 사용될 수 있다.

[0046] 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.

[0047] 도 1은 일 실시예에 따른 데이터 관리 시스템(100)을 설명하기 위한 블록도이다.

[0048] 도시된 바와 같이, 일 실시예에 따른 데이터 관리 시스템(100)은 사용자 단말(110), 서비스 서버(120), 인증 기관(130) 및 마이너 노드(140)를 포함한다. 사용자 단말(110)은 서비스 서버(120), 인증 기관(130) 및 마이너 노드(140)와 통신 네트워크(150)를 통해 상호 통신 가능하게 연결된다.

[0049] 몇몇 실시예들에서, 통신 네트워크(150)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] 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0051] 또한, 일 실시예에서, 서비스 서버(120), 인증 기관(130) 및 마이너 노드(140)는 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0052] 한편 개시되는 실시예에서, 블록체인은 프라이빗(Private) 블록체인일 수 있으나, 이에 한정되는 것은 아니며, 퍼블릭(Public) 블록체인 또는 컨소시움(Consortium) 블록체인일 수도 있다.

[0053] 사용자 단말(110)은 사용자 관련 정보를 포함하여 트랜잭션(Transaction)을 생성할 수 있다. 이하의 실시예들에서, '사용자 관련 정보'는 일련의 서비스와 관련된 사용자의 입력 정보를 포함할 수 있으며, 예를 들어 상품 또는 서비스와 관련된 리뷰 정보, 온라인 게시판에 쓰여지는 게시물 정보, 온라인 설문 조사와 관련된 응답 정보, 온라인 상담과 관련된 증상 정보 등을 포함할 수 있으나, 이에 한정되는 것은 아니며 사용자가 향유하는 상품 또는 서비스의 종류에 따라 다양한 정보가 포함될 수 있다. 이때, 사용자가 향유하는 일련의 서비스는 서비스 서버(120)에 의해 블록체인 망에서 제공되는 서비스일 수 있다.

[0054] 서비스 서버(120)는 블록체인 망을 통해 사용자 단말(110)에 데이터 관리 서비스를 제공하는 장치를 의미한다. 이하의 실시예들에서, 데이터 관리 서비스라 함은 사용자 단말(110)이 블록체인 망에 개시하는 데이터를 블록체인을 구성하는 노드(Node) 사이에서 공유하되, 사용자 단말(110)이 블록체인 망에 개시하는 데이터로부터 사용자 단말(110)을 식별할 수 있는 '공개 데이터 서비스'와, 사용자 단말(110)이 블록체인 망에 개시하는 데이터로부터 사용자 단말(110)을 식별할 수 없는 '비공개 데이터 서비스'를 포함한다.

[0055] 일 실시예에 따르면, 서비스 서버(120)는 블록체인 망에서 풀 노드(Full node)로 동작할 수 있으나, 이에 한정되는 것은 아니며, 실시예에 따라서는 후술할 마이너 노드(140)를 겸하여 동작할 수도 있다.

[0056] 인증 기관(130)은 사용자 단말(110)이 생성하는 가명(Pseudonym)에 대해 인증서를 발급하는 장치를 의미한다. 일 실시예에서, 도시된 블록체인 망이 프라이빗 블록체인을 기반으로 하는 경우, 인증 기관(130)은 블록체인 망을 구성하는 참여자가 사전 등록된 참여자인지 검증하기 위한 인증서를 발급할 수도 있다.

[0057] 일 실시예에 따르면, 인증 기관(130)은 사용자 단말과 상호 간 블라인드 서명을 수행함으로써 가명에 대한 인증서를 발급할 수 있다. 예시적으로, 상세한 발급 과정은 다음과 같이 진행될 수 있다.

[0058] (1) 인증 기관(130)은 사전 정의된 블라인드 서명 키 생성 알고리즘을 실행하고, 이에 따라 공개 검증키(cvk)와 개인 서명키(csk)를 획득

[0059] (2) 인증 기관(130)은 cvk를 블록체인 망에 공개하고, csk를 비밀로 유지

[0060] (3) 인증 기관(130) 및 인증 기관(130)에 대해 인증된 사용자 단말(110)이 인증할 가명의 수 v에 동의

[0061] (4) 인증 기관(130)은 사용자 단말(110)이 선택한 가명 pk에 대해, 사용자 단말(110)을 수신자(receiver)로 하고, 인증 기관(130)을 서명자(signer)로 하여 인증서 s를 발급

[0062] (5) 인증할 가명들 중 나머지 가명 각각에 대해 (4)의 과정을 반복

[0063] 일 실시예에 따르면, 인증 기관(130)은 블록체인 망에서 풀 노드(Full node)로 동작할 수 있으나, 이에 한정되

는 것은 아니며, 실시예에 따라서는 후술할 마이너 노드(140)를 겸하여 동작할 수도 있다.

[0064] 마이너 노드(140)는 블록체인 상에서 유효성이 검증된 트랜잭션을 블록에 기록하여 공유하는 작업을 수행하는 장치를 의미한다.

[0065] 구체적으로, 마이너 노드(140)는 블록체인 망에서 각 사용자 단말(110)들이 전송하는 트랜잭션들을 수집하여 블록을 생성할 수 있으며, 생성한 블록을 블록체인에 연결할 수 있다.

[0066] 일 실시예에 따르면, 마이너 노드(140)는 블록을 구성하는 각 트랜잭션에 포함된 사용자 관련 정보와 가명을 이용하여 블룸 필터(Bloom Filter)를 생성할 수 있다. 즉, 마이너 노드(140)는 각 트랜잭션에 포함된 사용자 관련 정보 및 가명을 블룸 필터의 멤버(Member)로 하여 블룸 필터를 생성할 수 있다. 이때, 블룸 필터는 소정 멤버가 집합에 속하는지 여부를 검사하기 위해 사용되는 확률적 자료 구조를 의미할 수 있다. 이와 관련해서는, 이하의 도 8을 참조하여 후술하기로 한다.

[0067] 도 2는 제1 실시예에 따른 사용자 단말(110)을 설명하기 위한 블록도이다.

[0068] 도시된 바와 같이, 제1 실시예에 따른 사용자 단말(110)은 서명 생성 모듈(111), 트랜잭션 생성 모듈(113) 및 통신 모듈(115)을 포함한다.

[0069] 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0070] 또한, 일 실시예에서, 서명 생성 모듈(111), 트랜잭션 생성 모듈(113) 및 통신 모듈(115)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0071] 서명 생성 모듈(111)은 인증된 가명(Pseudonym)에 기초하여 사용자 관련 정보에 대한 서명을 생성한다.

[0072] 일 실시예에 따르면, '가명'은 사용자 단말(110)과 일대일 대응되는 사용자 단말(110)의 공개키일 수 있다.

[0073] 일 실시예에 따르면, 서명 생성 모듈(111)은 가명 및 가명에 대응되는 비밀키를 생성하고, 비밀키를 이용하여 사용자 관련 정보에 대한 서명을 생성할 수 있다.

[0074] 트랜잭션 생성 모듈(113)은 가명, 사용자 관련 정보 및 서명을 포함하는 트랜잭션을 생성한다.

[0075] 일 실시예에 따르면, 트랜잭션 생성 모듈(113)은 통신 모듈(115)을 통해 획득한 가명에 대한 인증서를 부가하여, 가명, 가명에 대한 인증서, 사용자 관련 정보 및 서명을 포함하는 트랜잭션을 생성할 수 있다.

[0076] 이때, '가명에 대한 인증서'는 블록체인 망에 포함된 인증 기관(130)으로부터 사용자 단말(110)로 발급되는 인증서일 수 있다.

[0077] 통신 모듈(115)은 생성된 트랜잭션을 블록체인 망에 게시한다.

[0078] 일 실시예에 따르면, 통신 모듈(115)은 블록체인 망을 통해 가명에 대한 인증서를 획득할 수 있다.

[0079] 한편, 일 실시예에 따르면, 제1 실시예에 따른 사용자 단말(110)은 서비스 서버(120)로부터 제공받는 서비스에 대한 비용을 지불하기 위한 결제 모듈(미도시)을 더 포함할 수 있다.

[0080] 구체적으로, 결제 모듈(미도시)은 사용자 단말(110)이 인증 기관(130)으로부터 가명에 대한 인증서를 획득하는 경우, 해당 인증서에 지정된 가격만큼의 비용을 서비스 서버(120)에 지불할 수 있다.

[0081] 더욱 상세하게, 결제 모듈(미도시)은 비용을 지불함에 있어서, 블록체인 망에서 서비스에 대한 비용 지불 수단으로 설정, 유통되는 토큰(token)으로 상기 비용을 지불할 수 있다. 예를 들어, 결제 모듈(미도시)은 블록체인 망에서 사용되는 암호화폐로 상기 비용을 지불할 수 있다.

[0082] 이때, 가명에 대한 인증서에 지정된 가격은 정적 가격 측정(Static pricing)에 따라 고정된 값을 가질 수도 있고, 동적 가격 측정(Dynamic pricing)에 따라 기 설정된 단위 시간마다 새로이 책정되는 값을 가질 수도 있다.

[0083] 한편, 이상의 결제 모듈(미도시)과 관련된 실시예는 후술할 제2 실시예에서도 적용될 수 있다.

[0084] 도 3은 제1 실시예에 따른 서비스 서버(120)를 설명하기 위한 블록도이다.

[0085] 도시된 바와 같이, 제1 실시예에 따른 서비스 서버(120)는 가명 검증 모듈(121) 및 사용자 관련 정보 검증 모듈

(123)을 포함한다.

[0086] 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0087] 또한, 일 실시예에서, 가명 검증 모듈(121) 및 사용자 관련 정보 검증 모듈(123)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0088] 가명 검증 모듈(121)은 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명의 유효성을 검증한다.

[0089] 일 실시예에 따르면, 가명 검증 모듈(121)은 마지막 블록의 블룸 필터를 조회하고, 검증 대상인 가명에 대한 블룸 필터의 조회 결과에 기초하여 해당 가명의 유효성을 검증할 수 있다.

[0090] 구체적으로, 가명 검증 모듈(121)은 마지막 블록의 블룸 필터를 조회한 결과, 블룸 필터가 검증 대상인 가명에 대해 예(Yes)를 보고하면 해당 가명을 유효한 것으로 판단할 수 있다.

[0091] 한편, 가명 검증 모듈(121)은 마지막 블록의 블룸 필터를 조회한 결과, 블룸 필터가 검증 대상인 가명에 대해 아니오(No)를 보고하면 해당 가명을 유효하지 않은 것으로 판단할 수 있다.

[0092] 다른 실시예에 따르면, 가명 검증 모듈(121)은 마지막 블록에서 검증 대상인 가명이 포함된 트랜잭션을 탐색하고, 탐색된 트랜잭션에 포함된 검증 대상인 가명에 대한 인증서를 검증함으로써 해당 가명의 유효성을 검증할 수 있다.

[0093] 구체적으로, 가명 검증 모듈(121)은 인증 기관(130)에 의해 생성된 공개키로 검증 대상인 가명에 대한 인증서를 검증할 수 있다.

[0094] 또 다른 실시예에 따르면, 가명 검증 모듈(121)은 상술한 각 실시예의 '블룸 필터를 조회하는 방식'과 '가명에 대한 인증서를 검증하는 방식'을 모두 사용하여 가명의 유효성을 검증할 수도 있다. 예를 들어, 가명 검증 모듈(121)은 '블룸 필터를 조회하는 방식'을 적용한 후, 블룸 필터의 조회 결과가 예(Yes)인 경우에 '가명에 대한 인증서를 검증하는 방식'을 사용할 수도 있다.

[0095] 사용자 관련 정보 검증 모듈(123)은 검증된 가명에 기초하여 마지막 블록 내 사용자 관련 정보의 유효성을 검증한다.

[0096] 일 실시예에 따르면, 사용자 관련 정보는 가명 검증 모듈(121)에 의해 검증된 가명에 대응되는 비밀키로 서명될 수 있고, 사용자 관련 정보 검증 모듈(123)은 검증된 가명을 이용하여 마지막 블록 내 사용자 관련 정보에 대한 서명을 검증함으로써 해당 사용자 관련 정보의 유효성을 검증할 수 있다.

[0097] 즉 다시 말하면, 사용자 관련 정보 검증 모듈(123)은 검증된 가명이 사용자 관련 정보의 서명에 사용된 비밀키에 대응되는 공개키인 경우, 해당 사용자 관련 정보가 유효한 것으로 판단할 수 있다.

[0098] 이로써, 제1 실시예에 따라 유효한 것으로 검증된 사용자 관련 정보는 서비스 서버(120)가 제공하는 서비스에 이용될 때, 해당 사용자 관련 정보와 대응되는 가명과 함께 블록체인 망 하에서 공개될 수 있다.

[0099] 도 4는 제2 실시예에 따른 사용자 단말(110)을 설명하기 위한 블록도이다.

[0100] 도시된 바와 같이, 제2 실시예에 따른 사용자 단말(110)은 서명 생성 모듈(111), 트랜잭션 생성 모듈(113), 통신 모듈(115) 및 암호화 모듈(117)을 포함한다.

[0101] 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0102] 또한, 일 실시예에서, 서명 생성 모듈(111), 트랜잭션 생성 모듈(113), 통신 모듈(115) 및 암호화 모듈(117)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0103] 암호화 모듈(117)은 블록체인 망에 포함된 서비스 서버(120)의 공개키를 이용하여 사용자 관련 정보에 대한 암호문을 생성한다.

[0104] 즉 다시 말하면, 암호화 모듈(117)은 사용자 관련 정보를 처리하는 엔티티(Entity)인 서비스 서버(120)의 공개키로 사용자 관련 정보를 암호화함으로써, 서비스 서버(120) 및 인증 기관(130)이 사용자 단말(110)과 가명 사이의 연관 관계를 식별할 수 없도록 할 수 있다.

[0105] 이로써, 제2 실시예에 따르면, 추후 유효한 것으로 검증된 사용자 관련 정보가 서비스 서버(120)가 제공하는 서비스에 이용되더라도, 블록체인 망에 포함된 각 주체들은 해당 사용자 관련 정보 및 가명을 통해 대응되는 사용자 단말을 식별할 수 없게 되어, 사용자 단말(110)의 프라이버시(Privacy)가 유지될 수 있다.

[0106] 서명 생성 모듈(111)은 인증된 가명에 기초하여 암호문에 대한 서명을 생성한다.

[0107] 일 실시예에 따르면, 서명 생성 모듈(111)은 가명 및 가명에 대응되는 비밀키를 생성하고, 생성된 비밀키를 이용하여 암호문에 대한 서명을 생성할 수 있다.

[0108] 트랜잭션 생성 모듈(113)은 가명, 암호문 및 암호문에 대한 서명을 포함하는 트랜잭션을 생성한다.

[0109] 일 실시예에 따르면, 트랜잭션 생성 모듈(113)은 가명, 가명에 대한 인증서, 암호문 및 암호문에 대한 서명을 포함하는 트랜잭션을 생성할 수 있다.

[0110] 통신 모듈(115)은 생성된 트랜잭션을 블록체인 망에 게시한다.

[0111] 일 실시예에 따르면, 통신 모듈(115)은 블록체인 망을 통해 가명에 대한 인증서를 획득할 수 있다.

[0112] 이때, 가명에 대한 인증서는 블록체인 망에 포함된 인증 기관으로부터 사용자 단말(110)로 발급될 수 있다.

[0113] 도 5는 제2 실시예에 따른 서비스 서버(120)를 설명하기 위한 블록도이다.

[0114] 도시된 바와 같이, 제2 실시예에 따른 서비스 서버(120)는 가명 검증 모듈(121), 암호문 검증 모듈(125) 및 복호화 모듈(127)을 포함한다.

[0115] 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0116] 또한, 일 실시예에서, 가명 검증 모듈(121), 암호문 검증 모듈(125) 및 복호화 모듈(127)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0117] 가명 검증 모듈(121)은 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명의 유효성을 검증한다.

[0118] 일 실시예에 따르면, 가명 검증 모듈(121)은 마지막 블록의 블룸 필터를 조회하고, 검증 대상인 가명에 대한 블룸 필터의 조회 결과에 기초하여 해당 가명의 유효성을 검증할 수 있다.

[0119] 다른 실시예에 따르면, 가명 검증 모듈(121)은 마지막 블록에서 검증 대상인 가명이 포함된 트랜잭션을 탐색하고, 탐색된 트랜잭션에 포함된 검증 대상인 가명에 대한 인증서를 검증함으로써 해당 가명의 유효성을 검증할 수 있다.

[0120] 암호문 검증 모듈(125)은 검증된 가명에 기초하여 마지막 블록 내 암호문의 유효성을 검증한다. 이때, 암호문은 서비스 서버(120)의 공개키로 마지막 블록 내 사용자 관련 정보를 암호화하여 생성된 후, 가명에 기초하여 서명된다.

[0121] 일 실시예에 따르면, 암호문은 가명 검증 모듈(121)에 의해 검증된 가명에 대응되는 비밀키로 서명되고, 암호문 검증 모듈(125)은 검증된 가명을 이용하여 마지막 블록 내 암호문에 대한 서명을 검증함으로써 해당 암호문의 유효성을 검증할 수 있다.

[0122] 복호화 모듈(127)은 서비스 서버의 비밀키로 검증된 암호문을 복호화한다.

[0123] 도 6은 제1 실시예에 따라 사용자 단말(110)에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도이다.

[0124] 우선, 사용자 단말(110)은 인증된 가명에 기초하여 사용자 관련 정보에 대한 서명을 생성한다(610).

[0125] 이후, 사용자 단말(110)은 인증된 가명, 사용자 관련 정보 및 사용자 관련 정보에 대한 서명을 포함하는 트랜잭션을 생성한다(620).

[0126] 이후, 사용자 단말(110)은 생성된 트랜잭션을 블록체인 망에 게시한다(630).

[0127] 도 7은 제1 실시예에 따라 서비스 서버(120)에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도이다.

[0128] 우선, 서비스 서버(120)는 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명의 유효성을 검증한다(710).

[0129] 이후, 서비스 서버(120)는 검증된 가명에 기초하여 마지막 블록 내 사용자 관련 정보의 유효성을 검증한다(720).

[0130] 상기 도시된 흐름도 도 6 및 도 7에서는 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.

[0131] 도 8은 일 실시예에서 블록에 블룸 필터를 생성하는 상태를 나타내는 도면이다. 도 8을 참조하면, 블록체인의 첫 번째 블록(S1)이 6개의 트랜잭션으로 구성되고, 마지막 트랜잭션은 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 기반으로 생성된 제1 블룸 필터(BF1)일 수 있다.

[0132] 여기서, 두 번째 블록(S2)을 첫 번째 블록(S1)에 연결하는 경우, 마이너 노드(140)는 첫 번째 블록(S1)의 제1 블룸 필터(BF1)에 두 번째 블록(S2)의 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 추가하여 제2 블룸 필터(BF2)를 생성할 수 있다. 이때, 제2 블룸 필터(BF2)는 두 번째 블록(S2)의 마지막 트랜잭션일 수 있다.

[0133] 그리고, 세 번째 블록(S3)을 두 번째 블록(S2)에 연결하는 경우, 마이너 노드(140)는 두 번째 블록(S2)의 제2 블룸 필터(BF2)에 세 번째 블록(S3)의 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 추가하여 제3 블룸 필터(BF3)를 생성할 수 있다. 이때, 제3 블룸 필터(BF3)는 세 번째 블록(S3)의 마지막 트랜잭션일 수 있다.

[0134] 이러한 방식으로 블룸 필터를 생성하면, 블록체인에서 각 블록의 블룸 필터는 이전 블록의 블룸 필터가 누적된 값을 가지게 된다. 이 경우, 블록체인의 마지막 블록의 블룸 필터는 블록체인에 포함된 각 트랜잭션들에 포함된 사용자 관련 정보들을 멤버로 하게 되므로, 멤버쉽 체크가 필요한 경우 블록체인의 마지막 블록의 블룸 필터를 이용하여 용이하게 수행할 수 있게 된다.

[0135] 즉, 블록체인 내에서 소정 사용자에 대한 멤버쉽 체크가 필요한 경우, 블록체인의 마지막 블록의 블룸 필터를 조회하고, 소정 사용자의 사용자 관련 정보(예를 들어, 사용자의 가명 등)에 대해 블룸 필터가 예스(Yes) 또는 노(No)를 보고하는지를 확인하여 멤버쉽 체크를 진행할 수 있다. 블룸 필터가 예스(Yes)로 보고하는 경우, 마이너 노드(140)는 해당 사용자가 유효한 멤버인 것으로 판단할 수 있다. 블룸 필터가 노(No)로 보고하는 경우, 마이너 노드(140)는 해당 사용자가 유효하지 않은 멤버인 것으로 판단할 수 있다.

[0136] 여기서, 각 블록의 블룸 필터는 이전 블록의 블룸 필터가 누적된 상태이므로, 어떤 시점에서는 블룸 필터의 긍정 오류(False Positive)가 무시할 수 없는 수준에 도달할 수 있게 된다. 이에, 마이너 노드(140)는 블룸 필터의 긍정 오류가 기 설정된 임계 값을 초과하는 경우, 블룸 필터의 크기를 키울 수 있다.

[0137] 구체적으로, 마이너 노드(140)는 소정 블록에 대해 블룸 필터를 생성하는 경우, 이전 블록의 블룸 필터를 조회하여 긍정 오류(False Positive)를 산출할 수 있다. 여기서, 긍정 오류(FP)는 하기의 수학식을 통해 산출할 수 있다.

[0138] [수학식]

$$FP = (1 - (1 - \frac{1}{M})^{l-N})^{l}$$

[0139]

[0140] 여기서, M은 현재 블룸 필터의 크기를 나타내고, l은 블룸 필터를 위한 해쉬 함수의 수를 나타내며, N은 블룸 필터의 축적된 수를 나타낸다.

[0141] 마이너 노드(140)는 산출된 긍정 오류(FP)가 기 설정된 임계 값을 초과하는 경우, 블룸 필터의 크기를 리사이징(Resizing) 할 수 있다. 즉, 블룸 필터의 크기를 현재 블룸 필터의 크기보다 크게 리사이징 할 수 있다. 이때, 마이너 노드(140)는 블록체인의 모든 트랜잭션(즉, 첫 번째 블록에서 현재 블록에 포함된 모든 트랜잭션)들에 포함된 사용자 관련 정보들을 사용하여 블룸 필터를 재구성할 수 있다. 블룸 필터의 크기는 블룸 필터의 크기의 성장 속도에 따라 조정될 수 있다.

[0142] 한편, 개시되는 실시예에서는 블룸 필터로 카운팅 블룸 필터(Counting Bloom Filter)를 사용할 수도 있다. 일반적인 블룸 필터는 멤버의 삭제가 불가능하나, 카운팅 블룸 필터는 멤버의 삭제가 가능하다.

[0143] 예시적인 실시예에서, 사용자 단말(110)은 특정 사용자 관련 정보의 삭제를 마이너 노드(140)에 요청할 수 있다. 이를 위해, 블록체인의 트랜잭션은 멤버의 삽입 요청인지 삭제 요청인지를 나타내는 필드를 포함할 수 있다. 마이너 노드(140)는 트랜잭션의 해당 필드에서 멤버의 삽입 요청인지 삭제 요청인지를 확인하여 삭제 요청인 경우 해당 셀에서 해당 멤버의 해쉬값에 대응하는 카운트를 줄일 수 있다. 만약, 멤버의 삽입 요청인 경우, 마이너 노드(140)는 해당 멤버의 해쉬 값에 해당하는 각 셀의 카운트를 증가시킬 수 있다.

[0144] 또한, 개시되는 실시예에서는 취소된 멤버를 위한 블룸 필터를 별도로 사용할 수도 있다. 이 경우, 2개의 블룸 필터가 존재할 수 있다. 즉, 유효한 멤버를 위한 블룸 필터(유효 멤버 블룸 필터)와 취소된 멤버를 위한 블룸 필터(취소 멤버 블룸 필터)가 있을 수 있다.

[0145] 사용자 단말(110)은 특정 사용자 관련 정보에 대해 삭제 또는 추가를 마이너 노드(140)에 요청할 수 있다. 마이너 노드(140)는 트랜잭션에서 멤버의 삽입 요청인지 삭제 요청인지를 나타내는 필드를 확인하여 삭제 요청이면 해당 사용자 관련 정보를 취소 멤버 블룸 필터에 추가하고, 삽입 요청이면 해당 사용자 관련 정보를 유효 멤버 블룸 필터에 추가할 수 있다.

[0146] 개시되는 실시예에 의하면, 사용자 단말(110)이 사용자 관련 정보를 포함하는 트랜잭션을 서명하여 블록체인 망에 브로드캐스팅 하고, 블록체인 망의 마이너 노드(140)에서 트랜잭션을 기반으로 각 블록에 대해 블룸 필터를 생성함으로써, 탈 중앙화된(Decentralized) 방식으로 블룸 필터를 생성할 수 있게 된다.

[0147] 또한, 블록체인의 각 블록에서 이전 블록의 블룸 필터를 누적시킴으로써, 블록체인의 마지막 블록의 블룸 필터를 확인하면 해당 블록체인 망에 대해 멤버쉽 체크를 용이하게 수행할 수 있게 된다. 또한, 블룸 필터를 통해 사용자 멤버쉽의 삭제 및 추가 기능을 제공할 수 있게 된다.

[0148] 도 9는 제2 실시예에 따라 사용자 단말(110)에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도이다.

[0149] 우선, 사용자 단말(110)은 블록체인 망에 포함된 서비스 서버의 공개키를 이용하여 사용자 관련 정보에 대한 암호문을 생성한다(910).

[0150] 이후, 사용자 단말(110)은 인증된 가명에 기초하여 암호문에 대한 서명을 생성한다(920).

[0151] 이후, 사용자 단말(110)은 인증된 가명, 암호문 및 암호문에 대한 서명을 포함하는 트랜잭션을 생성한다(930).

[0152] 이후, 사용자 단말(110)은 생성된 트랜잭션을 블록체인 망에 게시한다(940).

[0153] 도 10은 제2 실시예에 따라 서비스 서버(120)에서 수행되는 데이터 관리 방법을 설명하기 위한 흐름도이다.

[0154] 우선, 서비스 서버(120)는 블록체인 망의 블록체인을 구성하는 하나 이상의 블록 중 마지막 블록을 참조하여, 마지막 블록 내 가명의 유효성을 검증한다(1010).

[0155] 이후, 서비스 서버(120)는 검증된 가명에 기초하여 마지막 블록 내 암호문의 유효성을 검증한다(1020).

[0156] 이후, 서비스 서버(120)는 서비스 서버의 비밀키로 검증된 암호문을 복호화한다(1030).

[0157] 상기 도시된 흐름도 도 9 및 도 10에서는 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.

[0158] 도 11은 일 실시예에 따른 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.

[0159] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 사용자 단말(110)일 수 있다. 또한, 컴퓨팅 장치(12)는 서비스 서버(120)일 수 있다. 또한, 컴퓨팅 장치(12)는 인증 기관(130)일 수 있다. 또한, 컴퓨팅 장치(12)는 마이너 노드(140)일 수 있다.

[0160] 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 있

다. 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.

[0161] 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.

[0162] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0163] 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.

[0164] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0165] 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 청구범위 뿐만 아니라 이 청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0167] 10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

100: 데이터 관리 시스템

110: 사용자 단말

111: 서명 생성 모듈

113: 트랜잭션 생성 모듈

115: 통신 모듈

117: 암호화 모듈

120: 서비스 서버

121: 가명 검증 모듈

123: 사용자 관련 정보 검증 모듈

125: 암호문 검증 모듈

127: 복호화 모듈

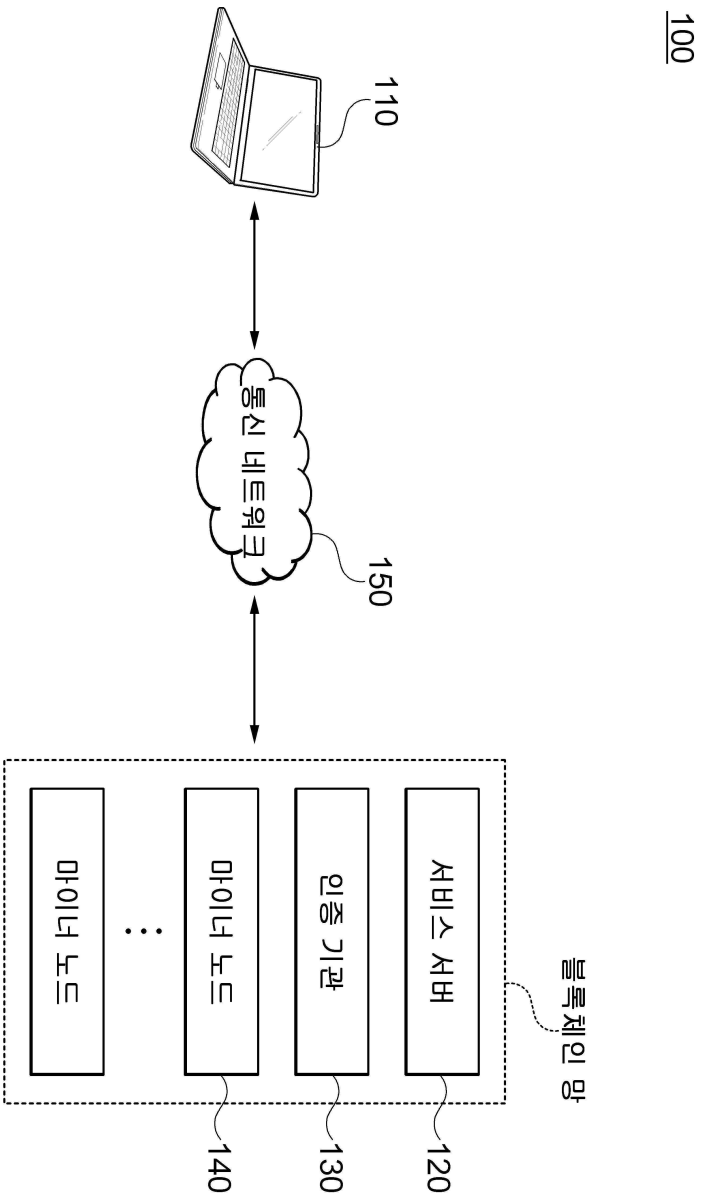
130: 인증 기관

140: 마이너 노드

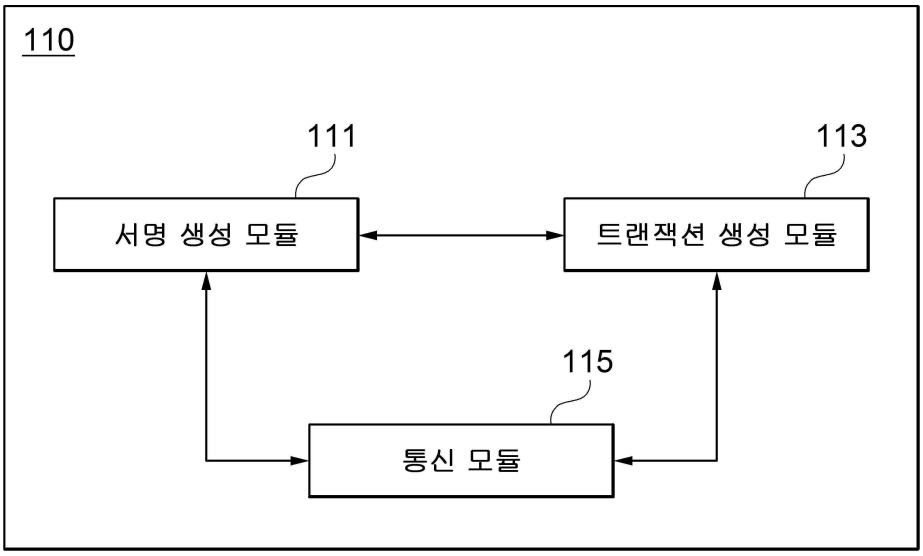
150: 통신 네트워크

도면

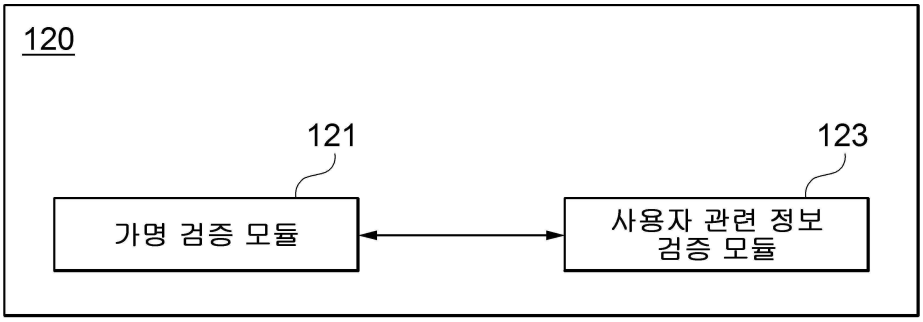
도면1



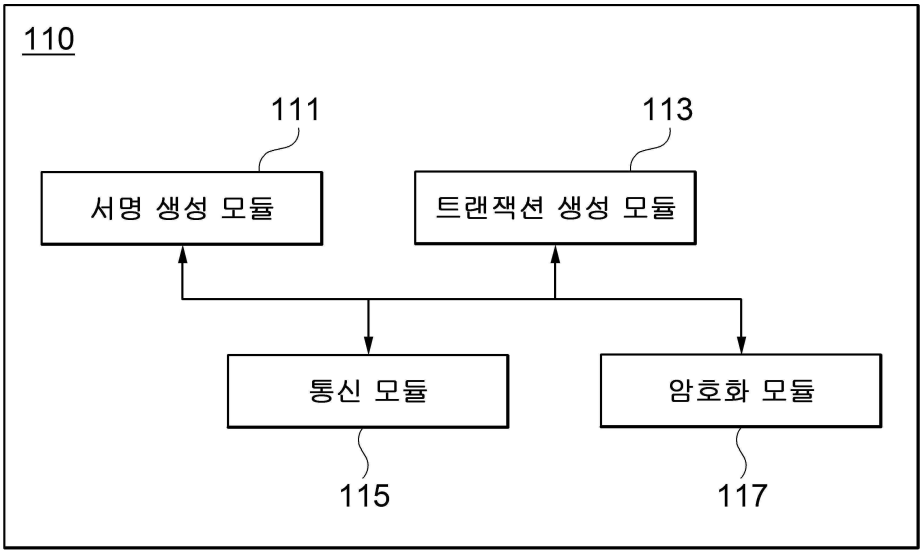
도면2


110
111
113
서명 생성 모듈
트랜잭션 생성 모듈
115
통신 모듈

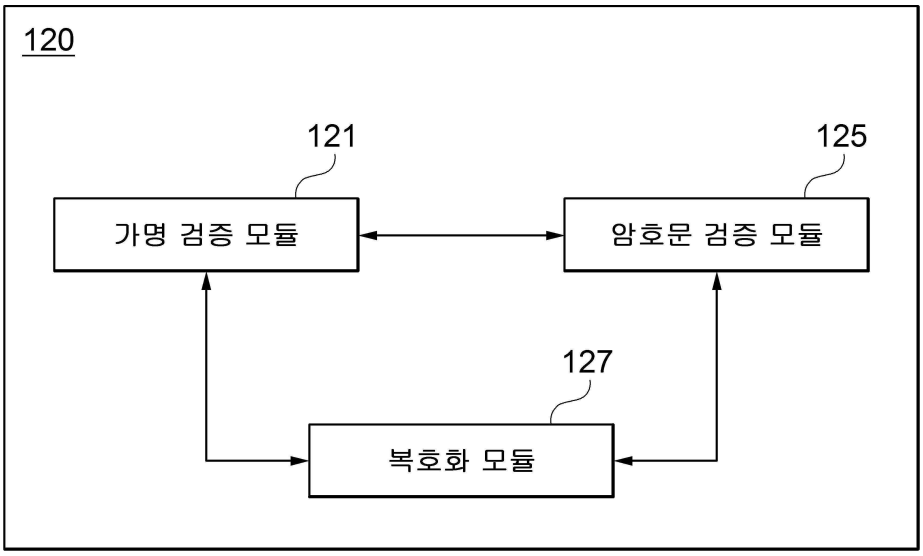
도면3


120
121
123
가명 검증 모듈
사용자 관련 정보
검증 모듈

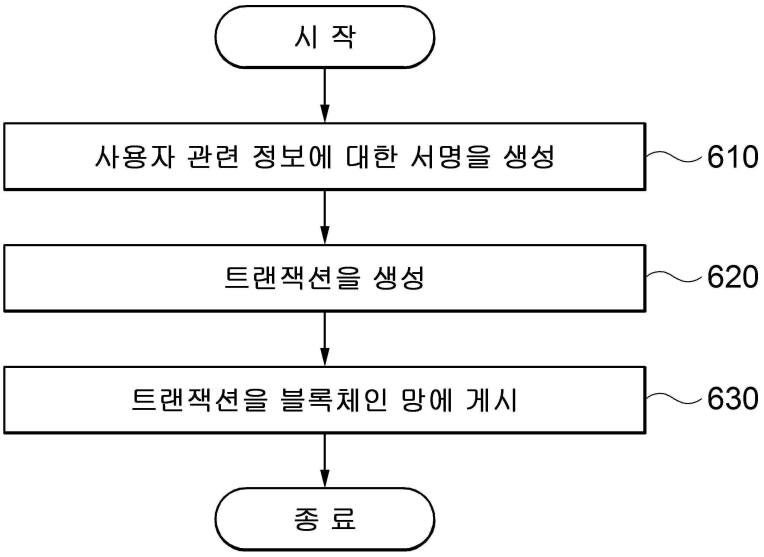
도면4


110
111
113
서명 생성 모듈
트랜잭션 생성 모듈
통신 모듈
암호화 모듈
115
117

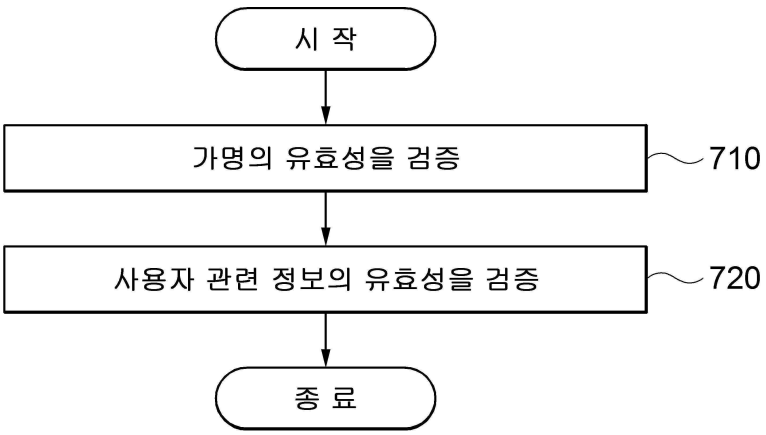
도면5


120
121
125
가명 검증 모듈
암호문 검증 모듈
127
복호화 모듈

도면6

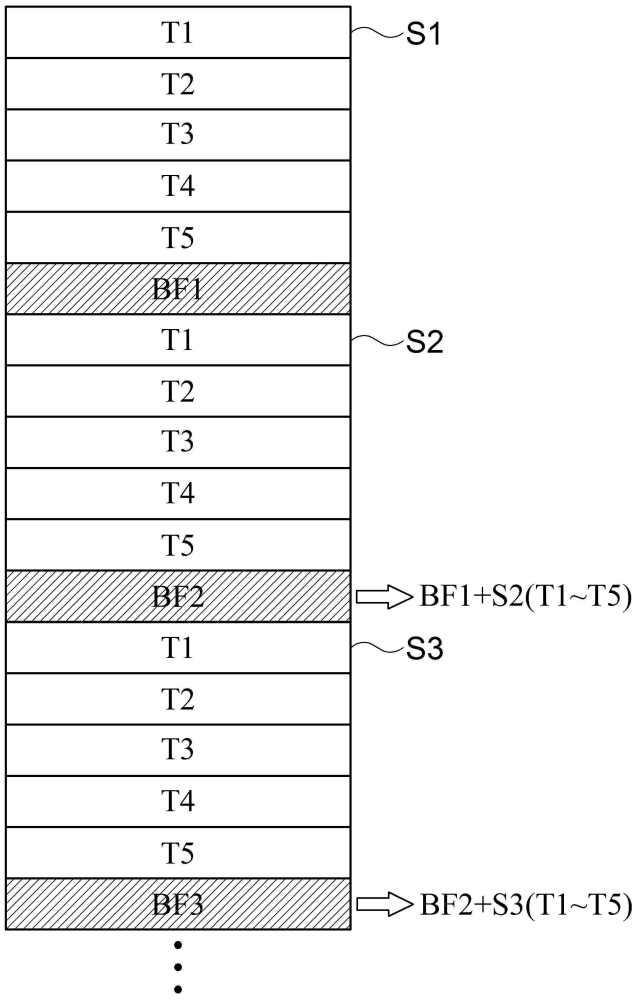

시 작
사용자 관련 정보에 대한 서명을 생성
610
트랜잭션을 생성
620
트랜잭션을 블록체인 망에 게시
630
종 료

도면7

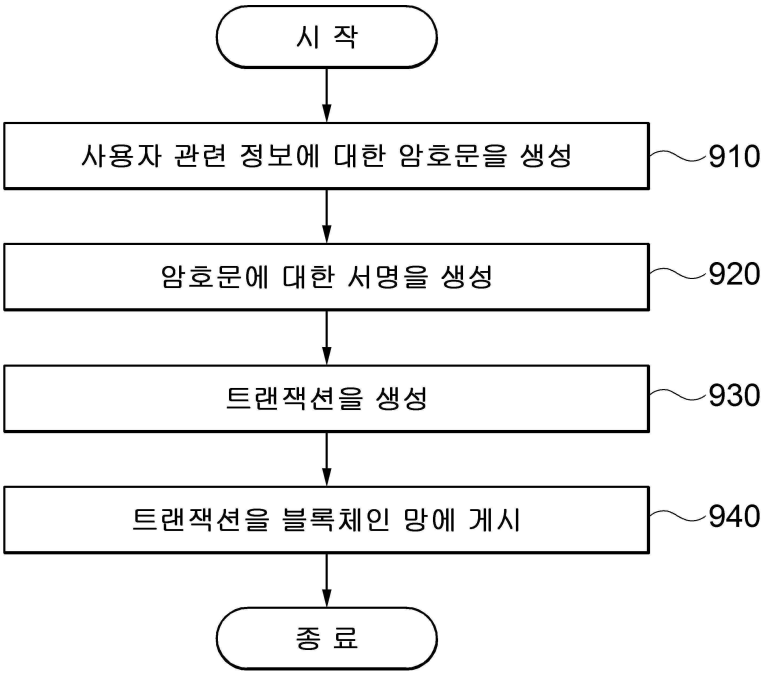

시 작
가명의 유효성을 검증
710
사용자 관련 정보의 유효성을 검증
720
종 료

도면8

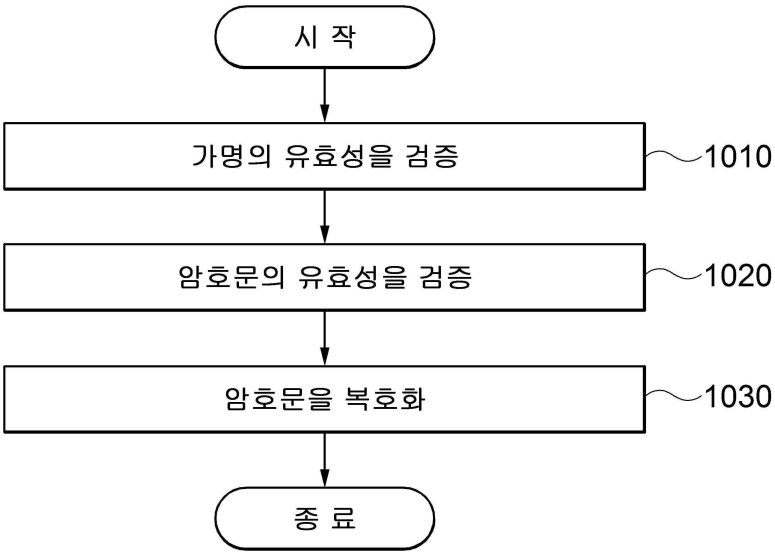
800


T1
S1
T2
T3
T4
T5
BF1
T1
S2
T2
T3
T4
T5
BF2
BF1+S2(T1~T5)
T1
S3
T2
T3
T4
T5
BF3
BF2+S3(T1~T5)

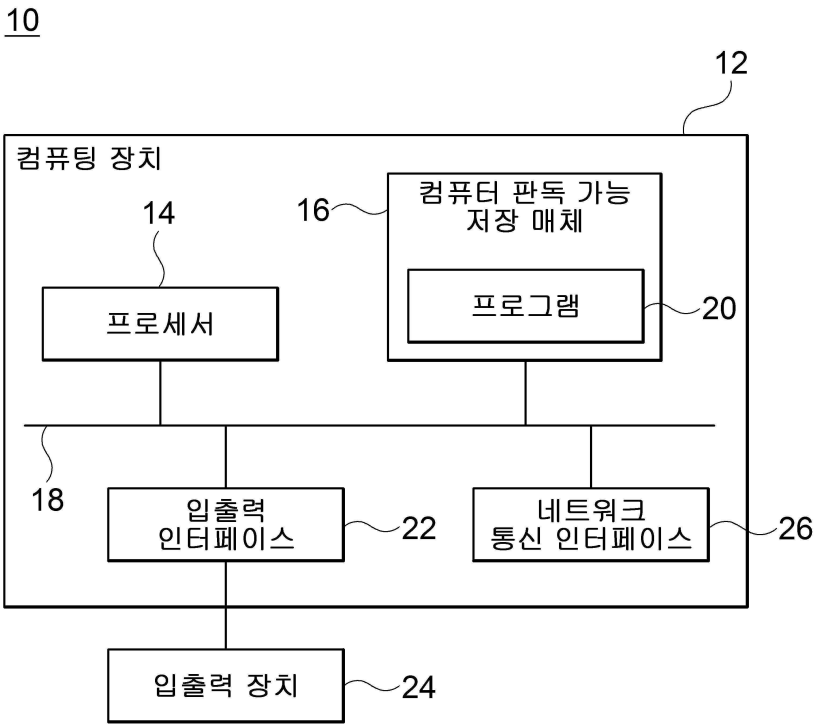
도면9


시 작
사용자 관련 정보에 대한 암호문을 생성
910
암호문에 대한 서명을 생성
920
트랜잭션을 생성
930
트랜잭션을 블록체인 망에 게시
940
종 료

도면10


시 작
가명의 유효성을 검증
1010
암호문의 유효성을 검증
1020
암호문을 복호화
1030
종 료

도면11


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