(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0080671
(43) 공개일자 2020년07월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/321 (2013.01)
H04L 9/0833 (2013.01)
(21) 출원번호 10-2018-0170353
(22) 출원일자 2018년12월27일
심사청구일자 2018년12월27일

(71) 출원인
한림대학교 산학협력단
강원도 춘천시 한림대학길 1, 한림대학교(옥천동)
(72) 발명자
조효진
강원도 춘천시 한림대학길 1, 한림대학교 공학관 1305호
정수지
서울특별시 성동구 장터5길 11-6, 301호
(74) 대리인
김남혁

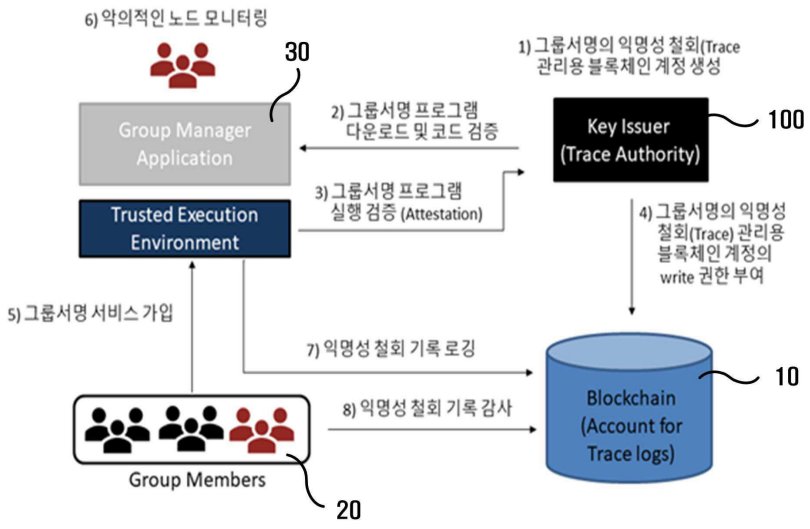
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법, 장치 및 프로그램**

(57) 요 약

컴퓨터에 의하여 수행되는 방법에 있어서, 그룹서명 키를 생성하는 단계, 하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계, 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계, 상기 그룹서명의 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계, 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 TEE 환경(Trusted Execution Environment: 신뢰컴퓨팅 환경)에서 수행하는 단계 및 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계를 포함하고, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 하는, 공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법이 개시된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0894 (2013.01)
H04L 9/3247 (2013.01)
H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2018-0-00216
부처명 정보통신기술진흥센터
연구관리전문기관 한림대학교 산학협력단
연구사업명 SW중심대학
연구과제명 SW중심대학(한림대학교)
기 여 율 1/2
주관기관 한림대학교 산학협력단
연구기간 2018.09.01 ~ 2018.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 H20180758
부처명 한국연구재단
연구관리전문기관 한림대학교 산학협력단
연구사업명 생애 첫 연구사업
연구과제명 차량 해킹 공격에 강건한 스마트 자동차 시스템을 위한 인증, 도스 미티게이터, 그리고 로깅 기술의 연구
기 여 율 1/2
주관기관 한림대학교 산학협력단
연구기간 2018.09.01 ~ 2019.02.28

명 세 서

청구범위

청구항 1

컴퓨터에 의하여 수행되는 방법에 있어서,

그룹서명 키를 생성하는 단계;

하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계;

상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계;

상기 그룹서명의 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계;

상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 TEE 환경(Trusted Execution Environment: 신뢰컴퓨팅 환경)에서 수행하는 단계; 및

상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계; 를 포함하고,

상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 2

제1 항에 있어서,

상기 그룹서명을 수행하기 위한 프로그램을 획득하는 단계; 및

상기 프로그램에 대한 코드 검증을 수행하는 단계; 를 더 포함하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 3

제2 항에 있어서,

상기 TEE 환경에 기반하여 상기 그룹 매니저가 상기 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 상기 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인하는, 단계; 를 더 포함하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 4

제3 항에 있어서,

상기 확인하는 단계는,

상기 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계; 를 포함하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 5

제1 항에 있어서,

상기 그룹서명 키를 발급하는 단계는,

상기 하나 이상의 사용자를 그룹서명 프로그램에 등록하는 단계; 및

상기 하나 이상의 사용자에게 상기 그룹서명 생성에 필요한 공개 값(Group Public Values) 및 상기 그룹서명 키를 발급하는 단계; 를 포함하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 6

제1 항에 있어서,

상기 하나 이상의 사용자에 의하여 생성되는 그룹서명 값 중 악의적인 행동과 관련된 그룹서명 값이 확인되는 경우, 상기 그룹서명 값에 대한 익명성 철회를 요청하는 단계; 를 더 포함하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 7

제1 항에 있어서,

상기 하나 이상의 사용자 중 적어도 일부로부터 제1 익명성 철회 기록에 대한 이의제기 정보를 수신하는 단계;

상기 하나 이상의 사용자 중 절반 이상으로부터 상기 제1 익명성 철회 기록에 대한 이의제기 정보가 수신되는 경우, 상기 그룹 매니저에 대한 재신임 여부를 상기 하나 이상의 사용자에 질의하는 단계;

상기 하나 이상의 사용자 중 절반 이상의 합의에 기반하여 상기 그룹 매니저의 재신임 여부를 결정하는 단계;

상기 그룹 매니저의 해임이 결정되는 경우, 상기 하나 이상의 사용자 중 하나를 그룹 매니저로 선임하는 단계;

상기 해임된 그룹 매니저의 상기 블록체인 계정에 대한 쓰기 권한을 박탈하는 단계; 및

상기 선임된 그룹 매니저가 상기 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 선임된 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 상기 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인하는, 단계; 및

상기 선임된 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 선임된 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계; 를 더 포함하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 8

컴퓨터에 의하여 수행되는 방법에 있어서,

그룹서명 키를 생성하는 단계;

하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계;

상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계;

상기 TEE 환경에 기반하여 상기 그룹서명의 그룹 매니저가 상기 그룹서명을 수행하기 위한 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인하는, 단계;

상기 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계;

상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 상기 TEE 환경에서 수행하는 단계; 및

상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계; 를 포함하고,

상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법.

청구항 9

하나 이상의 인스트럭션을 저장하는 메모리; 및

상기 메모리에 저장된 상기 하나 이상의 인스트럭션을 실행하는 프로세서를 포함하고,

상기 프로세서는 상기 하나 이상의 인스트럭션을 실행함으로써,

제1 항의 방법을 수행하는,

공개적으로 감사가 가능한 그룹서명 프레임워크 제공장치.

청구항 10

하드웨어인 컴퓨터와 결합되어, 제1 항의 방법을 수행할 수 있도록 컴퓨터에서 독출가능한 기록매체에 저장된 컴퓨터프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법, 장치 및 프로그램에 관한 것이다.

배 경 기 술

[0002] 기존의 일반적인 전자서명 알고리즘(예를 들어, RSA, ECDSA)은 익명성(Anonymity)을 제공하지 못하므로 익명성을 보장하는 그룹서명 알고리즘이 제안되었다.

[0003] 그룹서명은 일반적으로 키발급기관/추적기관(Key Issuer/Trace Authority), 그룹 관리자(Group Manager) 및 그룹멤버(Group Member)로 이루어진다.

[0004] 그룹 관리자는 키발급기관/추적기관으로부터 그룹 멤버들에게 그룹 서명키를 만들어 줄 수 있는 권한을 받고, 그룹 멤버들에게 그룹서명키를 발급한다. 그룹 멤버는 발급받은 그룹 서명키를 사용하여 그룹 서명을 수행할 수 있다. 그룹 서명 방법은 그룹 서명값이 임의의 그룹에서 발생했다는 것을 검증과정을 통해 알 수 있지만, 해당 그룹에서 어떤 멤버가 그룹서명을 수행했는지 알 수 없도록 설계된다.

[0005] 만약 그룹 서명된 메시지에서 문제가 발생 할 경우, 키발급기관/추적기관은 그룹서명에 대한 익명성을 철회(Revocation)하여, 그룹 서명값을 만들 그룹 멤버를 추적 (Traceability) 할 수 있다.

[0006] 최근 프라이버시에 대한 관심도가 증가하면서 그룹서명에 대한 수요가 증가하였고, 그룹 서명을 효율적으로 설계하는 연구들이 많이 수행되었다.

[0007] 하지만, 그룹서명값은 키발급기관/추적기관에 의해 서명을 수행한 특정 개체를 추적할 수 있는 바, 키발급기관/추적기관을 신뢰해야 하는 가정이 있다. 따라서 키발급기관/추적기관에 권한이 집중되는 “Big Brother” 문제가 생길 수도 있는 등 문제점이 존재한다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 등록특허공보 제10-1780774호

발명의 내용

해결하려는 과제

[0009] 본 발명이 해결하고자 하는 과제는 공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법, 장치 및 프로그램을 제공하는 것이다.

[0010] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 상술한 과제를 해결하기 위한 본 발명의 일 면에 따른 공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법은, 그룹서명 키를 생성하는 단계, 하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계, 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계, 상기 그룹서명의 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계, 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 TEE 환경(Trusted Execution Environment: 신뢰컴퓨팅 환경)에서 수행하는 단계 및 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계를 포함하고, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 한다.

[0012] 또한, 상기 그룹서명을 수행하기 위한 프로그램을 획득하는 단계 및 상기 프로그램에 대한 코드 검증을 수행하는 단계를 더 포함할 수 있다.

[0013] 또한, 상기 TEE 환경에 기반하여 상기 그룹 매니저가 상기 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 상기 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인하는, 단계를 더 포함할 수 있다.

[0014] 또한, 상기 확인하는 단계는, 상기 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계를 포함할 수 있다.

[0015] 또한, 상기 그룹서명 키를 발급하는 단계는, 상기 하나 이상의 사용자를 그룹서명 프로그램에 등록하는 단계 및 상기 하나 이상의 사용자에게 상기 그룹서명 생성에 필요한 공개 값(Group Public Values) 및 상기 그룹서명 키를 발급하는 단계를 포함할 수 있다.

[0016] 또한, 상기 하나 이상의 사용자에 의하여 생성되는 그룹서명 값 중 악의적인 행동과 관련된 그룹서명 값이 확인되는 경우, 상기 그룹서명 값에 대한 익명성 철회를 요청하는 단계를 더 포함할 수 있다.

[0017] 또한, 상기 하나 이상의 사용자 중 적어도 일부로부터 제1 익명성 철회 기록에 대한 이의제기 정보를 수신하는 단계, 상기 하나 이상의 사용자 중 절반 이상으로부터 상기 제1 익명성 철회 기록에 대한 이의제기 정보가 수신되는 경우, 상기 그룹 매니저에 대한 재신임 여부를 상기 하나 이상의 사용자에 질의하는 단계, 상기 하나 이상의 사용자 중 절반 이상의 합의에 기반하여 상기 그룹 매니저의 재신임 여부를 결정하는 단계, 상기 그룹 매니저의 해임이 결정되는 경우, 상기 하나 이상의 사용자 중 하나를 그룹 매니저로 선임하는 단계, 상기 해임된 그룹 매니저의 상기 블록체인 계정에 대한 쓰기 권한을 박탈하는 단계 및 상기 선임된 그룹 매니저가 상기 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 선임된 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 상기 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인하는, 단계 및 상기 선임된 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 선임된 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계를 더 포함할 수 있다.

[0018] 상술한 과제를 해결하기 위한 본 발명의 일 면에 따른 공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법은, 그룹서명 키를 생성하는 단계, 하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계, 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계, 상기 TEE 환경에 기반하여 상기 그룹서명의 그룹 매니저가 상기 그룹서명을 수행하기 위한 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인하는, 단계, 상기 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계, 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 상기 TEE 환경에서 수행하는 단계 및 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계를 포함하고, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 할 수 있다.

[0019] 상술한 과제를 해결하기 위한 본 발명의 일 면에 따른 공개적으로 감사가 가능한 그룹서명 프레임워크 제공장치는, 하나 이상의 인스트럭션을 저장하는 메모리 및 상기 메모리에 저장된 상기 하나 이상의 인스트럭션을 실행

하는 프로세서를 포함하고, 상기 프로세서는 상기 하나 이상의 인스트럭션을 실행함으로써, 그룹서명 키를 생성하는 단계, 하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계, 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계, 상기 그룹서명의 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계, 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 TEE 환경(Trusted Execution Environment: 신뢰컴퓨팅 환경)에서 수행하는 단계 및 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계를 포함하고, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 하는 방법을 수행할 수 있다.

[0020] 상술한 과제를 해결하기 위한 본 발명의 일 면에 따른 공개적으로 감사가 가능한 그룹서명 프레임워크 제공 프로그램은, 하드웨어인 컴퓨터와 결합되어, 그룹서명 키를 생성하는 단계, 하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계, 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계, 상기 그룹서명의 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계, 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 TEE 환경(Trusted Execution Environment: 신뢰컴퓨팅 환경)에서 수행하는 단계 및 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계를 포함하고, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 하는 방법을 수행할 수 있도록 컴퓨터에서 독출가능한 기록매체에 저장된다.

[0021] 본 발명의 기타 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

[0022] 개시된 실시 예에 따르면, 그룹서명 사용자들로 하여금 공개적으로 그룹 매니저의 활동을 감사할 수 있도록 하는 프레임워크가 제공되는 효과가 있다.

[0023] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0024] 도 1은 일 실시 예에 따른 시스템을 도시한 도면이다.

도 2는 일 실시 예에 따른 공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법을 도시한 흐름도이다.

도 3은 일 실시 예에 따른 그룹 매니저 검증방법을 도시한 흐름도이다.

도 4는 일 실시 예에 따른 그룹 매니저 관리방법을 도시한 흐름도이다.

도 5는 일 실시 예에 따른 장치의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0026] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.

[0027] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0028] 명세서에서 사용되는 "부" 또는 “모듈”이라는 용어는 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, "부" 또는 “모듈”은 어떤 역할들을 수행한다. 그렇지만 "부" 또는 “모듈”은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. "부" 또는 “모듈”은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 "부" 또는 “모듈”은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 "부" 또는 “모듈”들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 "부" 또는 “모듈”들로 결합되거나 추가적인 구성요소들과 "부" 또는 “모듈”들로 더 분리될 수 있다.

[0029] 공간적으로 상대적인 용어인 "아래(below)", "아래(beneath)", "하부(lower)", "위(above)", "상부(upper)" 등은 도면에 도시되어 있는 바와 같이 하나의 구성요소와 다른 구성요소들과의 상관관계를 용이하게 기술하기 위해 사용될 수 있다. 공간적으로 상대적인 용어는 도면에 도시되어 있는 방향에 더하여 사용시 또는 동작시 구성요소들의 서로 다른 방향을 포함하는 용어로 이해되어야 한다. 예를 들어, 도면에 도시되어 있는 구성요소를 뒤집을 경우, 다른 구성요소의 "아래(below)"또는 "아래(beneath)"로 기술된 구성요소는 다른 구성요소의 "위(above)"에 놓여질 수 있다. 따라서, 예시적인 용어인 "아래"는 아래와 위의 방향을 모두 포함할 수 있다. 구성요소는 다른 방향으로도 배향될 수 있으며, 이에 따라 공간적으로 상대적인 용어들은 배향에 따라 해석될 수 있다.

[0030] 본 명세서에서, 컴퓨터는 적어도 하나의 프로세서를 포함하는 모든 종류의 하드웨어 장치를 의미하는 것이고, 실시 예에 따라 해당 하드웨어 장치에서 동작하는 소프트웨어적 구성도 포괄하는 의미로서 이해될 수 있다. 예를 들어, 컴퓨터는 스마트폰, 태블릿 PC, 데스크톱, 노트북 및 각 장치에서 구동되는 사용자 클라이언트 및 애플리케이션을 모두 포함하는 의미로서 이해될 수 있으며, 또한 이에 제한되는 것은 아니다.

[0031] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.

[0032] 본 명세서에서 설명되는 각 단계들은 컴퓨터에 의하여 수행되는 것으로 설명되나, 각 단계의 주체는 이에 제한되는 것은 아니며, 실시 예에 따라 각 단계들의 적어도 일부가 서로 다른 장치에서 수행될 수도 있다.

[0033] 도 1은 일 실시 예에 따른 시스템을 도시한 도면이다.

[0034] 도 1을 참조하면, 시스템은 블록체인(10), 그룹 멤버(20), 그룹 매니저(30) 및 키 발행자(Key Issuer: 100)를 포함한다.

[0035] 일 실시 예에서, 블록체인(10)은 블록체인 보유서버들을 의미할 수 있으나 이에 제한되는 것이 아니며, 특정한 대상을 지칭하는 것이 아닌 개시된 실시 예에 따른 블록체인 시스템 및 이에 저장된 정보들을 포괄하는 의미로도 이해될 수 있다.

[0036] 일 실시 예에서, 블록체인(10)은 추적 로그를 저장하기 위한 블록체인 계정에 대응할 수 있다.

[0037] 개시된 실시 예에서, 키 발행자(100)는 그룹서명을 위한 키를 생성 및 제공하며, 또한 그룹 매니저(30)에 익명성 철회 및 추적 권한을 부여할 수 있다.

[0038] 그룹 멤버(20)에 포함된 사용자들은 그룹서명을 이용하고자 하는 경우 키 발행자(100)로부터 그룹서명 키를 발급받아 이용할 수 있다.

[0039] 그룹서명의 경우 그 서명자를 확인할 수 없는 것을 특징으로 하나, 키 발행자(100)로부터 권한을 수여받은 그룹 매니저(30)의 경우 익명성을 철회하고, 서명자를 추적하는 것이 가능하다.

[0040] 이는 그룹서명의 익명성을 악용하는 것을 방지하기 위함이나, 이 경우 그룹 매니저를 신뢰할 수 있어야 한다는 전제조건이 요구된다.

[0041] 따라서, 개시된 실시 예에 따르면 그룹 멤버(20)들에 의하여 공개적으로 그룹 매니저(30)에 대한 감사가 가능하

도록 하는 프레임워크를 제공하는 방법이 제공된다.

[0042] 도 2는 일 실시 예에 따른 공개적으로 감사가 가능한 그룹서명 프레임워크 제공방법을 도시한 흐름도이다.

[0043] 개시된 실시 예에 따른 방법은 이하에서 컴퓨터에 의하여 수행되는 것으로 서술되나, 그 구체적인 주체는 제한되지 않는다. 예를 들어, 컴퓨터는 키 발행자를 의미할 수 있으나 이에 제한되지 않으며, 그룹 매니저 및 그룹 멤버들에 속하는 사용자 등을 포함할 수 있고, 또한 이에 제한되지 않는다.

[0044] 단계 S110에서, 컴퓨터는 그룹서명 키를 생성한다.

[0045] 단계 S120에서, 컴퓨터는 하나 이상의 사용자에게 상기 그룹서명 키를 발급한다.

[0046] 단계 S130에서, 컴퓨터는 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성한다.

[0047] 일 실시 예에서, 컴퓨터는 그룹서명의 익명성 철회(Trace) 기록을 저장할 수 있는 블록체인 계정을 생성하고, 해당 계정에 그룹서명의 Trace 기록을 write(쓰기)할 수 있는 권한 관리 스마트컨트랙트를 구현하며, 이를 블록체인 노드들에 배포할 수 있다.

[0048] 단계 S140에서, 컴퓨터는 상기 그룹서명의 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여한다.

[0049] 단계 S150에서, 컴퓨터는 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 TEE 환경(Trusted Execution Environment: 신뢰컴퓨팅 환경)에서 수행한다.

[0050] 단계 S160에서, 컴퓨터는 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록한다.

[0051] 도 2에 도시된 실시 예에서, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 한다.

[0052] 즉, 그룹 매니저는 익명성 철회 과정을 수행할 수 있으나 이는 TEE 환경 하에서 수행되며, 익명성 철회기록은 블록체인 계정에 기록되어 위변조 불가능할뿐 아니라 그룹 멤버들에 의하여 접근 및 열람가능하게 됨으로써, 그룹 매니저에 대한 그룹 멤버들의 감사를 가능케 한다.

[0053] 또한, 개시된 실시 예에서, 컴퓨터는 그룹서명을 수행하기 위한 프로그램을 획득하고, 상기 프로그램에 대한 코드 검증을 수행할 수 있다.

[0054] 예를 들어, 그룹 매니저 혹은 그룹 멤버들은 키 발행자로부터 그룹서명을 수행하기 위한 프로그램을 획득하고, 해당 프로그램에 악의적인 내용(예를 들어, 키 발행자의 백도어 코드 등)이 포함되어 있는지 여부를 확인하기 위한 코드 검증을 수행할 수 있다.

[0055] 일 실시 예에서, 상술한 그룹서명 키를 발급하는 단계에서, 컴퓨터는 상기 하나 이상의 사용자를 그룹서명 프로그램에 등록하는 단계를 수행할 수 있다.

[0056] 또한, 컴퓨터는 상기 하나 이상의 사용자에게 상기 그룹서명 생성에 필요한 공개 값(Group Public Values) 및 상기 그룹서명 키를 발급하는 단계를 수행할 수 있다.

[0057] 일 실시 예에서, 컴퓨터는 상기 하나 이상의 사용자에 의하여 생성되는 그룹서명 값 중 악의적인 행동과 관련된 그룹서명 값이 확인되는 경우, 상기 그룹서명 값에 대한 익명성 철회를 요청하는 단계를 수행할 수 있다.

[0058] 예를 들어, 그룹 매니저는 상기 하나 이상의 사용자에 의하여 생성되는 그룹서명 값 중 악의적인 행동과 관련된 그룹서명 값이 확인되는 경우, 상기 그룹서명 값에 대한 익명성 철회를 요청하는 단계를 수행할 수 있다.

[0059] 도 3은 일 실시 예에 따른 그룹 매니저 검증방법을 도시한 흐름도이다.

[0060] 도 3에 도시된 방법은 도 2에 도시된 방법의 일 실시 예에 해당하므로, 도 2와 관련하여 설명된 내용은 도 3의 방법에도 적용될 수 있다.

[0061] 단계 S210에서, 컴퓨터는 그룹서명 키를 생성할 수 있다.

[0062] 단계 S220에서, 컴퓨터는 하나 이상의 사용자에게 상기 그룹서명 키를 발급할 수 있다.

[0063] 단계 S230에서, 컴퓨터는 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성할 수

있다.

[0064] 단계 S240에서, 컴퓨터는 상기 TEE 환경에 기반하여 상기 그룹서명의 그룹 매니저가 상기 그룹서명을 수행하기 위한 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인할 수 있다.

[0065] 단계 S250에서, 컴퓨터는 상기 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여할 수 있다.

[0066] 단계 S260에서, 컴퓨터는 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 상기 TEE 환경에서 수행할 수 있다.

[0067] 단계 S270에서, 컴퓨터는 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록할 수 있다.

[0068] 도 3에 도시된 실시 예에서, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 할 수 있다.

[0069] 도 4는 일 실시 예에 따른 그룹 매니저 관리방법을 도시한 흐름도이다.

[0070] 단계 S310에서, 컴퓨터는 상기 하나 이상의 사용자 중 적어도 일부로부터 제1 익명성 철회 기록에 대한 이의제기 정보를 수신할 수 있다.

[0071] 단계 S320에서, 컴퓨터는 상기 하나 이상의 사용자 중 절반 이상으로부터 상기 제1 익명성 철회 기록에 대한 이의제기 정보가 수신되는 경우, 상기 그룹 매니저에 대한 재신임 여부를 상기 하나 이상의 사용자에 질의할 수 있다.

[0072] 단계 S330에서, 컴퓨터는 상기 하나 이상의 사용자 중 절반 이상의 합의에 기반하여 상기 그룹 매니저의 재신임 여부를 결정할 수 있다.

[0073] 단계 S340에서, 컴퓨터는 상기 그룹 매니저의 해임이 결정되는 경우, 상기 하나 이상의 사용자 중 하나를 그룹 매니저로 선임할 수 있다.

[0074] 단계 S350에서, 컴퓨터는 상기 해임된 그룹 매니저의 상기 블록체인 계정에 대한 쓰기 권한을 박탈할 수 있다.

[0075] 단계 S360에서, 컴퓨터는 상기 선임된 그룹 매니저가 상기 프로그램을 정당하게 실행하는지 여부를 확인하되, 상기 선임된 그룹 매니저가 익명성 철회에 사용하는 추적 키(Trace Key)를 상기 TEE 환경에 기반한, 외부로 노출되지 않는 저장공간에 저장하는지 여부를 확인할 수 있다.

[0076] 단계 S370에서, 컴퓨터는 상기 선임된 그룹 매니저가 상기 프로그램을 정당하게 실행하는 것으로 확인되는 경우, 상기 선임된 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여할 수 있다.

[0077] 도 5는 일 실시 예에 따른 장치의 구성도이다.

[0078] 프로세서(402)는 하나 이상의 코어(core, 미도시) 및 그래픽 처리부(미도시) 및/또는 다른 구성 요소와 신호를 송수신하는 연결 통로(예를 들어, 버스(bus) 등)를 포함할 수 있다.

[0079] 일 실시예에 따른 프로세서(402)는 메모리(404)에 저장된 하나 이상의 인스트럭션을 실행함으로써, 도 1 내지 도 4와과 관련하여 설명된 방법을 수행한다.

[0080] 예를 들어, 프로세서(402)는 메모리에 저장된 하나 이상의 인스트럭션을 실행함으로써 그룹서명 키를 생성하는 단계, 하나 이상의 사용자에게 상기 그룹서명 키를 발급하는 단계, 상기 그룹서명에 대한 익명성 철회 기록을 저장할 수 있는 블록체인 계정을 생성하는 단계, 상기 그룹서명의 그룹 매니저 계정에 상기 블록체인 계정에 대한 쓰기 권한을 부여하는 단계, 상기 그룹 매니저에 의한 익명성 철회 과정이 성공적으로 수행되는 경우, 상기 그룹서명의 로깅 함수를 TEE 환경(Trusted Execution Environment: 신뢰컴퓨팅 환경)에서 수행하는 단계 및 상기 로깅 함수를 수행함에 따라, 상기 익명성 철회에 따른 익명성 철회 기록을 상기 블록체인 계정에 기록하는 단계를 수행하고, 상기 블록체인 계정에 기록된 상기 익명성 철회 기록은, 상기 하나 이상의 사용자에 의하여 접근 및 열람가능한 것을 특징으로 할 수 있다.

[0081] 한편, 프로세서(402)는 프로세서(402) 내부에서 처리되는 신호(또는, 데이터)를 일시적 및/또는 영구적으로 저장하는 램(RAM: Random Access Memory, 미도시) 및 롬(ROM: Read-Only Memory, 미도시)을 더 포함할 수 있다.

또한, 프로세서(402)는 그래픽 처리부, 램 및 롬 중 적어도 하나를 포함하는 시스템온칩(SoC: system on chip) 형태로 구현될 수 있다.

[0082] 메모리(404)에는 프로세서(402)의 처리 및 제어를 위한 프로그램들(하나 이상의 인스트럭션들)을 저장할 수 있다. 메모리(404)에 저장된 프로그램들은 기능에 따라 복수 개의 모듈들로 구분될 수 있다.

[0083] 본 발명의 실시예와 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 발명이 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 판독가능 기록매체에 상주할 수도 있다.

[0084] 본 발명의 구성 요소들은 하드웨어인 컴퓨터와 결합되어 실행되기 위해 프로그램(또는 애플리케이션)으로 구현되어 매체에 저장될 수 있다. 본 발명의 구성 요소들은 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있으며, 이와 유사하게, 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블러(assembler) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다.

[0085] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.

부호의 설명

[0086] 10 : 블록체인

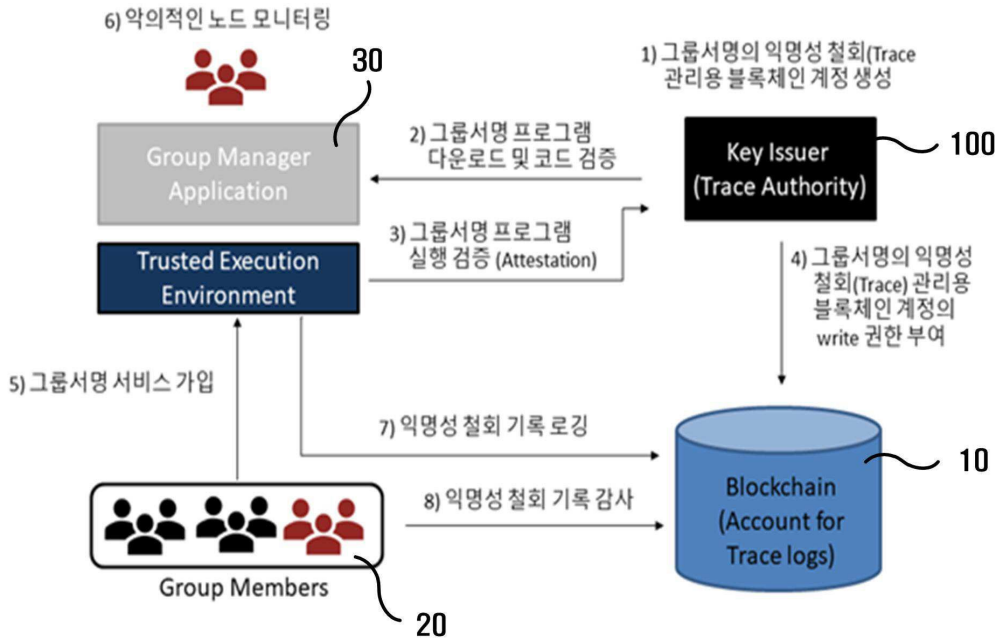
20 : 그룹 멤버

30 : 그룹 매니저

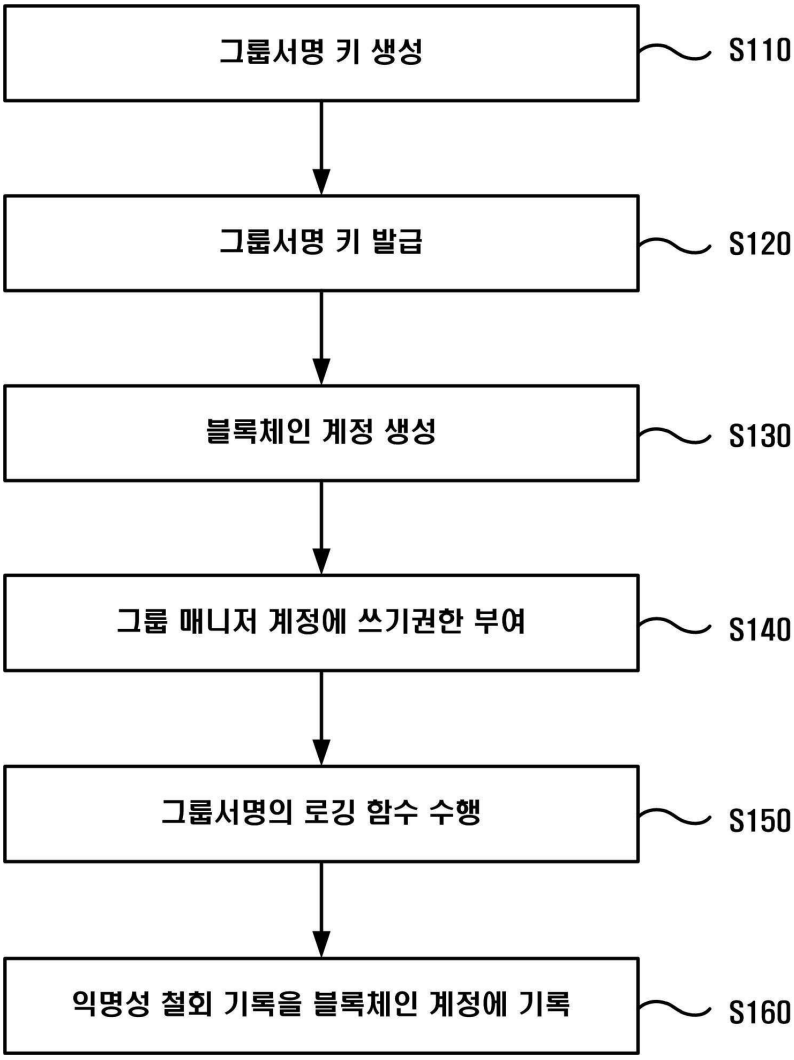
100 : 키 발행자

도면

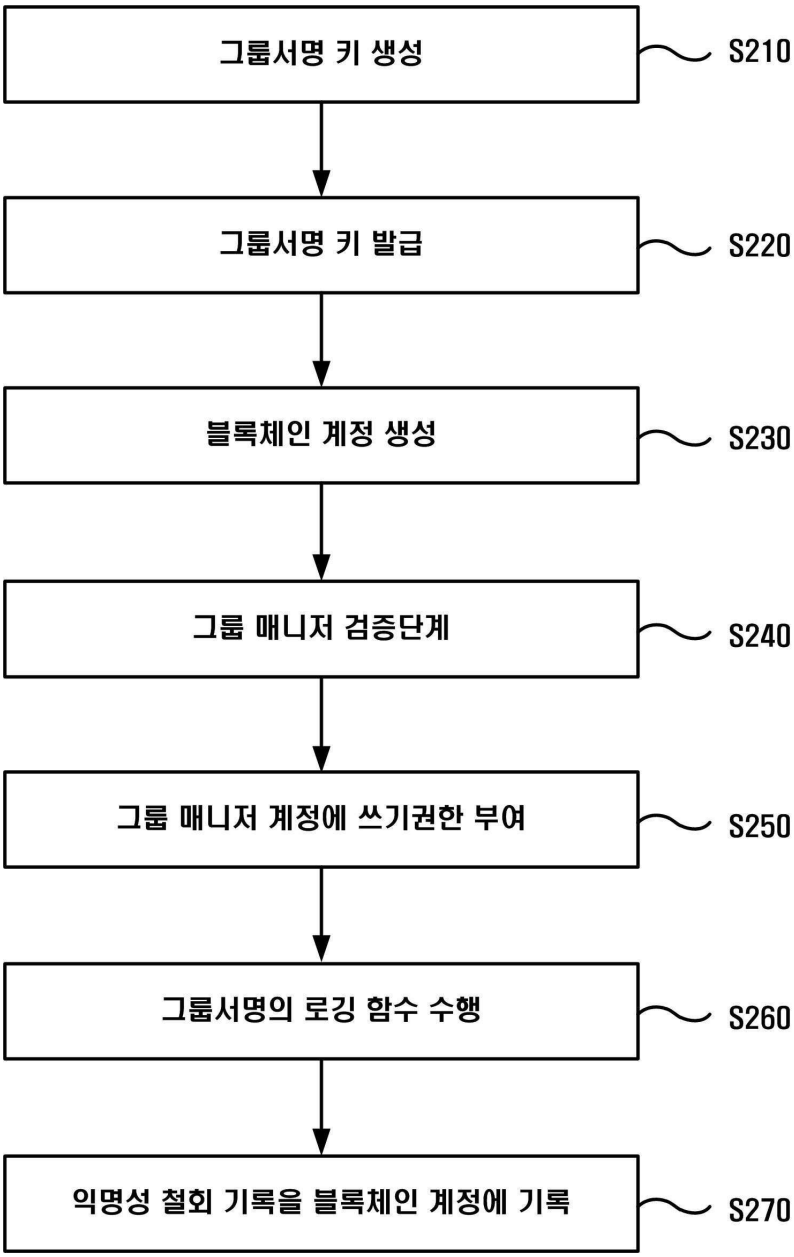
도면1



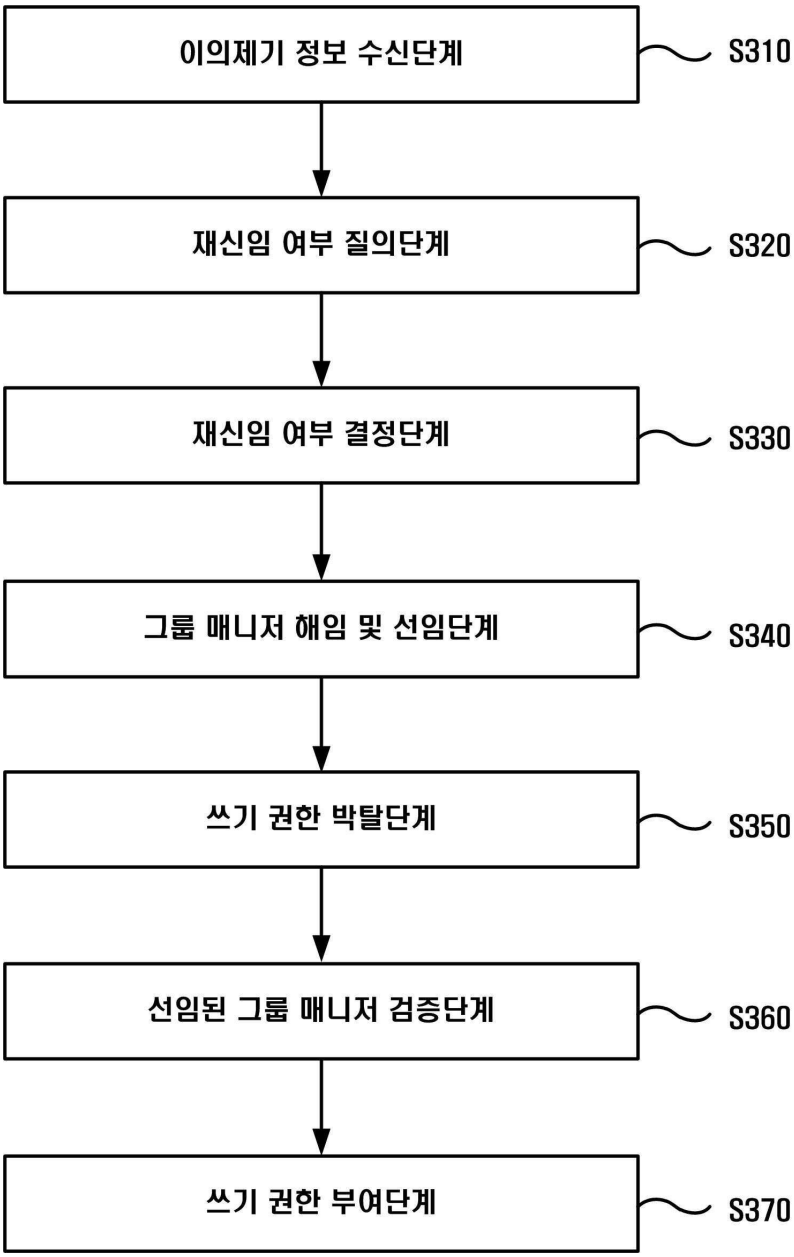
도면2


그룹서명 키 생성
S110
그룹서명 키 발급
S120
블록체인 계정 생성
S130
그룹 매니저 계정에 쓰기권한 부여
S140
그룹서명의 로깅 함수 수행
S150
익명성 철회 기록을 블록체인 계정에 기록
S160

도면3


그룹서명 키 생성
S210
그룹서명 키 발급
S220
블록체인 계정 생성
S230
그룹 매니저 검증단계
S240
그룹 매니저 계정에 쓰기권한 부여
S250
그룹서명의 로깅 함수 수행
S260
익명성 철회 기록을 블록체인 계정에 기록
S270

도면4


이의제기 정보 수신단계
S310
재신임 여부 질의단계
S320
재신임 여부 결정단계
S330
그룹 매니저 해임 및 선임단계
S340
쓰기 권한 박탈단계
S350
선임된 그룹 매니저 검증단계
S360
쓰기 권한 부여단계
S370

도면5