(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년07월06일
(11) 등록번호 10-2130651
(24) 등록일자 2020년06월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06Q 20/38* (2012.01)
(52) CPC특허분류
H04L 9/321 (2013.01)
G06Q 20/38215 (2013.01)
(21) 출원번호 10-2018-0094457
(22) 출원일자 2018년08월13일
심사청구일자 2018년08월13일
(65) 공개번호 10-2020-0018967
(43) 공개일자 2020년02월21일
(56) 선행기술조사문헌
JP2007108973 A*
(뒷면에 계속)
전체 청구항 수 : 총 18 항

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
마정현
경기도 안산시 단원구 당곡2로 30, 903동 301호
(74) 대리인
특허법인이상

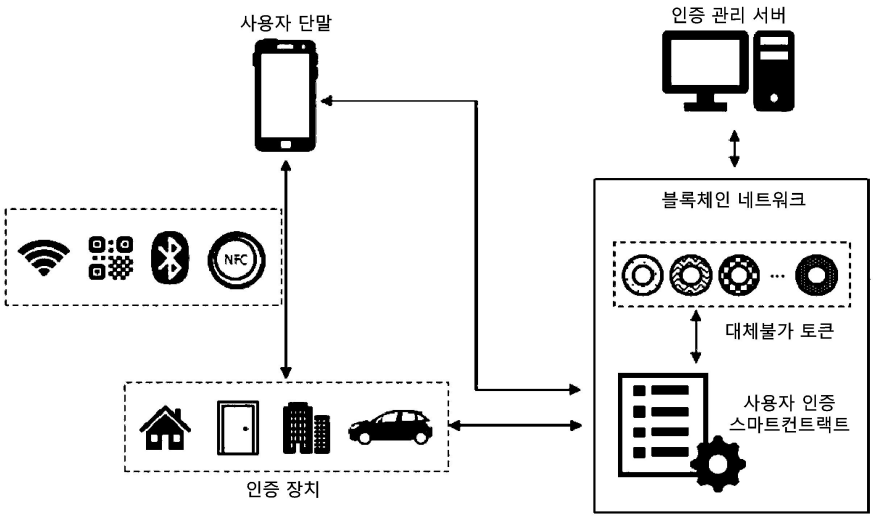
심사관 : 최재귀

(54) 발명의 명칭 **블록체인 기반 사용자 인증 방법 및 장치**

(57) 요 약

인증 장치로부터 사용자의 인증 정보 및 상기 인증 장치의 고유 값을 포함하는 트랜잭션을 수신하는 단계, 인증 정보를 기초로 스마트 컨트랙트에 저장된 사용자의 토큰을 결정하는 단계 및 토큰의 유효성 정보, 토큰의 소유권 정보 및 트랜잭션을 기초로 사용자를 인증하는 단계를 포함하는 인증 장치와 블록체인 네트워크를 구성하는 인증 관리 서버의 사용자 인증 방법이 개시된다.

대 표 도



(52) CPC특허분류
G06Q 20/385 (2020.05)
H04L 2209/38 (2013.01)

(56) 선행기술조사문헌
KR101857223 B1*
WO2018127923 A1*
최연규 외 2인, 블록체인 기반 확장 가능한 사용자 인증 시스템, 한국정보과학회 학술발표논문집, 2018.06. 1165-1167페이지
최상용, 블록체인 기반 온라인 신분증명 스킴, 한국컴퓨터정보학회 학술발표논문집 26(2), 2018.7, 157-160페이지.
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업
과제고유번호 1711093075
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신기술인력양성
연구과제명 크로스 도메인 호환성을 위한 블록체인 플랫폼 및 비즈모델 개발
기 여 율 6/10
주관기관 포항공과대학교 산학협력단
연구기간 2019.01.01 ~ 2019.09.30
이 발명을 지원한 국가연구개발사업
과제고유번호 1711070442
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신기술인력양성
연구과제명 미래IT융합연구원
기 여 율 4/10
주관기관 포항공과대학교 산학협력단
연구기간 2018.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

인증 장치와 블록체인 네트워크를 구성하는 인증 관리 서버의 사용자 인증 방법으로서,

상기 인증 장치로부터 사용자의 인증 정보 및 상기 인증 장치의 고유 값을 포함하는 트랜잭션을 수신하는 단계;

상기 인증 정보를 기초로 스마트 컨트랙트에 저장된 상기 사용자의 토큰을 결정하는 단계;

상기 토큰의 유효성 정보, 상기 토큰의 소유권 정보 및 상기 트랜잭션을 기초로 상기 사용자를 인증하는 단계; 및

상기 토큰의 유효성 정보를 기초로 상기 토큰이 유효한지 결정하는 단계를 포함하는, 사용자 인증 방법.

청구항 2

청구항 1에 있어서,

상기 사용자를 인증하는 단계는,

상기 토큰이 유효한 경우, 상기 토큰의 소유권 정보 및 상기 트랜잭션을 기초로 상기 사용자를 인증하는 단계를 포함하는, 사용자 인증 방법.

청구항 3

청구항 1에 있어서,

상기 사용자의 인증에 대한 결과를 상기 인증 장치로 송신하는 단계를 더 포함하는, 사용자 인증 방법.

청구항 4

청구항 1에 있어서,

상기 토큰은,

상기 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함하는, 사용자 인증 방법.

청구항 5

청구항 1에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함하는, 사용자 인증 방법.

청구항 6

사용자 단말과 블록체인 네트워크를 구성하는 인증 관리 서버의 토큰 발행 방법으로서,

상기 사용자 단말로부터 사용자의 인증 정보, 토큰의 속성값을 설정하는 매개변수 및 토큰 생성 요청 정보를 포함하는 트랜잭션을 수신하는 단계;

스마트 컨트랙트의 정책 정보 및 상기 인증 정보를 기초로 상기 사용자의 토큰을 생성할지를 결정하는 단계; 및

상기 결정에 따라 상기 정책 정보 및 상기 트랜잭션을 기초로 유효성 정보 및 소유권 정보를 포함하는 상기 사용자의 토큰을 생성하여 상기 블록체인 네트워크에 발행하는 단계를 포함하며,

상기 토큰은,

상기 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함하는, 토큰 발행 방법.

청구항 7

청구항 6에 있어서,

상기 토큰의 생성에 대한 결과를 상기 사용자 단말로 송신하는 단계를 더 포함하는, 토큰 발행 방법.

청구항 8

삭제

청구항 9

청구항 6에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 상기 사용자 단말의 고유한 주소 정보를 포함하는, 토큰 발행 방법.

청구항 10

청구항 6에 있어서,

상기 매개변수는,

상기 사용자 단말이 인증하는 인증 장치에 대한 정보를 포함하는, 토큰 발행 방법.

청구항 11

인증 장치와 블록체인 네트워크를 구성하여 사용자 인증 방법을 수행하는 인증 관리 서버로서,

프로세서(processor); 및

상기 프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory)를 포함하고,

상기 적어도 하나의 명령은,

상기 인증 장치로부터 사용자의 인증 정보 및 상기 인증 장치의 고유 값을 포함하는 트랜잭션을 수신하도록 실행되고;

상기 인증 정보를 기초로 스마트 컨트랙트에 저장된 상기 사용자의 토큰을 결정하도록 실행되고;

상기 토큰의 유효성 정보, 상기 토큰의 소유권 정보 및 상기 트랜잭션을 기초로 상기 사용자를 인증하고; 그리고,

상기 토큰의 유효성 정보를 기초로 상기 토큰이 유효한지 결정하도록 실행되는, 인증 관리 서버.

청구항 12

청구항 11에 있어서,

상기 적어도 하나의 명령은,

상기 토큰이 유효한 경우, 상기 토큰의 소유권 정보 및 상기 트랜잭션을 기초로 상기 사용자를 인증하도록 실행되는, 인증 관리 서버.

청구항 13

청구항 11에 있어서,

상기 적어도 하나의 명령은,

상기 사용자의 인증에 대한 결과를 상기 인증 장치로 송신하도록 실행되는, 인증 관리 서버.

청구항 14

청구항 11에 있어서,

상기 토큰은,

상기 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함하는, 인증 관리 서버.

청구항 15

청구항 11에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함하는, 인증 관리 서버.

청구항 16

사용자 단말과 블록체인 네트워크를 구성하여 토큰 발행 방법을 수행하는 인증 관리 서버로서,

프로세서(processor); 및

상기 프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory)를 포함하고,

상기 적어도 하나의 명령은,

상기 사용자 단말로부터 사용자의 인증 정보, 토큰의 속성값을 설정하는 매개변수 및 토큰 생성 요청 정보를 포함하는 트랜잭션을 수신하도록 실행되고,

스마트 컨트랙트의 정책 정보 및 상기 인증 정보를 기초로 상기 사용자의 토큰을 생성할지를 결정하도록 실행되고,

상기 결정에 따라 상기 정책 정보 및 상기 트랜잭션을 기초로 유효성 정보 및 소유권 정보를 포함하는 상기 사용자의 토큰을 생성하여 상기 블록체인 네트워크에 발행하도록 실행되며,

상기 토큰은

상기 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함하는, 인증 관리 서버.

청구항 17

청구항 16에 있어서,

상기 적어도 하나의 명령은,

상기 토큰의 생성에 대한 결과를 상기 사용자 단말로 송신하도록 실행되는, 인증 관리 서버.

청구항 18

삭제

청구항 19

청구항 16에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 상기 사용자 단말의 고유한 주소 정보를 포함하는, 인증 관리 서버.

청구항 20

청구항 16에 있어서,

상기 매개변수는,

상기 사용자 단말이 인증하는 인증 장치에 대한 정보를 포함하는, 인증 관리 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 기반 사용자 인증 방법 및 장치에 관한 것으로, 더욱 상세하게는 스마트 컨트랙트(smart contract)를 이용하여 생성한 대체 불가능한(non-fungible) 토큰을 기초로 사용자를 인증하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 일반적으로 사용자 인증은 대부분 중앙 서버에서 사용자 신원을 확인한 후 해당 인증 정보를 사용자에게 전송하며, 사용자는 전송된 인증 정보를 스마트폰에 저장하고, 추후 저장된 인증 정보를 제출하여 검증받는 방식으로 수행되고 있다. 여기서, 인증 정보는 기본적으로 복제 및 위변조가 불가능하여야 하며, 추가적으로 다른 사용자에게 위임할 수 있는 기능도 지원할 수 있어야 한다.

[0003] 이러한 방법은 중앙 서버에서 인증 정보를 스마트폰에 전달하여 저장하는 경우, 스마트폰에 저장된 인증 정보의 복제가 불가능하기 때문에 스마트폰 분실 시 또는 변경 시 인증 정보를 재발급 받아야 하며, 인증 정보의 위임이 원칙적으로 불가능한 불편함이 있다. 또한, 인증 정보의 위변조를 불가능하도록 인증 정보를 발급하는 중앙 서버의 비밀키를 이용한 서명이 요구되므로, 인증 과정의 복잡도가 높아지는 문제점도 있다.

[0004] 최근 블록체인 기술이 확산됨에 따라, 블록체인을 사용자 인증에 적용하는 방법이 대두되고 있다. 통상적인 블록체인을 이용한 사용자 인증 방법은 공개키 인프라(public key infrastructure)를 이용하여 사용자에게 발급되는 공개키 및 개인키 쌍 중 공개키를 블록체인에 저장 및 유지하고, 사용자만이 알고 있는 개인키를 이용하여 서명 정보를 생성하고, 이를 블록체인에 저장된 공개키로 복호화함으로써 사용자를 인증하는 방법에 따라 수행되고 있다.

[0005] 기존의 블록체인을 이용한 사용자 인증 방법은 사용자에게 발급된 공개키를 중심으로 하는 정보만을 블록체인에 저장하는 형태이므로, 다양한 속성 정보를 설정할 수 없다는 한계점을 가지며, 또한 사용자 공개키 정보가 블록체인에 저장되어 있어 인증 실행에 따른 프라이버시 노출의 문제를 가진다.

[0006] 다른 통상적인 블록체인을 이용한 사용자 인증 방법(예를 들어, Civic)은 초기에 사용자의 데이터 증명 값을 블록체인에 저장하고, 추후 사용자 인증 기반의 제어 장치가 사용자로부터 전달받은 데이터 증명 값과 블록체인에 저장된 데이터 증명 값을 비교하여 사용자 인증을 처리하도록 수행되고 있다. 다만, 이러한 방법도 사용자가 소유한 데이터를 중심으로 인증 과정이 처리되기 때문에 복제가 가능하며 소유 데이터를 다른 사용자에게 위임하더라도 이전 소유주의 데이터 삭제 여부를 확인하기 어려운 문제점이 있다.

발명의 내용

해결하려는 과제

[0007] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 블록체인 기반 사용자 인증 방법을 제공하는 데 있다.

[0008] 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 목적은 블록체인 기반의 사용자 인증을 위한 토큰 발행 방법을 제공하는 데 있다.

[0009] 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 목적은 블록체인을 기반으로 사용자를 인증하는 인증 관리 서버를 제공하는 데 있다.

[0010] 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 목적은 블록체인을 기반으로 토큰을 발행하는 인증 관리 서버를 제공하는 데 있다.

과제의 해결 수단

[0011] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 사용자 인증 방법은, 인증 장치로부터 사용자의 인증 정보 및 인증 장치의 고유 값을 포함하는 트랜잭션을 수신하는 단계, 인증 정보를 기초로 스마트 컨트랙트에 저장된 사용자의 토큰을 결정하는 단계 및 토큰의 유효성 정보, 토큰의 소유권 정보 및 트랜잭션을 기초로 사용자를 인증하는 단계를 포함할 수 있다.

[0012] 여기서, 사용자를 인증하는 단계는, 토큰의 유효성 정보를 기초로 토큰이 유효한지 결정하는 단계 및 토큰이 유효한 경우, 토큰의 소유권 정보 및 트랜잭션을 기초로 사용자를 인증하는 단계를 포함할 수 있다.

[0013] 여기서, 사용자의 인증에 대한 결과를 상기 인증 장치로 송신하는 단계를 더 포함할 수 있다.

[0014] 여기서, 토큰은, 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함할 수 있다.

[0015] 여기서, 인증 정보는, 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함할 수 있다.

[0016] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 토큰 발행 방법은, 사용자 단말로부터 사용자의 인증 정보, 토큰의 속성값을 설정하는 매개변수 및 토큰 생성 요청 정보를 포함하는 트랜잭션을 수신하는 단계, 스마트 컨트랙트의 정책 정보 및 인증 정보를 기초로 사용자의 토큰을 생성할지를 결정하는 단계 및 결정에 따라 정책 정보 및 트랜잭션을 기초로 유효성 정보 및 소유권 정보를 포함하는 사용자의 토큰을 생성하여 블록체인 네트워크에 발행하는 단계를 포함할 수 있다.

[0017] 여기서, 토큰의 생성에 대한 결과를 사용자 단말로 송신하는 단계를 더 포함할 수 있다.

[0018] 여기서, 토큰은, 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함할 수 있다.

[0019] 여기서, 인증 정보는, 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함할 수 있다.

[0020] 여기서, 매개변수는, 사용자 단말이 인증하는 인증 장치에 대한 정보를 포함할 수 있다.

[0021] 상기 다른 목적을 달성하기 위한 본 발명의 일 실시예에 따른 인증 관리 서버는, 프로세서(processor) 및 프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory)를 포함하고, 적어도 하나의 명령은, 인증 장치로부터 사용자의 인증 정보 및 인증 장치의 고유 값을 포함하는 트랜잭션을 수신하도록 실행될 수 있고, 인증 정보를 기초로 스마트 컨트랙트에 저장된 사용자의 토큰을 결정하도록 실행될 수 있고, 토큰의 유효성 정보, 토큰의 소유권 정보 및 트랜잭션을 기초로 사용자를 인증하도록 실행될 수 있다.

[0022] 여기서, 적어도 하나의 명령은, 토큰의 유효성 정보를 기초로 토큰이 유효한지 결정하도록 실행될 수 있고, 토큰이 유효한 경우, 토큰의 소유권 정보 및 트랜잭션을 기초로 사용자를 인증하도록 실행될 수 있다.

[0023] 여기서, 적어도 하나의 명령은, 사용자의 인증에 대한 결과를 인증 장치로 송신하도록 실행될 수 있다.

[0024] 여기서, 토큰은, 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함할 수 있다.

[0025] 여기서, 인증 정보는, 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함할 수 있다.

[0026] 상기 다른 목적을 달성하기 위한 본 발명의 일 실시예에 따른 인증 관리 서버는, 프로세서(processor) 및 프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory)를 포함하고, 적어도 하나의 명령은, 사용자 단말로부터 사용자의 인증 정보, 토큰의 속성값을 설정하는 매개변수 및 토큰 생성 요청 정보를 포함하는 트랜잭션을 수신하도록 실행될 수 있고, 스마트 컨트랙트의 정책 정보 및 인증 정보를 기초로 사용자의 토큰을 생성할지를 결정하도록 실행될 수 있고, 결정에 따라 정책 정보 및 트랜잭션을 기초로 유효성 정보 및 소유권 정보를 포함하는 사용자의 토큰을 생성하여 블록체인 네트워크에 발행하도록 실행될 수 있다.

[0027] 여기서, 적어도 하나의 명령은, 토큰의 생성에 대한 결과를 사용자 단말로 송신하도록 실행될 수 있다.

[0028] 여기서, 토큰은, 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 포함할 수 있다.

[0029] 여기서, 인증 정보는, 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함할 수 있다.

[0030] 여기서, 매개변수는, 사용자 단말이 인증하는 인증 장치에 대한 정보를 포함할 수 있다.

발명의 효과

[0031] 본 발명에 따르면, 대체 불가능한 토큰을 이용하여 사용자 인증을 수행하여 높은 보안성을 제공할 수 있다.

[0032] 본 발명에 따르면, 대체 불가능한 토큰에 대하여 소유권 이전 및 위임 등이 가능하여 높은 보안성을 유지하며, 유연한 사용자 인증을 제공할 수 있다.

[0033] 본 발명에 따르면, 토큰의 위임을 통해 차량의 키 인증 및 건물 등의 출입/시동 인증에도 블록체인을 적용할 수 있다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 일 실시예에 따른 토큰 발행 방법의 개념도이다.

도 2는 본 발명의 일 실시예에 따른 사용자 인증 방법의 개념도이다.

도 3은 본 발명의 일 실시예에 따른 사용자 단말의 블록 구성도이다.

도 4는 본 발명의 일 실시예에 따른 인증 관리 서버의 블록 구성도이다.

도 5는 본 발명의 다른 실시예에 따른 인증 관리 서버의 블록 구성도이다.

도 6은 본 발명의 일 실시예에 따른 토큰 발행 방법을 설명하는 순서도이다.

도 7은 본 발명의 일 실시예에 따른 사용자 인증 방법을 설명하는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0035] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0036] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는 데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. "및/또는"이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0037] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0038] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0039] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0040] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다. 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0042] 본 발명의 일 실시예에 따른 블록체인을 이용한 사용자 인증 방법은 사용자 인증에 이용되는 토큰을 발행하는 방법과 토큰을 이용하여 사용자를 인증하는 방법으로 구분될 수 있으며, 각 방법에 대한 상세한 설명은 도면과 함께 후술하겠다.

[0044] 도 1은 본 발명의 일 실시예에 따른 토큰 발행 방법의 개념도이다.

[0045] 도 1을 참조하면, 본 발명의 일 실시예에 따른 사용자 인증을 위한 토큰을 발행하는 방법은 사용자 단말 및 블록체인 네트워크의 스마트 컨트랙트(smart contract)를 관리하는 인증 관리 서버 간의 데이터 송수신에 의해 수행될 수 있다. 여기서, 사용자 단말은 사용자 인증을 위해 사용자가 사용하는 장치를 의미할 수 있으며, 스마트 폰 또는 컴퓨터 등 컴퓨팅이 가능한 스마트 디바이스를 모두 지칭할 수 있다.

[0046] 사용자 단말은 사용자 인증을 위한 인증 정보, 토큰의 속성값을 설정하는 매개변수 및 토큰 생성 요청 정보를 포함하는 토큰 생성 요청 트랜잭션(transaction)을 인증 관리 서버가 관리하는 블록체인 네트워크에 전파할 수 있으며, 후술하겠으나, 토큰 검증, 토큰 위임, 토큰의 소유권 공유, 토큰의 소유권 이전 등의 요청 트랜잭션도

블록체인 네트워크에 전파할 수 있다.

[0047] 여기서, 인증 정보는 사용자 인증에 이용되는 스마트 컨트랙트의 주소 값, 사용자 단말의 고유한 주소 값 및 사용자 정보 중 적어도 하나를 포함할 수 있으나, 이에 한정되는 것은 아니다. 또한, 인증 정보 및 매개변수는 사용자 단말에 이전부터 내장되어 있을 수 있고, 사용자 인증을 위해 추가적으로 저장될 수도 있다. 사용자 단말은 트랜잭션 생성 시 사용되는 개인키를 저장 및 관리할 수 있다.

[0048] 인증 관리 서버는 사용자 단말의 트랜잭션 전파에 따라 블록체인 네트워크 상의 스마트 컨트랙트를 관리할 수 있다. 인증 관리 서버는 사용자 단말에 의해 토큰 생성 요청 트랜잭션이 블록체인 네트워크에 전파된 경우, 트랜잭션에 포함된 정보를 이용하여 스마트 컨트랙트를 특정 또는 결정할 수 있으며, 스마트 컨트랙트의 정책에 기초하여 대체 불가능한 토큰을 생성할 수 있다.

[0049] 대체 불가능한 토큰은 블록체인 네트워크에서 고유한 값을 포함할 수 있으며, 적어도 하나의 속성값을 더 포함할 수 있다. 여기서, 속성값은 사용자 인증과 관련하여 매개변수에 의해 설정되는 정보 또는 값을 의미할 수 있으며, 토큰의 유효 기간, 사용 환경, 인증 범위 및 소유자 정보 중 적어도 하나를 포함할 수 있으나, 이에 한정되는 것은 아니다. 생성된 토큰은 속성값에 따라 사용자에게 종속될 수 있으며, 블록체인 내의 상태값으로 저장될 수 있다. 인증 관리 서버는 토큰 생성하여 저장한 후, 토큰 생성의 완료 정보를 사용자 단말에 제공할 수 있다. 다시 말해, 인증 관리 서버는 생성한 토큰에 대한 정보를 포함한 블록을 블록체인 네트워크에 전파하여 토큰을 발행할 수 있다.

[0051] 도 2는 본 발명의 일 실시예에 따른 사용자 인증 방법의 개념도이다.

[0052] 도 2를 참조하면, 본 발명의 일 실시예에 따른 토큰을 이용한 사용자 인증 방법은 사용자 단말, 인증 장치 및 스마트 컨트랙트를 관리하는 인증 관리 서버 간의 데이터 송수신에 의해 수행될 수 있다. 여기서, 인증 장치는 사용자가 사용자 인증을 통해 이용하고자 하는 장치를 의미할 수 있으며, 호텔 룸 도어 키 장치, 건물 출입 장치 또는 자동차 도어 키 장치 등의 컴퓨팅이 가능한 스마트 디바이스를 모두 지칭할 수 있다.

[0053] 우선, 사용자 단말은 사용자 인증을 위해 사용자 단말의 고유한 주소 값 및 스마트 컨트랙트 주소 값을 인증 장치로 송신할 수 있다. 여기서, 사용자 단말의 고유한 주소 값은 사용자의 지갑 주소 값을 의미할 수 있으나, 이에 한정하는 것은 아니다. 여기서, 지갑 주소 값은 블록체인 네트워크에서 이용될 수 있는 가상 화폐 등을 관리하는 지갑의 주소 값을 의미할 수 있다. 사용자 단말은 QR(Quick Response) 코드, NFC(Near Field Communication) 또는 블루투스(bluetooth) 등의 무선 통신 방법 중 어느 하나를 이용하여 사용자 단말의 고유한 주소 값 및 스마트 컨트랙트 주소 값을 인증 장치로 송신할 수 있으나, 송신 방법이 이에 한정되는 것은 아니다. 여기서, 사용자 단말의 고유한 주소 값 및 스마트 컨트랙트 주소 값은 인증 정보로 지칭할 수도 있고, 도 1의 인증 정보와 포함된 정보가 상이할 수 있으나, 이에 한정되는 것은 아니다.

[0054] 인증 장치는 수신한 인증 정보 및 자신의 고유 값을 포함하는 트랜잭션을 블록체인 네트워크에 전파할 수 있다. 여기서, 인증 장치는 직접 트랜잭션을 블로체인 네트워크에 전파할 수 있고, 백엔드 서버(back-end server)가 인증 장치로부터 인증 정보 및 인증 장치의 고유 값을 수신하여 트랜잭션을 블록체인 네트워크에 전파할 수도 있으나, 이에 한정되는 것은 아니다.

[0055] 여기서, 인증 장치의 고유 값은 사용자 인증에 이용될 수 있는 추가 정보를 의미할 수 있으며, 인증 장치의 위치, 모델 및 ID(Identification) 중 적어도 하나를 포함할 수 있으나, 이에 한정되는 것은 아니다.

[0056] 인증 관리 서버는 인증 장치에 의해 트랜잭션이 전파된 경우, 트랜잭션에 포함된 스마트 컨트랙트의 주소 값을 기초로 스마트 컨트랙트에 대한 토큰의 유효성을 확인할 수 있고, 토큰에 대한 소유권을 검증할 수 있다. 다시 말해, 인증 관리 서버는 토큰의 속성값 및 전파된 트랜잭션을 기초로 만료 기간 또는 권한 등을 확인할 수 있으며, 토큰의 소유권을 가지는 사용자 정보와 트랜잭션에 포함된 사용자 정보를 비교 검증하여 사용자 인증을 수행할 수 있다.

[0057] 인증 관리 서버는 비교 검증 결과, 토큰이 유효하고, 사용자 인증에 성공한 경우, 인증 장치가 전파한 트랜잭션을 포함하여 블록을 발행함으로써 블록체인을 연결할 수 있으며, 인증 완료에 대한 정보를 인증 장치로 송신할 수 있다. 다만, 인증 관리 서버는 토큰이 유효하지 않거나, 사용자 인증에 실패한 경우, 인증 장치가 전파한 트랜잭션을 포함한 블록을 발행하지 않을 수 있으며, 인증 실패에 대한 정보를 인증 장치로 송신할 수 있으나, 인증과 관련된 정보를 인증 장치로 송신하지 않을 수도 있다.

[0058] 본 발명의 일 실시예에 따른 토큰을 이용한 사용자 인증 방법은 사용자 단말이 토큰 검증, 토큰 위임, 토큰의

소유권 공유, 토큰의 소유권 이전 등의 요청 트랜잭션을 블록체인 네트워크에 전파한 경우, 이를 반영하여 상술한 과정의 비교 검증을 수행할 수 있다.

[0059] 예를 들어, 사용자 단말이 토큰의 소유권 위임 요청 트랜잭션을 블록체인 네트워크에 전파한 경우, 인증 관리 서버는 위임 요청 트랜잭션을 반영하여 토큰이 위임된 자의 정보와 인증 장치가 전파한 트랜잭션에 포함된 정보를 비교 검증할 수 있다.

[0061] 도 3은 본 발명의 일 실시예에 따른 사용자 단말의 블록 구성도이다.

[0062] 도 3을 참조하면, 본 발명의 일 실시예에 따른 사용자 단말(300)은 인증 관리부(310) 및 지갑 관리부(320)를 포함할 수 있다. 또한, 사용자 단말(300)은 도 3에 도시하지 않았으나, 블록체인 네트워크에 트랜잭션을 전파하고 결과를 수신하기 위한 통신부를 더 포함할 수 있다. 여기서, 통신부는 이더리움 상 web3 기반 원격 프로시저 호출(JavaScript Object Notation-Remote Procedure Call, JSON-RPC)을 담당하는 모듈 또는 하이퍼레저 패브릭(hyperledger fabric) 상 패브릭 SDK(Software Development Kit) 기반 트랜잭션 제출을 담당하는 모듈을 포함할 수 있다.

[0063] 인증 관리부(310)는 매개변수 및 스마트 컨트랙트의 주소 값을 관리 또는 저장할 수 있으며, 후술하는 지갑 관리부(320)가 관리 또는 저장하고 있는 사용자 단말의 고유한 값 또는 사용자 지갑의 고유한 주소 값과 함께 이를 이용하여 토큰 발행 또는 사용자 인증을 수행할 수 있다. 또한, 인증 관리부(310)는 매개변수, 스마트 컨트랙트의 주소 값 및 지갑 관리부(320)의 사용자 단말의 고유한 값 또는 사용자 지갑의 고유한 주소 값 중 적어도 하나를 이용하여 토큰 검증, 토큰 위임, 토큰의 소유권 공유 및 토큰의 소유권 이전 등을 수행할 수도 있다.

[0064] 지갑 관리부(320)는 토큰 발행, 토큰 검증, 토큰 위임, 토큰의 소유권 공유 및 토큰의 소유권 이전 등을 위한 트랜잭션 작성 또는 생성에 이용되는 개인키를 관리할 수 있으며, 사용자 단말의 고유한 값 또는 사용자 지갑의 고유한 주소 값을 관리 또는 저장하고 있을 수 있다.

[0066] 도 4는 본 발명의 일 실시예에 따른 인증 관리 서버의 블록 구성도이다.

[0067] 도 4를 참조하면, 본 발명의 일 실시예에 따른 인증 관리 서버(400)는 토큰 생성부(410), 정책 관리부(420) 및 토큰 관리부(430)를 포함할 수 있다. 또한, 인증 관리 서버(400)은 도 4에 도시하지 않았으나, 블록체인 네트워크에 트랜잭션 또는 블록을 전파하고, 결과를 수신하기 위한 통신부를 더 포함할 수 있다.

[0068] 토큰 생성부(410)는 사용자 단말이 전파한 토큰 생성 요청 트랜잭션을 수신한 경우, 토큰 생성 요청 트랜잭션에 포함된 정보 및 토큰 정책 정보를 기초로 사용자의 토큰을 생성할 수 있다. 다시 말해, 토큰 생성부(410)는 토큰 생성 요청 트랜잭션에 포함된 매개변수, 인증 정보 및 토큰 생성 요청 정보를 기초로 후술하는 정책 관리부(420)의 토큰 정책 정보에 부합하는지 판단할 수 있으며, 토큰 정책 정보에 부합하는 경우, 토큰을 생성할 수 있다. 여기서, 인증 정보는 사용자 단말의 고유한 값 또는 사용자 지갑의 고유한 주소 값을 포함할 수 있다.

[0069] 정책 관리부(420)는 토큰 생성을 위한 정책 정보를 관리 또는 저장할 수 있으며, 일정한 주기마다 또는 변경사항이 존재하는 경우마다 정책 정보를 업데이트할 수 있다. 여기서, 정책 정보는 토큰 생성이 허용되는 사용자의 소속 정보 등을 포함할 수 있으며, 인증 정보에 포함된 사용자의 소속 정보와 비교하여 토큰 생성을 결정할 수 있으나, 이에 한정되는 것은 아니다.

[0070] 토큰 관리부(430)는 인증 장치가 전파한 사용자 단말의 인증 정보 및 인증 장치의 고유의 값을 포함하는 트랜잭션을 수신한 경우, 이를 기초로 토큰 검증을 통한 사용자 인증, 토큰 위임, 토큰의 소유권 공유 및 토큰의 소유권 이전 등을 수행할 수 있다. 보다 상세히 설명하면, 토큰 관리부(430)는 사용자 인증을 위한 트랜잭션을 수신한 경우, 트랜잭션에 포함된 정보를 기초로 토큰의 유효성을 검증할 수 있으며, 유효성 검증 결과에 따라 토큰이 유효한 것으로 판단한 경우, 토큰의 소유권을 확인하여 사용자를 인증할 수 있다. 또한, 토큰 관리부(430)는 토큰 위임 및 토큰의 소유권 공유 등의 트랜잭션을 수신한 경우, 해당 정보를 토큰에 반영하여 토큰의 소유권 정보를 수정할 수 있다.

[0071] 통신부는 트랜잭션 또는 블록을 블록체인 네트워크에 전파할 수 있으며, 트랜잭션 또는 블록을 블록체인 네트워크로부터 수신할 수도 있다. 다시 말해, 통신부는 사용자 인증 또는 토큰의 위임 등과 관련된 정보에 대한 트랜잭션 또는 블록을 블록체인 네트워크에 전파할 수 있다. 또한, 통신부는 토큰 생성의 완료 정보를 사용자 단말로 송신할 수 있고, 사용자 인증 결과에 대한 정보를 인증 장치로 송신할 수도 있다.

[0073] 도 5는 본 발명의 다른 실시예에 따른 인증 관리 서버의 블록 구성도이다.

[0074] 도 5를 참조하면, 본 발명의 일 실시예에 따른 인증 관리 서버(500)는 적어도 하나의 프로세서(510), 메모리(520) 및 저장 장치(530)를 포함할 수 있다. 인증 관리 서버(500)는 사용자 단말 및 인증 장치와 블록체인 네트워크를 구성할 수 있다.

[0075] 프로세서(510)는 메모리(520) 및/또는 저장 장치(530)에 저장된 프로그램 명령(program command)을 실행할 수 있다. 프로세서(510)는 중앙 처리 장치(central processing unit, CPU), 그래픽 처리 장치(graphics processing unit, GPU) 또는 본 발명에 따른 방법들이 수행되는 전용의 프로세서를 의미할 수 있다. 메모리(520)와 저장 장치(530)는 휘발성 저장 매체 및/또는 비휘발성 저장 매체로 구성될 수 있다. 예를 들어, 메모리(520)는 읽기 전용 메모리(read only memory, ROM) 및/또는 랜덤 액세스 메모리(random access memory, RAM)로 구성될 수 있다.

[0076] 메모리(520)는 프로세서(510)를 통해 실행되는 적어도 하나의 명령을 저장하고 있을 수 있다. 적어도 하나의 명령은 사용자 인증을 위해 인증 장치로부터 사용자의 인증 정보 및 인증 장치의 고유 값을 포함하는 트랜잭션을 수신하는 명령, 인증 정보를 기초로 스마트 컨트랙트에 저장된 사용자의 토큰을 결정하는 명령 및 토큰의 유효성 정보, 토큰의 소유권 정보 및 트랜잭션을 기초로 상기 사용자를 인증하는 명령을 포함할 수 있다.

[0077] 여기서, 적어도 하나의 명령은 토큰의 유효성 정보를 기초로 토큰이 유효한지 결정하는 명령, 토큰이 유효한 경우, 토큰의 소유권 정보 및 트랜잭션을 기초로 사용자를 인증하는 명령 및 사용자의 인증에 대한 결과를 인증 장치로 송신하는 명령 중 적어도 하나를 더 포함할 수 있다.

[0078] 또한, 적어도 하나의 명령은 토큰 발행을 위해 사용자 단말로부터 사용자의 인증 정보, 토큰의 속성값을 설정하는 매개변수 및 토큰 생성 요청 정보를 포함하는 트랜잭션을 수신하는 명령, 스마트 컨트랙트의 정책 정보 및 인증 정보를 기초로 사용자의 토큰을 생성할지를 결정하는 명령 및 결정에 따라 정책 정보 및 트랜잭션을 기초로 유효성 정보 및 소유권 정보를 포함하는 사용자의 토큰을 생성하여 블록체인 네트워크에 발행하는 명령을 포함할 수 있다.

[0079] 여기서, 적어도 하나의 명령은 토큰의 생성에 대한 결과를 사용자 단말로 송신하는 명령을 더 포함할 수 있다.

[0080] 여기서, 토큰은 스마트 컨트랙트에 대한 정보가 발행된 블록체인 네트워크에서 고유의 값을 가질 수 있으며, 인증 정보는 스마트 컨트랙트의 주소 정보 및 상기 사용자 단말의 고유한 주소 정보를 포함할 수 있고, 매개변수는 사용자 단말이 인증하는 인증 장치에 대한 정보를 포함할 수 있다.

[0081] 사용자 단말 및 인증 장치도 인증 관리 서버와 마찬가지로 적어도 하나의 프로세서, 메모리 및 저장 장치를 포함할 수 있다.

[0083] 도 6은 본 발명의 일 실시예에 따른 토큰 발행 방법을 설명하는 순서도이다.

[0084] 도 6을 참조하면, 본 발명의 일 실시예에 따른 토큰 발행 방법은 우선 사용자 단말이 인증 정보, 토큰 생성 요청 정보 및 매개변수를 포함하는 트랜잭션을 생성할 수 있으며(S610), 생성한 트랜잭션을 블록체인 네트워크에 전파할 수 있다(S620). 여기서, 인증 정보는 스마트 컨트랙트의 주소 값 및 사용자 단말의 고유한 주소 값을 포함할 수 있으며, 사용자 단말의 고유한 주소 값은 사용자의 지갑 주소 값을 의미할 수 있으나, 이에 한정되는 것은 아니다. 또한, 매개변수는 토큰의 속성값을 설정하기 위한 정보 또는 값을 의미할 수 있다.

[0085] 인증 관리 서버는 사용자 단말이 전파한 트랜잭션을 수신한 경우, 인증 정보 및 토큰 생성 정책 정보를 기초로 토큰 생성 여부를 결정할 수 있다(S630). 여기서, 토큰 생성 정책 정보는 인증 관리 서버의 정책 관리부가 관리하는 정책 정보를 의미할 수 있으며, 정책 정보는 토큰 생성이 허용되는 사용자의 소속 정보 등을 포함할 수 있다. 또한, 인증 정보는 사용자 소속 정보 등을 포함하는 사용자 정보를 포함할 수 있으며, 인증 관리 서버는 정책 정보의 토큰 생성이 허용되는 사용자의 소속 정보와 인증 정보의 사용자 소속 정보를 비교하여 토큰 생성 여부를 결정할 수 있다.

[0086] 인증 관리 서버는 토큰을 생성하는 것으로 결정한 경우, 수신한 트랜잭션을 기초로 토큰을 생성할 수 있으며(S640), 생성한 토큰을 발행할 수 있다(S650). 여기서, 토큰은 스마트 컨트랙트에 상태값으로 저장될 수 있으며, 토큰 발행은 토큰에 대한 정보를 포함하는 트랜잭션 또는 블록을 블록체인 네트워크에 전파함으로써 수행될 수 있다.

[0087] 이후, 인증 관리 서버는 토큰 발행 완료에 대한 정보를 사용자 단말로 송신할 수 있다(S660).

[0089] 도 7은 본 발명의 일 실시예에 따른 사용자 인증 방법을 설명하는 순서도이다.

[0090] 도 7을 참조하면, 본 발명의 일 실시예에 따른 사용자 인증 방법은 우선, 사용자 단말이 스마트 컨트랙트의 주소 및 사용자 단말의 고유한 주소 값을 포함하는 인증 정보를 인증 장치로 송신할 수 있다(S710). 여기서, 인증 장치는 사용자가 사용자 인증을 통해 이용하기 위한 장치를 의미할 수 있으며, 사용자 단말의 고유한 주소 값은 사용자의 지갑 주소 값을 의미할 수도 있다.

[0091] 인증 장치는 사용자 단말로부터 수신한 인증 정보 및 인증 장치의 고유값을 포함하는 트랜잭션을 생성할 수 있으며(S720), 생성한 트랜잭션을 블록체인 네트워크에 전파할 수 있다(S730).

[0092] 인증 관리 서버는 인증 장치가 전파한 트랜잭션에 포함된 정보를 기초로 해당 스마트 컨트랙트 및 토큰을 결정할 수 있으며(S740), 트랜잭션에 포함된 정보 및 토큰의 유효성 정보를 기초로 토큰이 유효한지 판단할 수 있다(S750). 인증 관리 서버는 토큰이 유효하다고 판단한 경우, 토큰의 소유권 정보 및 트랜잭션에 포함된 정보를 기초로 사용자 인증을 수행할 수 있으며(S760), 사용자 인증에 성공한 경우, 인증 결과에 대한 정보를 인증 장치로 송신할 수 있다(S770). 사용자는 상술한 과정에 따라 사용자 인증을 수행한 후, 인증 결과에 대한 정보를 수신한 인증 장치를 이용할 수 있다.

[0094] 본 발명의 실시예에 따른 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0095] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

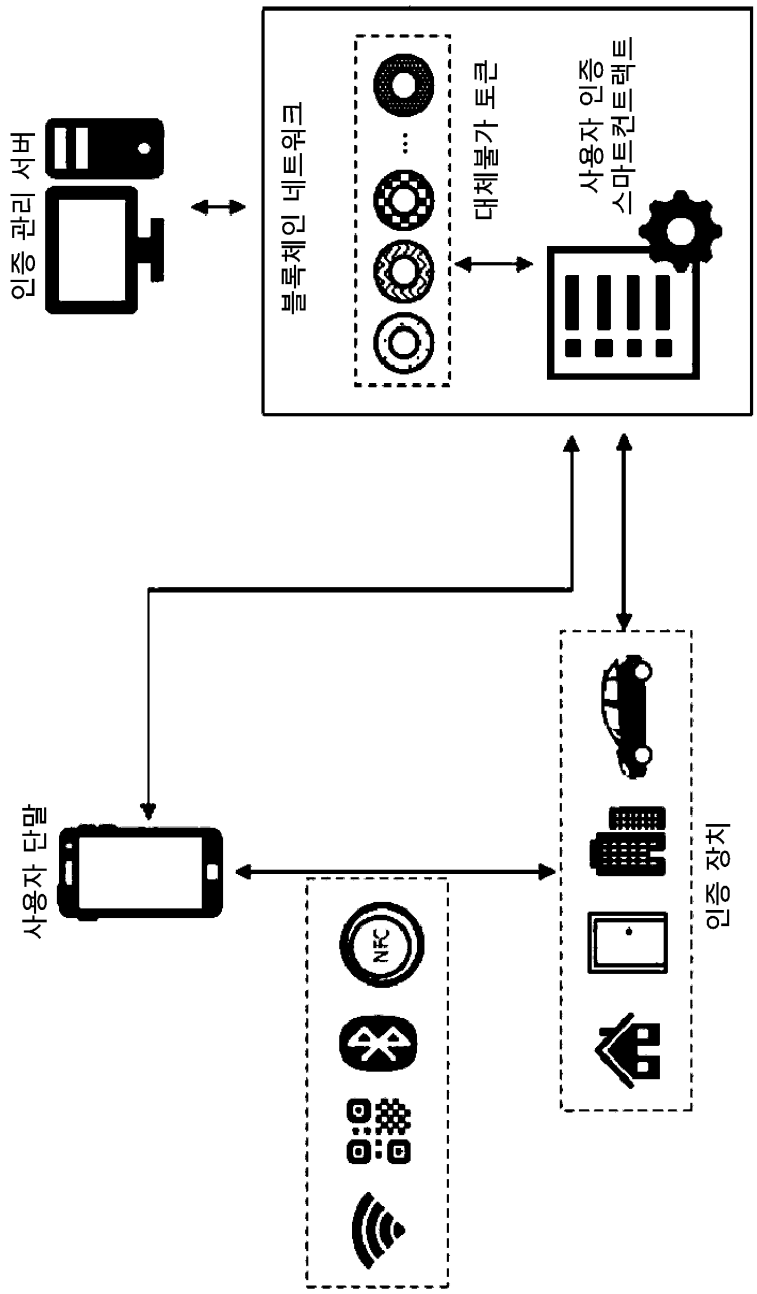
[0096] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0097] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

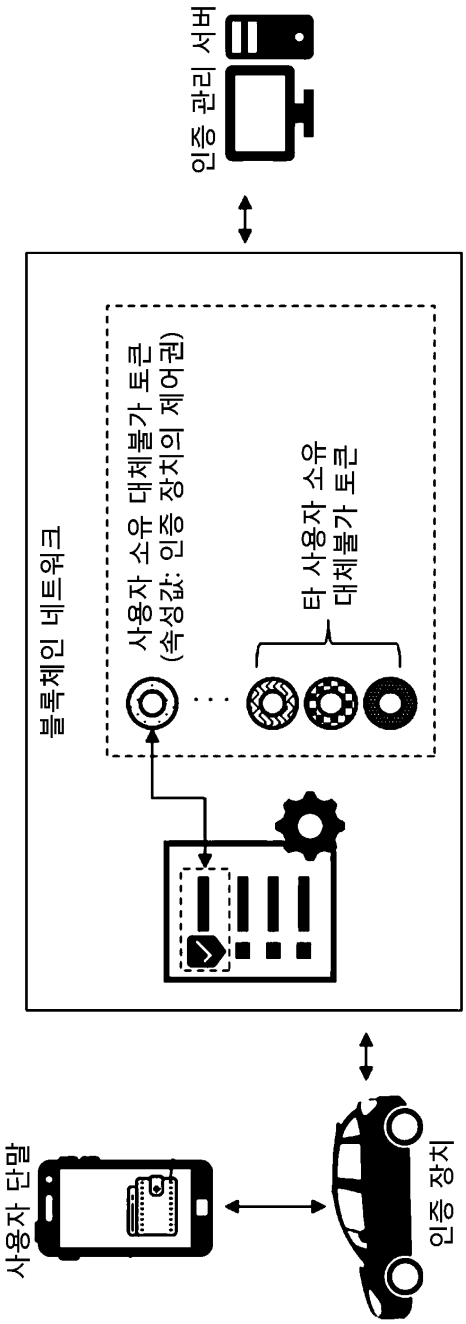
[0099] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

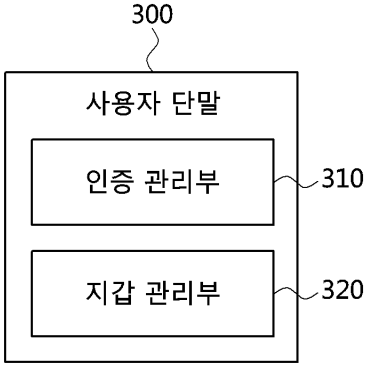
도면1



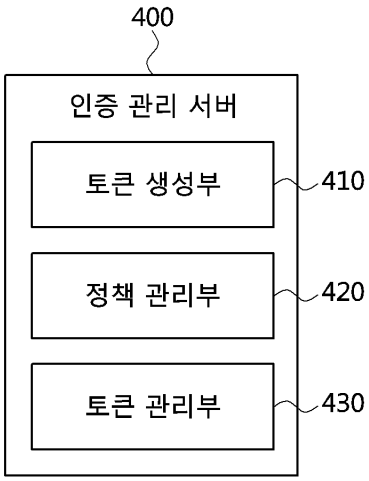
도면2


인증 관리 서버
블록체인 네트워크
사용자 소유 대체불가 토큰
(속성값: 인증 장치의 제어권)
타 사용자 소유
대체불가 토큰
사용자 단말
인증 장치

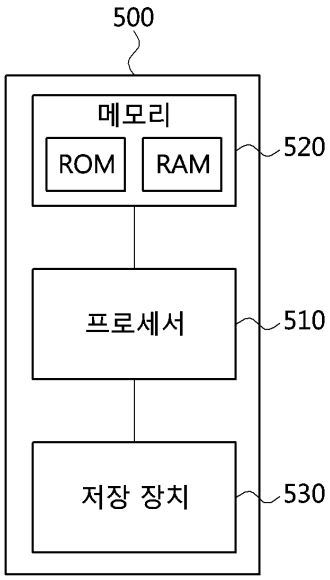
도면3


300
사용자 단말
인증 관리부
310
지갑 관리부
320

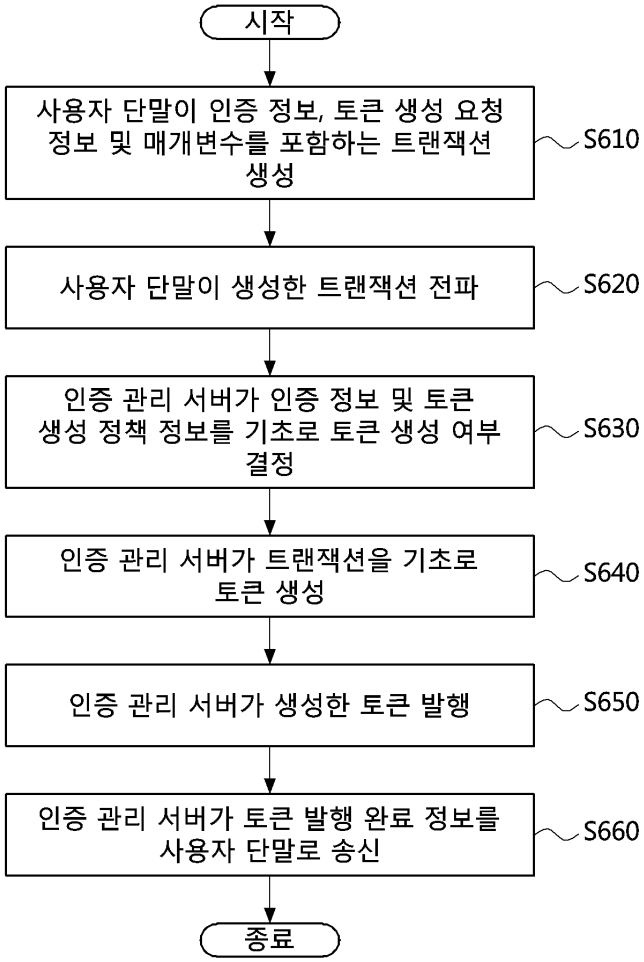
도면4


400
인증 관리 서버
토큰 생성부
410
정책 관리부
420
토큰 관리부
430

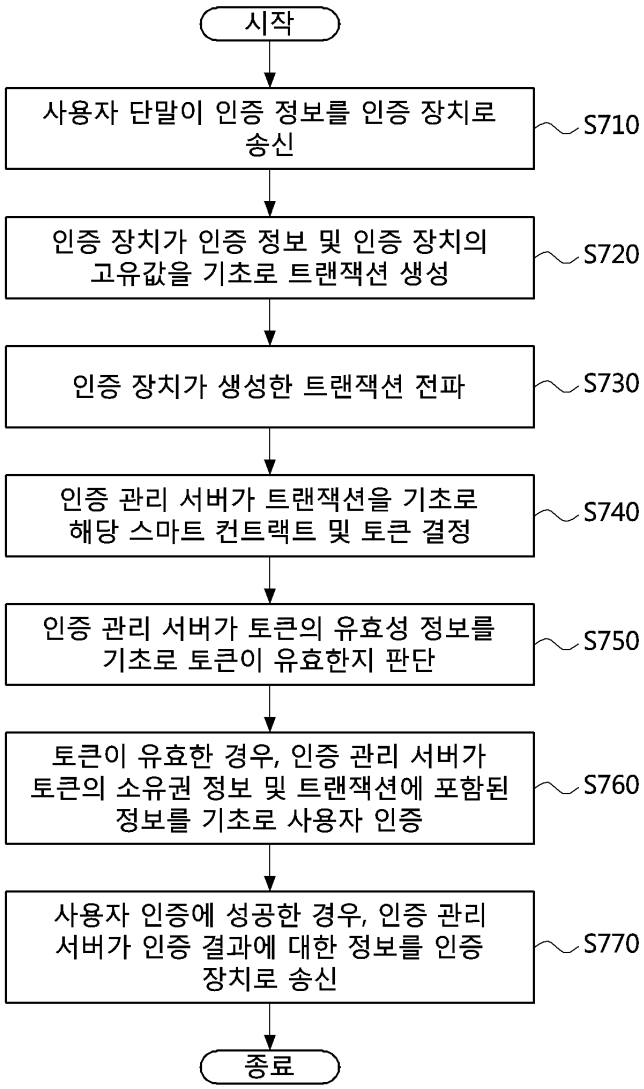
도면5


500
메모리
ROM
RAM
520
프로세서
510
저장 장치
530

도면6


시작
사용자 단말이 인증 정보, 토큰 생성 요청 정보 및 매개변수를 포함하는 트랜잭션 생성
S610
사용자 단말이 생성한 트랜잭션 전파
S620
인증 관리 서버가 인증 정보 및 토큰 생성 정책 정보를 기초로 토큰 생성 여부 결정
S630
인증 관리 서버가 트랜잭션을 기초로 토큰 생성
S640
인증 관리 서버가 생성한 토큰 발행
S650
인증 관리 서버가 토큰 발행 완료 정보를 사용자 단말로 송신
S660
종료

도면7



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 15

【변경전】

청구항 11에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 상기 사용자 단말의 고유한 주소 정보를 포함하는, 인증 관리 서버.

【변경후】

청구항 11에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함하는, 인증 관리 서버.

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 5

【변경전】

청구항 1에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 상기 사용자 단말의 고유한 주소 정보를 포함하는, 사용자 인증 방법.

【변경후】

청구항 1에 있어서,

상기 인증 정보는,

상기 스마트 컨트랙트의 주소 정보 및 사용자 단말의 고유한 주소 정보를 포함하는, 사용자 인증 방법.