



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년09월15일
(11) 등록번호 10-2302097
(24) 등록일자 2021년09월08일

(51) 국제특허분류(Int. Cl.)
G06Q 10/10 (2012.01) G06Q 50/26 (2012.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
G06Q 10/10 (2021.08)
G06Q 50/26 (2013.01)
(21) 출원번호 10-2021-0001511
(22) 출원일자 2021년01월06일
심사청구일자 2021년01월06일
(56) 선행기술조사문헌
KR102131206 B1*
KR102197218 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
채상미
서울특별시 종로구 평창11길 94 (평창동)
박민정
서울특별시 서초구 효령로34길 79, 1동 1303호 (방배동, 삼익아파트)
(74) 대리인
(뒷면에 계속)
특허법인메이저

전체 청구항 수 : 총 11 항

심사관 : 김은수

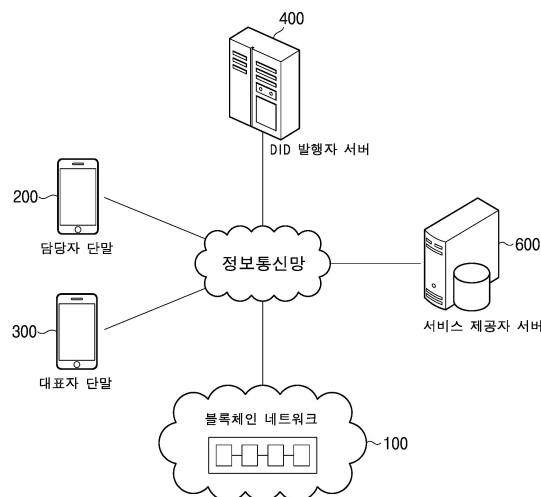
(54) 발명의 명칭 **블록체인 기반 법인DID 서비스 제공 시스템 및 방법**

(57) 요약

본 발명은 법인DID(Decentralized Identity) 서비스 제공 시스템을 개시한다. 보다 상세하게는, 본 발명은 블록체인 기술에 기반하여 분산화된 탈중앙화 신원증명을 통해 전자화된 법인 인증수단을 제공하는 블록체인 기반 법인 DID 서비스 제공 시스템 및 방법에 관한 것이다.

본 발명의 실시예에 따르면, 종래 개인 위주로 개발중인 DID의 개발 취지인 자기주권형 신원보장(SSI)과 데이터 소유권을 법인까지 확대할 수 있고, 현재, 전자계약, 전자등기 및 전자금융거래 등이 수반하는 보안 취약점 존재, 거래 당사자들 사이에 낮은 신뢰, 거래의 안전성 담보 불가, 개인의 정보악용 및, 전자 거래를 수행하기 위해 필요한 복잡하고 번거로운 서류 절차 등의 다양한 문제점을 해결할 수 있는 효과가 있다.

대 표 도 - 도1



(52) CPC특허분류

H04L 9/0643 (2013.01)

H04L 2209/38 (2013.01)

(72) 발명자

김중현

서울특별시 강남구 압구정로29길 68, 72동 407호(
압구정동, 현대아파트)

이명준

서울특별시 종로구 평창11길 94

명세서

청구범위

청구항 1

발급된 DID를 저장하는 블록체인 네트워크;

기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인인감 또는 법인인감카드를 대체하는 법인DID의 발급을 요청하는 담당자 단말;

상기 법인DID의 발급 요청에 응답하여 기업 대표자의 신원을 증명하는 제2 개인DID를 이용하여 상기 법인DID에 대한 사용을 승인하는 대표자 단말; 및

상기 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 상기 제1 및 제2 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하고, 발급된 법인DID를 상기 블록체인 네트워크에 등록 및 상기 담당자 단말에 배포하는 DID 발행자 서버를 포함하고,

상기 대표자 단말은,

상기 DID 발행자 서버에 상기 제2 개인DID의 발급을 요청하고, 발급된 제2 개인DID를 배포받는 개인DID 관리부;

기업 대표자 권한으로 상기 법인DID 발급 요청건에 대한 사용 승인을 입력받아 상기 DID 발행자 서버에 제공하는 사용 승인부; 및

상기 제2 개인DID를 저장하는 저장소를 포함하고,

상기 DID 발행자 서버는,

상기 제1 및 제2 개인DID를 이용하여 해당 기업 담당자 및 기업 대표자의 신원 검증을 수행하는 신원 검증부;

신원 검증된 법인DID 발급 요청건에 대하여 해당 기업 대표자의 대표자 단말에 사용 승인을 요청하는 승인 요청부; 및

신원 검증 및 사용 승인된 법인DID 발급 요청건에 대한 법인DID를 생성하여 상기 블록체인 네트워크에 등록하는 DID 생성부

를 포함하는 블록체인 기반 법인DID 서비스 제공 시스템.

청구항 2

제 1 항에 있어서,

상기 담당자 단말은,

상기 DID 발행자 서버에 상기 제1 개인DID의 발급을 요청하고, 발급된 제1 개인DID를 배포받는 개인DID 관리부;

상기 DID 발행자 서버에 상기 법인DID의 발급을 요청하고, 상기 법인관련 데이터를 입력받아 상기 DID 발행자 서버에 제출하고, 발급된 법인DID를 배포받는 법인DID 관리부;

배포된 법인DID를 사용목적에 따라 서비스 제공자 서버에 제출하는 법인DID 제출부; 및

상기 제1 개인DID 및 법인DID를 저장하는 저장소

를 포함하는 블록체인 기반 법인DID 서비스 제공 시스템.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 DID 발행자 서버는,
 상기 담당자 단말 및 대표자 단말로부터 DID 발급을 요청받는 발급 접수부; 및
 생성된 DID를 담당자 단말 또는 대표자 단말에 배포하는 DID 배포부
 를 포함하는 블록체인 기반 법인DID 서비스 제공 시스템.

청구항 5

제 4 항에 있어서,
 상기 DID 생성부는,
 상기 담당자 단말로부터 제공되는 법인인감 이미지 파일 및 사용목적용 가공하여 법인관련 데이터를 생성하고,
 상기 법인관련 데이터를 상기 법인DID의 DID 도큐먼트에 반영하는 블록체인 기반 법인DID 서비스 제공 시스템.

청구항 6

제 5 항에 있어서,
 상기 법인관련 데이터는,
 상기 법인인감 이미지 파일을 소정의 해시함수를 통해 해싱한 데이터를 포함하는 블록체인 기반 법인DID 서비스
 제공 시스템.

청구항 7

제 4 항에 있어서,
 상기 DID 발행자 서버는,
 상기 법인DID에 대하여 사용기간을 포함하는 사용내역 발생시, 상기 사용내역을 해싱하여 상기 법인DID의 DID
 도큐먼트에 추가하여 상기 블록체인 네트워크에 등록하고, 상기 사용기간을 경과하면 상기 법인DID를 폐기하고
 상기 블록체인 네트워크에 등록하는 DID 관리부
 를 더 포함하는 블록체인 기반 법인DID 서비스 제공 시스템.

청구항 8

발급된 DID를 저장하는 블록체인 네트워크를 이용한 법인DID 서비스 제공 방법에 있어서,
 담당자 단말이 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인인감 또
 는 법인인감카드를 대체하는 법인DID의 발급을 DID 발행자 서버에 요청하는 단계;
 상기 DID 발행자 서버가 신원 검증된 제1 개인DID에 의해 요청된 법인DID 발급 요청에 대하여 대표자 단말에 사
 용 승인을 회신하는 단계;
 상기 대표자 단말이 상기 법인DID의 발급 요청에 응답하여, 기업 대표자의 신원을 증명하는 제2 개인DID를 이용
 하여 상기 법인DID에 대한 사용 승인을 상기 DID 발행자 서버에 요청하는 단계;
 상기 DID 발행자 서버가 상기 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 상기 제1 및 제2
 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하는 단계; 및
 상기 DID 발행자 서버가 발급된 법인DID를 상기 블록체인 네트워크에 등록 및 상기 담당자 단말에 배포하는 단
 계를 포함하고,
 상기 대표자 단말이 상기 법인DID의 발급 요청에 응답하여, 기업 대표자의 신원을 증명하는 제2 개인DID를 이용
 하여 상기 법인DID에 대한 사용 승인을 상기 DID 발행자 서버에 요청하는 단계 이전에,
 상기 대표자 단말이 상기 DID 발행자 서버에 상기 제2 개인DID의 발급을 요청하는 단계;
 상기 DID 발행자 서버가 해당 기업 대표자에 대한 제2 개인DID를 발급 및 상기 블록체인 네트워크에 등록하는
 단계;

상기 DID 발행자 서버가 등록된 제2 개인DID를 상기 대표자 단말에 배포하는 단계; 및
상기 대표자 단말이 배포된 제2 개인DID를 저장소에 저장하는 단계
를 포함하는 블록체인 기반 법인DID 서비스 제공 방법.

청구항 9

제 8 항에 있어서,
상기 담당자 단말이 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인
DID의 발급을 DID 발행자 서버에 요청하는 단계 이전에,
상기 담당자 단말이 상기 DID 발행자 서버에 상기 제1 개인DID의 발급을 요청하는 단계;
상기 DID 발행자 서버가 해당 기업 담당자에 대한 제1 개인DID를 발급 및 상기 블록체인 네트워크에 등록하는
단계;
상기 DID 발행자 서버가 등록된 제1 개인DID를 상기 담당자 단말에 배포하는 단계; 및
상기 담당자 단말이 배포된 제1 개인DID를 저장소에 저장하는 단계
를 포함하는 블록체인 기반 법인DID 서비스 제공 방법.

청구항 10

삭제

청구항 11

제 8 항에 있어서,
상기 DID 발행자 서버가 상기 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 상기 제1 및 제2
개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하는 단계는,
상기 담당자 단말이 상기 DID 발행자 서버에 법인인감 이미지 파일 및 사용목적을 제공하는 단계;
상기 DID 발행자 서버가 제공된 법인인감 이미지 파일 및 사용목적을 가공하여 법인관련 데이터를 생성하는 단
계; 및
상기 DID 발행자 서버가 상기 법인관련 데이터를 상기 법인DID의 DID 도큐먼트에 반영하는 단계
를 포함하는 블록체인 기반 법인DID 서비스 제공 방법.

청구항 12

제 11 항에 있어서,
상기 법인관련 데이터는,
상기 법인인감 이미지 파일을 소정의 해시함수를 통해 해싱한 데이터를 포함하는 블록체인 기반 법인DID 서비스
제공 방법.

청구항 13

제 8 항에 있어서,
상기 DID 발행자 서버가 발급된 법인DID를 상기 블록체인 네트워크에 등록 및 상기 담당자 단말에 배포하는 단
계 이후,
상기 DID 발행자 서버가 상기 법인DID에 대하여 사용기간을 포함하는 사용내역 발생시, 상기 사용내역을 해싱하
고 상기 법인DID의 DID 도큐먼트에 추가하여 상기 블록체인 네트워크에 등록하는 단계; 및
상기 DID 발행자 서버가 상기 사용기간을 경과하면 상기 법인DID를 폐기하고, 상기 블록체인 네트워크에 등록하
는 단계

를 포함하는 블록체인 기반 법인DID 서비스 제공 방법.

발명의 설명

기술 분야

[0001] 본 발명은 법인DID(Decentralized Identity) 서비스 제공 시스템에 관한 것으로, 특히 블록체인 기술에 기반하여 분산화된 탈중앙화 신원증명을 통해 전자화된 법인 인증수단을 제공하는 블록체인 기반 법인DID 서비스 제공 시스템 및 방법에 관한 것이다.

배경 기술

- [0002] 일반적으로, 법인은 기업에서 처리해야 하는 여러 업무에 대하여 법인인감 증명이 필요한 상황이 종종 발생하곤 한다.
- [0003] 특히, 법인이 정부기관과의 계약 체결 또는 은행 등 금융기관을 대상으로 하는 업무를 처리하기 위해서는 법인 등기부등본, 법인인감도장, 사용자등록증, 대리인 체결 시 위임장(대리인, 위임인의 법인 인감도장, 인감증명서 필요) 등 상당한 구비서류를 요구함에 따라, 편의성이 저하되고 계약의 신뢰성 및 안정성이 결여되는 원인이 된다.
- [0004] 전술한 구비서류 중, 법인인감증명서 및 법인등기부등본 등을 발급하기 위해서는 법인임을 증명하기 위한 법인 인감카드가 요구된다. 상기의 법인인감카드는 물리카드로서 업무 처리의 편의성을 목적으로 도입되었으며, 전자 등기 및 무인 서류발급기 등의 이용이 가능하다는 점에서 장점이 있으나, 실질적으로 법인인감카드를 관리 및 보유하는 자, 일례로서 기업의 업무 담당자가 법인의 대표 승낙없이 악용할 경우, 법인 서류를 발급하여 악용 가능하다는 위험이 존재한다.
- [0005] 또한, 법인의 금융 업무 처리에 반드시 요구되는 공인인증서, 개인용 컴퓨터, USB 장치 등에 쉽게 복사 및 저장이 가능함에 따라 악용 가능성이 수반되며, 해킹에 따른 유출 혹은 분실의 위험이 상시 존재한다고 할 수 있다.
- [0006] 이러한 법인인감카드는 공인인증서, 법인인감카드 등 업무 진행에 필요한 서류 발급 및 제출 등의 절차를 실질적으로 기업 대표가 모두 처리할 수 없다는 한계가 있으며, 결국 전자기반 거래의 기능을 통한 편의성 증진의 취지로 개발되었으나 직원의 악용 가능성, 해킹 등에 따른 낮은 보안성과 안전성 문제에서 자유롭지 않다.
- [0007] 한편, 공지의 공인인증서는 신뢰할 수 있는 승인기관(CA)을 통하여 발급되고, 발급기관 내 신원정보를 일괄 저장한다는 점에서 개인의 자기 주권과 보안성이 보장되지 않는 한계가 있다.
- [0008] 또한, 전자서명은 전자계약 및 전자상거래 이용 등을 위하여 개발되었으며, 서명된 문서의 내용을 변경하거나 삭제하는 것과, 서명 사실을 부인하는 것 등이 불가능하도록 무결성 및 부인 방지 기능을 제공하는 것이 목적이거나, 검증하는 키가 공개된 공개키 방식을 이용함에 따라, 서명의 검증은 누구나 가능하다는 문제가 있다. 이는 송신자의 공개키가 맞는지 확인이 불가하며, 이에 따라 해커가 자신을 송신자로 속여서 전송하는 경우 문제가 발생할 가능성이 있다.
- [0009] 따라서, 현재까지 법인에서 전자계약 체결 요건인 전자서명을 포함하여 각종 법인 증명 기술, 체결된 계약의 신뢰성 및 무결성 등을 담보하기 위한 효율적인 수단이 없는 실정이라 할 수 있다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 등록특허공보 제10-2131206호(공고일자: 2020.08.05.)

발명의 내용

해결하려는 과제

[0011] 본 발명은 전술한 문제점을 해결하기 위해 안출된 것으로, 본 발명은 기존의 법인인감카드를 대체할 수 있는 탈

중앙화 신원증명(Decentralized Identity; DID) 기술에 기반한 새로운 개념의 인증수단인 법인DID를 제공하는 데 과제가 있다.

과제의 해결 수단

- [0012] 전술한 과제를 해결하기 위해, 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템은, 발급된 DID를 저장하는 블록체인 네트워크, 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인DID의 발급을 요청하는 담당자 단말, 상기 법인DID의 발급 요청에 응답하여 기업 대표자의 신원을 증명하는 제2 개인DID를 이용하여 상기 법인DID에 대한 사용을 승인하는 대표자 단말 및, 상기 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 상기 제1 및 제2 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하고, 발급된 법인DID를 상기 블록체인 네트워크에 등록 및 상기 담당자 단말에 배포하는 DID 발행자 서버를 포함할 수 있다.
- [0013] 상기 담당자 단말은, 상기 DID 발행자 서버에 상기 제1 개인DID의 발급을 요청하고, 발급된 제1 개인DID를 배포받는 개인DID 관리부, 상기 DID 발행자 서버에 상기 법인DID의 발급을 요청하고, 상기 법인관련 데이터를 입력받아 상기 DID 발행자 서버에 제출하고, 발급된 법인DID를 배포받는 법인DID 관리부, 배포된 법인DID를 사용목적에 따라 서비스 제공자 서버에 제출하는 법인DID 제출부 및, 상기 제1 개인DID 및 법인DID를 저장하는 저장소를 포함할 수 있다.
- [0014] 상기 대표자 단말은, 상기 DID 발행자 서버에 상기 제2 개인DID의 발급을 요청하고, 발급된 제2 개인DID를 배포받는 개인DID 관리부, 기업 대표자 권한으로 상기 법인DID 발급 요청건에 대한 사용 승인을 입력받아 상기 DID 발행자 서버에 제공하는 사용 승인부 및, 상기 제2 개인DID를 저장하는 저장소를 포함할 수 있다.
- [0015] 상기 DID 발행자 서버는, 상기 담당자 단말 및 대표자 단말로부터 DID 발급을 요청받는 발급 접수부, 상기 제1 및 제2 개인DID를 이용하여 해당 기업 담당자 및 기업 대표자의 신원 검증을 수행하는 신원 검증부, 신원 검증된 법인DID 발급 요청건에 대하여 해당 기업 대표자의 대표자 단말에 사용 승인을 요청하는 승인 요청부, 신원 검증 및 사용 승인된 법인DID 발급 요청건에 대한 법인DID를 생성하여 상기 블록체인 네트워크에 등록하는 DID 생성부 및, 생성된 DID를 담당자 단말 또는 대표자 단말에 배포하는 DID 배포부를 포함할 수 있다.
- [0016] 상기 DID 생성부는, 상기 담당자 단말로부터 제공되는 법인인감 이미지 파일 및 사용목적용을 가공하여 법인관련 데이터를 생성하고, 상기 법인관련 데이터를 상기 법인DID의 DID 도큐먼트에 반영할 수 있다.
- [0017] 상기 법인관련 데이터는, 상기 법인인감 이미지 파일을 소정의 해시함수를 통해 해싱한 데이터를 포함할 수 있다.
- [0018] 상기 DID 발행자 서버는, 상기 법인DID에 대하여 사용기간을 포함하는 사용내역 발생시, 상기 사용내역을 해싱하여 상기 법인DID의 DID 도큐먼트에 추가하여 상기 블록체인 네트워크에 등록하고, 상기 사용기간을 경과하면 상기 법인DID를 폐기하고 상기 블록체인 네트워크에 등록하는 DID 관리부를 더 포함할 수 있다.
- [0019] 또한, 전술한 과제를 해결하기 위해, 본 발명의 다른 양태의 실시예에 따른 블록체인 네트워크를 이용한 법인DID 서비스 제공 방법은, 발급된 DID를 저장하는 블록체인 네트워크를 이용한 법인DID 서비스 제공 방법에 있어서, 담당자 단말이 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인DID의 발급을 DID 발행자 서버에 요청하는 단계, 상기 DID 발행자 서버가 신원 검증된 제1 개인DID에 의해 요청된 법인DID 발급 요청에 대하여 대표자 단말에 사용 승인을 회신하는 단계, 상기 대표자 단말이 상기 법인DID의 발급 요청에 응답하여, 기업 대표자의 신원을 증명하는 제2 개인DID를 이용하여 상기 법인DID에 대한 사용 승인을 상기 DID 발행자 서버에 요청하는 단계, 상기 DID 발행자 서버가 상기 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 상기 제1 및 제2 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하는 단계 및, 상기 DID 발행자 서버가 발급된 법인DID를 상기 블록체인 네트워크에 등록 및 상기 담당자 단말에 배포하는 단계를 포함할 수 있다.
- [0020] 상기 담당자 단말이 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인DID의 발급을 DID 발행자 서버에 요청하는 단계 이전에, 상기 담당자 단말이 상기 DID 발행자 서버에 상기 제1 개인DID의 발급을 요청하는 단계, 상기 DID 발행자 서버가 해당 기업 담당자에 대한 제1 개인DID를 발급 및 상기 블록체인 네트워크에 등록하는 단계, 상기 DID 발행자 서버가 등록된 제1 개인DID를 상기 담당자 단말에 배포하는 단계 및, 상기 담당자 단말이 배포된 제1 개인DID를 저장소에 저장하는 단계를 포함할 수 있다.
- [0021] 상기 대표자 단말이 상기 법인DID의 발급 요청에 응답하여, 기업 대표자의 신원을 증명하는 제2 개인DID를 이용

하여 상기 법인DID에 대한 사용 승인을 상기 DID 발행자 서버에 요청하는 단계 이전에, 상기 대표자 단말이 상기 DID 발행자 서버에 상기 제2 개인DID의 발급을 요청하는 단계, 상기 DID 발행자 서버가 해당 기업 대표자에 대한 제2 개인DID를 발급 및 상기 블록체인 네트워크에 등록하는 단계, 상기 DID 발행자 서버가 등록된 제2 개인DID를 상기 대표자 단말에 배포하는 단계 및, 상기 대표자 단말이 배포된 제2 개인DID를 저장소에 저장하는 단계를 포함할 수 있다.

[0022] 상기 DID 발행자 서버가 상기 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 상기 제1 및 제2 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하는 단계는, 상기 담당자 단말이 상기 DID 발행자 서버에 법인인감 이미지 파일 및 사용목적용 제공받는 단계, 상기 DID 발행자 서버가 제공된 법인인감 이미지 파일 및 사용목적용 가공하여 법인관련 데이터를 생성하는 단계; 및, 상기 DID 발행자 서버가 상기 법인관련 데이터를 상기 법인DID의 DID 도큐먼트에 반영하는 단계를 포함할 수 있다.

[0023] 상기 법인관련 데이터는, 상기 법인인감 이미지 파일을 소정의 해시함수를 통해 해싱한 데이터를 포함할 수 있다.

[0024] 상기 DID 발행자 서버가 발급된 법인DID를 상기 블록체인 네트워크에 등록 및 상기 담당자 단말에 배포하는 단계 이후, 상기 DID 발행자 서버가 상기 법인DID에 대하여 사용기간을 포함하는 사용내역 발생시, 상기 사용내역을 해싱하고 상기 법인DID의 DID 도큐먼트에 추가하여 상기 블록체인 네트워크에 등록하는 단계 및, 상기 DID 발행자 서버가 상기 사용기간을 경과하면 상기 법인DID를 폐기하고, 상기 블록체인 네트워크에 등록하는 단계를 포함할 수 있다.

발명의 효과

[0025] 본 발명의 실시예에 따르면, 종래 개인 위주로 개발중인 DID의 개발 취지인 자기주권형 신원보장(SSI)과 데이터 소유권을 법인까지 확대할 수 있고, 현재, 전자계약, 전자등기 및 전자금융거래 등이 수반하는 보안 취약점 존재, 거래 당사자들 사이에 낮은 신뢰, 거래의 안전성 담보 불가, 개인의 정보악용 및, 전자 거래를 수행하기 위해 필요한 복잡하고 번거로운 서류 절차 등의 다양한 문제점을 해결할 수 있는 효과가 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 전체 구조를 개략적으로 나타낸 도면이다.

도 2는 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 담당자 단말의 구조를 나타낸 도면이다.

도 3은 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 DID 발행자 서버의 구조를 나타낸 도면이다.

도 4는 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템에 의한 법인DID 서비스 제공 방법을 나타낸 도면이다.

도 5는 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템에 적용되는 개인DID 또는 법인DID 발급절차를 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0027] 설명에 앞서, 명세서 전체에서 어떤 부분이 어떤 구성요소를 "구비" 또는 "포함" 한다고 할 때, 이는 특별히 반대되는 기재가 없는 한, 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부(Unit)", "...서버(Server)", "...시스템(System)" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어, 소프트웨어 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0028] 또한, 본 명세서에서 "실시예"라는 용어는 예시, 사례 또는 도해의 역할을 하는 것을 의미하나, 발명의 대상은 그러한 예에 의해 제한되지 않는다. 또한, "포함하는", "구비하는", "갖는" 및 다른 유사한 용어가 사용되고 있으나, 청구범위에서 사용되는 경우 임의의 추가적인 또는 다른 구성요소를 배제하지 않는 개방적인 전환어(Transition word)로서 "포함하는(Comprising)"이라는 용어와 유사한 방식으로 포괄적으로 사용된다.

- [0029] 본 명세서에 설명된 다양한 기법은 하드웨어 또는 소프트웨어와 함께 구현될 수 있거나, 적절한 경우에 이들 모두의 조합과 함께 구현될 수 있다. 본 명세서에 사용된 바와 같은 "...부(Unit)", "...서버(Server)", "...시스템(System)" 등의 용어는 마찬가지로 컴퓨터 관련 엔티티(Entity), 즉 하드웨어, 하드웨어 및 소프트웨어의 조합, 소프트웨어 또는 실행 시의 소프트웨어와 등가로 취급할 수 있다. 또한, 본 발명의 시스템에서 구현하는 각 기능은 모듈단위의 프로그램으로 구성될 수 있고, 하나의 물리적 메모리에 기록되거나, 둘 이상의 메모리 및 기록매체 사이에 분산되어 기록될 수 있다.
- [0030] 이하의 설명에서, 본 발명의 실시예에 따른 '블록체인 기반 법인DID 서비스 제공 시스템'을 가리키는 용어는 '법인DID 서비스 제공 시스템' 또는 '시스템' 등으로 약식 표기될 수 있다.
- [0031] 또한, 이하의 설명에서, '~ 단말'은 시스템에 접속하여 서비스를 요청하는 소정의 컴퓨팅 장치 또는, 소정의 컴퓨팅 장치에서 구동되는 어플리케이션 프로그램 자체를 가리키는 개념이다.
- [0032] 이하, 도면을 참조하여 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템 및 방법을 상세히 설명한다.
- [0033] 도 1은 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 전체 구조를 개략적으로 나타낸 도면이다.
- [0034] 도 1을 참조하면, 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템은, 발급된 DID를 저장하는 블록체인 네트워크(100), 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인DID의 발급을 요청하는 담당자 단말(200), 법인DID의 발급 요청에 응답하여 기업 대표자의 신원을 증명하는 제2 개인DID를 이용하여 상기 법인DID에 대한 사용을 승인하는 대표자 단말(300) 및 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 제1 및 제2 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하고, 발급된 법인DID를 블록체인 네트워크(100)에 등록 및 담당자 단말(200)에 배포하는 DID 발행자 서버(400)를 포함할 수 있다.
- [0035] 블록체인 네트워크(100)는, 신원증명을 위한 복수의 분산원장(Distributed ledger)을 포함하고, 이러한 블록체인 네트워크(100)의 참여자는 소정의 합의절차에 따라 스마트 컨트랙트(Smart contract)를 통해 분산원장에 정보를 기록하거나 불러올 수 있다.
- [0036] 특히, 블록체인 네트워크(100)에는 발급된 법인DID 및 DID 문서가 복수의 블록에 분산 저장되며, 서비스 제공자 서버(600)의 요청에 따라 담당자 단말(200)로부터 제공되는 법인DID에 대한 DID 문서를 제공함으로써, 서비스 제공자 서버(600)가 해당 기업 및 법인DID의 목적을 식별하고, 권한을 확인하여 요청한 서비스를 제공할 수 있도록 한다.
- [0037] 담당자 단말(200)은 해당 기업에 소속된 직원이 이용하는 단말장치 또는 어플리케이션 프로그램으로서, 법인등기부 등본, 법인인감도장 및 사용자 등록증 등을 관리, 사용하는 권한을 가진 직원이 본 발명의 시스템을 통해 법인 거래 계약 등의 절차를 진행하기 위한 법인 신원증명수단으로서 법인DID를 신청 및 발급받고 서비스 제공자 측에 제공할 수 있다.
- [0038] 이를 위해, 기업 담당자는 자신의 담당자 단말(200)을 이용하여 시스템을 통해 우선적으로 자신이 해당 업무의 권한을 갖는 담당자임을 증명할 수 있는 개인DID를 발급받고, 그 개인DID를 이용하여 해당 기업의 대표자에게 승인을 요청함과 아울러, 승인 완료시 자신의 개인DID 및 대표자의 개인DID를 이용하여 법인DID 발급을 요청하게 된다.
- [0039] 여기서, 동일 기업이라 할지라도 일반 직원은 위임장 발급 및 위임장 승인을 위한 대표 호출 권한을 제한되며 해당 업무의 권한을 갖는 기업 담당자인 참여자만이 시스템에 접근 권한을 가질 수 있다. 이러한 권한은 전술한 개인DID 발급시의 신원증명 절차에서 필터링되며, 권한없는 개인DID로는 이후 법인DID 발급절차의 진행이 불가능하도록 제한될 수 있다.
- [0040] 그리고, 담당자 단말(200)에 의해 정상적으로 법인DID가 발급되어 블록체인 네트워크(100)에 등록되면, 기업 담당자는 목적한 업무 수행을 위한 서비스 제공자 서버(600)에 법인DID를 제공하여 신원증명 절차를 수행하고, 해당 업무를 처리할 수 있다.
- [0041] 대표자 단말(300)은 해당 기업의 대표이사 등 법인인감을 소지 및 관리하는 대표자가 이용하는 단말장치 또는 어플리케이션 프로그램으로서, 법인 계약 등 법인인감의 날인이 요구되는 업무에 대하여 기업 담당자에 의한 법

인인감을 대체하는 법인DID의 사용을 승인할 수 있다.

- [0042] 이를 위해, 기업 대표자는 자신의 대표자 단말(300)을 이용하여 시스템을 통해 자신이 대표자임을 증명할 수 있는 개인DID를 발급받고, 이후 담당자 단말(200)로부터 법인DID의 발급을 위한 승인이 요청되면, 자신의 개인DID를 이용하여 신원 증명을 수행하고, 발급 요청건에 대한 승인을 처리함으로써 기업 담당자가 법인DID를 발급받을 수 있도록 한다.
- [0043] 전술한 담당자 단말(200) 및 대표자 단말(300)을 실행하기 위한 하드웨어 장치로는, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말, 스마트폰(smartphone), 스마트 패드(smartpad), 태블릿 PC(Tablet PC) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 모바일 단말 장치, 거치형PC 및 노트북과 같은 컴퓨팅 장치가 이용될 수 있다.
- [0044] DID 발행자 서버(400)는 등록된 각 기업의 담당자 단말(200) 및 대표자 단말(300)의 요청에 따라 신원증명을 위한 개인DID를 발급 및 블록체인 네트워크(100)에 등록할 수 있고, 또한 권한을 갖는 담당자 단말(200)의 요청에 따라 법인인감에 대한 관리, 사용 등의 의무를 갖는 대표자 단말(300)에 사용에 대한 승인을 요청할 수 있다.
- [0045] 여기서, DID 발행자 서버(400)는 별도의 업체 또는 기관에서 운영되거나, 법인DID 서비스를 이용하고자 하는 기업에 의해 자체적으로 운영될 수 있다. 일례로서, 본 발명의 DID 발행자 서버(400)는 본 발명의 시스템을 도입하고자 하는 기관, 기업 등에서 운영하는 서버 자체에 탑재되거나, 또는 기업 서버와 연계하여 서비스를 제공할 수 있다.
- [0046] 또한, DID 발행자 서버(400)는 대표자 단말(300)에 의해 정상적으로 승인된 사용 요청건에 대하여 법인DID를 생성 및 블록체인 네트워크(100)에 등록하고, 요청한 담당자 단말(200)에 법인DID를 배포할 수 있다.
- [0047] 또한, 본 발명의 실시예에 따르면, DID 발행자 서버(400)는 담당자 단말(200) 및 대표자 단말(300)의 DID 발급 요청시, 그 요청자가 제출한 DID 소유권을 확인하기 위해 별도의 기업 또는 기관 등에서 운영하는 서버에 DID 소유권에 대한 인증을 요청할 수도 있다.
- [0048] 이러한 DID 발행자 서버(400)로는 다수의 담당자 단말(200) 및 대표자 단말(300)의 개인DID 및 법인DID 발급 요청, 사용 승인 등에 대하여 오류 및 지연없이 신속하게 응답하기 위해, 고성능의 마이크로프로세서, 대용량 메모리 및 저장소를 탑재한 서버장치가 이용될 수 있다.
- [0050] 이후, DID 발행자 서버(400) 또는 서비스 제공자 서버(600)에서 개인DID의 사용자에 대한 신원 증명시, 사용자가 소지한 비밀키에 의해 생성된 인증값을 이용하여, 블록체인 네트워크에 저장된 개인DID의 DID 문서에 포함된 공개키를 통해 검증함으로써 사용자, 즉 기업 담당자 또는 기업 대표자에 대한 검증을 수행할 수 있다.
- [0051] 서비스 제공자 서버(600)는 기업에서 법인인감 또는 법인인감카드를 통해 수행하는 다양한 기업업무 서비스를 제공하는 서버 장치로서, 협약된 기업에서 전자계약, 전자금융거래 및 전자상거래 등을 법인인감카드가 아닌 본 발명의 시스템이 제공하는 법인DID를 통해 수행할 수 있도록 한다.
- [0052] 이러한 서비스 제공자 서버(600)는 담당자 단말(200)이 법인DID를 통해 소정의 법인업무 처리를 요청하면, 블록체인 네트워크로부터 법인DID를 통해 식별되는 DID 문서를 참조하여 법인DID의 DID 소유권, 사용 목적 및 범위 등을 확인하고, 신원증명절차를 거쳐 신원 증명된 법인DID를 통해 요청된 서비스를 제공할 수 있다.
- [0053] 전술한 구조에 따라, 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템은 각 기업에서 법인계약 등의 업무를 수행하기 위해 요구되는 법인등기부등본, 법인인감도장 등의 다수의 필요서류를 대체하여 기업 담당자가 자신의 담당자 단말을 통해 목적에 따라 일회성의 법인DID를 발급받아 관련 업무를 수행할 수 있어, 복잡한 서류 절차 처리, 법인 서류 악용 및 보안 취약점 등의 다양한 문제점을 해결하고 안정적인 법인거래 및 업무를 처리할 수 있는 효과가 있다.
- [0054] 이하, 도면을 참조하여 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 담당자 단말을 상세히 설명한다.
- [0055] 도 2는 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 담당자 단말의 구조를 나타낸 도면이다. 이하의 설명에서 담당자 단말(200) 및 담당자 단말(200)을 구성하는 각 구성부는 공지의 마이크로프로

세서에 의해 실행 가능한 컴퓨터 프로그램으로 구성될 수 있고, 읽고 쓰기가 가능한 기록매체에 기록되어 단말 장치에 탑재될 수 있다.

- [0056] 도 2는 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 담당자 단말(200)은, DID 발행자 서버(400)에 상기 제1 개인DID의 발급을 요청하고, 발급된 제1 개인DID를 배포받는 개인DID 관리부(210), DID 발행자 서버(400)에 법인DID의 발급을 요청하고, 법인관련 데이터를 입력받아 DID 발행자 서버(400)에 제출하고, 발급된 법인DID를 배포받는 법인DID 관리부(220), 배포된 법인DID를 사용목적에 따라 서비스 제공자 서버(600)에게 제출하는 법인DID 제출부(230) 및, 제1 개인DID 및 법인DID를 저장하는 저장소(240)를 포함할 수 있다.
- [0057] 개인DID 관리부(210)는, 기업 담당자에게 발급된 DID인 제1 개인DID에 대한 다양한 관리 기능을 제공할 수 있다. 개인DID 관리부(210)는 해당 기업의 소속된 자로서 신원 증명을 위한 제1 개인DID의 발급을 DID 발행자 서버(400) 또는, 기업, 기관에서 운영하는 서버 등에 요청할 수 있고, 발급된 제1 개인DID를 저장소(240)에 저장하고, 추후 기업 담당자가 자신의 신원을 증명하고자 할 때 저장된 제1 개인DID를 제출하여 신원 증명 절차를 수행할 수 있다.
- [0058] 법인DID 관리부(220)는 법인DID와 관련된 기능을 제공할 수 있다. 본 발명의 실시예에서 제1 개인DID를 발급받을 수 있고, 이에 기초하여 업무처리를 위한 법인DID를 생성 및 배포 받을 수 있다. 제1 개인DID를 보유한 기업 담당자는 법인 계약 등의 법인인감을 요구하는 업무 진행시 담당자 단말(200)을 통해 법인DID 발급을 요청할 수 있고, 이에 법인DID 관리부(220)는 저장소(240)에 저장된 법인DID가 존재하지 않은 경우, 제1 개인DID를 DID 발행자 서버(400)에 제출함과 아울러, 법인DID의 발급을 신청할 수 있다. 이때, 법인DID 관리부(220)는 기업 담당자로부터 법인DID의 사용목적, 제출기관(업체), 법인 대표자명 및 일자 등의 정보를 입력 받을 수 있다.
- [0059] 이에, DID 발행자 서버(400)는 법인DID 발급 신청건에 대하여, 기업 대표자를 식별하고, 그 대표자 단말에 법인DID 발급에 대한 승인을 요청할 수 있다.
- [0060] 이후, 정상적으로 법인DID가 발급되어 배포되면, 법인DID 관리부(220)는 배포되는 법인DID를 저장소(240)에 저장할 수 있다.
- [0061] 법인DID 제출부(230)는, 기업 담당자의 실행에 따라 저장소(240)에 저장된 법인DID를 서비스 제공자 서버(600)에 제출할 수 있다. 이때, 법인DID 제출부(230)는 법인DID의 제출처, 사용내역 등의 정보를 블록체인 네트워크에 등록할 수 있다.
- [0062] 저장소(240)는, 현재 효력이 있는 개인DID 및 법인DID를 저장할 수 있다. 이중, 일반적으로 법인DID는 사용기간이 존재함에 따라, 사용기간이 경과된 법인DID는 자동으로 폐기될 수 있다.
- [0063] 또한, 본 발명의 실시예에 따른 담당자 단말(200)은 기업 담당자가 개인DID를 비롯하여 자신의 개인정보를 관리할 수 있도록 단말 내 신뢰 실행 환경(Trusted Execution Environment; TEE) 영역상에 저장할 수 있으며, 이에 따라 상기의 저장소(240)는 TEE 영역내 존재할 수 있다.
- [0064] 전술한 TEE는 일반적인 어플리케이션이 실행된 비보안 영역(secure normal area)과 보안 영역(secure area)이 따로 분리된 프로세서상에 DID를 포함하는 개인정보를 저장하는 것으로서, 일반 영역과의 정보 교환이 통제되고 보안 소프트웨어가 안전하게 실행될 수 있도록 지원하는 특징이 있다.
- [0065] 예를 들면, 스마트폰과 같은 모바일 단말기에는 암(ARM)사의 아키텍처 기반 프로세서가 널리 이용되고 있으며, 이에 담당자 단말(200)에 암 프로세서가 탑재된 경우 TEE 지원을 위한 트러스트존(TrustZone)에 개인정보가 기록 및 관리될 수 있다.
- [0066] 또한, 담당자 단말(200)이 모바일 단말이 아닌, x86, x64 기반 데스크탑 또는 노트북 등인 경우, 별도의 보안 모듈인 신뢰 플랫폼 모듈(Trusted Platform Module; TPM)이 탑재될 수 있고, 저장소(240)는 TPM 내 생성되어 개인정보에 이를 통해 기록 및 관리 될 수 있다.
- [0067] 이에 따라, 담당자 단말(200)에서 개인정보에 접근하고자 하는 경우, 자체 어플리케이션을 통해서만 제한적으로 접근이 가능하게 된다.
- [0068] 한편, 도시되어 있지는 않지만 본 발명의 실시예에 따르면, 전술한 담당자 단말(200)이외에도, 법인DID 요청건에 대한 승인을 수행하는 대표자가 사용하는 대표자 단말 또한 시스템을 이용하기 위한 구성부를 포함할 수 있다. 상세하게는, 대표자 단말은, DID 발행자 서버에 제2 개인DID의 발급을 요청하고 발급된 개인DID를 배포받는

개인DID 관리부, 기업 대표자 권한으로 담당자 단말(200)로부터 요청된 법인DID 발급 요청건에 대한 사용 승인을 입력받아 DID 발행자 서버(400)에 제공하는 사용 승인부 및, 제2 개인DID를 저장하는 저장소를 포함할 수 있다.

- [0069] 이하, 도면을 참조하여 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 DID 발행자 서버를 상세히 설명한다.
- [0070] 도 3은 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 DID 발행자 서버의 구조를 나타낸 도면이다.
- [0071] 도 3을 참조하면, 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템의 DID 발행자 서버(400)는, 담당자 단말(200) 및 대표자 단말(300)로부터 DID 발급을 요청받는 발급 접수부(410), 제1 및 제2 개인DID를 이용하여 신원 검증을 수행하는 신원 검증부(420), 신원 검증된 법인DID 발급 요청건에 대하여 해당 기업 대표자의 대표자 단말에 사용 승인을 요청하는 승인 요청부(430), 신원 검증 및 사용 승인된 법인DID 발급 요청건에 대한 법인DID를 생성하여 블록체인 네트워크(100)에 등록하는 DID 생성부(440), 생성된 DID를 담당자 단말(200) 또는 대표자 단말(300)에 배포하는 DID 배포부(450) 및 법인DID에 대하여 사용기간을 포함하는 사용내역 발생시, 사용내역을 해싱하고 법인DID의 DID 도큐먼트에 추가하여 블록체인 네트워크(100)에 등록하고, 사용 허가시간을 경과하면 법인DID를 폐기하고, 블록체인 네트워크(100)에 등록하는 DID 관리부(460)를 포함할 수 있다.
- [0072] 발급 접수부(410)는 담당자 단말(200)의 요청에 따라 제1 개인DID를 제공받아 법인DID에 대한 발급 요청을 접수할 수 있다. 법인DID를 업무에 이용하고자 하는 기업 담당자는 담당자 단말(200)에 저장된 제1 개인DID를 DID 발행자 서버(400)에 제출 및 법인DID 발급을 신청할 수 있고, 이에 발급 접수부(410)는 제1 개인DID와, 법인DID 발급에 필요한 각종 정보를 입력 받을 수 있다.
- [0073] 신원 검증부(420)는 법인DID 발급 요청건에 대하여, 제출된 제1 개인DID에 대한 신원증명 절차를 수행할 수 있다. 신원 검증부(420)는 제1 개인DID를 통해 블록체인 네트워크(100)로부터 DID 도큐먼트를 획득하여 공개키를 확인함으로써 제1 개인DID에 대한 신원증명을 요청할 수 있다. 또한, 담당자 단말(200)은 비밀키를 이용한 공개키 인증값을 생성하여 신원 검증부(420)에 제공하게 되며, 신원 검증부(420)는 공개키를 이용하여 인증값을 확인함으로써 기업 담당자의 신원을 검증하게 된다.
- [0074] 또한, 신원 검증부(420)는 상기와 동일한 절차에 따라, 제2 개인DID, 즉 기업 대표자에 대한 신원을 검증할 수 있다.
- [0075] 승인 요청부(430)는 법인DID 요청건의 접수시, 식별된 기업의 기업 대표자의 대표자 단말(300)에 법인DID 요청건에 대한 사용 승인을 요청할 수 있고, 제2 개인 DID를 통해 신원증명된 기업 대표자의 대표자 단말(300)로부터 사용 승인을 회신받아 법인DID 발급을 확정할 수 있다.
- [0076] DID 생성부(440)는 대표자 단말(300)의 사용 승인에 따라 법인DID 발급이 확정된 법인DID 요청건에 대하여 법인DID를 생성할 수 있다. 특히, 본 발명의 실시예에 따른 DID 생성부(440)는 해당 기업의 법인DID를 생성함에 있어서, 신원증명된 제1 및 제2 개인DID와, 실제 법인 인감에 대한 이미지 파일 및 담당자 단말(200)에 의해 입력된 법인인감의 사용목적, 사용기간 등을 포함하는 정보를 결합하고 공지의 암호화 해시함수를 이용하여 해싱(hashing)함으로써 고유의 인덱스(index)를 생성할 수 있고, 생성된 인덱스를 DID 도큐먼트에 반영하여 법인DID 및 그의 DID 도큐먼트를 생성할 수 있다. 여기서, 개인DID 및 법인 DID의 생성시, 적용된 블록체인 네트워크(100)의 플랫폼의 특징에 따라 주어진 방식으로 해시함수 등이 사용될 수 있고, 특정 플랫폼에 적용된 방식에 한정되지는 않는다.
- [0077] DID 배포부(450)는 생성된 법인DID를 담당자 단말(200)에 배포함과 아울러, 법인DID 및 DID 도큐먼트를 블록체인 네트워크(100)에 기록 및 등록할 수 있다. 이때, DID 생성부(440)는 법인DID의 등록을 위한 스마트 컨트랙트를 실행하여 트랜잭션을 생성하고, 블록체인 네트워크(100)는 공지의 합의 알고리즘을 통해 트랜잭션의 정당성을 판단하여 분산원장에 분산 및 저장하게 된다.
- [0078] 이후, 담당자 단말(200)은 업무진행을 위해 법인DID를 사용할 수 있으며, 법인DID 사용시 서비스 제공 서버는 신원증명 절차 등에서 미리 설정된 사용 목적에 부합하는지 여부에 따라 절차를 정상적으로 진행할 수 있다. 즉, 본 발명의 실시예에 따른 법인DID는 미리 설정된 사용목적에 부합하는 경우에만 법인인감의 날인 효과가 발생하게 된다.

- [0079] DID 관리부(460)는 법인DID의 배포 이후, 담당자 단말(200)에 의한 법인DID를 이용한 업무 발생시, 해당 업무를 처리하는 서비스 제공자 서버의 신원증명, DID 문서먼트 참조 등의 절차가 진행되면 그 내역을 추적하고, 이후 그 법인DID 관련 분산원장을 갱신하거나, 법인DID 폐기에 따른 내역을 추가 기록할 수 있다.
- [0080] 즉, DID 관리부(460)는 법인DID에 대하여 사용기간을 포함하는 사용내역 발생시, 사용내역을 해싱하고, 블록체인 네트워크(100)에 대한 트랜잭션을 발생시켜 법인DID의 DID 문서먼트에 추가함으로써 블록체인 네트워크에 등록할 수 있다.
- [0081] 여기서, 법인DID에는 사용목적뿐만 아니라, DID 문서먼트에 정의된 사용가능 시간, 즉 허가시간이 더 설정되어 있고, DID 관리부(460)는 그 허가시간이 경과하면 더 이상 법인DID를 사용하지 못하도록 폐기 처리 할 수 있다. 이는 법인DID와 관련된 모든 거래 내역을 보존함으로써 거래 내역의 투명성을 확보하기 위함이다.
- [0082] 이하, 도면을 참조하여 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템에 의한 법인DID 서비스 제공 방법을 상세히 설명한다.
- [0083] 도 4는 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템에 의한 법인DID 서비스 제공 방법을 나타낸 도면이다.
- [0084] 도 4를 참조하면, 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템에 의한 법인DID 서비스 제공 방법은, 발급된 DID를 저장하는 블록체인 네트워크(100)를 이용한 법인DID 서비스 제공 방법에 있어서, 담당자 단말(200)이 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인DID의 발급을 DID 발행자 서버(400)에 요청하는 단계(S100), DID 발행자 서버(400)가 신원 검증된 제1 개인DID에 의해 요청된 법인DID 발급 요청에 대하여 대표자 단말(300)에 사용 승인을 요청하는 단계(S200), 대표자 단말(300)이 법인DID의 발급 요청에 응답하여, 기업 대표자의 신원을 증명하는 제2 개인DID를 이용하여 법인DID에 대한 사용 승인을 DID 발행자 서버에 회신하는 단계(S300), DID 발행자 서버가 대표자 단말(300)로부터 사용 승인된 법인DID 발급 요청건에 대하여, 제1 및 제2 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하는 단계(S400) 및, DID 발행자 서버(400)가 발급된 법인DID를 블록체인 네트워크(100)에 등록 및 담당자 단말(200)에 배포하는 단계(S500)를 포함할 수 있다.
- [0085] 먼저, 담당자 단말이 기업 담당자의 신원을 증명하는 제1 개인DID를 이용하여 기업 담당자가 속한 기업의 법인DID의 발급을 DID 발행자 서버에 요청하는 단계(S100)로서, 본 발명의 시스템과 협약된 기업에 속한 임직원 등의 기업 담당자가 자신의 신원증명을 위한 제1 개인DID를 이용하여 법인인감이 요구되는 업무를 수행하기 위해, 제1 개인DID가 저장된 자신의 스마트폰 등을 이용하여 DID 발행자 서버에 법인DID의 발급을 요청할 수 있다.
- [0086] 여기서, 제1 개인DID는 자신이 속한 기업에서 운영하는 기업 서버에서 직접 발급받을 수 있고, 또는 본 발명의 DID 발행자 서버의 개인DID 발행 서비스를 통해 DID 발행자 서버로부터 발급받을 수도 있다.
- [0087] 다음으로, DID 발행자 서버가 신원 검증된 제1 개인DID에 의해 요청된 법인DID 발급 요청에 대하여 대표자 단말에 사용 승인을 요청하는 단계(S200)에서는, 정상적으로 신원 증명된 담당자 단말에 의한 법인DID 요청건에 대하여 해당 기업의 대표자를 식별하고, 그 대표자 단말에 법인DID 발급에 대한 사용 승인을 요청할 수 있다.
- [0088] 다음으로, 대표자 단말이 법인DID의 발급 요청에 응답하여, 기업 대표자의 신원을 증명하는 제2 개인DID를 이용하여 법인DID에 대한 사용 승인을 DID 발행자 서버에 요청하는 단계(S300)에서는, 사용 승인요청에 따라 기업 대표자가 승인하면 대표자 단말은 저장된 제2 개인DID를 DID 발행자 서버에 제출함과 아울러 법인DID의 발행을 승인한다.
- [0089] 여기서, 제2 개인DID는 전술한 제1 개인DID와 주체만 다를 뿐, 동일한 절차에 의해 발급될 수 있다.
- [0090] 다음으로, DID 발행자 서버가 대표자 단말로부터 사용 승인된 법인DID 발급 요청건에 대하여, 제1 및 제2 개인DID와 법인관련 데이터를 조합하여 법인DID를 발급하는 단계(S400)에서는, 전술한 단계들에 의해 신원증명된 제1 및 제2 개인DID와, 법인DID 사용목적 및 사용기간 등을 포함하는 정보와, 실제 법인인감에 대한 이미지 파일을 조합하고, 조합결과를 해싱하여 고유 인덱스를 생성한 후, 고유 인덱스를 DID 문서먼트에 포함하는 법인DID를 생성 및 블록체인 네트워크에 등록함으로써, 요청건에 대한 법인DID를 발급하게 된다.
- [0091] 다음으로, DID 발행자 서버가 발급된 법인DID를 블록체인 네트워크에 등록 및 담당자 단말에 배포하는 단계(S500)에서는, DID 발행자 서버가 S400 단계에서 발급된 법인DID를 발급 요청한 담당자 단말에 전송함으로 배포 절차를 수행하게 된다.

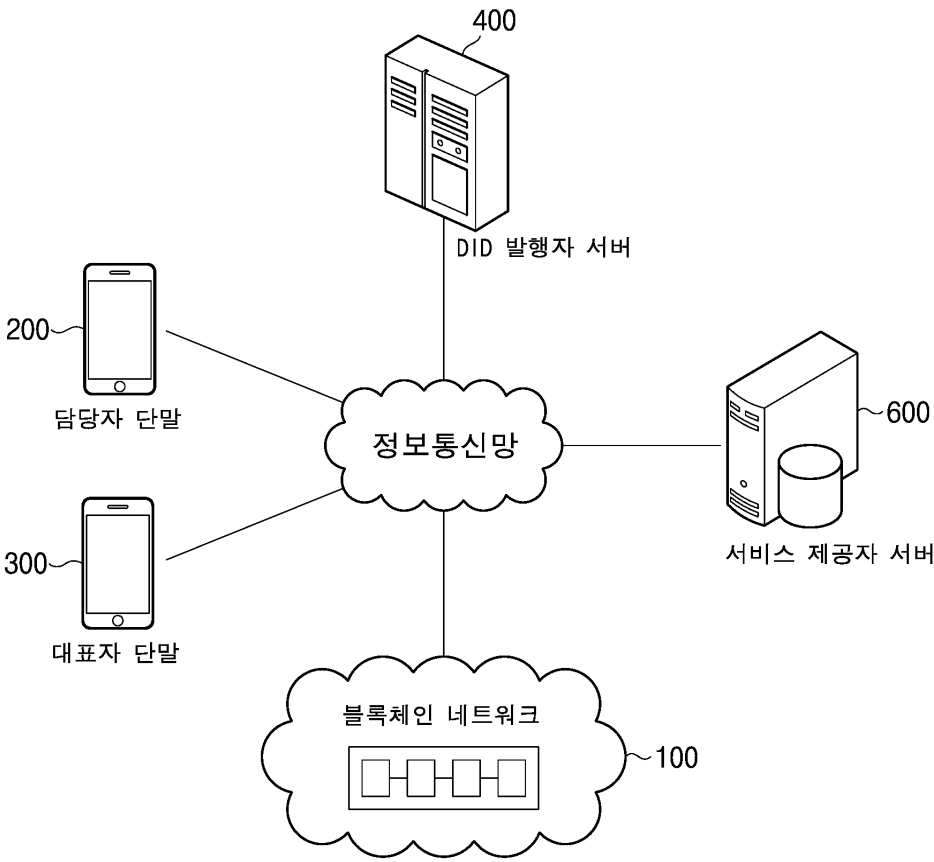
- [0092] 이후, 담당자 단말은 내부에 저장되는 법인DID를 이용하여 사용목적에 따라 법인인감을 대체하여 법인 계약과 같은 업무를 처리할 수 있다.
- [0093] 또한, S500 단계 이후, 법인DID 사용목적에 따라 서비스 제공자 서버에 제출되거나, 사용기간이 경과되면 DID 발행자 서버는 블록체인 네트워크의 법인DID의 DID 도큐먼트에 그 사용내역을 추가 기록하고, 법인DID를 폐기할 수 있다.
- [0094] 이하, 도면을 참조하여 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템에 적용된 DID 발급 절차의 예시를 통해 본 발명의 기술적 사상을 상세히 설명한다.
- [0095] 도 5는 본 발명의 실시예에 따른 블록체인 기반 법인DID 서비스 제공 시스템에 적용되는 개인DID 또는 법인DID 발급절차를 예시한 도면이다. 이하의 설명은 DID를 본 발명의 DID 발행자 서버에서 신원증명을 수행하는 방식을 예시한 것으로, DID발급 및 신원검증의 주체 및 구체적인 절차는 시스템이 도입한 DID 플랫폼에 따라 기업, 기관 서버 등에서 수행하는 방식으로 일부 변경될 수 있다.
- [0096] 특히, 본 발명의 시스템이 전제하고 있는 탈중앙화 신원증명 기술은 개인정보를 사용자의 단말기에 저장하여 개인정보 인증 시 필요한 정보만 골라서 제출하도록 해주는 전자신원 증명 기술이다. 이는 블록체인 네트워크를 활용하여 개인들이 자신의 데이터를 직접 관리함으로써 중앙화된 기관을 거치지 않고서도 신원 검증이 가능한 자기 주권형 신원인증(Self-Sovereign Identity)이 가능하도록 하는 특징이 있다.
- [0097] 도 5를 참조하면, 이러한 SSI에 기반하여 본 발명의 실시예에 따른 DID 발급절차에 의하면, 기업 담당자가 자신의 신원을 증명하는 개인DID를 이용하여 법인DID를 발급받겠다고 할 때, 담당자 단말(200)에 저장된 개인DID, 일례로서 'did:sov:abcdef' 형식의 DID 발행자 서버(400)에 제출할 수 있다(a).
- [0098] 이를 통해, DID 발행자 서버(400)는 블록체인 네트워크(100)에 등록된 'did:sov:abcdef'으로부터 DID 도큐먼트를 식별 및 획득할 수 있다(b). 아울러, DID 발행자 서버(400)는, 'did:sov:abcdef'에 대하여 자체적으로 운영하는 데이터 베이스를 참조하여 당해 기업에서 발급한 것인지 발급 내역을 확인한다(c).
- [0099] 이에 따라, 개인DID의 'abcdef'를 통해 보관중인 DID 발급내역에서 기록이 있음이 확인되면, 담당자 단말(200)로부터 개인키에 의해 생성된 인증값을 제공받고, DID 발행자 서버(400)는 해당 개인DID의 DID 도큐먼트로부터 추출한 공개키를 이용하여 인증값을 검증함으로써 담당자 단말(200)이 개인DID의 주인임을 확인하게 된다(d).
- [0100] 상기한 설명에 많은 사항이 구체적으로 기재되어 있으나 이것은 발명의 범위를 한정하는 것이라기보다 바람직한 실시예의 예시로서 해석되어야 한다. 따라서, 발명은 설명된 실시예에 의하여 정할 것이 아니고 특허청구범위와 특허청구범위에 균등한 것에 의하여 정하여져야 한다.

부호의 설명

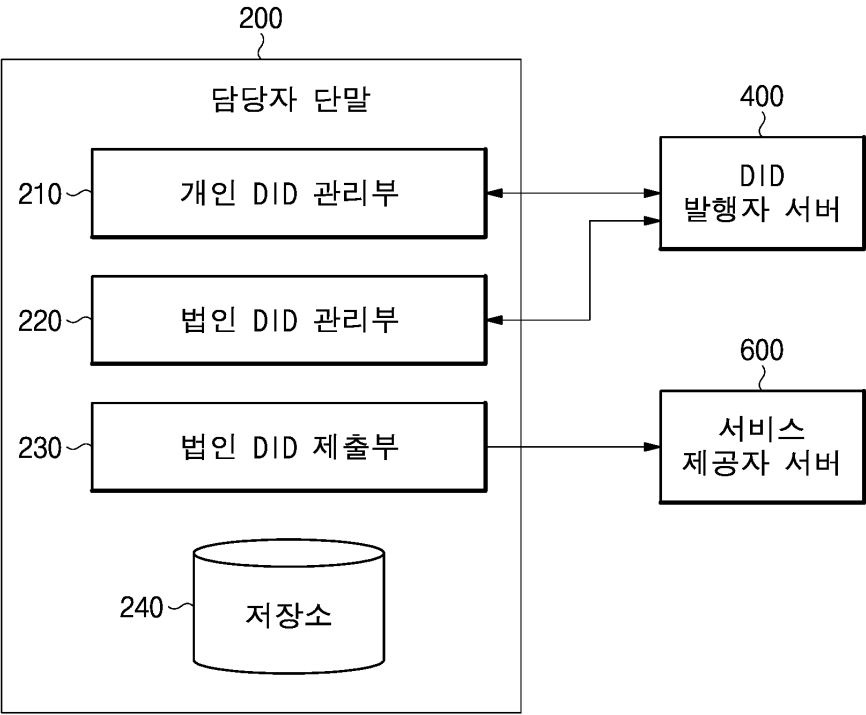
- [0101]
- | | |
|------------------|------------------|
| 100 : 블록체인 네트워크 | 200 : 담당자 단말 |
| 210 : 개인DID 관리부 | 220 : 법인DID 관리부 |
| 230 : 법인DID 제출부 | 240 : 저장소 |
| 300 : 대표자 단말 | 400 : DID 발행자 서버 |
| 410 : 발급 접속부 | 420 : 신원 검증부 |
| 430 : 승인 요청부 | 440 : DID 생성부 |
| 450 : DID 배포부 | 460 : DID 관리부 |
| 600 : 서비스 제공자 서버 | |

도면

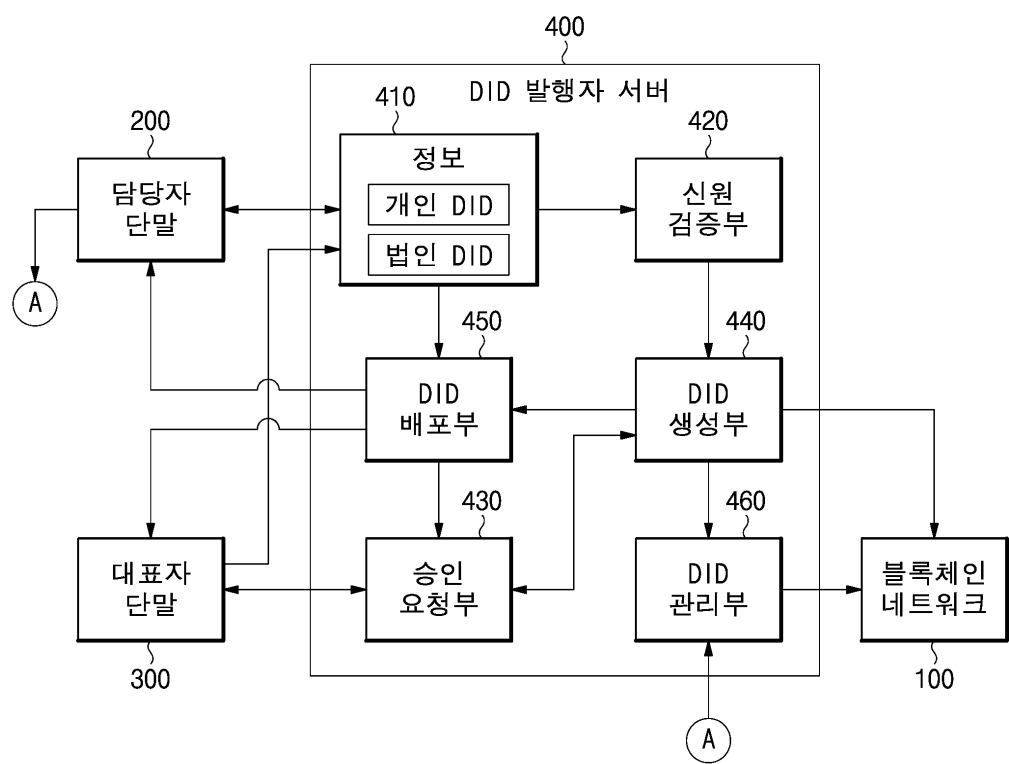
도면1



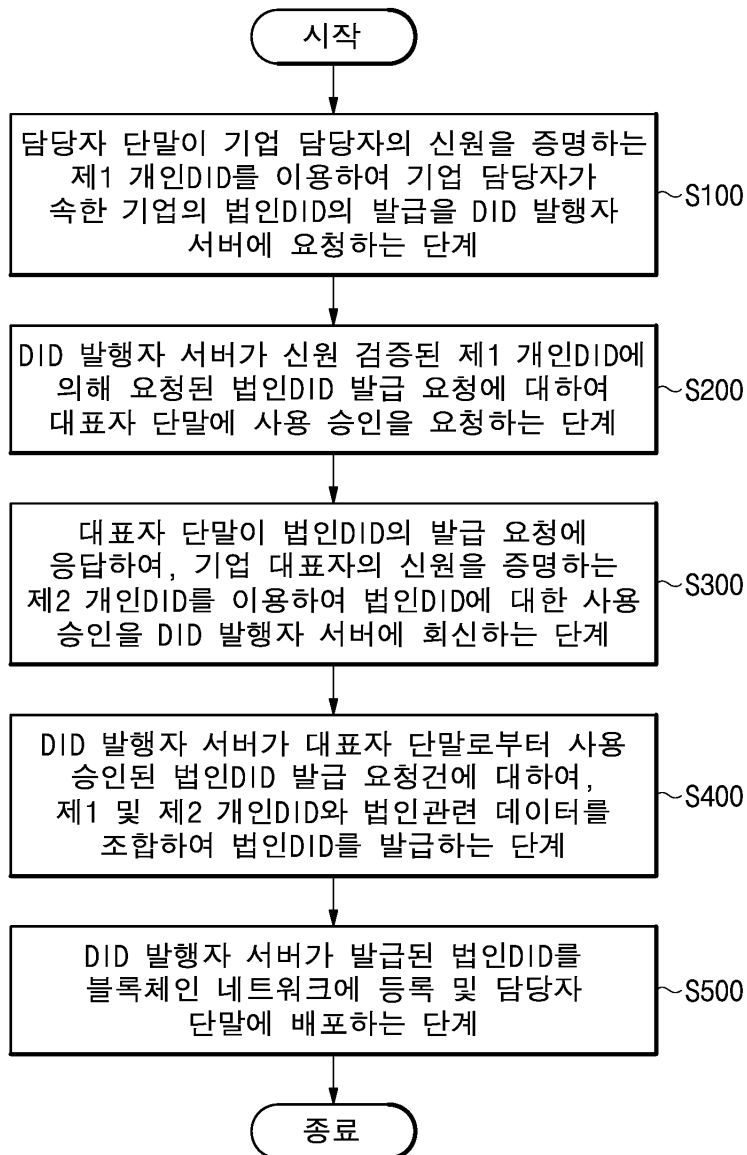
도면2



도면3



도면4



도면5

