(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0160286
(43) 공개일자 2022년12월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06F 21/62* (2013.01)
H04L 65/40 (2022.01)
(52) CPC특허분류
H04L 63/0815 (2013.01)
G06F 21/6218 (2013.01)
(21) 출원번호 10-2021-0068292
(22) 출원일자 2021년05월27일
심사청구일자 2021년05월27일

(71) 출원인
울산대학교 산학협력단
울산광역시 남구 대학로 93(무거동)
(72) 발명자
이명준
울산광역시 중구 평동3길 1, 108동 2001호(유곡동, 울산 유곡푸르지오)
권민호
울산광역시 중구 오산3길 51- 7(태화동)
(74) 대리인
특허법인 무한

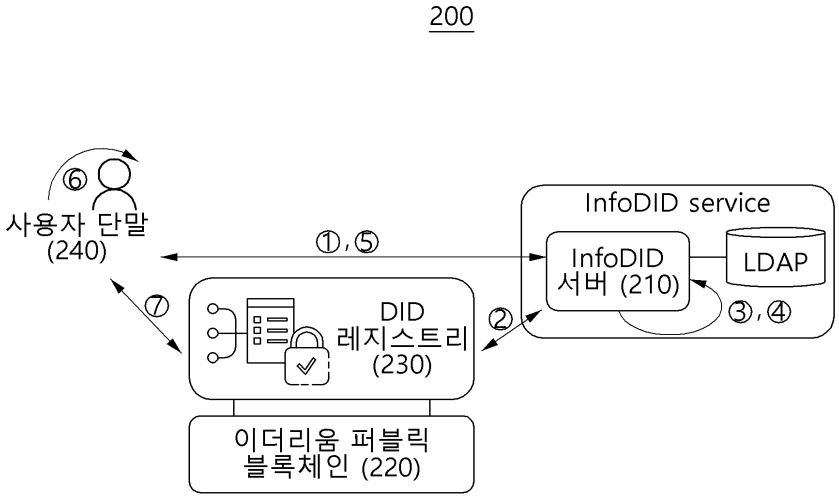
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **DID 기반의 사용자 정보 관리 서비스 제공 방법 및 시스템**

(57) 요 약

DID 기반의 사용자 정보 관리 서비스 제공 방법 및 시스템이 개시된다. 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 방법은, DID 기반의 사용자 정보 관리 서비스를 이용 중인 사용자 단말에서 타 서비스에 대한 이용 요청이 발생됨에 따라, 타 서비스와 연관된 서비스 서버로부터 입력되는 서비스 인증 정보를, 블록체인의 DID 레지스트리에서 로딩한 서비스 서버의 DID 문서를 이용해 검증하여 서비스 서버를 신원 인증하는 단계와, 서비스 서버가 신원 인증되면, 사용자 단말에 관한 사용자 인증 정보를, DID 레지스트리에서 로딩한 사용자 단말의 DID 문서를 이용해 검증하여 사용자 단말을 신원 인증하는 단계, 및 사용자 단말이 신원 인증되면, 스토리지에서 사용자 단말의 사용자 정보를 리드해 서비스 서버에 전달함으로써, 사용자 단말에서 상기 타 서비스를 이용하도록 하는 단계를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 63/0435 (2013.01)
H04L 67/567 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1345342988
과제번호	2019R1I1A3A01052970
부처명	교육부
과제관리(전문)기관명	한국연구재단
연구사업명	이공학학술연구기반구축(R&D)
연구과제명	블록체인 응용 서비스의 견고성 및 신속 재가동을 지원하는 블록체인 기반 서비스 관리 시스템 개발
기 여 율	100/100
과제수행기관명	울산대학교
연구기간	2021.03.01 ~ 2022.02.28

명 세 서

청구범위

청구항 1

DID 기반의 사용자 정보 관리 서비스를 이용 중인 사용자 단말에서, 타 서비스에 대한 이용 요청이 발생됨에 따라,

상기 타 서비스와 연관된 서비스 서버로부터 입력되는 서비스 인증 정보를, 블록체인의 DID 레지스트리에서 로딩한 상기 서비스 서버의 DID 문서를 이용해 검증하여, 상기 서비스 서버를 신원 인증하는 단계;

상기 서비스 서버가 신원 인증되면, 상기 사용자 단말에 관한 사용자 인증 정보를, 상기 DID 레지스트리에서 로딩한 상기 사용자 단말의 DID 문서를 이용해 검증하여, 상기 사용자 단말을 신원 인증하는 단계; 및

상기 사용자 단말이 신원 인증되면, 스토리지에서 상기 사용자 단말의 사용자 정보를 리드해 상기 서비스 서버에 전달함으로써, 상기 사용자 단말에서 상기 타 서비스를 이용하도록 하는 단계

를 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 2

제1항에 있어서,

상기 서비스 인증 정보는,

상기 사용자 인증 정보를 상기 서비스 서버의 비밀키로 암호화한 시그니처값 및 상기 서비스 서버의 DID를 포함하고,

상기 서비스 서버를 신원 인증하는 단계는,

상기 서비스 서버의 DID를 이용하여, 상기 DID 레지스트리에 기록된 상기 서비스 서버의 DID 문서를 로딩하는 단계;

로딩한 상기 서비스 서버의 DID 문서에 기재된 공개키아이디로부터 상기 서비스 서버의 비밀키에 대칭되는 공개키를 생성하는 단계; 및

생성한 상기 서비스 서버의 공개키로 상기 서비스 인증 정보 내 시그니처값을 복호화하는 단계

를 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 3

제2항에 있어서,

상기 복호화된 시그니처값으로부터 상기 사용자 인증 정보가 추출되면,

상기 사용자 단말을 신원 인증하는 단계는,

상기 사용자 인증 정보에 포함된 상기 사용자 단말의 DID를 이용하여, 상기 DID 레지스트리에 기록된 상기 사용자 단말의 DID 문서를 로딩하는 단계;

로딩한 상기 사용자 단말의 DID 문서에 기재된 공개키아이디로부터 상기 사용자 단말의 비밀키에 대칭되는 공개키를 생성하는 단계; 및

생성한 상기 사용자 단말의 공개키로 상기 사용자 인증 정보에 포함된 상기 사용자 단말의 시그니처값을 복호화하는 단계

를 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 4

제1항에 있어서,

상기 사용자 단말에서 정보 저장 요청이 발생됨에 따라,

상기 사용자 단말로부터 입력되는 제1 사용자 인증 정보를, 상기 DID 레지스트리에서 로딩한 상기 사용자 단말의 DID 문서를 이용해 검증하여, 상기 사용자 단말을 신원 인증하는 단계;

상기 사용자 단말이 신원 인증되면, 상기 제1 사용자 인증 정보로부터 상기 정보 저장 요청과 관련한 사용자 정보를, 추출하는 단계; 및

추출된 사용자 정보를 암호화하여, 상기 제1 사용자 인증 정보와 연관시켜 상기 스토리지에 저장함으로써, 상기 사용자 정보의 저장 서비스를 제공하는 단계

를 더 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 5

제4항에 있어서,

상기 사용자 정보의 저장 후에, 저장 완료를 알리는 관리증명서를 상기 사용자 단말에 발급하고, 상기 스토리지에 보관하는 단계

를 더 포함하고,

상기 사용자 단말은,

발급받은 상기 관리증명서가 포함되도록, 상기 DID 레지스트리에 기록된 상기 사용자 단말의 DID 문서를 갱신하는

DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 6

제5항에 있어서,

상기 사용자 단말의 DID 문서에 대한 갱신에 따라,

상기 DID 레지스트리에서 상기 사용자 단말에 의해 갱신된 DID 문서를 로딩하는 단계;

로딩한 상기 DID 문서에 포함되는 관리증명서가, 상기 사용자 정보의 저장 후에 상기 스토리지에 보관한 관리증명서와 일치하는지 비교하는 단계; 및

일치하는 경우, 상기 스토리지에 저장된 사용자 정보를 '변경없음'으로 확인하여, 상기 서비스 서버에 전달하는 단계

를 더 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 7

제5항에 있어서,

상기 사용자 단말의 DID 문서에 대한 갱신에 따라,

상기 서비스 서버에서, 상기 전달된 사용자 정보를 상기 서비스 서버에 마련된 데이터베이스에 저장 시, 상기 DID 레지스트리에서 상기 사용자 단말에 의해 갱신된 DID 문서를 로딩하고, 로딩한 상기 DID 문서에 포함된 관리증명서를 상기 데이터베이스에 함께 저장하는 단계;

상기 서비스 서버에서, 일정 주기로 상기 DID 레지스트리에서 재로딩한 상기 사용자 단말의 DID 문서에 포함되는 관리증명서가, 상기 데이터베이스에 저장한 관리증명서와 일치하는지 비교하는 단계; 및

일치하지 않을 경우,

상기 서비스 서버에서, 상기 데이터베이스에 저장한 사용자 정보에 대해 갱신 조건이 성립하는 것으로 판단하고, 상기 사용자 단말에 관한 사용자 정보의 전달 서비스 요청을, 상기 서비스 인증 정보를 포함하여 발생하는 단계

를 더 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 8

제7항에 있어서,

상기 서비스 서버로 상기 사용자 정보를 전달한 후에, 상기 서비스 서버로의 사용자 정보의 전달 기록을 상기 스토리지에 생성하는 단계;

상기 갱신 조건의 성립에 따라, 상기 서비스 서버에서 상기 사용자 정보의 전달 서비스 요청이 발생하면,

상기 전달 서비스 요청을 발생한 서비스 서버에 대해, 상기 전달 기록이 상기 스토리지에 생성되어 있는지 확인하는 단계; 및

상기 전달 기록이 생성되어 있으면, 상기 스토리지에서 상기 사용자 단말에 관한 업데이트된 사용자 정보를 리드해 상기 서비스 서버에 전달하는 단계

를 더 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 방법.

청구항 9

DID 기반의 사용자 정보 관리 서비스를 이용 중인 사용자 단말에서, 타 서비스에 대한 이용 요청이 발생됨에 따라,

상기 타 서비스와 연관된 서비스 서버로부터 입력되는 서비스 인증 정보를, 블록체인의 DID 레지스트리에서 로딩한 상기 서비스 서버의 DID 문서를 이용해 검증하여, 상기 서비스 서버를 신원 인증하는 서버 인증부;

상기 서비스 서버가 신원 인증되면, 상기 사용자 단말에 관한 사용자 인증 정보를, 상기 DID 레지스트리에서 로딩한 상기 사용자 단말의 DID 문서를 이용해 검증하여, 상기 사용자 단말을 신원 인증하는 사용자 인증부; 및

상기 사용자 단말이 신원 인증되면, 스토리지에서 상기 사용자 단말의 사용자 정보를 리드해 상기 서비스 서버에 전달함으로써, 상기 사용자 단말에서 상기 타 서비스를 이용하도록 하는 전달 처리부

를 포함하는 DID 기반의 사용자 정보 관리 서비스 제공 시스템.

청구항 10

제9항에 있어서,

상기 서비스 인증 정보는,

상기 사용자 인증 정보를 상기 서비스 서버의 비밀키로 암호화한 시그니처값 및 상기 서비스 서버의 DID를 포함하고,

상기 서버 인증부는,

상기 서비스 서버의 DID를 이용하여, 상기 DID 레지스트리에 기록된 상기 서비스 서버의 DID 문서를 로딩하고,

로딩한 상기 서비스 서버의 DID 문서에 기재된 공개키아이디로부터 상기 서비스 서버의 비밀키에 대칭되는 공개키를 생성하고,

생성한 상기 서비스 서버의 공개키로 상기 서비스 인증 정보 내 시그니처값을 복호화하는

DID 기반의 사용자 정보 관리 서비스 제공 시스템.

청구항 11

제10항에 있어서,

상기 복호화된 시그니처값으로부터 상기 사용자 인증 정보를 추출하는 추출부

를 더 포함하고,

상기 사용자 인증부는,

상기 사용자 인증 정보에 포함된 상기 사용자 단말의 DID를 이용하여, 상기 DID 레지스트리에 기록된 상기 사용

자 단말의 DID 문서를 로딩하고,

로딩한 상기 사용자 단말의 DID 문서에 기재된 공개키아이디로부터 상기 사용자 단말의 비밀키에 대칭되는 공개키를 생성하고,

생성한 상기 사용자 단말의 공개키로 상기 사용자 인증 정보에 포함된 상기 사용자 단말의 시그니처값을 복호화하는

DID 기반의 사용자 정보 관리 서비스 제공 시스템.

청구항 12

제9항에 있어서,

상기 사용자 단말에서 정보 저장 요청이 발생됨에 따라, 상기 사용자 정보의 저장 서비스를 제공하는 저장 처리부

를 더 포함하고,

상기 사용자 인증부는,

상기 사용자 단말로부터 입력되는 제1 사용자 인증 정보를, 상기 DID 레지스트리에서 로딩한 상기 사용자 단말의 DID 문서를 이용해 검증하여, 상기 사용자 단말을 신원 인증하고,

상기 사용자 단말이 신원 인증되면,

상기 저장 처리부는,

추출부에 의해, 상기 제1 사용자 인증 정보에 포함된 상기 사용자 단말에서 저장하려는 사용자 정보를, 상기 제1 사용자 인증 정보로부터 추출하고,

추출된 사용자 정보를 암호화하여, 상기 제1 사용자 인증 정보와 연관시켜 상기 스토리지에 저장하는

DID 기반의 사용자 정보 관리 서비스 제공 시스템.

청구항 13

제12항에 있어서,

상기 저장 처리부는,

상기 사용자 정보의 저장 후에, 저장 완료를 알리는 관리증명서를 상기 사용자 단말에 발급하고, 상기 스토리지에 보관하고,

상기 사용자 단말은,

발급받은 상기 관리증명서가 포함되도록, 상기 DID 레지스트리에 기록된 상기 사용자 단말의 DID 문서를 갱신하는

DID 기반의 사용자 정보 관리 서비스 제공 시스템.

청구항 14

제13항에 있어서,

상기 사용자 단말의 DID 문서에 대한 갱신에 따라,

상기 전달 처리부는,

상기 DID 레지스트리에서 상기 사용자 단말에 의해 갱신된 DID 문서를 로딩하고,

로딩한 상기 DID 문서에 포함되는 관리증명서가, 상기 사용자 정보의 저장 후에 상기 스토리지에 보관한 관리증명서와 일치하는지 비교하고,

일치하는 경우, 상기 스토리지에 저장된 사용자 정보를 '변경없음'으로 확인하여, 상기 서비스 서버에 전달하는

DID 기반의 사용자 정보 관리 서비스 제공 시스템.

청구항 15

제13항에 있어서,

상기 사용자 단말의 DID 문서에 대한 갱신에 따라,

상기 서비스 서버는,

상기 전달된 사용자 정보를 상기 서비스 서버에 마련된 데이터베이스에 저장 시, 상기 DID 레지스트리에서 상기 사용자 단말에 의해 갱신된 DID 문서를 로딩하고, 로딩한 상기 DID 문서에 포함된 관리증명서를 상기 데이터베이스에 함께 저장하고,

일정 주기로 상기 DID 레지스트리에서 재로딩한 상기 사용자 단말의 DID 문서에 포함되는 관리증명서가, 상기 데이터베이스에 저장한 관리증명서와 일치하는지 비교하고,

일치하지 않을 경우, 상기 데이터베이스에 저장한 사용자 정보에 대해 갱신 조건이 성립하는 것으로 판단하고, 상기 사용자 단말에 관한 사용자 정보의 전달 서비스 요청을, 상기 서비스 인증 정보를 포함하여 발생하는

DID 기반의 사용자 정보 관리 서비스 제공 시스템.

청구항 16

제15항에 있어서,

상기 전달 처리부는,

상기 서비스 서버로 상기 사용자 정보를 전달한 후에, 상기 서비스 서버로의 사용자 정보의 전달 기록을 상기 스토리지에 생성하고,

상기 갱신 조건의 성립에 따라, 상기 서비스 서버에서 상기 사용자 정보의 전달 서비스 요청이 발생하면,

상기 전달 서비스 요청을 발생한 서비스 서버에 대해, 상기 전달 기록이 상기 스토리지에 생성되어 있는지 확인하고,

상기 전달 기록이 생성되어 있으면, 상기 스토리지에서 상기 사용자 단말에 관한 업데이트된 사용자 정보를 리드해 상기 서비스 서버에 전달하는

DID 기반의 사용자 정보 관리 서비스 제공 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 사용자의 정보를 신뢰성 있게 저장, 업데이트, 타 서비스로 제공하는 DID 기반의 견고한 사용자 정보 관리 서비스(InfoDID)의 제공에 연관된다.

배 경 기 술

[0002] 일반적으로, 사용자는 디지털 기반의 서비스를 이용하기 위해 각 서비스에 자신의 정보를 제공하고 서비스 계정을 만드는 개별 가입 방식으로 신원을 인증하게 된다. 이 같은 방식은 사용자가 새로운 서비스를 사용할 때마다 자신의 개인 정보를 서비스에 일일이 제공해 회원가입을 해야 하는 번거로움이 있다.

[0003] 또한, 각 서비스 마다 서비스 계정을 만들지 않고, OpenID, OAuth 등의 기반 기술을 이용해 구글이나 페이스북의 기존 서비스 계정으로 신원을 인증하는 연합 신원 인증 방식도 널리 사용되고 있으나, 이 방식에서는 사용자의 정보가 어느 수준까지 제공되는지 사용자가 알기 어렵고, 신원 증명 제공자의 서비스가 중지될 경우 신원 인증이 불가능하게 된다.

[0004] 최근에는 무결성, 탈중앙화, 높은 보안성 등의 특징을 가진 블록체인 기술을 이용한 DID(Decentralized IDentifiers, 분산식별자) 기술이 차세대 신원 인증 기술로 등장함에 따라, 이러한 DID 기술을 이용한 다양한 블록체인 응용서비스가 개발, 이용되고 있다.

[0005] DID 기술을 활용하는 블록체인 관련 선행기술로는, 분산 ID를 발급받아 블록체인 데이터로 저장하고, 신원 증명 요청이 수신되면 저장된 블록체인 데이터를 조회하여 신원 인증을 수행하는 구성을 개시하는 한국 등록번호 10-2139645와, 블록체인 네트워크 사용자들이 자신의 프라이빗 키를 효과적으로 관리, 백업, 복원할 수 있게 지원하는 한국 공개번호 10-2021-0020851, 및 블록체인 네트워크로부터 발급받은 DID를 통해 본인 인증하는 구성을 개시하는 한국 등록번호 10-2201679 등에 블록체인 기반의 DID를 활용하여 사용자 정보를 관리하는 기술이 개시되고 있다.

[0006] 하지만, 블록체인 기반의 DID을 활용해 사용자의 개인 정보를 신뢰성 있게 제어하여 사용자가 이용하려는 여러 다른 서비스에 꼭 필요한 사용자의 정보만을 제공하고, 사용자의 각종 서비스 이용을 위한 편리하고 안정적인 신원 인증을 지원하는 기술은 아직까지 부재하다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예는 블록체인 기반의 DID 기술을 이용한 신원 인증을 통해 사용자 정보를 신뢰성 있게 저장 및 업데이트하고 사용자가 이용하려는 타 서비스로 사용자 정보를 신뢰성 있게 제공하는 견고한 사용자 정보 관리 서비스(InfoDID)를 구현함으로써, 사용자의 각종 서비스 이용의 편의성을 향상시키는 것을 목적으로 한다.

[0008] 본 발명의 실시예는 타 서비스로의 사용자 정보 제공 이후 업데이트되는 사용자 정보의 지속적인 제공을 통해 최신의 사용자 정보 제공을 구현함으로써, 사용자 정보 수정으로 인한 불편함을 해소하고, 사용자의 각종 서비스 이용 편의성을 보다 향상시키는 것을 목적으로 한다.

과제의 해결 수단

[0009] 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 방법은, DID 기반의 사용자 정보 관리 서비스를 이용 중인 사용자 단말에서 타 서비스에 대한 이용 요청이 발생됨에 따라, 타 서비스와 연관된 서비스 서버로부터 입력되는 서비스 인증 정보를, 블록체인의 DID 레지스트리에서 로딩한 서비스 서버의 DID 문서를 이용해 검증하여 서비스 서버를 신원 인증하는 단계와, 서비스 서버가 신원 인증되면, 사용자 단말에 관한 사용자 인증 정보를, DID 레지스트리에서 로딩한 사용자 단말의 DID 문서를 이용해 검증하여 사용자 단말을 신원 인증하는 단계, 및 사용자 단말이 신원 인증되면, 스토리지에서 사용자 단말의 사용자 정보를 리드해 서비스 서버에 전달함으로써, 사용자 단말에서 상기 타 서비스를 이용하도록 하는 단계를 포함할 수 있다.

[0010] 또한, 본 발명의 실시예에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템은, DID 기반의 사용자 정보 관리 서비스를 이용 중인 사용자 단말에서 타 서비스에 대한 이용 요청이 발생됨에 따라, 타 서비스와 연관된 서비스 서버로부터 입력되는 서비스 인증 정보를, 블록체인의 DID 레지스트리에서 로딩한 서비스 서버의 DID 문서를 이용해 검증하여 서비스 서버를 신원 인증하는 서버 인증부와, 서비스 서버가 신원 인증되면, 사용자 단말에 관한 사용자 인증 정보를, DID 레지스트리에서 로딩한 사용자 단말의 DID 문서를 이용해 검증하여 사용자 단말을 신원 인증하는 사용자 인증부, 및 사용자 단말이 신원 인증되면, 스토리지에서 사용자 단말의 사용자 정보를 리드해 서비스 서버에 전달함으로써, 사용자 단말에서 상기 타 서비스를 이용하도록 하는 전달 처리부를 포함할 수 있다.

발명의 효과

[0011] 본 발명에 따르면, 블록체인 기반의 DID 기술을 이용한 신원 인증을 통해 사용자 정보를 신뢰성 있게 관리(저장/업데이트)하는 한편, 사용자가 이용하고자 하는 서비스를 제공하는 서비스 서버로 사용자 정보를 신뢰성 있게 제공해 사용자의 각종 서비스의 편리한 이용을 지원하고, 이후에도 최신의 사용자 정보를 지속적으로 제공하는 사용자 정보 관리 서비스(InfoDID)를 구현할 수 있다.

[0012] 본 발명에 따르면, 이더리움 블록체인의 스마트 컨트랙트로 개발된 DID 레지스트리를 DID 신원 인증 서비스에 활용해 사용자의 개인 정보를 신뢰성 있게 제어하여, 사용자가 이용하려는 여러 다른 서비스에 꼭 필요한 사용자의 정보만을 제공하고, 기존의 신원 증명 제공자의 서비스 중지의 우려 없이 안정적인 신원 인증을 바탕으로 사용자의 각종 서비스 이용을 지원할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템의 구성을 도시한 블록도이다.

도 2는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템을 포함한 네트워크를 도시한 도면이다.

도 3은 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 확장된 DID 레지스트리에 기록되는 DID 문서를 도시한 도면이다.

도 4a 및 도 4b는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 사용자 단말의 DID 문서를 이용한 신원 인증 절차를 도시한 도면이다.

도 5a는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 사용자 정보의 전달 서비스 제공 과정을 설명하기 위한 도면이다.

도 5b는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 최신의 사용자 정보를 제공하기 위한 과정을 설명하기 위한 도면이다.

도 6a 및 도 6b는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 방법의 순서를 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 그러나, 실시예들에는 다양한 변경이 가해질 수 있어서 특허출원의 권리 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 실시예들에 대한 모든 변경, 균등물 내지 대체물이 권리 범위에 포함되는 것으로 이해되어야 한다.

[0015] 실시예에서 사용한 용어는 단지 설명을 목적으로 사용된 것으로, 한정하려는 의도로 해석되어서는 안된다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 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.

[0016] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 실시예가 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.

[0017] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0018] 본 발명에 따른 사용자 정보 관리 서비스 제공 시스템은, 블록체인의 DID 기술을 이용하여 사용자 정보를 신뢰성 있게 저장 및 업데이트하고, 타 서비스로 제공하는 견고한 사용자 정보 관리 서비스(InfoDID)를 제안한다.

[0019] 여기서 DID는, 중앙화된 신원 제공자, 레지스트리, 인증 기관 등으로부터 탈피해 독립적으로 검증하는 분산 디지털 신원 인증에 사용되는 분산 식별자로서, DID를 가진 주체는 해당 주체를 설명할 수 있는 DID 문서를 통해 자신의 정보에 대한 제어권을 가지게 된다. DID를 가진 주체는, 블록체인 기반의 DID 레지스트리에 저장된 DID 문서를 이용한 DID 인증(DID auth)에 의해 블록체인 상에서 언제나 식별될 수 있다.

[0020] 본 발명에 따른 사용자 정보 관리 서비스 제공 시스템은, DID 기반의 블록체인 응용 서비스의 형태로 사용자 정보 관리 서비스(InfoDID)를 실행하여 사용자 정보의 저장, 업데이트를 관리하고, DID 인증 기법을 이용하여 사용자가 이용하려는 다른 서비스에 사용자 정보를 손쉽게 전달할 수 있다.

[0021] 또한, 본 발명에 따른 사용자 정보 관리 서비스 제공 시스템은, 이더리움 블록체인(Ethereum Blockchain)에서 관리하는 확장된 형태의 DID 레지스트리를 이용해, 사용자 정보를 저장(업데이트)하려는 사용자 단말의 신원 인증에 필요한 DID 문서를 관리함으로써, 사용자 정보가 사용자의 승인 없이 임의로 변경되어 사용되지 못하도록 방지할 수 있다.

[0022] 여기서, 이더리움 블록체인은 전자 계약인 스마트 컨트랙트 기능을 제공하며 탈중앙 블록체인 애플리케이션을 개발하고 운영할 수 있는 블록체인 플랫폼으로서, 이더리움 블록체인에서는 스마트 컨트랙트 기반으로 간단한

거래뿐만 아니라 사용자가 원하는 복잡한 계약을 수행할 수 있다. 이더리움 블록체인 네트워크에 연결된 모든 노드는, 스마트 컨트랙트를 실행시키는 이더리움 가상머신을 통해 모든 트랜잭션을 실행하여, 모든 노드는 동일한 계산을 수행하고 같은 상태를 가진다. 여기서, 스마트 컨트랙트란 기존 대면 방식의 계약에서 벗어나 블록체인에서 특정 조건에 따라 계약을 자동으로 수행하는 스마트 계약 기능이다.

[0023] 도 1은 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템의 구성을 도시한 블록도이다.

[0024] 도 2를 참조하면, 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템(100)은, 서버 인증부(110), 추출부(120), 사용자 인증부(130) 및 전달 처리부(140)를 포함하여 구성할 수 있다. 실시예에 따라, 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템(100)은, 저장 처리부(150) 및 스토리지(160)를 각각 추가하여 구성할 수 있다.

[0025] 서버 인증부(110)는 DID 기반의 사용자 정보 관리 서비스(infoDID)를 이용 중인 사용자 단말(101)에서, 타 서비스에 대한 이용 요청이 발생됨에 따라, 상기 타 서비스와 연관된 서비스 서버(102)로부터 입력되는 서비스 인증 정보를, 블록체인(170)의 DID 레지스트리(171)에서 로딩한 서비스 서버(102)의 DID 문서를 이용해 검증하여, 서비스 서버(102)를 신원 인증하는 기능을 한다.

[0026] 일례로, 상기 타 서비스의 이용하려는 사용자 단말(101)에서는, 자신의 사용자 인증 정보를 상기 타 서비스를 제공하는 서비스 서버(102)로 입력할 수 있다. 그러면 서비스 서버(102)에서는 상기 사용자 인증 정보를 입력한 사용자 단말(101)에 관한 사용자 정보를 획득하기 위해, 자신의 서비스 인증 정보를 포함하여 상기 사용자 정보의 전달 요청을 발생할 수 있다.

[0027] 여기서, 상기 서비스 인증 정보는, 사용자 단말(101)이 입력한 사용자 인증 정보를 서비스 서버(102)의 비밀키로 암호화한 시그니처값 및 서비스 서버(102)의 DID를 포함할 수 있다.

[0028] 즉, 상기 타 서비스에 대한 이용 요청을 발생하는 사용자 단말에서, 상기 타 서비스의 서비스 서버(102)로 상기 사용자 인증 정보를 입력함에 따라, 서비스 서버(102)로부터, 상기 사용자 인증 정보를 서비스 서버(102)의 비밀키로 암호화한 시그니처값 및 서비스 서버(102)의 DID를 포함한 상기 서비스 인증 정보가 입력되면, 서버 인증부(110)는 상기 서비스 인증 정보 내 서비스 서버(102)의 DID를 이용하여, DID 레지스트리(171)에 기록된 서비스 서버(102)의 DID 문서를 로딩하고, 로딩한 서비스 서버(102)의 DID 문서에 기재된 공개키아이디로부터 서비스 서버(102)의 비밀키에 대칭되는 공개키를 생성하고, 상기 공개키로 상기 서비스 인증 정보 내 시그니처값을 복호화하여, 상기 시그니처값의 유효성을 검증함으로써, 서비스 서버(102)를 신원 인증할 수 있다.

[0029] 추출부(120)는 서비스 서버(102)가 신원 인증되면, 상기 서비스 인증 정보에 포함된 사용자 단말(101)에 관한 사용자 인증 정보를, 상기 서비스 인증 정보로부터 추출하는 기능을 한다.

[0030] 일례로, 추출부(120)는 상기 공개키로 상기 서비스 인증 정보 내 시그니처값의 복호화되어 시그니처값의 유효성이 검증되면, 상기 복호화된 시그니처값으로부터 상기 사용자 인증 정보를 추출할 수 있다.

[0031] 사용자 인증부(130)는, 추출된 사용자 인증 정보를, DID 레지스트리(171)에서 로딩한 사용자 단말(101)의 DID 문서를 이용해 검증하여, 사용자 단말(101)을 신원 인증하는 기능을 한다.

[0032] 일례로, 사용자 인증부(130)는, 상기 사용자 인증 정보에 포함된 사용자 단말(101)의 DID를 이용하여, DID 레지스트리(171)에 기록된 사용자 단말(101)의 DID 문서를 로딩하고, 상기 사용자 인증 정보에 포함된 사용자 단말(101)의 시그니처값을, 사용자 단말(101)의 DID 문서에 기재된 공개키아이디로부터 생성한 공개키로 복호화하여 상기 시그니처값의 유효성을 검증함으로써, 사용자 단말(101)을 신원 인증할 수 있다.

[0033] 전달 처리부(140)는 사용자 단말(101)이 신원 인증되면, 스토리지(160)에 기저장된 사용자 단말(101)에 관한 사용자 정보를, 스토리지(160)에서 리드해 서비스 서버(102)에 전달함으로써, 상기 사용자 정보의 신뢰성 있는 전달 서비스를 제공하는 기능을 한다. 전달 처리부(140)는 서비스 서버(102)로 상기 사용자 정보를 전달한 후에, 서비스 서버(102)로의 사용자 정보의 전달 기록을 스토리지(160)에 생성할 수 있다.

[0034] 상기 사용자 정보의 전달 서비스의 구현에 앞서, 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템(100)은, 상기 사용자 정보의 저장(업데이트) 서비스 구현을 위한 저장 처리부(150)를 더 포함하여 구성할 수 있다.

[0035] 저장 처리부(150)는 상기 타 서비스에 대한 이용 요청의 발생 전/후에, 정보 저장 요청을 발생하는 사용자 단말로부터 입력되는 사용자 정보를 저장하거나 기저장된 사용 정보를 업데이트함으로써, 사용자 정보의 신뢰성 있

는 저장 서비스를 제공하는 기능을 한다.

[0036] 구체적으로, 사용자 인증부(130)는 상기 저장 요청을 발생하는 사용자 단말로부터 입력되는 제1 사용자 인증 정보를, DID 레지스트리(171)에서 로딩한 사용자 단말(101)의 DID 문서를 이용해 검증하여, 사용자 단말(101)을 신원 인증하고, 추출부(120)는 사용자 단말(101)이 신원 인증되면, 상기 제1 사용자 인증 정보에 포함된 사용자 단말(101)에서 저장하려는 사용자 정보를, 상기 제1 사용자 인증 정보로부터 추출하고, 저장 처리부(150)는 추출된 사용자 정보를 암호화하여, 상기 제1 사용자 인증 정보와 연관시켜 스토리지(160)에 저장할 수 있다.

[0037] 여기서, 스토리지(160)는 대용량의 사용자 정보를 저장 가능한 LDAP(Lightweight Directory Access Protocol) 기반의 데이터베이스로 구현될 수 있다.

[0038] 즉, 저장 처리부(150)는 블록체인(170)의 저장 용량 한계와 비용 증가로 인해 블록체인(170)에 대용량의 사용자 정보를 모두 저장하기 어렵다는 점을 고려하여, 사용자 정보 관리 서비스 제공 시스템(100)의 내부 혹은 외부에 구현된 스토리지(160)를 활용해 사용자 정보를 저장, 유지할 수 있다.

[0039] 상기 사용자 정보는, 사용자의 식별자인 DID, 사용자 정보 관리 시작 시간, 사용자 정보의 마지막 업데이트 시간, 사용자 정보의 유효기간, 사용자의 성과 이름, 프로필 사진, 학력 목록, 경력 중 적어도 하나의 데이터일 수 있다.

[0040] 저장 처리부(150)는 상기 사용자 정보의 저장 후에, 저장 완료를 알리는 관리증명서를 사용자 단말(101)에 발급하고, 사용자 단말(101)에 발급한 관리증명서를, 스토리지(160)에 보관할 수 있다.

[0041] 이때, 사용자 단말(101)은, 발급받은 관리보증서의 시그니처값을 검증해서 자신의 사용자 정보가 위변조되지 않고 스토리지(160)에 저장되었음을 확인할 수 있고, 그 후, 발급받은 관리증명서를 DID 레지스트리(171)에 기록된 DID 문서에 보관할 수 있다. 사용자 단말(101)은 발급받은 관리증명서가 포함되도록, DID 레지스트리(171)에 기록된 사용자 단말(101)의 DID 문서를 갱신할 수 있다.

[0042] 즉 사용자 단말(101)은 자신의 사용자 정보를 저장(업데이트)할 때 마다 발급받은 관리증명서를 DID 레지스트리(171)에 기록된 DID 문서에 보관하여 DID 문서를 반복적으로 갱신할 수 있다. 본 발명에서 DID 문서는 종래보다 개인항목(Privacy)이 추가되어 확장된 형태를 이루고, 관리증명서는 DID 문서의 개인항목에 보관될 수 있다.

[0043] 전달 처리부(140)는 사용자 단말(101)에 관한 사용자 정보를 서비스 서버(102)로 전달하기에 앞서, 스토리지(160)에 저장된 사용자 정보의 사용자 단말의 승인 없는 비정상적인 변경이 있는지 확인하는 절차를 가짐으로써, 잘못된 사용자 정보가 타 서비스로 제공되는 것을 사전에 방지할 수 있다.

[0044] 구체적으로, 전달 처리부(140)는 스토리지(160)에서 리드한 사용자 단말(101)에 관한 사용자 정보를 서비스 서버(102)로 전달하기 전에, DID 레지스트리(171)에 기록된 사용자 단말의 DID 문서를 로딩할 수 있다. 이때 로딩되는 DID 문서는, 사용자 단말이 가장 최근에 발급받은 관리증명서를 포함하여 갱신된 DID 문서일 수 있다.

[0045] 전달 처리부(140)는 로딩한 DID 문서에 포함되는 관리증명서가, 저장 처리부(150)에서 상기 사용자 정보의 저장 후에 스토리지(160)에 보관한 관리증명서와 일치하는지 비교할 수 있다. 이때, 스토리지(160)에 보관한 관리증명서가 여러 개인 경우, 전달 처리부(140)는 가장 최근에 발급되어 보관된 관리증명서를, 로딩한 DID 문서 내 관리증명서와 비교할 수 있다.

[0046] 양 관리증명서가 일치하는 경우, 전달 처리부(140)는 스토리지(160)에 저장된 사용자 정보를 '변경없음'으로 확인하여, 서비스 서버(102)에 전달할 수 있다.

[0047] 만일, 양 관리증명서가 일치하지 않으면, 전달 처리부(140)는 스토리지(160)에 저장된 사용자 정보에, 사용자 단말의 승인 없는 비정상적인 변경이 발생한 것으로 확인하고, 저장 처리부(150)를 통해 서비스 서버(102)로 전달할 사용자 정보의 저장(업데이트)을 먼저 수행할 수 있다.

[0048] 전달 처리부(140)에 의해 스토리지(160)에 저장된 사용자 정보가 서비스 서버(102)로 전달되면, 서비스 서버(102)는, 전달된 사용자 정보를 이용해 사용자 단말이 이용 요청한 타 서비스를 사용자 단말이 이용하도록 할 수 있다.

[0049] 이때 서비스 서버(102)는, 전달 처리부(140)에 의해 전달된 사용자 정보를 이용해 사용자 단말에 타 서비스를 제공하는 동안에도, 전달된 사용자 정보에 갱신 조건이 성립하는지 지속적으로 확인하여, 스토리지(160)에 저장된 사용자 정보가 업데이트되어 갱신 조건이 성립할 경우 스토리지(160)에 업데이트된 사용자 정보의 전달을 요청함으로써, 최신의 사용자 정보를 획득할 수 있다.

[0050] 구체적으로 설명하면, 서비스 서버(102)는, 사용자 단말(101)에 관한 사용자 정보를 전달받은 시점에, DID 레지스트리(171)로부터 사용자 단말(101)의 DID 문서를 로딩하여, 로딩한 DID 문서에 포함된 관리증명서를, 제공된 사용자 정보와 함께 데이터베이스에 저장하고, 일정 주기로 DID 레지스트리(171)에서 재로딩한 사용자 단말(101)의 DID 문서에 포함되는 관리증명서가, 상기 데이터베이스에 저장한 관리증명서와 일치하는지 비교하고, 일치하지 않을 경우, 상기 데이터베이스에 저장한 사용자 정보에 대해 갱신 조건이 성립(스토리지(160)에 저장된 사용자 정보의 업데이트 발생)하는 것으로 판단하고, 서비스 서버(102)에 관한 서비스 인증 정보를 포함하여, 사용자 단말(101)의 업데이트된 사용자 정보의 전달 요청을 발생할 수 있다.

[0051] 이에 따라 서버 인증부(110)에서 상기 서비스 인증 정보를 이용해 상기 전달 요청을 발생한 서비스 서버(102)를 신원 인증하면, 전달 처리부(140)는, 해당 서비스 서버(102)로 업데이트된 사용자 정보를 전달해 최신의 사용자 정보를 지속적으로 제공할 수 있다.

[0052] 상기 갱신 조건의 성립에 따라, 서비스 서버(102)에서 상기 사용자 정보의 전달 서비스 요청이 발생하면, 전달 처리부(140)는 상기 전달 서비스 요청을 발생한 서비스 서버(102)에 대해, 상기 전달 기록이 스토리지(160)에 생성되어 있는지 확인하고, 상기 전달 기록이 생성되어 있으면, 스토리지(160)에서 상기 사용자 단말에 관한 업데이트된 사용자 정보를 리드해 서비스 서버(102)에 전달할 수 있다.

[0053] 즉, 전달 처리부(140)는 상기 갱신 조건의 성립에 따라 상기 사용자 정보의 전달 서비스 요청을 발생한 서비스 서버(102)에 대해, 상기 전달 기록이 남겨져 있으면, 서버 인증부(110)에 의한 상기 서비스 인증 정보의 검증 과정을 생략하여, 보다 빠르게 업데이트된 최신의 사용자 정보를 서비스 서버(102)로 제공할 수 있다.

[0054] 다른 일례로, 저장 처리부(150)에서 사용자 단말에 의해 사용자 정보가 업데이트될 때마다, 전달 처리부(140)는, 스토리지(160)에 상기 사용자 정보의 전달 기록이 생성되어 있는 서비스 서버(102)를 모두 식별하여, 업데이트된 사용자 정보를 일시에 전달함으로써, 서비스 서버(102)에서 최신의 사용자 정보를 별도로 요청하지 않아도, 사용자 단말에 관해 업데이트된 사용자 정보를 지속적으로 전달할 수도 있다.

[0055] 이와 같이, 전달 처리부(140)는 사용자 단말이 이용하는 서비스 서버(102)에 항상 최신의 사용자 정보를 제공하여, 사용자 단말에서 직접 서비스 서버(102)에 접속해 자신의 정보를 수정하는 번거로움 없이 최신의 사용자 정보에 근거한 상기 타 서비스를 이용하게 할 수 있다. 한편 실시예에 따라 업데이트된 사용자 정보가 불필요한 일부의 서비스 서버(102)에는 최신의 사용자 정보의 제공이 생략될 수도 있다.

[0056] 도 2는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템을 포함한 네트워크를 도시한 도면이다.

[0057] 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스(InfoDID) 제공 시스템은, 도 2에 도시된 InfoDID 서버(210)에 의해 구현될 수 있다.

[0058] 도 2를 참조하면, 네트워크(200)는 InfoDID 서버(210), 이더리움 퍼블릭 블록체인(220), DID 레지스트리(230) 및 사용자 단말(240)을 포함하여 구성할 수 있다.

[0059] InfoDID 서버(210)는, 이더리움 블록체인(220) 자체의 저장 용량과 비용 한계로 인해 사용자 정보를 LDAP 기반의 데이터베이스에 저장하여 관리하고, 이더리움 블록체인(220)에 배포된 확장된 DID 레지스트리(230)와, 상기 데이터베이스와 상호작용하여, 사용자 단말(240)에 사용자 정보 관리 서비스(infoDID)를 제공할 수 있다.

표 1

DID	분산식별자
createdTime	사용자 정보의 관리 시작 시간
updatedTime	사용자 정보의 최근 업데이트 시간
validTime	사용자 정보 관리를 위한 잔여 시간
sn	사용자의 성(Last name)
cn	사용자의 이름(First name)
gender	사용자의 성별
brith	사용자의 생년월일
country	사용자의 사는곳
address	사용자의 주소
job	사용자의 현재 직업
email	사용자의 Email
contact	사용자의 전화번호
…	
profile picture	사용자의 프로필 사진
education list	사용자의 학력
hobby	사용자의 취미

[0060]

[0061] 상기 데이터베이스에 저장되는 사용자 정보는, [표 1]과 같이, 사용자의 분산식별자(DID), 사용자 정보의 관리 시작 시간(createdTime), 사용자 정보의 마지막 업데이트 시간(updatedTime), 사용자 정보의 유효 기간(validTime), 사용자의 성(sn)과 이름(cn), 성별(gender), 생년월일(brith), 사는 곳(country), 주소(address), 현재 직업(job), Email, 전화번호(contact), 프로필 사진, 취미(hobby), 학력(education), 경력(career) 등이 저장된다.

[0062] 이러한 사용자 정보들은 DID 기반의 사용자 요청을 통해 저장되거나 업데이트 될 수 있다. InfoDID 서버(210)에서 사용자의 정보를 저장(업데이트)하는 과정은 다음과 같다.

[0063] 먼저, 사용자 단말(240)은 InfoDID 서버(210)에 저장(업데이트)할 자신의 정보와 자신의 신원을 증명하기 위한 사용자 인증 정보를 보낸다(도 2의 ①).

[0064] 여기서, 사용자 인증 정보는, 사용자 단말(240)의 DID와, DID 문서에 저장된 공개키의 대칭키인 비밀키(Private key)로 사용자 정보를 서명하여 만든 시그니처값, 그리고 시그니처값을 복호화할 수 있는 사용자 DID 문서의 공개키에 대한 공개키아이디(Public Key ID)가 포함된다.

[0065] 다음으로, InfoDID 서버(210)는 사용자 단말(240)로부터 받은 사용자 인증 정보 내 DID에 해당하는 DID 문서를 DID 레지스트리(230)에서 가져온다(도 2의 ②). 이 DID 문서는 개인항목(Privacy)을 포함하여 사용자 단말(240)에 의해 사전에 작성된 것일 수 있다.

[0066] 다음으로, InfoDID 서버(210)는 가져온 사용자 단말(240)의 DID 문서에서 사용자 인증 정보의 공개키아이디를 사용하여 공개키를 추출한 뒤, 대칭키 암호의 복호화 과정을 거쳐 사용자 인증 정보의 시그니처값이 유효한지 검증한다(도 2의 ③). 이 과정을 통해 InfoDID 서버(210)는 사용자 정보의 저장을 요청한 사용자 단말(240)의 신원 인증을 수행하고, 사용자 정보가 사용자 단말(240)로부터 전달되어 오는 과정에서 위조 또는 변조되었는지

여부를 확인할 수 있다.

[0067] 상기 사용자 인증 정보의 시그니처값이 유효하다면, InfoDID 서버(210)는 사용자 단말(240)로부터 받은 사용자 정보를 선정된 암호화 기법에 의해 암호화하여, 연결된 데이터베이스에 저장(업데이트)한다(도 2의 ④).

[0068] 이후, InfoDID 서버(210)는 사용자 정보를 위변조 없이 저장(업데이트)했음을 보장하는 관리증명서(Management certificate)를 사용자 단말(240)에 발급한다(도 2의 ⑤). 또한, InfoDID 서버(210)는 사용자 단말(240)에 발급한 관리증명서를, 데이터베이스에도 보관하여, 데이터베이스에 저장한 사용자 정보를 이후에 다른 서비스에 전달할 때, 저장된 사용자 정보가 비정상적으로 변경되었는지 확인하는데 관리증명서를 이용할 수 있다.

[0069] 여기서, 사용자 단말(240)에 발급되는 관리증명서는, 사용자의 DID, 사용자가 보내온 사용자 인증 정보의 시그니처값(User signature), 사용자 정보의 최근 처리 타입(저장 또는 업데이트), 현재 저장된 모든 사용자 정보(Informations), InfoDID 서버(210)의 DID, InfoDID 서버(210)가 발급하는 관리증명서의 시그니처값을 복호화할 수 있는 DID 문서의 공개키아이디, 보증서 생성 시간(Created time), 그리고 앞서 기술한 모든 항목을 InfoDID 서버(210)의 비밀키로 서명한 시그니처값으로 구성된다.

[0070] 사용자 단말(240)은 DID 레지스트리(230)에서 InfoDID 서버(210)의 DID 문서를 가져와서, 발급받은 관리증명서의 시그니처값의 유효성을 검증한다(도 2의 ⑥). 이를 통해, 사용자 단말(240)은 InfoDID 서버(210)에서 사용자 정보를 임의로 변경하지 않고 원본 그대로 저장(업데이트)하였음을 확인할 수 있다.

[0071] 그 후, 사용자 단말(240)은 발급받은 관리증명서를 자신의 DID 문서에 등록된 첫 번째 공개키로 암호화하고, 암호화된 값을 해시 함수인 Keccak-256을 통해 해시하여, 자신의 DID 문서에 있는 개인항목(Privacy)에 저장하여 보관한다(도 2의 ⑦). 사용자 단말(240)의 DID 문서에 저장된 개인항목의 값은 오직 사용자의 비밀키에 의해서만 복호화될 수 있다.

[0072] 이를 정리하면, 사용자 단말(240)에서 자신의 신원을 증명하기 위한 사용자 인증 정보(사용자 DID, 사용자 정보를 서명한 시그니처값, 공개키아이디)와, 저장/업데이트하려는 자신의 사용자 정보를 InfoDID 서버(210)로 보내면, InfoDID 서버(210)는 사용자 DID를 이용해, DID 레지스트리(230)에서 가져온 사용자 DID 문서에서 공개키를 추출한 후, 이 공개키로 사용자가 보낸 사용자 인증 정보의 시그니처값을 복호화해서 유효성 검증하고, 이를 통해 사용자 신원 인증과 사용자 정보가 전달되는 과정에서 위조/변조되지 않았음이 확인되면, 데이터베이스에 사용자 정보를 저장/업데이트 할 수 있고, 사용자 정보의 위조/변조 없는 저장(업데이트)을 보장하는 관리증명서를 사용자 단말(240)에 발급하는 동시에, 발급한 관리증명서를 InfoDID 서버(210)와 연결된 데이터베이스에도 보관하여, 이후에 데이터베이스에 저장된 사용자 정보를 다른 서비스에 전달할 때, 비정상적인 변경이 있었는지 확인하는데 관리증명서를 활용할 수 있다.

[0073] 도 3은 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 확장된 DID 레지스트리에 기록되는 DID 문서를 도시한 도면이다.

[0074] 도 3을 참조하면, 본 발명에 따른 사용자 정보 관리 서비스 제공 시스템은, 이더리움 블록체인에서 관리하는 확장된 형태의 DID 레지스트리(330)에 사용자 단말(310)에 의해 작성된 DID 문서(340)를 기록하고, 이후, 사용자 단말(310)에서 사용자 정보를 저장(업데이트)하려는 경우, InfoDID 서버(320)에서는 DID 레지스트리(330)에서 가져온 사용자 단말(310)의 DID 문서(340)를 이용해 사용자 단말(310)의 신원 인증을 수행할 수 있다.

[0075] InfoDID 서버(320)에서 제공하는 사용자 정보 관리 서비스(InfoDID)는 모두 DID(분산식별자)를 기반으로 동작하기 때문에, InfoDID 서버(320)에서는 사용자 정보의 위변조를 방지하기 위한 정보를 담을 수 있는 W3C의 DID 표준 규격을 확장한 DID 레지스트리(330)를 이용하고 있다.

[0076] 확장된 DID 레지스트리(330)에 저장되는 사용자 단말(310)의 DID 문서(340)는, 문서 주체의 분산 식별자(DID), 해당 DID 문서의 편집 권한을 가진 주체인 컨트롤러(Controller List) 리스트, 신원 증명에 사용되는 비대칭 암호화의 공개키 리스트(Public Key List), 해당 DID 문서 주체와 상호작용하는 서비스 리스트(Service List), 그리고 DID 문서의 작성 주체의 개인정보를 보관하기 위한 항목인 개인항목(Privacy)(350), 임시값(Nonce)을 포함한다.

[0077] 여기서 개인항목(350)은, 종래의 DID 문서에 추가된 항목으로서, 사용자가 발급받은 관리증명서를 보관하는데 이용될 수 있다.

[0078] 또한, DID 문서(340)에서 임시값(Nonce)은, 문서 주체가 문서의 편집 작업을 시그니처값을 통해 진행할 때 사용

되는 값으로, 문서에서 편집 작업이 완료될 때마다 문서의 임시값은 순차적으로 증가한다.

[0079] DID 문서(340)는 문서 주체인 사용자 단말(310)이 자신의 시그니처값을 직접 사용하여 문서에 대한 작성/항목 편집을 진행할 수도 있고, 문서 주체가 아닌 타인에게 자신의 시그니처값을 전달하여 문서에 대한 작성/항목 편집을 진행할 수도 있다.

[0080] 도 4a 및 도 4b는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 사용자 단말의 DID 문서를 이용한 신원 인증(DID 인증) 절차를 도시한 도면이다.

[0081] 도 4a에 도시된 DID 인증 절차에 따르면, 먼저, DID 사용자(User)는 infoDID 서비스를 제공받기 위하여, 비대칭 암호화 방식의 비밀키(Private key)가 저장된 개인 모바일 단말기나 브라우저를 통해 자신의 DID가 담긴 사용자 요청을 서비스에게 보낸다(도 4a의 step 1).

[0082] 사용자 요청을 수취한 infoDID 서버는, 사용자 DID를 이용하여 DID 레지스트리에 저장된 사용자 DID 문서에서 사용자 공개키를 가져오고(도 4a의 step 2), 신원 인증에 필요한 값을 암호화하여 사용자에게 보낸다(DID 인증: Challenge)(도 4a의 step 3).

[0083] infoDID 서버로부터 암호화된 값을 받은 DID 사용자는, 자신의 비밀키를 통해 해당 값을 복호화하고 서비스에게 다시 보내 신원 인증 요청에 응답한다(DID 인증: Response)(도 4a의 step 4).

[0084] 그러면, infoDID 서버는 사용자가 보낸 복호화된 인증값이 유효한지 확인하여 사용자에 대한 신원 인증을 완료하고, 서비스를 제공하기 위한 채널을 만들어 사용자에게 서비스를 제공한다(도 4a의 step 5).

[0085] 상술한 도 4a의 DID 인증 절차에서는, infoDID 서버에서 신원 인증에 필요한 값을 암호화하여 사용자에게 보내는 Challenge(step 3)와, DID 사용자가 자신의 비밀키를 통해 복호화한 값을 수취해 신원 인증하는 Response(step 4)에 의해 DID 인증이 이루어지고 있는 반면, 후술하는 도 4b의 DID 인증 절차에서는, 이 두 단계를 생략하여 종래보다 간략화된 DID 인증을 수행하고 있다.

[0086] 구체적으로, 도 4b의 DID 인증 절차에서는, DID 사용자(User)가 자신의 DID가 담긴 사용자 요청을 서비스에게 보내면(도 4b의 step 1), 사용자 요청을 수취한 infoDID 서버는, 사용자 DID를 이용하여 DID 레지스트리에 저장된 사용자 DID 문서에서 사용자 공개키를 가져오고(도 4a의 step 2), 사용자 단말의 DID 문서에 기재된 공개키 아이디로부터, 사용자 단말이 시그니처값 생성시 사용한 비밀키에 대칭되는 공개키를 추출하여 DID 사용자가 보낸 사용자 인증 정보의 서명값을 직접 검증하고(도 4b의 step 3), 서명값이 검증됨에 따라 사용자에 대한 신원 인증이 완료되면, 서비스를 제공하기 위한 채널을 만들어 사용자에게 서비스를 제공한다(도 4b의 step 5).

[0087] 즉, 도 4b의 간략화된 DID 인증 절차에 의해서는, DID 문서에서 가져온 값을 사용자에게 보내서 사용자의 비밀키로 복호화된 값을 받아낼 필요 없이, infoDID 서버에서 DID 문서의 공개키아이디에서 추출한 공개키로 서명값이 유효한지 직접 검증할 수 있기 때문에 신원 인증의 처리 속도를 향상시킬 수 있다.

[0088] 도 5a 및 도 5b에서는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템이 infoDID 서버(510)에 의해 구현되는 예를 설명한다.

[0089] 도 5a는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 사용자 정보의 전달 서비스 제공 과정을 설명하기 위한 도면이다.

[0090] 도 5a에는, 사용자 단말에서 사용자 정보 관리 서비스(infoDID) 외에 타 서비스(예, '은행 서비스')를 이용하려는 경우, 타 서비스를 제공하는 서비스 서버(520)에서 필요로 하는 사용자 정보를 infoDID 서버(510)에서 전달하는 과정이 도시된다.

[0091] 도 5a를 참조하면, 사용자 단말에서 이용하고자 하는 타 서비스의 서비스 서버(520)로 자신의 사용자 인증 정보를 보내면(도 5a의 ①), 서비스 서버(520)에서는, 자신의 서비스 인증 정보를, 사용자 단말로부터 받은 사용자 인증 정보를 포함하여 생성하고, 이를 infoDID 서버(510)로 보내서, 사용자 단말에 관해 저장된 사용자 정보의 전달을 요청한다(도 5a의 ②).

[0092] 여기서, 사용자 단말에 관한 사용자 인증 정보에는, 사용자 DID, 사용자 정보를 전달받을 서비스 서버(520)의 DID, 사용자 정보, 사용자 정보의 유효시간, 앞서 기술한 모든 항목을 비밀키로 서명한 시그니처값, 시그니처값을 복호할 수 있는 사용자 DID 문서의 공개키아이디 등이 포함될 수 있다.

[0093] 또한, 서비스 서버(520)에 관한 서비스 인증 정보에는, 서비스 서버(520)의 DID, 사용자 단말로부터 받은 사용

자 인증 정보, 서비스 서버(520)의 비밀키로 앞서 기술한 두 값을 서명한 시그니처값, 시그니처값을 복호화하기 위한 서비스 서버(520)의 공개키아이디 등이 포함될 수 있다.

[0094] 서비스 서버(520)로부터 사용자 정보의 전달을 요청받은 infoDID 서버(510)는, 각 주체의 DID를 이용하여, 서비스 서버(520)의 DID 문서와 사용자 단말의 DID 문서를 DID 레지스트리(530)에서 각각 가져온다(도 5a의 ③)

[0095] infoDID 서버(510)는, 서비스 서버(520)의 DID 문서를 이용해, 서비스 인증 정보 내 서비스 서버(520)의 서명값의 유효성을 검증하고, 사용자 단말의 DID 문서를 이용해, 검증된 서비스 인증 정보에서 추출한 사용자 인증 정보 내 서명값의 유효성을 검증할 수 있다(도 5a의 ④).

표 2

	user { *service* { DID DID attributes publicKeyID validTime signature } publicKeyID signature }
1.	**IF** *user*.validTime is not timeout*&user*.DID exists in LDAP
2.	**IF** *user & service* document exists in DID registry
3.	Get *user & service* document from DID registry
4.	Extract public keys from *service, user* document as *service*.publicKeyID, *user*.publicKeyID
5.	Verification *service*.signature using public key of *service, user*
6.	Verification *user*.signature using public key of *user, user* (except *user*.signature)

[0096]

[0097] [표 2]는 서비스 서버(520)로부터 수신된 서비스 인증 정보를 infoDID 서버(510)에서 처리하는 절차를 도시한 코드 일례이다. infoDID 서버(510)는 서비스 서버(520)로부터 받은 서비스 인증 정보를 수취하면, [표 2]에 있는 line 1~6에 따라, 사용자 단말에 대한 신원 인증, '은행 서비스'를 제공하는 서비스 서버(520)에 대한 신원 인증, 서비스 서버(520)에서 사용자 정보를 읽는 기능에 대한 사용자 승인 여부를 확인할 수 있다.

[0098] 위 과정에 의해 서비스 서버(520)와 사용자 단말에 대한 모든 검증이 완료되면, infoDID 서버(510)는 데이터베이스에 저장된 사용자 정보를 사용자 단말에 전달하고, 서비스 서버(520)로의 사용자 정보 제공 기록을 데이터베이스에 기록한다(도 5a의 ⑤).

[0099] 이때, infoDID 서버(510)는 데이터베이스에 저장된 사용자 정보를 사용자 단말에 전달하기 전에, 사용자 단말의 DID 문서에 저장된 관리증명서와 데이터베이스에 저장된 관리증명서가 일치하는지 비교하여, 데이터베이스에 저장된 사용자 정보에 사용자의 승인 없는 비정상적인 변경이 없는지를 확인할 수 있다. 예를 들면, InfoDID 서버는 해당 사용자에게 마지막으로 발급해준 관리보증서**를** 사용자 DID 문서의 첫 번째 공개키로 암호화하고 Keccak-256으로 해시한 값이 사용자 DID 문서에 저장된 Privacy 항목의 값과 같은지 비교할 수 있다. 이를 통해 사용자 정보에 변경이 없는 것으로 확인되면 infoDID 서버(510)는 사용자 정보를 전달할 수 있다.

[0100] 서비스 서버(520)에서는, infoDID 서버(510)에 의해 전달된 사용자 정보를 저장할 때, DID 레지스트리에 기록된 사용자의 DID 문서 중 개인항목(Privacy)에 저장되어 있는 관리증명서를 가져오고, 이후 주기적으로 DID 레지스트리에 기록된 사용자의 DID 문서에서 다시 가져온 관리증명서를 처음에 가져온 관리증명서와 비교해서, 사용자 정보의 갱신 조건이 성립하는지 확인한다(도 5a의 ⑥).

[0101] 양 관리증명서가 일치하지 않으면, 서비스 서버(520)에서는, infoDID 서버(510)에서 관리하는 데이터베이스에 저장된 사용자 정보에 업데이트가 생긴 것으로 보고, infoDID 서버(510)에 사용자 정보의 갱신을 요청할 수 있다. 도 5b에는 최신의 사용자 정보를 제공하기 위한 과정이 도시된다.

[0102] 도 5b는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 시스템에서, 최신의 사용자 정보를 제공하기 위한 과정을 설명하기 위한 도면이다.

[0103] 도 5b를 참조하면, 서비스 서버(520)는 사용자 단말의 DID를 이용해 현시점에 사용자 DID 문서에서 Privacy 항목값(관리증명서)을 가져오고, 이를 infoDID 서버(510)에 의해 사용자 정보가 전달될 때 사용자 DID 문서에서 가져온 Privacy 항목값(관리증명서)과 비교하여, 두 관리증명서가 일치하는지 확인한다(도 5b의 ①).

[0104] 두 관리증명서가 일치하면, 서비스 서버(520)는 현재 해당 사용자에 대한 최신의 사용자 정보를 보유한 상태로 판단할 수 있다.

[0105] 두 관리증명서가 다르면, 서비스 서버(520)는 사용자 정보의 갱신이 필요한 것으로 판단하고, infoDID 서버(510)로 자신의 서비스 인증 정보를 보내, 업데이트된 사용자 정보의 전달을 요청한다(도 5b의 ②).

[0106] infoDID 서버(510)는, 서비스 서버(520)의 DID 문서를 DID 레지스트리에서 가져와 서비스 서버(520)에서 보내온 서비스 인증 정보 내 서명값의 유효성을 검증하고(도 5b의 ③), 사용자 단말의 DID 문서를 DID 레지스트리에서 가져와 상기 서비스 인증 정보에서 추출한 사용자 인증 정보 내 서명값의 유효성을 검증하고(도 5b의 ④), 추가적으로 서비스 서버(520)에서 사용자 정보를 읽는 기능에 대한 사용자 승인 여부를 확인한다(도 5b의 ⑤).

[0107] 이후, infoDID 서버(510)는 데이터베이스에 업데이트된 사용자 정보를 서비스 서버(520)로 전달하고 업데이트된 사용자 정보의 전달 기록을 데이터베이스에 생성한다(도 5b의 ⑥).

[0108] 이러한 과정에 의해, 서비스 서버(520)는 항상 최신의 사용자 정보에 기초해서 사용자에게 유용한 서비스를 제공할 수 있고, 사용자 단말은 자신이 이용 중인 여러 서비스 서버(520)에 일일이 방문해 사용자 정보를 수정할 필요가 없게 된다.

[0109] 도 6a 및 도 6b는 본 발명에 따른 DID 기반의 사용자 정보 관리 서비스 제공 방법의 순서를 도시한 흐름도이다.

[0110] 본 실시예들에 따른 DID 기반의 사용자 정보 관리 서비스 제공 방법은, 도 1에서 설명한 사용자 정보 관리 서비스 제공 시스템(100)에 의해 수행될 수 있고, 상술한 사용자 정보 관리 서비스 제공 시스템(100)은, 도 5a 및 도 5b에서 설명한 infoDID 서버(510)에 의해 구현될 수 있다.

[0111] 도 6a에는 사용자 정보의 신뢰성 있는 저장/업데이트의 처리 과정이 도시되고, 도 6b에는 저장/업데이트된 사용자 정보의 타 서비스 전달 처리 과정이 도시된다.

[0112] 먼저 도 6a를 참조하면, 단계(601)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 infoDID 서비스를 이용하는 사용자 단말에서 정보 저장 요청이 발생하는지 확인한다.

[0113] 정보 저장 요청의 발생에 따라, 단계(602)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 블록체인의 DID 레지스트리에 기록된 사용자 단말의 DID 문서를 로딩하여, 사용자 인증 정보를 검증한다.

[0114] 사용자 인증 정보의 검증으로 사용자 단말의 신원이 인증되면, 단계(603)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 사용자 단말에서 저장하려는 사용자 정보를 검증된 사용자 인증 정보에서 추출한다.

[0115] 단계(604)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 추출한 사용자 정보를 스토리지에 저장/업데이트한다(사용자 정보 저장 서비스 제공). 여기서, 상기 사용자 정보가 유지되는 스토리지는, 예를 들면, infoDID 서버(510)에서 관리하는 LDAP 기반의 데이터베이스로 구현될 수 있다.

[0116] 상기 사용자 정보의 저장 후에, 단계(605)에서 사용자 정보 관리 서비스 제공 시스템(100)은 상기 사용자 단말에서 보낸 사용자 정보가 위조나 변조 없이 그대로 저장되었음을 보장하는 관리증명서를 상기 사용자 단말에 발급하고, 발급한 관리증명서를 스토리지에 보관한다.

[0117] 이후, 사용자 정보 관리 서비스 제공 시스템(100)은 상기 사용자 단말의 요청에 의해 상기 스토리지에 저장된 사용자 정보가 업데이트될 때마다, 상기 사용자 단말에서 보낸 사용자 정보가 위조나 변조 없이 그대로 저장되어 업데이트되었음을 보장하는 관리증명서를 사용자 단말에 재발급하고, 업데이트된 사용자 정보와 함께, 재발급한 관리증명서를 스토리지에 보관할 수 있다.

[0118] 단계(606)에서, 사용자 단말은 발급받은 관리증명서를 DID 레지스트리에 기록된 DID 문서의 개인항목(Privacy)에 보관하여, 추후, 타 서비스로의 사용자 정보 전달 시 사용되게 한다.

[0119] 단계(607)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 사용자 단말에 관한 사용자 정보를 스토리지에 저

장한 이후, 사용자 단말로부터 정보 업데이트 요청이 발생하는지 확인하고, 정보 업데이트 요청의 발생 시, 상술한 단계(602 내지 606)의 과정을 반복하여, 스토리지에 저장된 사용자 정보를 업데이트 한다.

[0120] 도 6b를 참조하면, 단계(608)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 사용자 단말에서 타 서비스(예, '은행 서비스')의 이용 요청이 발생하는지 확인한다.

[0121] 사용자 단말에서 타 서비스의 이용 요청이 발생하는 경우, 단계(609)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 타 서비스와 연관된 서비스 서버의 DID 문서를 DID 레지스트리에서 가져와 서비스 인증 정보를 검증하여, 서비스 서버의 신원을 인증한다.

[0122] 서비스 서버의 신원이 인증되면, 단계(610, 611)에서, 사용자 정보 관리 서비스 제공 시스템(100)은 서비스 인증 정보에 포함된 사용자 인증 정보를 추출하고, 추출된 사용자 인증 정보를 사용자 단말의 DID 문서를 이용해 검증하여, 사용자 단말의 신원을 인증한다.

[0123] 사용자 단말의 신원이 인증되면, 단계(612)에서, 사용자 정보 관리 서비스 제공 시스템(100)은, 스토리지에서 사용자 정보를 리드해 서비스 서버로 전달한다(사용자 정보 전달 서비스 제공).

[0124] 이때, 상기 사용자 정보를 전달받은 서비스 서버에서는, 블록체인의 DID 레지스트리에서 사용자의 DID 문서를 로딩하여, 로딩한 DID 문서의 개인항목에 저장된 관리증명서(이하, 제1 관리증명서)를, 전달된 사용자 정보와 함께 서비스 서버에서 관리하는 데이터베이스에 저장한다. 상기 제1 관리증명서는, 상기 스토리지에서 사용자 정보의 업데이트가 발생했는지, 사용자 정보의 갱신 조건이 성립하는지 확인할 때의 기준으로 사용될 수 있다.

[0125] 단계(613)에서, 사용자 정보가 전달된 각 서비스 서버는, 블록체인의 DID 레지스트리에서 사용자의 DID 문서를 주기적으로 재로딩하여, 재로딩한 DID 문서의 개인항목에 저장된 관리증명서(이하, 제2 관리증명서)를 상기 제1 관리증명서와 일치하는지 비교하여, 사용자 정보의 갱신 조건이 성립하는지 확인한다.

[0126] 즉, 주기적으로 가져온 제2 관리증명서가 상기 제1 관리증명서와 일치하면, 서비스 서버는, 현재 데이터베이스에 저장된 사용자 정보가 최신의 사용자 정보인 것으로 확인한다(단계(613)에서 No).

[0127] 한편, 주기적으로 가져온 제2 관리증명서가 상기 제1 관리증명서와 일치하지 않으면, 서비스 서버는, 상기 스토리지에서 사용자 정보가 업데이트되어 제2 관리증명서가 재발급된 것으로 판단하고, 현재 데이터베이스에 저장된 사용자 정보에 갱신이 필요한 것으로 확인한다(단계(613)에서 Yes).

[0128] 이처럼 양 관리증명서가 서로 달라서, 현재 데이터베이스에 저장된 사용자 정보의 갱신 조건이 성립하면, 서비스 서버는, 업데이트된 사용자 정보의 전달 요청을 발생하고, 상기 전달 요청에 응답하여 사용자 정보 관리 서비스 제공 시스템(100)은 상기 스토리지에 업데이트된 최신의 사용자 정보를 서비스 서버로 전달한다(최신의 사용자 정보 제공)(단계(614)).

[0129] 이와 같이 본 발명에 의하면, 사용자 정보 관리 서비스(InfoDID)의 실행에 의해, 도 6a 및 도 6b에서 설명한 단계(601 내지 614)를 수행하여, 사용자 정보의 저장, 업데이트, 타 서비스로의 제공을 구현할 수 있다.

[0130] 따라서, 본 발명에서는, 이더리움 블록체인의 스마트 컨트랙트로 개발된 DID 레지스트리와의 연계를 통해 DID 신원 인증 서비스에 활용하여, 사용자의 정보를 신뢰성 있게 관리하고 편리한 형태로 사용자가 자신의 정보를 다른 서비스에게 제공할 수 있게 된다.

[0131] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0132] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의

조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0133] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기를 기초로 다양한 기술적 수정 및 변형을 적용할 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0134] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.

부호의 설명

[0135] 200: 사용자 정보 관리 서비스 제공 시스템

210: InfoDID 서버

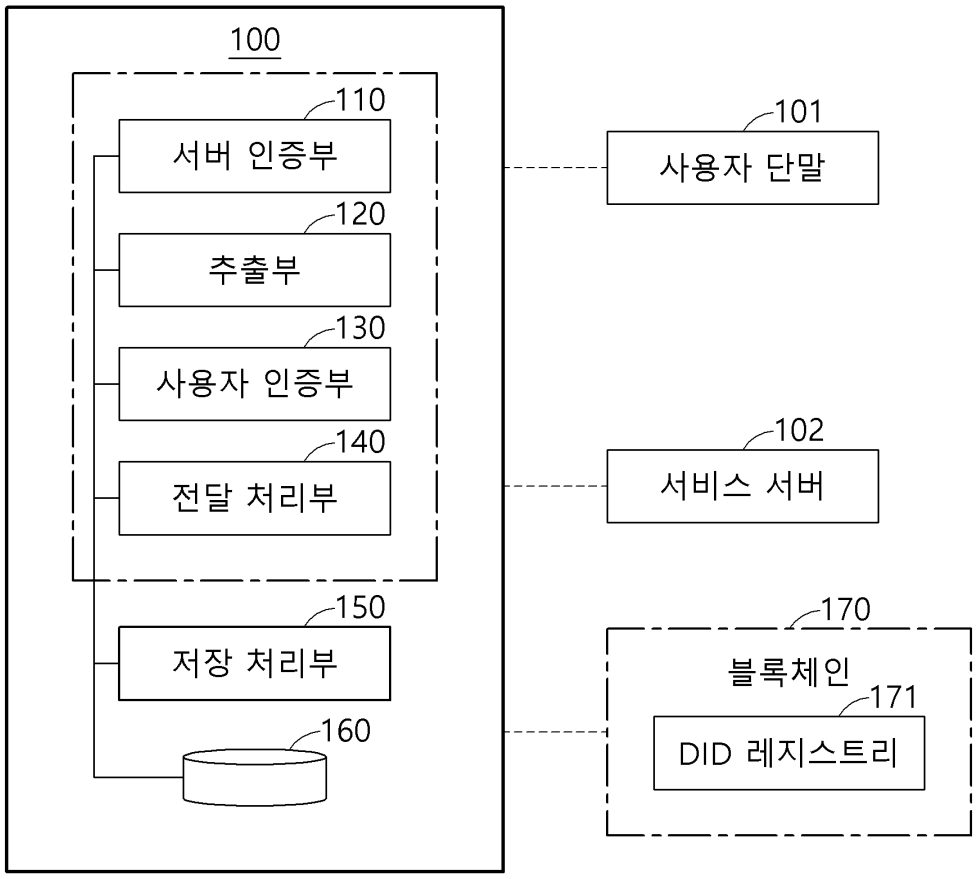
220: 이더리움 퍼블릭 블록체인

230: DID 레지스트리

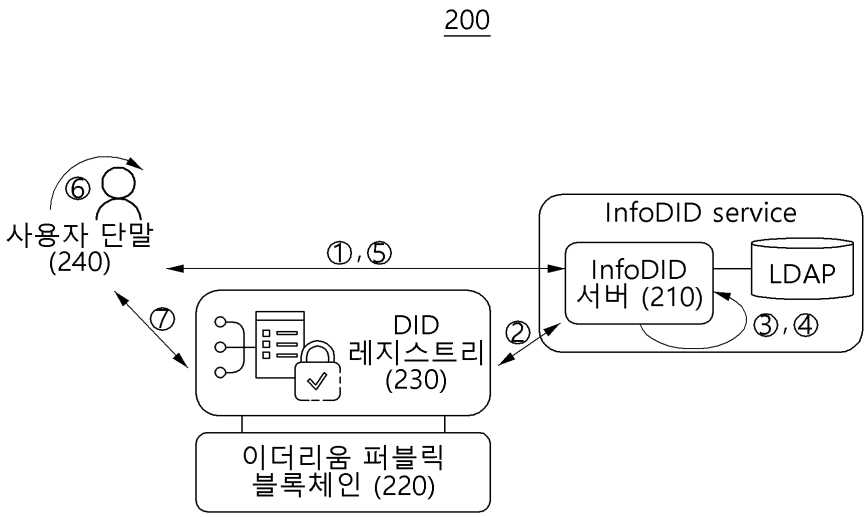
240: 사용자 단말

도면

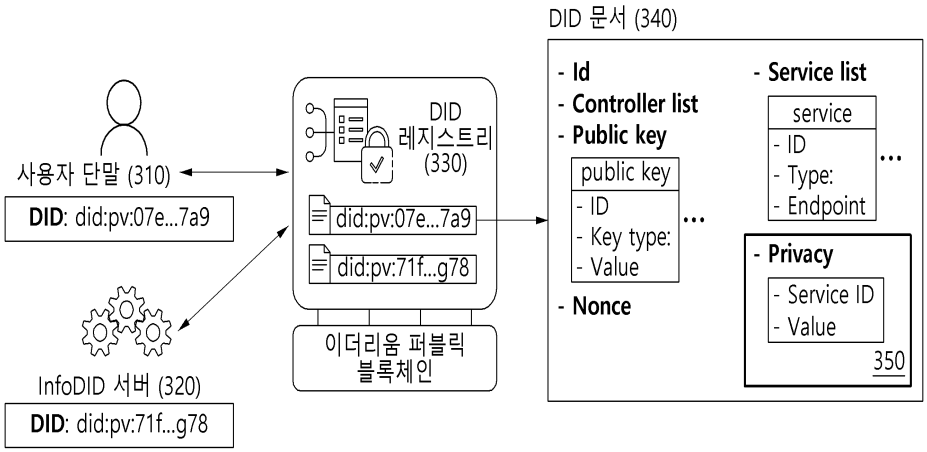
도면1


100
110
서버 인증부
120
추출부
130
사용자 인증부
140
전달 처리부
150
저장 처리부
160
101
사용자 단말
102
서비스 서버
170
블록체인
171
DID 레지스트리

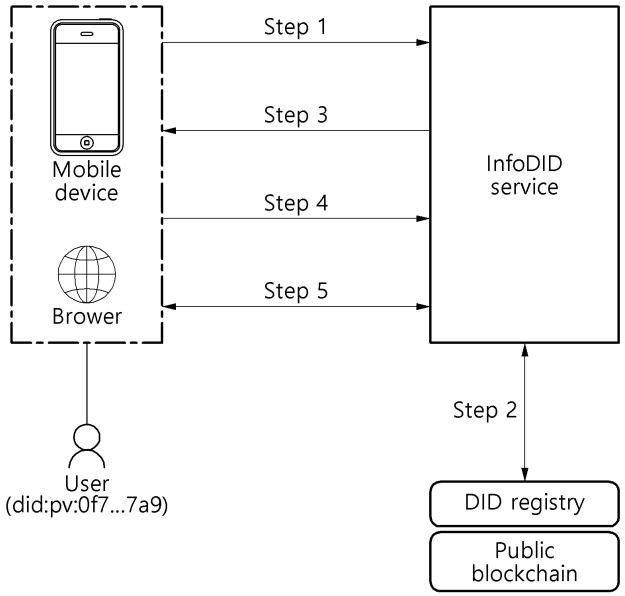
도면2


200
⑥
사용자 단말
(240)
①,⑤
⑦
InfoDID service
InfoDID
서버 (210)
LDAP
③,④
②
DID
레지스트리
(230)
이더리움 퍼블릭
블록체인 (220)

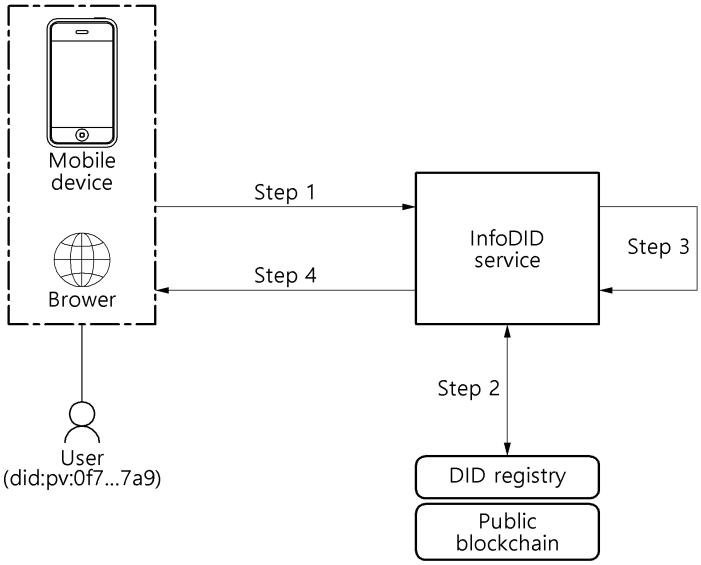
도면3


DID 문서 (340)
- Id
- Controller list
- Public key
- Nonce
- Service list
service
- ID
- Type:
- Endpoint
public key
- ID
- Key type:
- Value
- Privacy
- Service ID
- Value
350
DID
레지스트리
(330)
did:pv:07e...7a9
did:pv:71f...g78
이더리움 퍼블릭
블록체인
사용자 단말 (310)
DID: did:pv:07e...7a9
InfoDID 서버 (320)
DID: did:pv:71f...g78

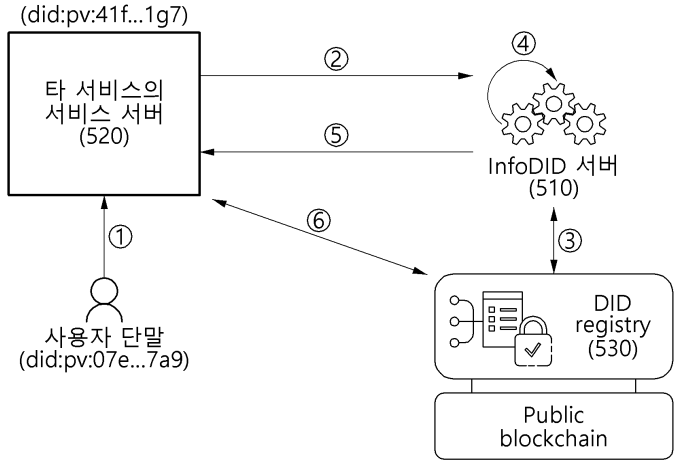
도면4a


Step 1
Step 3
Step 4
Step 5
Step 2
InfoDID
service
Mobile
device
Brower
User
(did:pv:0f7...7a9)
DID registry
Public
blockchain

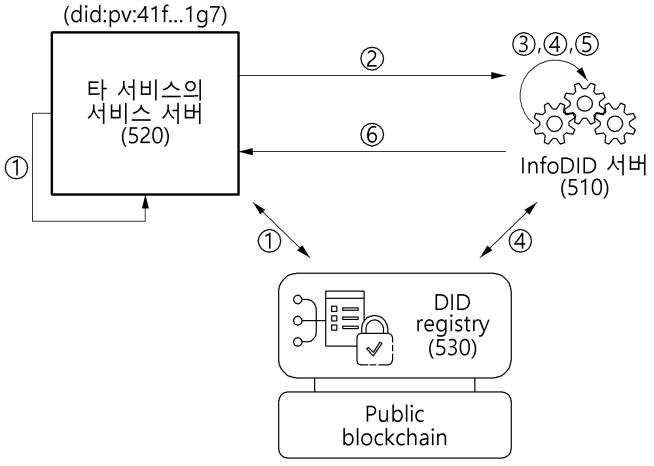
도면4b



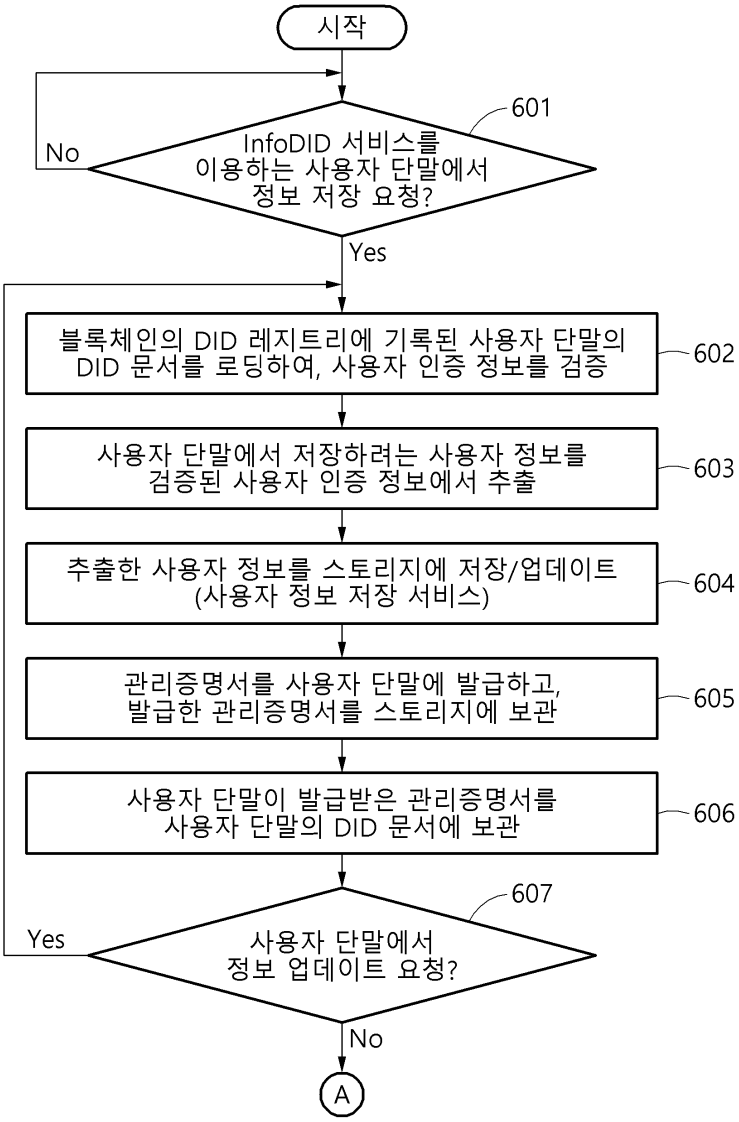
도면5a



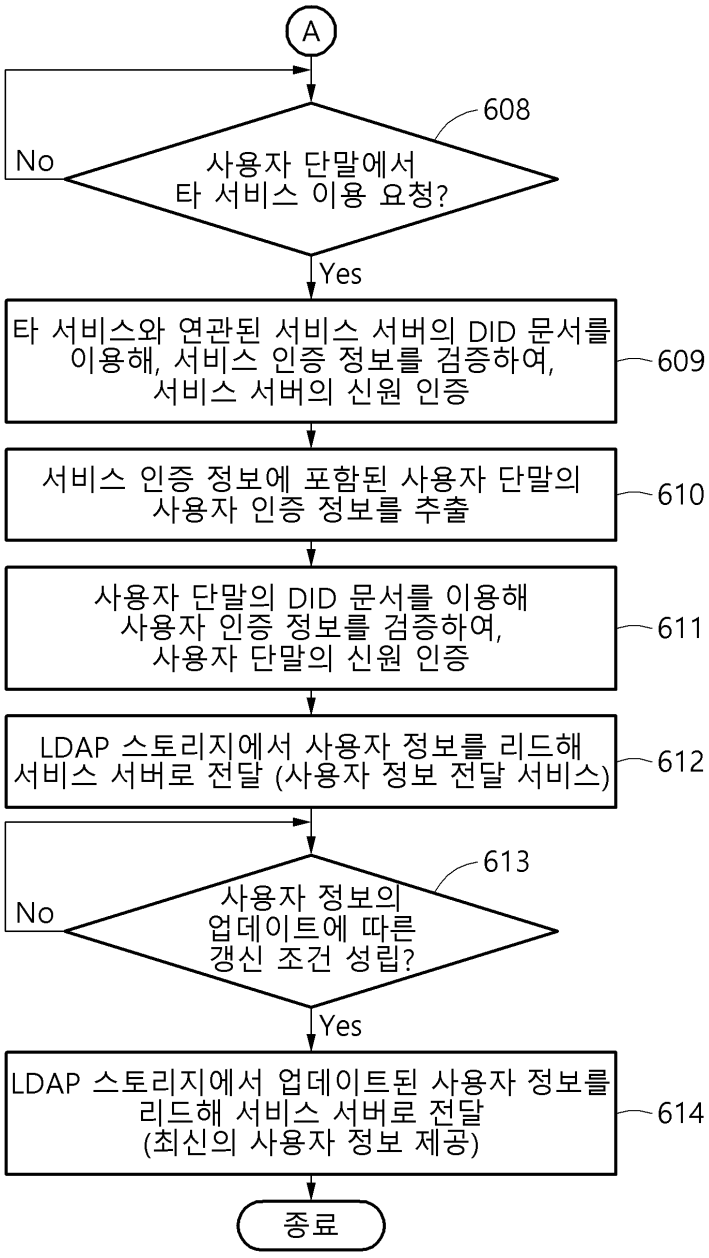
도면5b



도면6a


시작
601
InfoDID 서비스를
이용하는 사용자 단말에서
정보 저장 요청?
No
Yes
블록체인의 DID 레지트리에 기록된 사용자 단말의
DID 문서를 로딩하여, 사용자 인증 정보를 검증
602
사용자 단말에서 저장하려는 사용자 정보를
검증된 사용자 인증 정보에서 추출
603
추출한 사용자 정보를 스토리지에 저장/업데이트
(사용자 정보 저장 서비스)
604
관리증명서를 사용자 단말에 발급하고,
발급한 관리증명서를 스토리지에 보관
605
사용자 단말이 발급받은 관리증명서를
사용자 단말의 DID 문서에 보관
606
607
사용자 단말에서
정보 업데이트 요청?
Yes
No
A

도면6b


A
608
No
사용자 단말에서
타 서비스 이용 요청?
Yes
타 서비스와 연관된 서비스 서버의 DID 문서를
이용해, 서비스 인증 정보를 검증하여,
서비스 서버의 신원 인증
609
서비스 인증 정보에 포함된 사용자 단말의
사용자 인증 정보를 추출
610
사용자 단말의 DID 문서를 이용해
사용자 인증 정보를 검증하여,
사용자 단말의 신원 인증
611
LDAP 스토리지에서 사용자 정보를 리드해
서비스 서버로 전달 (사용자 정보 전달 서비스)
612
613
No
사용자 정보의
업데이트에 따른
갱신 조건 성립?
Yes
LDAP 스토리지에서 업데이트된 사용자 정보를
리드해 서비스 서버로 전달
(최신의 사용자 정보 제공)
614
종료