



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년03월04일
(11) 등록번호 10-2774744
(24) 등록일자 2025년02월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/00 (2022.01)
(52) CPC특허분류
H04L 9/321 (2013.01)
H04L 9/3268 (2013.01)
(21) 출원번호 10-2023-0193455
(22) 출원일자 2023년12월27일
심사청구일자 2023년12월27일
(30) 우선권주장
1020230157110 2023년11월14일 대한민국(KR)
(56) 선행기술조사문헌
KR1020210157550 A*
김근형, 신뢰가 보장된 데이터 경제를 위한 자기
주권 데이터 유통플랫폼 설계, 디지털콘텐츠학회
논문지 Vol.22, No. 3, pp.483-490 (2021.03.)*
KR102256730 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학
교)
(72) 발명자
이중혁
충청남도 천안시 서북구 북일로 21, 104동 1503
호(두정동, e편한세상두정3차)
김지혜
서울특별시 광진구 천호대로110길 111, 106호(능
동, 파크빌라)
(74) 대리인
성병기

전체 청구항 수 : 총 18 항

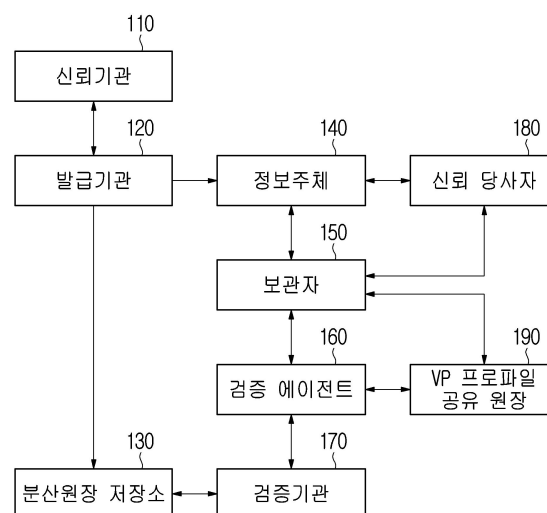
심사관 : 양종필

(54) 발명의 명칭 분산원장 기반 신원증명 시스템에서 신원정보 보호 서비스를 제공하기 위한 방법 및 장치

(57) 요약

본 개시는 분산원장 기반 신원증명 시스템에서 신원정보 보호 서비스를 제공하기 위한 방법 및 장치에 관한 것으로, 보관자의 방법은, 신뢰 당사자로부터, VP(verifiable presentation) 프로파일을 포함하는 정보주체의 신원 증명 요청 신호를 수신하는 단계, 기 저장된 정보주체의 신원정보 및 상기 VP 프로파일을 기반으로 상기 정보주체의 VP를 생성하는 단계, 및 검증 에이전트에게, 상기 생성된 VP를 포함하는 검증 요청 신호를 송신하는 단계를 포함하며, 상기 검증 요청 신호는 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 요청하는 신호일 수 있다.

대표도 - 도1



(52) CPC특허분류
H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1781000011
과제번호	RS-2023-00253686
부처명	개인정보보호위원회
과제관리(전문)기관명	한국인터넷진흥원
연구사업명	개인정보기술표준개발지원(R&D)
연구과제명	블록체인 환경에서의 개인정보보호 표준개발
기 여 율	1/1
과제수행기관명	세종대학교산학협력단
연구기간	2023.04.01 ~ 2023.12.31

명세서

청구범위

청구항 1

분산원장 기반 신원증명 시스템에서 보관자의 방법에 있어서,

신뢰 당사자로부터, VP(verifiable presentation) 프로파일을 포함하는 정보주체의 신원증명 요청 신호를 수신하는 단계;

기 저장된 정보주체의 신원정보 및 상기 VP 프로파일을 기반으로 상기 정보주체의 VP를 생성하는 단계; 및

검증 에이전트에게, 상기 생성된 VP를 포함하는 검증 요청 신호를 송신하는 단계를 포함하며,

상기 검증 요청 신호는 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 요청하는 신호이고,

상기 정보주체의 신원증명 요청 신호는, 상기 정보주체의 신원정보에 대한 보관증명서를 더 포함하며,

상기 보관증명서는, 상기 보관자가 상기 정보주체의 신원정보를 보관함을 나타내는 정보, 또는 상기 보관자가 상기 정보주체로부터 상기 신원정보의 관리 권한을 위임받았음을 나타내는 정보 중 적어도 하나를 포함하는 방법.

청구항 2

청구항 1에 있어서,

상기 VP 프로파일을 VP 프로파일 공유 원장에 등록하는 단계를 더 포함하며,

상기 VP 프로파일은, 신원증명에 필요한 클레임 목록을 포함하는 방법.

청구항 3

청구항 2에 있어서,

상기 검증 에이전트로부터 VP 프로파일 등록을 요청받는 단계를 더 포함하며,

상기 검증 에이전트는, 상기 보관자의 VP 프로파일 수신 상태를 모니터링하는, 방법.

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 보관증명서를 기반으로, 상기 정보주체의 신원을 확인하는 단계를 더 포함하며,

상기 VP는 상기 정보주체의 신원이 확인된 후에 생성되는, 방법.

청구항 6

청구항 5에 있어서,

상기 정보주체로부터 신원정보 및 신원정보에 대한 관리 권한을 위임받는 단계; 및

상기 신원정보에 대한 보관증명서를 상기 정보주체에게 발급하는 단계를 더 포함하는 방법.

청구항 7

분산원장 기반 신원증명 시스템에서 검증 에이전트의 방법에 있어서,

보관자로부터 상기 보관자에 의해 생성된 VP(verifiable presentation)에 대한 검증을 요청받는 단계;

VP 프로파일 공유 원장에 등록된 VP 프로파일을 획득하는 단계;

상기 VP 프로파일을 기반으로 신원증명에 필요한 클레임 목록을 확인하는 단계; 및

상기 신원증명에 필요한 클레임 목록을 기반으로 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 수행하는 단계를 포함하며,

상기 VP는 상기 보관자에서 신뢰 당사자로부터 수신한 보관증명서에 기반하여 정보주체의 신원이 확인된 이후에 생성되며,

상기 보관증명서는, 상기 보관자가 상기 정보주체의 신원정보를 보관함을 나타내는 정보, 또는 상기 보관자가 상기 정보주체로부터 상기 신원정보의 관리 권한을 위임받았음을 나타내는 정보 중 적어도 하나를 포함하는 방법.

청구항 8

청구항 7에 있어서,

상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 수행하는 단계는,

상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하는지 여부를 확인하는 단계를 포함하는 방법.

청구항 9

청구항 8에 있어서,

상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하는 경우, 상기 보관자에게 VP 재생성을 요청하는 단계를 더 포함하는 방법.

청구항 10

청구항 8에 있어서,

상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하지 아니하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하지 아니하는 경우, 검증 기관에 VP를 제출하는 단계를 더 포함하는 방법.

청구항 11

분산원장 기반 신원증명 시스템에서 보관자에 있어서,

송수신기; 및

상기 송수신기와 연결된 프로세서를 포함하며, 상기 프로세서는,

신뢰 당사자로부터, VP(verifiable presentation) 프로파일을 포함하는 정보주체의 신원증명 요청 신호를 수신하고,

기 저장된 정보주체의 신원정보 및 상기 VP 프로파일을 기반으로 상기 정보주체의 VP를 생성하고; 및
 검증 에이전트에게, 상기 생성된 VP를 포함하는 검증 요청 신호를 송신하도록 제어하며,
 상기 검증 요청 신호는 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 요청하는 신호이고,
 상기 정보주체의 신원증명 요청 신호는, 상기 정보주체의 신원정보에 대한 보관증명서를 더 포함하며,
 상기 보관증명서는, 상기 보관자가 상기 정보주체의 신원정보를 보관함을 나타내는 정보, 또는 상기 보관자가
 상기 정보주체로부터 상기 신원정보의 관리 권한을 위임받았음을 나타내는 정보 중 적어도 하나를 포함하는 보
 관자.

청구항 12

청구항 11에 있어서,
 상기 프로세서는,
 상기 VP 프로파일을 VP 프로파일 공유 원장에 등록하고,
 상기 VP 프로파일은, 신원증명에 필요한 클레임 목록을 포함하는 보관자.

청구항 13

청구항 12에 있어서,
 상기 프로세서는,
 상기 검증 에이전트로부터 상기 VP 프로파일의 등록을 요청받고,
 상기 검증 에이전트는, 상기 보관자의 상기 VP 프로파일의 수신 상태를 모니터링하는, 보관자.

청구항 14

삭제

청구항 15

청구항 11에 있어서,
 상기 프로세서는,
 상기 보관증명서를 기반으로, 상기 정보주체의 신원을 확인한 후, 상기 VP를 생성하는, 보관자.

청구항 16

청구항 11에 있어서,
 상기 프로세서는,
 상기 정보주체로부터 신원정보 및 신원정보에 대한 관리 권한을 위임받고,
 상기 신원정보에 대한 보관증명서를 상기 정보주체에게 발급하는, 보관자.

청구항 17

분산원장 기반 신원증명 시스템에서 검증 에이전트에 있어서,

송수신기; 및

상기 송수신기와 연결된 프로세서를 포함하며, 상기 프로세서는,

보관자로부터 상기 보관자에 의해 생성된 VP(verifiable presentation)에 대한 검증을 요청받고,

VP 프로파일 공유 원장에 등록된 VP 프로파일을 획득하고,

상기 VP 프로파일을 기반으로 신원증명에 필요한 클레임 목록을 확인하고,

상기 신원증명에 필요한 클레임 목록을 기반으로 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 수행하도록 제어하며,

상기 VP는 상기 보관자에서 신뢰 당사자로부터 수신한 보관증명서에 기반하여 정보주체의 신원이 확인된 이후에 생성되며,

상기 보관증명서는, 상기 보관자가 상기 정보주체의 신원정보를 보관함을 나타내는 정보, 또는 상기 보관자가 상기 정보주체로부터 상기 신원정보의 관리 권한을 위임받았음을 나타내는 정보 중 적어도 하나를 포함하는 검증 에이전트.

청구항 18

청구항 17에 있어서,

상기 프로세서는, 상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하는지 여부를 확인하는 검증 에이전트.

청구항 19

청구항 17에 있어서,

상기 프로세서는, 상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하는 경우, 상기 보관자에게 VP 재생성을 요청하고,

상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하지 아니하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하지 아니하는 경우, 보관자에게 VP를 제공하는 검증 에이전트.

청구항 20

분산원장 기반 신원증명 시스템에 있어서,

신원정보에 대한 보관증명서를 포함하는 서비스 제공 요청 신호를 신뢰 당사자에게 송신하는 정보주체;

상기 보관증명서 및 VP(verifiable presentation) 프로파일을 포함하는 정보주체의 신원증명 요청 신호를 보관자에게 송신하는 신뢰 당사자;

상기 정보주체의 신원정보를 저장하고, 상기 정보주체의 신원증명 요청 신호에 응답하여, 상기 정보주체의 신원정보 및 상기 VP 프로파일을 기반으로 상기 정보주체의 VP를 생성하는 보관자; 및

상기 보관자에서 생성된 VP의 클레임 제공 범위를 검증하는 검증 에이전트를 포함하며,

상기 정보주체의 신원증명 요청 신호는, 상기 정보주체의 신원정보에 대한 보관증명서를 더 포함하며,

상기 보관증명서는, 상기 보관자가 상기 정보주체의 신원정보를 보관함을 나타내는 정보, 또는 상기 보관자가 상기 정보주체로부터 상기 신원정보의 관리 권한을 위임받았음을 나타내는 정보 중 적어도 하나를 포함하는, 분산원장 기반 신원증명 시스템.

발명의 설명

기술 분야

[0001] 본 개시는 분산원장 기반 신원증명 시스템에 관한 것으로, 특히, 정보주체의 신원정보를 보호하기 위한 장치 및 방법에 관한 것이다.

배경 기술

[0002] 기존의 신원 인증 방식은 중앙집중형 인증 시스템을 통해 이루어졌다. 중앙집중형 인증 시스템은 정보주체가 신원 인증을 요청하는 경우, 정보주체의 개인정보를 대신 관리 및 인증하는 기능을 제공한다. 그러나, 기존의 신원 인증 방식은 현존하는 중앙집중형 인증 시스템이 정보주체의 개인정보를 이용함으로써 수익을 얻는 과정에서 논란이 발생하는 문제가 존재한다. 이와 같은 기존 신원 인증 시스템의 개인정보 침해 우려를 해결하고자 등장한 개념이 분산형 신원 인증 방식인 분산형 인증 시스템이다. 분산형 신원 인증 방식은, 인증이 필요할 때 마다 검증기관에서 요구하는 개인정보를 정보주체가 직접 선택하여 제출해야 한다. 대부분의 사용자는 이러한 분산형 신원 인증 방식에서 강조하는 개인정보를 보호하기 위한 방식에 대한 번거로움을 호소하고 있는 실정이다.

발명의 내용

해결하려는 과제

- [0003] 본 개시는 분산원장 기반 신원증명 시스템에서 신원정보를 보호하기 위한 방법 및 장치를 제공할 수 있다.
- [0004] 본 개시는 분산원장 기반 신원증명 시스템에서 보관자를 이용하여 정보주체의 신원정보를 보관 및 관리하기 위한 방법 및 장치를 제공할 수 있다.
- [0005] 본 개시는 분산원장 기반 신원증명 시스템에서 보관자를 이용하여 정보주체의 신원인증을 수행하기 위한 방법 및 장치를 제공할 수 있다.
- [0006] 본 개시는 분산원장 기반 신원증명 시스템에서 보관자를 통해 신뢰 가능한 VP(verifiable presentation)를 생성하기 위한 방법 및 장치를 제공할 수 있다.
- [0007] 본 개시는 분산원장 기반 신원증명 시스템에서 보관자가 제출하는 VP를 검증하기 위한 방법 및 장치를 제공할 수 있다.
- [0008] 본 개시는 분산원장 기반 신원증명 시스템에서 보관자가 정보주체의 신원 정보에 대한 보관증명서를 발급하기 위한 방법 및 장치를 제공할 수 있다.
- [0009] 본 개시는 분산원장 기반 신원증명 시스템에서 보관자가 수신한 VP 프로파일을 공유 원장에 등록함으로써, 신뢰 당사자가 요청한 클레임에 대해 블록체인 네트워크 참여자가 공유할 수 있도록 하기 위한 방법 및 장치를 제공할 수 있다.
- [0010] 본 개시는 분산원장 기반 신원증명 시스템에서 공유 원장에 등록된 VP 프로파일을 기반으로 VP에 포함된 클레임에 대한 제공 범위를 검증하기 위한 방법 및 장치를 제공할 수 있다.
- [0011] 본 개시는 분산원장 기반 신원증명 시스템에서 신뢰기관의 신뢰기관 목록을 통해 발급기관이 발급하는 VC(verifiable credential)에 대한 신뢰성을 부여하기 위한 방법 및 장치를 제공할 수 있다.
- [0012] 본 개시는 분산원장 기반 신원증명 시스템에서 VC의 상태를 포함하는 VC 발급 정보를 분산원장 저장소에 등록하기 위한 방법 및 장치를 제공할 수 있다.
- [0013] 본 개시는 분산원장 기반 신원증명 시스템에서 보관자가 정보주체의 신원정보를 이용하여 정보주체의 신원을 증명하는 과정을 모니터링함으로써 신원정보를 보호하기 위한 방법 및 장치를 제공할 수 있다.
- [0014] 본 개시에서 이루고자 하는 기술적 목적들은 이상에서 언급한 사항들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 이하 설명할 본 개시의 실시예들로부터 본 개시의 기술 구성이 적용되는 기술분야에서 통상의 지식을 가진 자에 의해 고려될 수 있다.

과제의 해결 수단

[0015] 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 보관자의 방법은, 신뢰 당사자로부터, VP(verifiable presentation) 프로파일을 포함하는 정보주체의 신원증명 요청 신호를 수신하는 단계, 기 저장된 정보주체의 신

원정보 및 상기 VP 프로파일을 기반으로 상기 정보주체의 VP를 생성하는 단계, 및 검증 에이전트에게, 상기 생성된 VP를 포함하는 검증 요청 신호를 송신하는 단계를 포함하며, 상기 검증 요청 신호는 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 요청하는 신호일 수 있다.

[0016] 일 실시예에 따르면, 상기 VP 프로파일을 VP 프로파일 공유 원장에 등록하는 단계를 더 포함하며, 상기 VP 프로파일은, 신원증명에 필요한 클레임 목록을 포함할 수 있다.

[0017] 일 실시예에 따르면, 상기 검증 에이전트로부터 VP 프로파일 등록을 요청받는 단계를 더 포함하며, 상기 검증 에이전트는, 상기 보관자의 VP 프로파일 수신 상태를 모니터링할 수 있다.

[0018] 일 실시예에 따르면, 상기 정보주체의 신원증명 요청 신호는, 상기 정보주체의 신원정보에 대한 보관증명서를 더 포함하며, 상기 보관증명서는, 상기 보관자가 상기 정보주체의 신원정보를 보관함을 나타내는 정보, 또는 상기 보관자가 상기 정보주체로부터 상기 신원정보의 관리 권한을 위임받았음을 나타내는 정보 중 적어도 하나를 포함할 수 있다.

[0019] 일 실시예에 따르면, 상기 보관증명서를 기반으로, 상기 정보주체의 신원을 확인하는 단계를 더 포함하며, 상기 VP는 상기 정보주체의 신원이 확인된 후에 생성될 수 있다.

[0020] 일 실시예에 따르면, 상기 정보주체로부터 신원정보 및 신원정보에 대한 관리 권한을 위임받는 단계, 및 상기 신원정보에 대한 보관증명서를 상기 정보주체에게 발급하는 단계를 더 포함할 수 있다.

[0021] 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 검증 에이전트의 방법은, 보관자로부터 VP에 대한 검증을 요청받는 단계, VP 프로파일 공유 원장에 등록된 VP 프로파일을 획득하는 단계, 상기 VP 프로파일을 기반으로 신원증명에 필요한 클레임 목록을 확인하는 단계, 및 상기 신원증명에 필요한 클레임 목록을 기반으로 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 수행하는 단계를 포함할 수 있다.

[0022] 일 실시예에 따르면, 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 수행하는 단계는, 상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하는지 여부를 확인하는 단계를 포함할 수 있다.

[0023] 일 실시예에 따르면, 상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하는 경우, 상기 보관자에게 VP 재생성을 요청하는 단계를 더 포함할 수 있다.

[0024] 일 실시예에 따르면, 상기 VP가 상기 신원증명에 필요한 클레임을 중복으로 포함하지 아니하거나, 상기 신원증명에 필요하지 않은 다른 클레임을 더 포함하지 아니하는 경우, 검증 기관에 VP를 제출하는 단계를 더 포함할 수 있다.

[0025] 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 보관자는, 송수신기, 및 상기 송수신기와 연결된 프로세서를 포함하며, 상기 프로세서는, 신뢰 당사자로부터, VP 프로파일을 포함하는 정보주체의 신원증명 요청 신호를 수신하고, 기 저장된 정보주체의 신원정보 및 상기 VP 프로파일을 기반으로 상기 정보주체의 VP를 생성하고, 및 검증 에이전트에게, 상기 생성된 VP를 포함하는 검증 요청 신호를 송신하도록 제어하며, 상기 검증 요청 신호는 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 요청하는 신호일 수 있다.

[0026] 일 실시예에 따르면, 분산원장 기반 신원증명 시스템에서 검증 에이전트는, 송수신기, 및 상기 송수신기와 연결된 프로세서를 포함하며, 상기 프로세서는, 보관자로부터 VP에 대한 검증을 요청받고, VP 프로파일 공유 원장에 등록된 VP 프로파일을 획득하고, 상기 VP 프로파일을 기반으로 신원증명에 필요한 클레임 목록을 확인하고, 상기 신원증명에 필요한 클레임 목록을 기반으로 상기 VP에 포함된 클레임의 제공 범위에 대한 검증을 수행하도록 제어할 수 있다.

[0027] 일 실시예에 따른 분산원장 기반 신원증명 시스템은, 신원정보에 대한 보관증명서를 포함하는 서비스 제공 요청 신호를 신뢰 당사자에게 송신하는 정보주체, 상기 보관증명서 및 VP 프로파일을 포함하는 정보주체의 신원증명 요청 신호를 보관자에게 송신하는 신뢰 당사자, 상기 정보주체의 신원정보를 저장하고, 상기 정보주체의 신원증명 요청 신호에 응답하여, 상기 정보주체의 신원정보 및 상기 VP 프로파일을 기반으로 상기 정보주체의 VP를 생성하는 보관자, 및 상기 보관자에서 생성된 VP의 클레임 제공 범위를 검증하는 검증 에이전트를 포함할 수 있다.

발명의 효과

[0028] 본 개시의 실시예에 따르면, 신원정보의 도난, 분실, 및/또는 유출 등을 방지하고, 개인정보 침해를 예방할 수

있다.

[0029] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0030] 도 1은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템 구조도이다.

도 2는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 제공되는 서비스의 예를 도시한다.

도 3은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 정보주체 신원정보 보관 서비스 개요를 도시한다.

도 4는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 정보주체 신원정보 보관 절차의 예를 도시한다.

도 5는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 정보주체의 절차의 예를 도시한다.

도 6은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 발급기관의 절차의 예를 도시한다.

도 7은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 신뢰기관의 절차의 예를 도시한다.

도 8은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 보관자의 절차의 예를 도시한다.

도 9는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 정보주체의 신원증명 서비스 개요를 도시한다.

도 10은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명 절차의 예를 도시한다.

도 11은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명을 위한 보관자의 절차의 예를 도시한다.

도 12는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명을 위한 검증 에이전트의 절차의 예를 도시한다.

도 13은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명을 위한 검증기관의 절차의 예를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0031] 본 개시는 다양한 변형을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 개시를 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 개시의 사상 및 기술 범위에 포함되는 모든 변형, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다. 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다. 후술하는 예시적 실시예들에 대한 상세한 설명은, 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 실시예를 실시할 수 있기에 충분하도록 상세히 설명된다. 다양한 실시예들은 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예에 관련하여 본 개시의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 실시예의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 예시적 실시예들의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다.

[0032] 본 개시에서 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기

용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 개시의 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.

[0033] 본 개시의 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있으나, 중간에 다른 구성 요소가 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.

[0034] 본 개시의 실시예에 나타나는 구성부들은 서로 다른 특징적인 기능들을 나타내기 위해 독립적으로 도시되는 것으로, 각 구성부들이 분리된 하드웨어나 하나의 소프트웨어 구성단위로 이루어짐을 의미하지 않는다. 즉, 각 구성부는 설명의 편의상 각각의 구성부로 나열하여 포함한 것으로 각 구성부 중 적어도 두 개의 구성부가 합쳐져 하나의 구성부로 이루어지거나, 하나의 구성부가 복수 개의 구성부로 나뉘어져 기능을 수행할 수 있고 이러한 각 구성부의 통합된 실시예 및 분리된 실시예도 본 개시의 본질에서 벗어나지 않는 한 본 개시의 권리범위에 포함된다.

[0035] 본 개시에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 개시를 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 개시에서, "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. 즉, 본 개시에서 특정 구성을 "포함"한다고 기술하는 내용은 해당 구성 이외의 구성을 배제하는 것이 아니며, 추가적인 구성이 본 개시의 실시 또는 본 개시의 기술적 사상의 범위에 포함될 수 있음을 의미한다.

[0036] 본 개시의 일부의 구성 요소는 본 개시에서 본질적인 기능을 수행하는 필수적인 구성 요소는 아니고 단지 성능을 향상시키기 위한 선택적 구성 요소일 수 있다. 본 개시는 단지 성능 향상을 위해 사용되는 구성 요소를 제외한 본 개시의 본질을 구현하는데 필수적인 구성부만을 포함하여 구현될 수 있고, 단지 성능 향상을 위해 사용되는 선택적 구성 요소를 제외한 필수 구성 요소만을 포함한 구조도 본 개시의 권리범위에 포함된다.

[0037] 이하, 도면을 참조하여 본 개시의 실시 형태에 대하여 구체적으로 설명한다. 본 명세서의 실시예를 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 명세서의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략하고, 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성 요소에 대해서 중복된 설명은 생략한다.

[0038] 본 개시는 분산원장 기술 기반의 신원증명 시스템에서 정보주체의 신원정보를 보호하기 위한 서비스를 제공하는 방법 및 장치에 관한 것이다. 구체적으로, 본 개시는 분산원장 기술 기반의 신원증명 시스템에서 보관자를 통해 신원정보를 보관 및 관리하고, 이를 기반으로 정보주체의 신원을 증명하는 방법 및 장치에 대해 설명한다. 또한, 본 개시는 분산원장 기술 기반의 신원증명 시스템에서 분산원장 기술을 통해 요청된 클레임 목록인 VP 프로파일을 공유하고, 공유된 VP 프로파일을 이용하여 정보주체의 신원정보를 보호하는 방법 및 장치에 대해 설명한다. 즉, 본 개시는 분산원장 기술, 분산신원 인증, 분산형 ID(DID) 및/또는 개인정보 보호에 관한 것이다.

[0039] 탈중앙화된 신원관리 서비스 모델은 신원증명을 활용하는 사례에 따라 기본 모델, 수탁 및 위임 모델, 셀프 발행 모델로 구분된다. 수탁 및 위임 모델 형태로 탈중앙화된 신원을 관리하는 서비스에서는 정보주체의 신원정보를 보관 및 관리하기 위한 보관자가 등장한다. 보관자는 기존의 분산형 신원 인증 방식에서 사용자가 매번 개인 정보를 직접 선택 및 제출해야 하는 번거로움을 해결하기 위해 제안된 기관으로서, 사용자로부터 사용자의 신원 정보에 대한 보관 및 관리 권한을 위임받고, 검증기관이 요구하는 사용자의 개인정보를 대신 선택하여 및 제출하는 기능을 수행한다. 즉, 수탁 및 위임 모델에서 보관자는 사용자인 정보주체를 대신하여 정보주체의 신원을 증명하기 위해, 정보주체의 신원정보를 검증기관에 전달한다. 이러한 과정에서 보관자가 서비스 제공을 위해 요청된 신원정보를 필요 이상으로 제출하는 경우, 개인정보의 노출 및 유출로 인한 침해가 발생할 수 있다. 그러나, 현재 분산형 인증 시스템에서 신원증명 시, 보관자가 정보주체의 개인정보를 최소화하여 제출하는지에 대한 확인 방법에는 한계가 있다. 이에 따라, 정보주체 대신 보관자가 검증기관과 개인정보를 주고받으며 인증하는 경우, 보관자가 제출하는 개인정보에 대한 모니터링하는 기능이 제안될 필요가 있다.

[0040] 따라서, 본 개시는 분산원장 기술 기반의 신원증명 시스템에서 정보주체의 신원정보를 보호하기 위한 방법 및

장치에 대해 설명한다. 구체적으로, 본 개시는 분산원장 기반 신원증명 시스템에서의 보관자를 이용하여 신원정보를 보관 및 관리하는 서비스를 제공하기 위한 방법 및 장치에 대해 설명한다. 즉, 본 개시는 신원정보를 보관하기 위해 기본 모델에 보관자를 추가한 수탁 및 위임 모델 구조를 활용하며, 검증 에이전트를 추가하여 신원정보에 대한 검증을 수행한다.

[0042] 도 1은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템 구조도이다.

[0043] 도 1을 참고하면, 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템(100)은 신뢰기관(110), 발급기관(120), 분산원장 저장소(130), 정보주체(140), 보관자(150), 검증 에이전트(160), 검증기관(170), 신뢰 당사자(180), 및 VP 프로파일 공유 원장(190)을 포함한다.

[0044] 신뢰기관(110)은 정보주체(140)의 신원 또는 자격에 대한 정보를 유지하는 기관으로서, 발급기관(120)을 신뢰할 수 있는 보증 기관에 해당한다. 발급기관(120)은 정보주체(140)의 신원을 보증하기 위한 VC(verifiable credential)를 생성하는 기관으로서, VC를 생성하고, 신뢰기관(110)을 통해 VC에 신뢰성을 부여하는 과정을 거침으로써 신뢰할 수 있는 발급기관임을 보증받는다. 또한, 발급기관(120)은 VC 발급 내역 정보 및 VC의 상태 정보를 포함하는 VC 발급 정보를 분산원장 저장소(130)에 등록한다. VC의 상태 정보는 VC가 유효한 상태인지 여부를 지시한다. 이와 같은 과정은 추후 검증기관이 클레임에 대한 유효성 검증을 수행하기 위해 활용된다.

[0045] 정보주체(140)는 특정 서비스를 이용하기 위해 신원을 증명해야 하는 주체에 해당한다. 정보주체(140)는 신원증명을 위해 발급기관(120)으로부터 VC를 발급받고, 자신의 개인키 및 VC를 포함하는 신원정보를 보관자(150)에게 전달한다. 즉, 정보주체(140)는 보관자(150)에게 신원정보를 전달하고, 신원정보의 보관 및 관리에 대한 권한을 위임한다. 보관자(150)는 정보주체(140)로부터 신원정보를 수신하고, 신원정보를 보관 및 관리에 대한 권한을 위임받음으로써, 정보주체(140)를 대신하여 정보주체(140)의 신원정보를 보관하고, 정보주체(140)에 대한 신원증명 절차를 수행한다. 보관자(150)는 정보주체(140)의 신원정보를 수신한 후, 정보주체(140)에게 신원정보의 보관 및 관리를 증명하는 보관증명서를 제공한다. 정보주체(140)는 추후 신뢰 당사자(180)에게 서비스 제공 요청 시, 보관자(150)로부터 제공받은 보관증명서를 함께 제출함으로써, 해당 보관자(150)를 통해 자신의 신원증명이 가능함을 알릴 수 있다. 이후 보관자(150)는 신뢰 당사자(180)로부터 수신되는 보관증명서를 통해 자신에게 권한을 위임한 정보주체(140)의 신원을 확인할 수 있다.

[0046] 신뢰 당사자(180)는 정보주체(140)에게 서비스를 제공하기 위한 주체에 해당한다. 신뢰 당사자(180)는 정보주체(140)로부터 서비스 제공을 요청받는다. 이때, 서비스 제공 요청은 보관증명서를 포함할 수 있다. 신뢰 당사자(180)는 서비스 제공 요청에 포함된 보관증명서를 기반으로 해당 보관자(150)로부터 정보주체(140)의 신원을 확인하고, 신원 확인이 완료된 정보주체(140)에게 서비스를 제공한다.

[0047] 검증 에이전트(160)는 보관자(150)를 모니터링하는 에이전트로서, 보관자(150)에게 VP 프로파일 공유 원장(190)에 VP 프로파일을 등록할 것을 요청한다. 또한, 검증 에이전트(160)는 보관자(150)에서 생성된 VP의 클레임 제공 범위를 검증하기 위한 기능을 수행한다. VP 프로파일은 신뢰 당사자가 요청하는 클레임 목록, 즉, 신원증명에 필요한 클레임 목록을 포함한다. 또한, VP는 VP 프로파일을 기반으로 필요한 클레임만을 조합하여 생성한 데이터이다. 보관자(150)는 신뢰 당사자(180)로부터 수신되는 VP 프로파일을 VP 프로파일 공유 원장에 등록함으로써, 블록체인 네트워크 참여자가 이를 공유할 수 있도록 한다. 또한, 보관자(150)는 VP 프로파일을 기반으로, 정보주체(140)의 신원정보에 포함된 다양한 정보들 중 신원증명에 필요한 최소한의 정보들을 선택 및 조합하여 VP를 생성하고, 생성된 VP를 검증기관(170)에 제출할 수 있다. 이때, 보관자(150)에 의해 생성된 VP가 요청된 신원정보 이외의 정보들을 포함할 수 있다. 따라서, 본 개시의 일 실시예에 따르면, 보관자(150)가 생성된 VP를 검증기관(170)에 전달하기 전에, 검증 에이전트(160)를 통해 해당 VP에 포함된 신원정보인 클레임의 제공 범위에 대한 검증을 수행한다.

[0048] VP 프로파일이 VP 프로파일 공유 원장에 등록된 경우, 블록체인 네트워크 참여자는 신원증명을 위해 신뢰 당사자(180)로부터 요청된 클레임 목록, 즉, VP 프로파일을 확인할 수 있다. 이후, 보관자(150)가 검증기관(170)에 VP를 제출하고자 하는 경우, 검증 에이전트(160)는 VP 프로파일 공유 원장(190)에 등록된 VP 프로파일을 기반으로 보관자(150)에 의해 생성된 VP에 정보주체의 신원정보가 과도하게 포함되어 있지 않은지에 대한 검증을 수행한다.

[0049] 검증기관(170)은 보관자(150)가 정보주체(140)를 대신하여 제출한 VP를 기반으로 정보주체(140)의 신원증명을 검증하는 기관에 해당한다. 검증기관(170)은 전달받은 VP에 포함된 정보주체(140)의 클레임을 검증하는 절차를 수행한다. 검증기관(170)은 분산원장 저장소(130)를 통해 요청된 클레임에 대한 VC 발급 정보를 확인함으로써

모든 클레임에 대한 검증을 완료하고, 보관자(150)에게 검증 결과를 전달한다. 이때 분산원장 저장소(130)에는 클레임이 포함된 VC를 발급한 발급기관(120)의 정보인 VC 발급 정보가 등록되어 있다.

- [0050] 도 1을 참고하여 설명된 신뢰기관(110), 발급기관(120), 분산원장 저장소(130), 정보주체(140), 보관자(150), 검증 에이전트(160), 검증기관(170), 신뢰 당사자(180), 및 VP 프로파일 공유원장(190) 각각은 해당 장치의 동작을 제어하는 프로세서 및 신호를 송수신하는 송수신기를 포함할 수 있다. 이때, 프로세서는 송수신기를 제어할 수 있다. 즉, 도 1에서 설명된 각 장치들은 프로세서 및 송수신기를 포함함으로써, 도 1에서 설명된 서비스, 기능 및/또는 동작과 후술되는 도 2 내지 도 13에서 설명되는 서비스, 기능 및/또는 동작을 지원 및/또는 수행할 수 있다.
- [0051] 도 2는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 제공되는 서비스의 예를 도시한다.
- [0052] 도 2를 참고하면, 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템(100)은 정보주체 신원정보 보관 서비스(210) 및 정보주체 신원증명 서비스(220)를 제공한다.
- [0053] 정보주체 신원정보 보관 서비스(210)는 정보주체가 신원을 증명하기 위해 발급기관으로부터 신원정보를 확인받고, 이를 기반으로 VC를 발급받는 과정을 포함한다. 또한, 정보주체 신원정보 보관 서비스(210)는 정보주체의 VC를 보관자에게 수탁하고, 보관자에게 정보주체의 신원정보에 대한 보관 및 관리 권한을 위임함으로써, 보관자가 정보주체의 신원정보를 보관 및 관리할 수 있도록 하는 서비스를 포함한다.
- [0054] 정보주체 신원증명 서비스(220)는 보관자가 정보주체를 대신하여 정보주체의 신원정보를 기반으로 정보주체의 신원을 증명하는 과정을 포함한다. 즉, 보관자는 신뢰 당사자로부터 요청된 자격 증명을 위해, 정보주체를 대신하여 신원정보를 선택 및 조합하고, 이를 검증기관에게 제출하는 대리인의 역할을 수행한다. 정보주체 신원증명 서비스(220)는 VP 프로파일 공유 원장과 검증 에이전트를 통해 정보주체의 신원정보를 보호하는 서비스를 더 포함한다.
- [0055] 도 3은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 정보주체 신원정보 보관 서비스 개요를 도시한다.
- [0056] 도 3을 참고하면, 정보주체 신원정보 보관 서비스(210)는 정보주체의 VC 발급(310), 정보주체의 신원정보 관리 권한 위임(320) 과정을 포함한다. 즉, 정보주체는 발급기관 및 신뢰기관을 통해 VC를 발급받고, 이후 보관자에게 발급받은 VC 및 자신의 개인키를 포함하는 신원정보를 수탁함으로써, 정보주체의 신원정보 보관 및 관리 권한을 위임한다. 보관자는 정보주체의 신원 정보 보관 및 관리 권한을 위임받고, 정보주체의 신원정보에 대한 보관증명서를 정보주체에게 발급한다. 즉, 본 개시의 일 실시예에 따르면, 정보주체가 보관자에게 자신의 신원정보를 수탁하고 권한을 위임함으로써, 보관자가 정보주체 대신 정보주체의 신원정보를 보관 및 관리할 수 있다.
- [0057] 도 4는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 정보주체 신원정보 보관 절차의 예를 도시한다.
- [0058] 도 4를 참고하면, 정보주체(140)는 신뢰 당사자에게 신원을 증명함으로써 특정 서비스를 이용할 수 있다. 이를 위해, S401 단계에서, 정보주체(140)는 발급기관(120)에 정보주체(140)의 신원을 증명할 수 있는 정보를 포함하는 VC를 요청하는 신호를 송신한다. 이때, VC 요청 신호는 정보주체의 DID를 포함할 수 있다.
- [0059] 정보주체(140)로부터 VC 요청 신호를 수신한 발급기관(120)은 S403 단계에서 정보주체(140)의 공개키를 획득하고, 이를 기반으로 정보주체(140)의 신원을 확인하고, S405 단계에서 요청된 신원정보를 포함하는 VC를 생성한다. 이때, 생성된 VC는 발급기관(120)의 개인키로 서명될 수 있다.
- [0060] S407 단계에서, 발급기관(120)은 신뢰기관(110)에게 VC에 대한 신뢰성 부여를 요청하는 신호를 송신한다. VC에 대한 신뢰성 부여를 요청하는 신호는 발급기관(120)에서 생성된 VC 및 발급기관(120)의 공개키를 포함할 수 있다.
- [0061] S409 단계에서, 신뢰기관(110)은 VC의 신뢰성을 검증 및 부여한다. 즉, 신뢰기관(110)은 발급기관(120)의 공개키를 이용하여 VC의 유효성을 검증함으로써 신뢰 가능한 VC임을 검증할 수 있다. S411 단계에서, 신뢰기관(110)은 VC의 신뢰성 부여 결과를 발급기관(120)에게 반환한다.
- [0062] 신뢰기관(110)을 통해 VC의 신뢰성을 검증받은 발급기관(120)은 S413 단계에서 VC 발급 정보 및 발급기관(120)의 공개키를 분산원장 저장소(130)에 등록하고, S415 단계에서 해당 VC를 정보주체(140)에게 발급한다. VC 발급 정보는 VC의 발급상태, 폐기상태 등과 같은 VC의 상태를 비롯한 부가 정보를 포함할 수 있다.

- [0063] VC를 발급받은 정보주체(140)는 S417 단계에서, 보관자(150)에게 VC 보관 및 관리 권한을 위임한다. 즉, 정보주체(140)는 발급된 VC 및 개인키를 포함하는 신원정보를 보관자(150)에게 송신함으로써, 보관자(150)에게 신원정보를 수탁하고, 신원정보에 대한 보관 및 관리 권한을 위임할 수 있다. 일 실시예에 따르면, 정보주체(140)가 보관자(150)에게 송신하는 신원정보는 정보주체(140)가 가진 저장된 VC, VP, 클레임, 공개키, 또는 개인키 중 적어도 하나를 포함할 수 있다.
- [0064] S419 단계에서, 보관자(150)는 정보주체(140)의 신원정보에 대한 보관증명서를 생성하고, S421 단계에서 보관증명서를 정보주체(140)에게 발급한다. 이후, 보관자(150)는 신뢰 당사자(180)로부터 정보주체에 대한 신원증명을 요청받고, 정보주체를 대신하여 신원증명에 필요한 동작을 수행할 수 있다. 즉, 신뢰 당사자는 정보주체(140)의 보관증명서를 이용하여 보관자(150)에게 정보주체(140)에 대한 신원증명을 요청할 수 있다.
- [0065] 도 5는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 정보주체의 절차의 예를 도시한다. 도 5의 정보주체는 도 1 및 도 4의 정보주체(140)일 수 있다.
- [0066] 도 5를 참고하면, S501 단계에서, 정보주체는 발급기관에게 VC 발급을 요청한다. 이때, VC 발급 요청은 정보주체의 DID를 포함할 수 있다.
- [0067] S503 단계에서, 정보주체는 공개키 확인 요청이 수신되는지 여부를 결정한다. 즉, 발급기관에서 정보주체의 공개키 오류에 의해 유효성 검증이 실패된 경우, 정보주체는 발급기관으로부터 공개키 확인 요청 신호를 수신할 수 있다.
- [0068] 공개키 확인 요청이 수신되는 경우, S501단계에서, 정보주체는 정보주체의 공개키를 포함하는 VC 발급 요청 신호를 발급기관에게 재송신할 수 있다.
- [0069] 공개키 확인 요청이 수신되지 아니하는 경우, S505단계에서, 정보주체는 VC가 발급되는지 여부를 확인한다. 즉, 정보주체는 발급기관으로부터 VC가 발급되는지 여부를 확인한다. VC가 발급되지 아니하는 경우, 정보주체는 S501 단계를 재수행한다.
- [0070] VC가 발급되는 경우, S507 단계에서, 정보주체는 보관자에게 VC 보관 및 관리 권한을 위임한다. 즉, 정보주체는 발급기관으로부터 수신된 VC 및 개인키를 포함하는 신원정보를 보관자에게 송신하고, 보관자에게 신원정보에 대한 보관 및 관리 권한을 위임할 수 있다.
- [0071] S509 단계에서, 정보주체는 보관자로부터 보관증명서를 수신한다. 보관증명서는, 해당 보관자가 정보주체의 신원정보를 보관 및 관리함을 증명하는 데이터일 수 있다.
- [0072] 도 6은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 발급기관의 절차의 예를 도시한다. 도 6의 발급기관은 도 1 및 도 4의 발급기관(120)일 수 있다.
- [0073] 도 6을 참고하면, S601 단계에서, 발급기관은 정보주체로부터 VC 발급 요청을 수신한다. VC 발급 요청은 정보주체의 DID를 포함할 수 있다.
- [0074] S603 단계에서, 발급기관은 정보주체의 유효성 검증이 성공되는지 여부를 결정한다. 즉, 발급기관은 정보주체의 DID를 기반으로 분산원장 저장소로부터 정보주체의 DID 문서를 확인하고, DID 문서를 기반으로 정보주체의 공개키를 획득한다. 발급기관은 정보주체의 공개키를 기반으로 정보주체의 유효성을 검증함으로써, 정보주체의 신원을 확인할 수 있다. 만일, 정보주체의 공개키 오류와 같은 이유로 정보주체의 유효성을 검증할 수 없는 경우, S613단계에서, 발급기관은 정보주체에게 공개키 확인을 요청한다.
- [0075] 반면, 정보주체의 유효성 검증이 성공된 경우, S605 단계에서, 발급기관은 정보주체에 대한 VC를 생성한다. 즉, 정보주체의 신원이 확인된 경우, 발급기관은 정보주체가 요청하는 신원정보를 포함하는 VC를 생성한다. 이때, 발급기관은 발급기관의 개인키를 이용하여 VC에 전자서명을 수행한다.
- [0076] S607 단계에서, 발급기관은 신뢰기관을 통해 VC의 신뢰성을 확인한다. 즉, 발급기관은 발급기관의 개인키로 서명된 VC를 신뢰기관에게 전달하여 VC의 신뢰성 부여를 요청하고, 신뢰기관으로부터 VC 신뢰성 부여 결과를 수신한다.
- [0077] 신뢰기관을 통해 VC의 신뢰성이 확인되면, S609 단계에서, 발급기관은 정보주체에게 VC를 발급한다. 즉, 발급기관은 신뢰성이 부여된 VC를 정보주체에게 전달할 수 있다.
- [0078] S611 단계에서, 발급기관은 분산원장 저장소에 VC 발급 정보를 등록한다. VC 발급 정보는, 신뢰성이 검증된 VC

의 현재 상태 정보를 포함할 수 있다.

- [0079] 도 7은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 신뢰기관의 절차의 예를 도시한다. 도 7의 신뢰기관은 도 1 및 도 4의 신뢰기관(110)일 수 있다.
- [0080] 도 7을 참고하면, S701 단계에서, 신뢰기관은 발급기관으로부터 VC의 신뢰성 부여 요청을 수신한다. 즉, VC의 신뢰성 부여 요청 신호는 발급기관의 개인키로 서명된 VC를 포함할 수 있다.
- [0081] S703 단계에서, 신뢰기관은 발급기관의 유효성 검증이 성공되는지 여부를 확인한다. 신뢰기관은 분산원장 저장소에서 발급기관의 DID 문서를 통해 발급기관의 공개키를 획득하고, 획득된 발급기관의 공개키를 기반으로 발급기관의 유효성을 검증할 수 있다.
- [0082] 발급기관의 유효성 검증이 실패되는 경우, S709 단계에서, 신뢰기관은 검증 실패를 반환한다. 예를 들어, 신뢰기관은 발급기관의 공개키 오류와 같은 이유에 의해 발급기관의 유효성을 검증할 수 없는 경우, 발급기관에게 유효성 검증 실패를 나타내는 결과를 전달한다.
- [0083] 발급기관의 유효성 검증이 성공되는 경우, S705 단계에서, 신뢰기관은 발급기관의 정보를 신뢰기관 목록에 등록한다. 즉, 신뢰기관은 발급기관의 공개키에 기반하여 발급기관의 유효성이 검증된 경우, 신뢰기관 목록에 발급기관의 공개키를 등록함으로써, 해당 발급기관이 신뢰할 수 있는 기관임을 보증한다. 신뢰기관 목록은 신뢰기관이 보증하는 발급기관의 정보들을 포함하는 목록이다.
- [0084] S707 단계에서, 신뢰기관은 VC 신뢰성 부여 결과를 발급기관에게 전달한다.
- [0085] 도 8은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원정보 보관을 위한 보관자의 절차의 예를 도시한다. 도 8의 보관자는 도 1 및 도 4의 보관자(150)일 수 있다.
- [0086] 도 8을 참고하면, S801 단계에서, 보관자는 정보주체의 신원정보 보관 및 관리 권한을 획득한다. 즉, 보관자는 정보주체로부터 정보주체의 VC 및 개인키를 포함하는 신원정보를 수신함으로써, 이에 대한 보관 및 관리 권한을 획득할 수 있다.
- [0087] 보관자는 S803 단계에서 신원정보를 저장하고, S805단계에서 보관증명서를 생성 및 송신한다. 즉, 보관자는 정보주체의 신원정보를 보관 및 관리함을 증명하는 보관증명서를 생성하고, 생성된 보관증명서를 정보주체에게 발급할 수 있다. 보관증명서는 정보주체의 신원증명을 대신 수행할 보관자의 정보 및 정보주체가 보관자에게 권한을 위임한 사실에 대한 내용을 포함할 수 있다.
- [0088] 도 9는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 정보주체의 신원증명 서비스 개요를 도시한다.
- [0089] 도 9를 참고하면, 정보주체의 신원증명 서비스(220)는 검증 에이전트의 보관자 모니터링(910), 정보주체 신원증명을 위한 VP 검증(920) 과정을 포함한다. 즉, 정보주체의 신원증명 서비스(220)는 정보주체를 대신한 보관자가 정보주체의 신원을 확인하고, 신뢰 당사자로부터 요청되는 클레임을 포함한 VP를 생성 및 검증함으로써 정보주체의 신원을 증명하는 과정을 포함할 수 있다. 또한, 정보주체의 신원증명 서비스(220)는 검증 에이전트를 통해 VP에 포함된 클레임의 제공 범위를 검증하여 VP가 최소한의 클레임을 포함하도록 한 후, 검증기관을 통해 VP에 포함된 클레임의 유효성을 검증하는 과정을 포함한다.
- [0090] 도 10은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명 절차의 예를 도시한다.
- [0091] 도 10을 참고하면, S1001 단계에서, 정보주체(140)는 특정 서비스의 이용을 위해 신뢰 당사자(180)에게 서비스 제공을 요청한다. 이때, 정보주체(140)는 보관증명서를 함께 제출할 수 있다. 보관증명서는 정보주체(140)의 신원증명을 대신 수행해줄 보관자(150)의 정보 및 정보주체(140)가 보관자(150)에게 권한을 위임한 사실에 대한 내용을 포함할 수 있다.
- [0092] S1003 단계에서, 서비스 제공을 요청받은 신뢰 당사자(180)는 보관자(150)에게 정보주체의 신원증명을 요청한다. 즉, 신뢰 당사자(180)는 정보주체(140)로부터 수신된 보관증명서를 보관자(150)에게 제출함으로써, 정보주체(140)의 신원증명을 요청한다. 이때, 신뢰 당사자(180)는 보관증명서와 함께 VP 프로파일을 보관자(150)에게 제출할 수 있다. VP 프로파일은 신원증명을 위해 제출해야 할 정보주체의 클레임 목록을 포함한다.
- [0093] S1005 단계에서, 검증 에이전트(160)는 보관자(150)에게 VP 프로파일 수신 여부 확인 및 등록 요청을 송신한다. 즉, 검증 에이전트(160)는 보관자(150)를 주기적으로 모니터링함으로써, 보관자(150)가 VP 프로파일을 수신한

경우, 보관자에게 수신된 VP 프로파일을 VP 프로파일 공유 원장(190)에 등록할 것을 요청한다.

- [0094] S1007 단계에서, 보관자(150)는 신뢰 당사자(180)로부터 수신된 VP 프로파일을 VP 프로파일 공유 원장(190)에 등록할 수 있다. 즉, 보관자(150)는 검증 에이전트(160)의 요청에 따라 VP 프로파일을 VP 프로파일 공유 원장(190)에 등록함으로써, 블록체인 네트워크 참여자가 해당 내용을 공유할 수 있도록 한다.
- [0095] S1009 단계에서, 보관자(150)는 수신된 보관증명서를 기반으로 정보주체의 신원을 확인한다. 이후, 보관자(150)는 S1011 단계에서 VP를 생성한다. 즉, 보관자(150)는 VP 프로파일을 기반으로 신원증명을 위해 요청된 클레임을 정보주체의 VC로부터 확인하고, 확인된 클레임을 조합하여 VP를 생성한다.
- [0096] S1013 단계에서, 보관자(150)는 검증 에이전트(160)에게 VP에 포함된 클레임의 범위 검증을 요청한다. 즉, 보관자(150)는 생성된 VP를 검증 에이전트(160)에게 전달함으로써, 전달한 VP의 클레임 제공 범위에 대한 검증을 요청할 수 있다.
- [0097] S1015 단계에서, 검증 에이전트(160)는 VP 프로파일 공유 원장(190)에 VP 프로파일을 요청하고, S1017 단계에서 VP 프로파일을 획득한다. 이후, S1019 단계에서, 검증 에이전트(160)는 VP에 포함된 클레임 제공 범위를 검증한다. 즉, 검증 에이전트(160)는 VP 프로파일을 기반으로 신원증명을 위해 제공되어야 하는 클레임 목록을 확인한 후, 확인된 클레임 목록과 생성된 VP에 포함된 클레임들을 비교하여, VP가 최소한의 클레임을 포함하는지 확인한다. 만일, 생성된 VP가 VP 프로파일을 기반으로 확인된 클레임 목록보다 더 많은 클레임을 포함하는 경우, 검증 에이전트(160)는 S1021 단계에서 보관자(150)에게 VP 재생성을 요청하고, S1013 단계 내지 S1019 단계를 재수행할 수 있다. 이때, VP 재생성 요청은, VP 프로파일에 대한 정보를 포함할 수 있다.
- [0098] 반면, 생성된 VP가 VP 프로파일을 기반으로 확인된 클레임 목록에 해당하는 클레임만을 포함하는 경우, 검증 에이전트(160)는 보관자에서 생성된 VP의 클레임의 범위 검증이 성공된 것으로 결정하고, 보관자(150)에게 VP 클레임의 범위 검증이 성공적으로 완료되었음을 알릴 수 있다. S1023 단계에서, 보관자(150)는 검증기관(170)에 VP를 제출하고, 정보주체의 신원증명을 요청한다.
- [0099] 검증기관(170)은 S1025 단계 및 S1027 단계를 통해, 분산원장 저장소(130)에 등록된 VC 발급 정보를 기반으로 VP에 포함된 클레임을 확인하고, S1029 단계에서 등록된 클레임을 기반으로 보관자(150)에 의해 생성된 VP에 포함된 클레임의 유효성을 검증함으로써, 정보주체의 신원을 증명한다.
- [0100] 이후, 검증기관(170)은 S1031 단계에서, VP 검증 결과에 따른 정보주체의 신원증명 결과를 보관자(150)에게 응답하고, 보관자(150)는 S1033 단계에서 VP 검증 결과에 따른 정보주체의 신원증명 결과를 신뢰 당사자(180)에게 응답한다. 신뢰 당사자(180)는 정보주체의 신원증명 결과가 신원증명 성공을 지시하는 경우, S1035 단계에서 정보주체(140)에게 서비스를 제공한다.
- [0101] 도 11은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명을 위한 보관자의 절차의 예를 도시한다. 도 11의 보관자는 도 1, 도 4, 및 도 10의 보관자(150)일 수 있다.
- [0102] 도 11을 참고하면, S1101 단계에서, 보관자는 신뢰 당사자로부터 정보주체의 신원증명 요청을 수신한다. 이때, 신뢰 당사자로부터 수신되는 정보주체의 신원증명 요청은, 정보주체의 보관증명서 및 VP 프로파일을 포함할 수 있다. 이때, 정보주체의 보관증명서는 신뢰 당사자로부터 서비스를 제공받고자 하는 정보주체가 신뢰 당사자에게 송신함으로써, 신뢰 당사자를 통해 보관자에게 수신될 수 있다. VP 프로파일은 신원증명을 위해 필요한 클레임 목록을 포함한다.
- [0103] S1103 단계에서, 보관자는 검증 에이전트로부터 VP 프로파일 등록 요청을 수신한다. 즉, 보관자는 보관자를 모니터링하는 검증 에이전트로부터 VP 프로파일을 VP 프로파일 공유 원장에 등록할 것을 요청하는 신호를 수신한다.
- [0104] S1105 단계에서, 보관자는 VP 프로파일 공유 원장에 VP 프로파일을 등록한다. 이를 통해, 블록체인 네트워크 참여자가 신원증명을 위해 요청된 클레임 목록을 확인할 수 있도록 한다. 반면, 보관자가 VP 프로파일을 수신하지 못한 상태에서 검증 에이전트로부터 VP 프로파일 등록을 요청받은 경우, 보관자는 신뢰 당사자에게 VP 프로파일을 재요청함으로써, 필요한 클레임 목록을 확인할 수 있다.
- [0105] S1107 단계에서, 보관자는 정보주체의 신원을 확인한다. 즉, 보관자는 정보주체의 신원증명에 앞서, 정보주체의 신원을 확인할 수 있다. 보관자는 신뢰 당사자로부터 수신된 보관증명서를 기반으로, 정보주체의 신원을 확인할 수 있다. 즉, 보관증명서에는 보관자가 해당 정보주체의 신원정보를 보관함과 동시에 해당 정보주체로부터 신원정보의 관리 권한을 위임받은 사실이 명시되어 있으므로, 보관자는 이러한 정보를 기반으로 정보주체의 신원을

확인할 수 있다. 만일, 신뢰 당사자로부터 보관증명서가 수신되지 아니한 경우, 보관자는 신뢰 당사자에게 보관 증명서를 요청하여 신원을 확인할 수 있다.

- [0106] S1109 단계에서, 보관자는 VP 생성에 필요한 클레임이 존재하는지 여부를 확인한다. 보관자는 신뢰 당사자로부터 수신된 VP 프로파일을 기반으로 VP 생성에 필요한 클레임을 확인하고, 보관자가 보관 중인 신원정보에 해당 클레임이 존재하는지 여부를 확인할 수 있다.
- [0107] VP 생성에 필요한 클레임이 존재하지 아니한 경우, S1123 단계에서, 보관자는 정보주체를 통해 VC를 재발급한다. VC 재발급은 도 4에서 설명한 바와 같은 절차를 통해 수행될 수 있다.
- [0108] VP 생성에 필요한 클레임이 존재하는 경우, S1111 단계에서, 보관자는 VP를 생성한다. 즉, 보관자는 VP 프로파일을 기반으로 정보주체의 신원정보 중 VP 생성에 필요한 클레임을 선택 및 조합하여 VP를 생성한다.
- [0109] S1113 단계에서, 보관자는 검증 에이전트에게 VP 클레임 제공 범위에 대한 검증을 요청한다. 즉, 보관자는 검증 에이전트에게 생성된 VP에 포함된 클레임에 대한 제공 범위를 검증해줄 것을 요청할 수 있다.
- [0110] S1115 단계에서, 보관자는 검증 에이전트로부터 VP 재생성이 요청되는지 여부를 확인한다. 검증 에이전트로부터 VP 재생성이 요청되는 경우는 클레임이 과도하게 포함된 경우이며, S1117 단계에서, 보관자는 VP를 재생성한다. 이때, 보관자는 검증 에이전트로부터 VP 프로파일을 수신하고, 수신된 VP 프로파일을 기반으로 VP를 재생성할 수 있다.
- [0111] 검증 에이전트로부터 VP 재생성이 요청되지 아니하는 경우, S1119 단계에서, 보관자는 검증기관에게 VP의 유효성 검증을 요청하고, S1121 단계에서, VP 검증 결과가 수신되는지 여부를 확인한다. VP 검증 결과는 VP 검증에 따른 정보주체의 신원증명 성공 또는 실패 여부를 나타낼 수 있다.
- [0112] VP 검증 결과가 수신되는 경우, S1123 단계에서, 보관자는 VP 검증 결과를 기반으로 정보주체의 신원증명 결과를 신뢰 당사자에게 송신한다.
- [0113] 도 12는 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명을 위한 검증 에이전트의 절차의 예를 도시한다. 도 12의 검증 에이전트는 도 1, 및 도 10의 검증 에이전트(160)일 수 있다.
- [0114] 도 12를 참고하면, S1201 단계에서, 검증 에이전트는 보관자에게 VP 프로파일 등록을 요청한다. 검증 에이전트는 보관자를 모니터링함으로써, 보관자의 VP 프로파일을 수신 상태를 감지하고, 보관자에게 VP 프로파일 등록을 요청할 수 있다.
- [0115] S1203 단계에서, 검증 에이전트는 보관자로부터 VP에 포함된 클레임 제공 범위에 대한 검증이 요청되는지 여부를 확인한다. 검증 에이전트는 보관자로부터 보관자에 의해 생성된 VP가 수신되는 경우, VP에 포함된 클레임 제공 범위에 대한 검증이 요청되었음을 확인할 수 있다.
- [0116] VP에 포함된 클레임 제공 범위에 대한 검증이 요청되는 경우, S1205 단계에서, 검증 에이전트는 VP 프로파일 공유 원장으로부터 VP 프로파일을 획득한다. 즉, 검증 에이전트는 보관자가 VP 프로파일 공유 원장에 등록한 VP 프로파일을 확인할 수 있다.
- [0117] S1207 단계에서, 검증 에이전트는 VP 프로파일을 기반으로 보관자에 의해 생성된 VP에 포함된 클레임 제공 범위를 검증한다. 즉, 검증 에이전트는 VP 프로파일에서 요구하는 클레임 목록과 생성된 VP에 포함된 클레임들을 비교할 수 있다. 이를 통해, 검증 에이전트는 VP가 신원증명에 필요한 클레임을 중복으로 포함하는지, 또는 신원증명에 필요하지 않은 다른 클레임을 더 포함하는지 여부를 확인할 수 있다.
- [0118] S1209 단계에서, 검증 에이전트는 보관자에 의해 생성된 VP가 최소한의 클레임들을 포함하는지 여부를 판단한다. 만일, 생성된 VP가 신원증명에 필요한 클레임만을 중복없이 포함하는 경우, 검증 에이전트는 생성된 VP가 최소한의 클레임들을 포함하는 것으로 판단할 수 있다. 반면, 생성된 VP가 신원증명에 필요한 클레임을 중복으로 포함하거나, 신원증명에 필요하지 않은 다른 클레임을 더 포함하는 경우, 검증 에이전트는 생성된 VP가 최소한의 클레임들 이외에 추가 클레임을 포함하는 것으로 판단할 수 있다.
- [0119] 생성된 VP가 최소한의 클레임들 이외에 추가 클레임을 포함하는 경우, S1213 단계에서, 검증 에이전트는 보관자에게 VP 재생성을 요청하고, S1203 단계를 재수행한다. 즉, 생성된 VP가 VP 프로파일에서 요구하는 클레임 목록에 해당하는 클레임들 이외의 클레임을 더 포함하는 경우, 검증 에이전트는 보관자에게 VP가 불필요한 신원정보를 포함함을 알리고, VP 재생성을 요청할 수 있다. 이는, 보관자가 생성하는 VP로부터 신원정보가 과도하게 노출 및/또는 유출되는 것을 방지하기 위함이다.

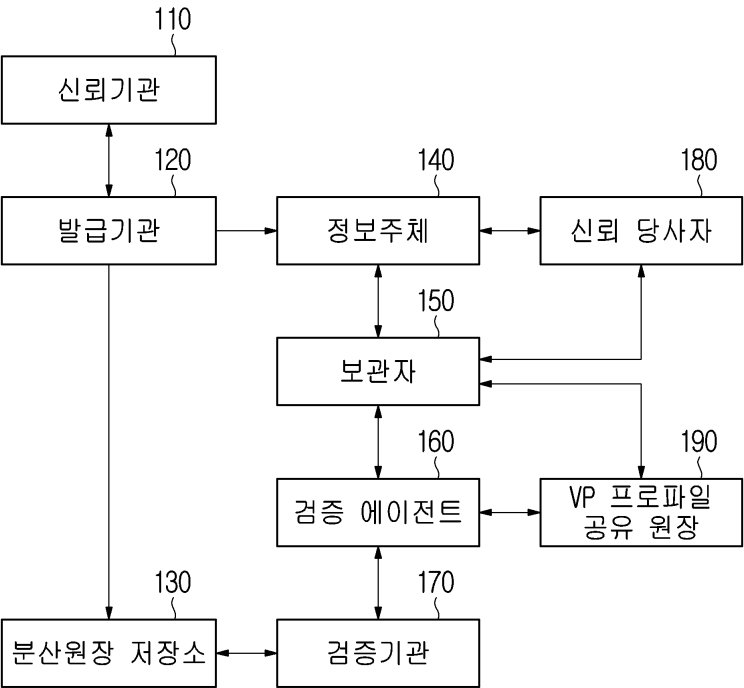
- [0120] 생성된 VP가 최소한의 클레임들만 포함하는 경우, S1211 단계에서, 검증 에이전트는 검증 기관에 VP를 제출하고, 정보주체의 신원증명을 요청한다.
- [0121] 도 13은 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 신원증명을 위한 검증기관의 절차의 예를 도시한다. 도 12의 검증기관은 도 1, 및 도 10의 검증 기관(170)일 수 있다.
- [0122] 도 13을 참고하면, S1301 단계에서, 검증기관은 검증 에이전트로부터 VP 및 정보주체의 신원증명 요청을 수신한다. 즉, 검증기관은 검증 에이전트로부터 보관자에 의해 생성된 VP를 수신하고, 해당 VP에 대한 정보주체의 신원증명을 요청받을 수 있다.
- [0123] S1303 단계에서, 검증기관은 VP의 클레임을 확인한다. 즉, 검증기관은 검증 에이전트로부터 수신된 VP에 포함된 클레임을 확인할 수 있다.
- [0124] S1305 단계에서, 검증기관은 VC 유효성 검증을 통해 VC가 유효한지 여부를 확인한다. 검증기관은 분산원장 저장소에 등록된 정보주체의 VC 발급 정보 중 해당 클레임을 포함하는 VC에 대한 VC 발급 정보를 통해 VC의 유효성을 검증할 수 있다.
- [0125] VC가 유효한 경우, S1307 단계에서, 검증기관은 보관자에게 정보주체의 신원증명이 완료되었음을 나타내는 결과를 전달할 수 있다.
- [0126] VC가 유효하지 아니한 경우, 즉, VC가 만료 및/또는 폐기 등에 의해 유효하지 아니한 경우, S1309 단계에서, 검증기관은 보관자에게 정보주체의 신원증명이 실패되었음을 나타내는 결과를 전달할 수 있다.
- [0127] 전술한 바와 같이, 본 개시의 일 실시예에 따른 분산원장 기반의 신원정보 보호 시스템은 정보주체가 보관자에게 신원정보를 수탁하고, 신원정보를 관리할 수 있는 권한을 위임함으로써, 보관자가 정보주체를 대신하여 정보주체의 신원정보를 보관 및 관리하는 구조를 가진다. 이때, 정보주체는 서비스를 제공받길 원하는 사용자를 의미한다. 본 개시의 일 실시예에 따른 분산원장 기반의 신원정보 보호 시스템은 정보주체에게 신원을 증명할 수 있도록 클레임을 포함한 VC를 발급해주는 발급기관, 발급기관의 신뢰성을 보장하는 신뢰기관, 발급기관이 VC를 발급한 후 VC의 상태를 포함한 VC 발급 정보를 저장하는 분산원장 저장소, 정보주체의 신원정보를 대신 보관 및 관리하는 보관자, 정보주체에게 서비스를 제공하는 신뢰 당사자, 보관자가 정보주체를 대신하여 정보주체의 신원을 증명하기 위해 만든 VP의 클레임 제공 범위를 검증하는 검증 에이전트, 신뢰 당사자가 정보주체의 신원증명을 위해 필요한 클레임을 목록화한 VP 프로파일을 등록하기 위한 VP 프로파일 공유 원장, 그리고 보관자가 제출한 VP의 클레임을 통해 정보주체의 신원을 증명하는 검증기관을 포함할 수 있다.
- [0128] 본 개시의 일 실시예에 따르면, 보관자는 정보주체의 신원정보를 관리할 수 있는 권한을 가짐에 따라, 해당 정보들을 악용할 가능성이 존재한다. 따라서, 본 개시의 일 실시예에 따른 분산원장 기반의 신원정보 보호 시스템은 검증 에이전트를 통해 보관자의 행동을 모니터링하고, 보관자가 정보주체의 신원정보를 기반으로 생성한 VP에 대한 검증을 수행한다. 이를 통해, 정보주체를 대신하는 보관자가 정보주체의 신원정보를 남용하는 것을 방지할 수 있다.
- [0129] 전술한 바와 같이, 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템은 보관자가 검증기관에 제출하는 개인정보에 대한 모니터링을 수행함으로써, 과도한 개인정보 또는 불필요한 개인정보가 신원증명용 제출 정보에 포함되지 않도록 하고, 이를 통해 사용자의 개인정보가 노출 및 유출되는 것을 방지 및 보호할 수 있다.
- [0130] 또한, 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템은 사용자가 보관자에게 개인정보를 비롯한 신원정보를 위탁하고 관리 권한을 위임함으로써, 신원정보의 도난이나 분실 등을 방지할 수 있다. 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 보관자는 사용자를 대신하여 사용자의 신원정보를 보관 및 관리함에 따라, 사용자가 매번 신뢰 당사자에게 신원정보를 선택하여 제공해야 하는 번거로움을 감소시킬 수 있다.
- [0131] 또한, 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템은 보관자를 모니터링하는 검증 에이전트를 추가적으로 포함함으로써, 보관자가 사용자의 개인정보를 과도하게 포함하거나 불필요한 개인정보를 제출 정보에 포함하는지에 대해 검증할 수 있고, 이를 통해 사용자의 개인정보 침해를 예방할 수 있다.
- [0132] 또한, 본 개시의 일 실시예에 따른 분산원장 기반 신원증명 시스템에서 검증 에이전트는 보관자가 수신한 VP 프로파일을 공유 원장에 등록하도록 함으로써, 신뢰 당사자가 요청한 클레임에 대해 블록체인 네트워크 참여자가 공유할 수 있도록 한다. 즉, 분산원장 기술을 기반으로 사용자의 신원을 증명하기 위한 VP 프로파일을 공유함으로써, 보관자가 VP에 필요한 정보만 조합하여 제출하는지 여부를 확인할 수 있다. 이를 기반으로, 보관자가 생

성한 VP의 클레임 제공 범위에 대한 신뢰가 가능하다.

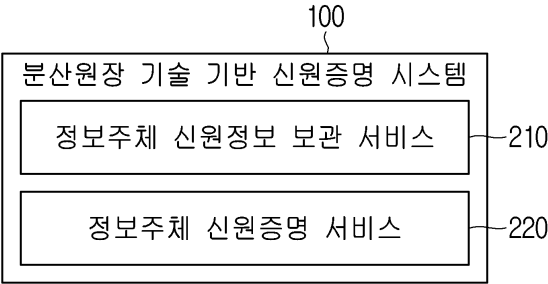
- [0133] 상술한 실시예들에서, 방법들은 일련의 단계 또는 유닛으로서 순서도를 기초로 설명되고 있으나, 본 개시는 단계들의 순서에 한정되는 것은 아니며, 어떤 단계는 상술한 바와 다른 단계와 다른 순서로 또는 동시에 발생할 수 있다. 또한, 당해 기술 분야에서 통상의 지식을 가진 자라면 순서도에 나타난 단계들이 배타적이지 않고, 다른 단계가 포함되거나, 순서도의 하나 또는 그 이상의 단계가 본 개시의 범위에 영향을 미치지 않고 삭제될 수 있음을 이해할 수 있을 것이다.
- [0134] 상술한 실시예에는 다양한 양태의 예시들을 포함한다. 다양한 양태들을 나타내기 위한 모든 가능한 조합을 기술할 수는 없지만, 해당 기술 분야의 통상의 지식을 가진 자는 다른 조합이 가능함을 인식할 수 있을 것이다. 따라서, 본 개시는 이하의 특허청구범위 내에 속하는 모든 다른 교체, 수정 및 변경을 포함한다고 할 것이다.
- [0135] 이상 설명된 본 개시에 따른 실시예들은 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 개시를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 개시에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0136] 이상에서 본 개시가 구체적인 구성요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나, 이는 본 개시의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 개시가 상기 실시예들에 한정되는 것은 아니며, 본 개시가 속하는 기술분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형을 꾀할 수 있다.
- [0137] 따라서, 본 개시의 사상은 상기 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등하게 또는 등가적으로 변형된 모든 것들은 본 개시의 사상의 범주에 속한다고 할 것이다.

도면

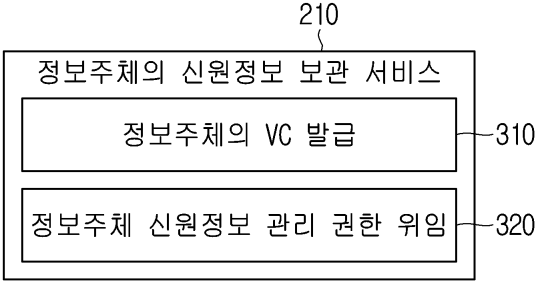
도면1



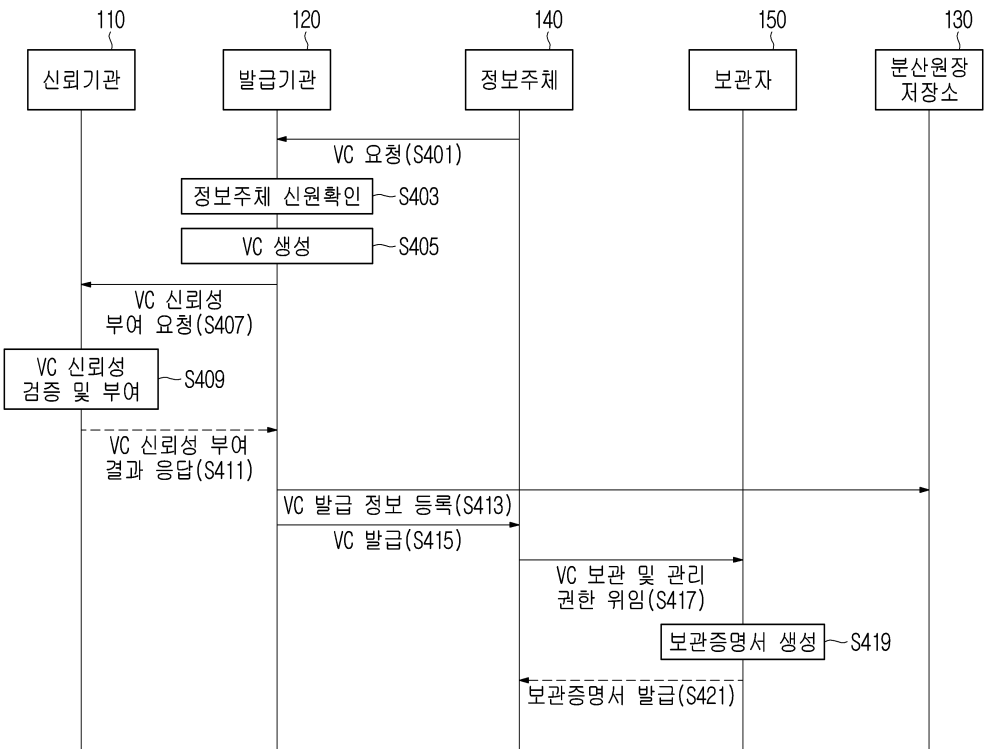
도면2



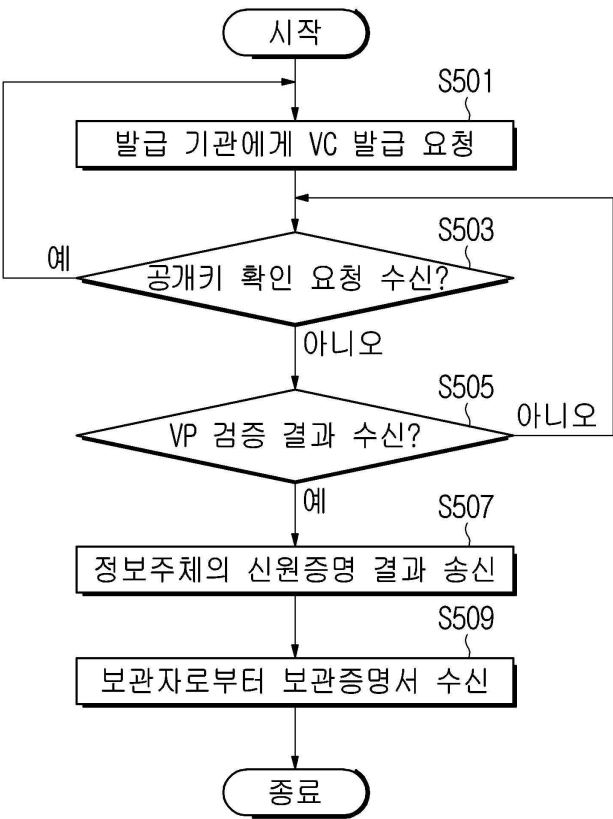
도면3



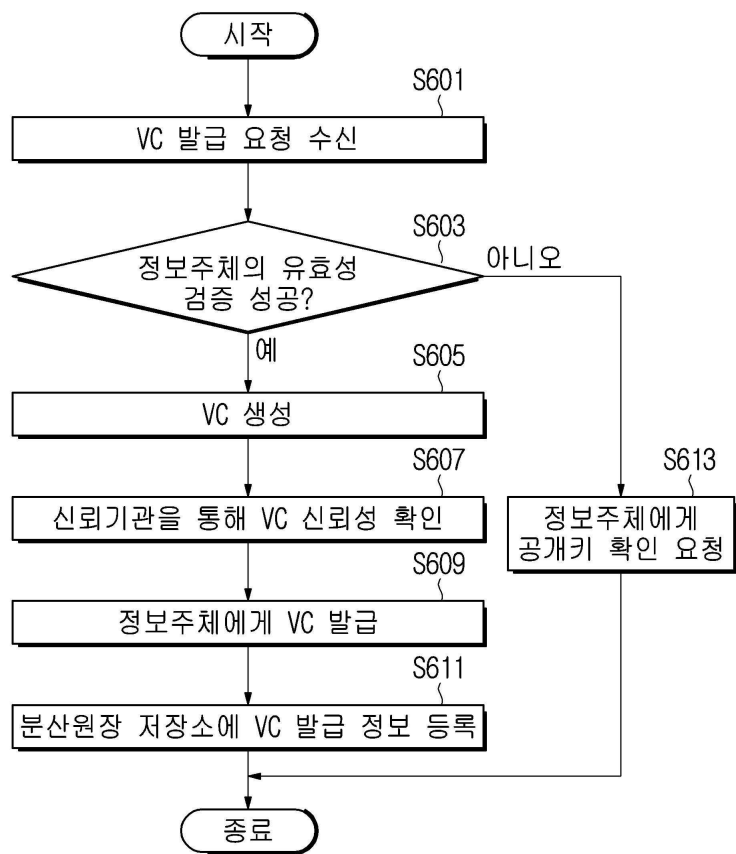
도면4



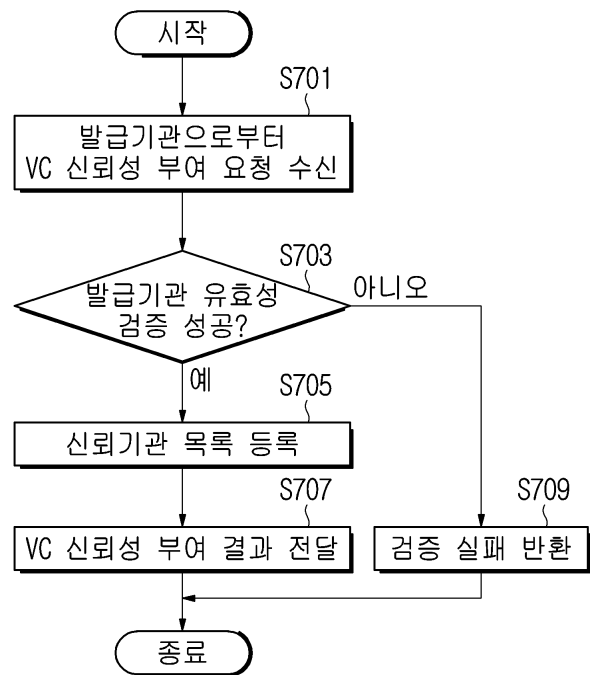
도면5



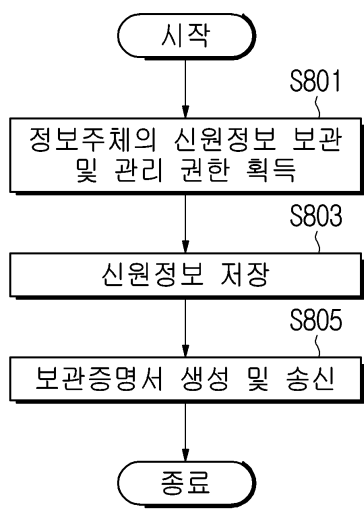
도면6



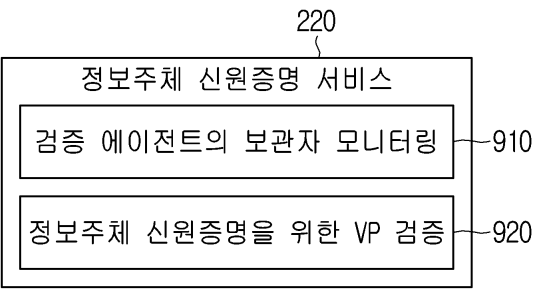
도면7



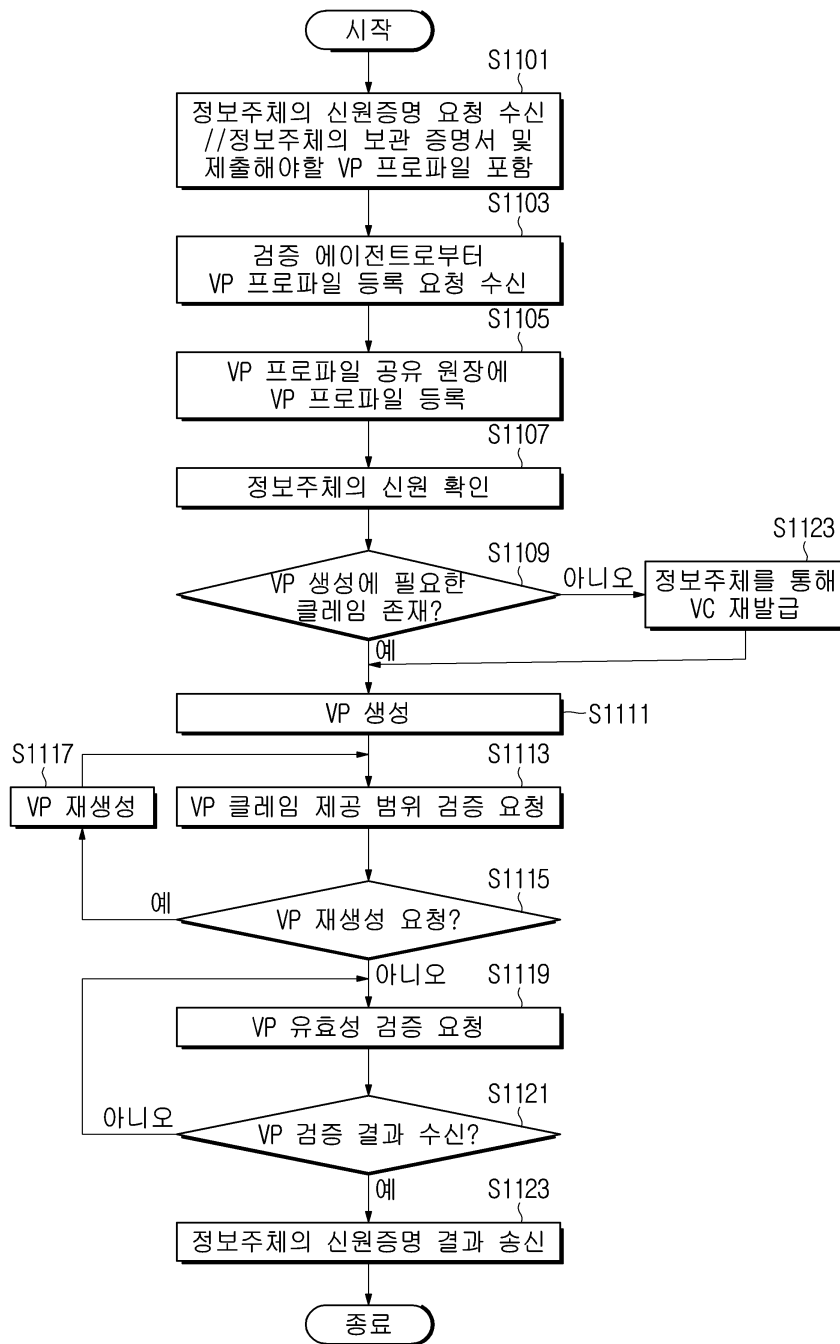
도면8



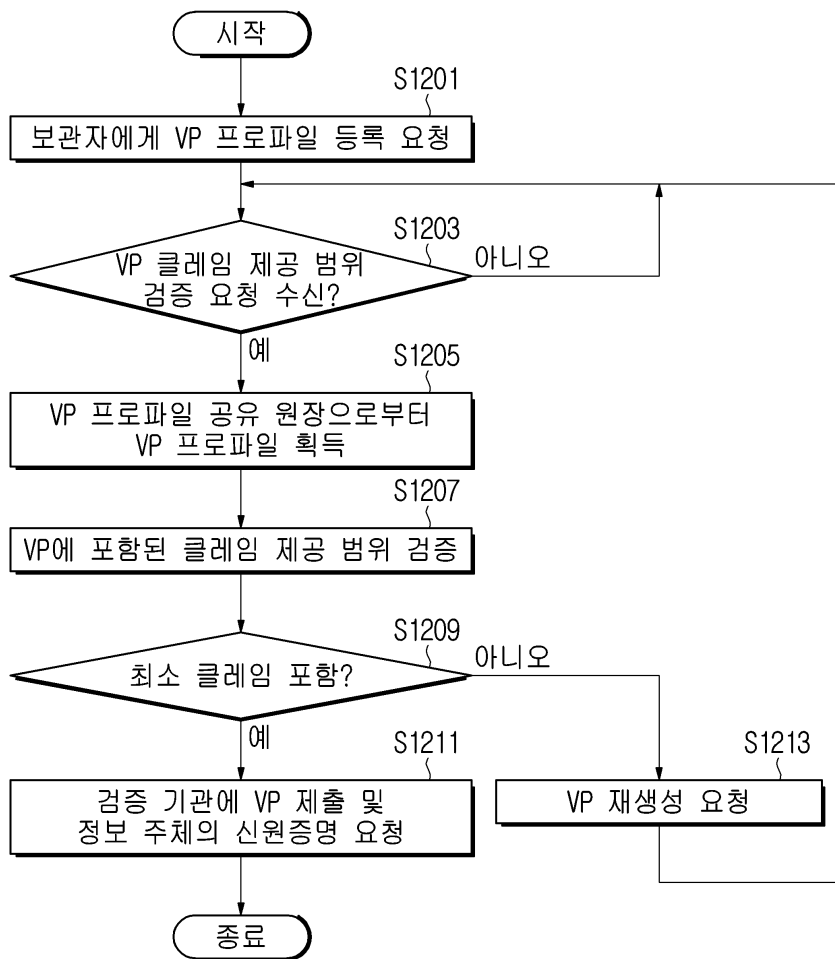
도면9



도면11



도면12



도면13

