



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0131661
(43) 공개일자 2024년09월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/00 (2022.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2023-0024995
(22) 출원일자 2023년02월24일
심사청구일자 2023년02월24일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57 한빛아파트 132-801
김근영
대전광역시 유성구 장대로 87 퍼스트캐슬 202호
김준석
대전광역시 유성구 대학로 53
(74) 대리인
이은철, 김재문

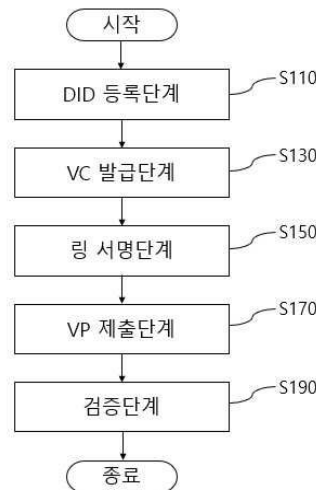
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 링 서명을 지원하는 DID 인증 방법 및 시스템

(57) 요약

본 발명은, 서명의 참여자인 복수의 사용자가 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록 단계; 복수의 사용자 중 임의 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급 단계; 검증자의 증명 요청을 받은 사용자가 VC에 대한 그룹 서명값을 생성하는 링 서명 단계; 증명 요청을 받은 사용자가 생성된 그룹 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출 단계; 및 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증 단계;를 포함하는 것을 일 특징으로 한다.

대표도 - 도1



(52) CPC특허분류

H04L 9/3263 (2013.01)

H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711157470
과제번호	2020R1A2C2008864
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)
연구과제명	영지식 증명을 지원하는 스마트 컨트랙트 프레임워크 연구
기 여 율	1/2
과제수행기관명	충남대학교
연구기간	2021.03.01 ~ 2023.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152724
과제번호	2020-0-00321-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(정진기금)
연구과제명	5G 서비스 환경에서 프라이버시가 보장되는 자기통제형 분산 디지털 신원 관리 및
보안 기술 개발	
기 여 율	1/2
과제수행기관명	한국전자통신연구원
연구기간	2022.01.01 ~ 2022.12.31

명세서

청구범위

청구항 1

서명의 참여자인 복수의 사용자가 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록단계;
 복수의 사용자 중 임의 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급단계;
 검증자의 증명 요청을 받은 사용자가 VC에 대한 그룹 서명값을 생성하는 링 서명단계;
 증명 요청을 받은 사용자가 생성된 그룹 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출단계; 및
 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증단계;를 포함하는 DID 인증 방법.

청구항 2

제 1 항에 있어서,
 상기 DID 등록단계는,
 복수의 사용자가 각각의 공개키쌍(개인키, 공개키)을 생성하고 생성된 공개키를 임의 사용자에게 전달하며,
 복수 사용자의 공개키(공개키 리스트)를 전달받은 임의 사용자가 링 서명을 위해 상기 공개키 리스트를 저장하는 DID 문서를 생성하는 것을 특징으로 하는 DID 인증 방법.

청구항 3

제 2 항에 있어서,
 상기 링 서명단계는,
 서명하고자 하는 메시지, 그룹의 공개키 리스트, 인덱스, 및 자신의 개인키를 입력으로 하여 그룹 서명값을 생성하는 것을 특징으로 하는 DID 인증 방법.

청구항 4

제 3 항에 있어서,
 상기 검증단계는,
 서명된 메시지, 그룹 서명값, 및 공개키 리스트를 입력으로 하고 검증 결과를 참 또는 거짓으로 반환하는 것을 특징으로 하는 DID 인증 방법.

청구항 5

서명의 참여자인 복수의 사용자가 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록부;
 복수의 사용자 중 임의 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급부;
 검증자의 증명 요청을 받은 사용자가 VC에 대한 그룹 서명값을 생성하는 링 서명부;
 증명 요청을 받은 사용자가 생성된 그룹 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출부; 및

검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증부;를 포함하는 DID 인증 시스템.

발명의 설명

기술 분야

- [0001] 본 발명은 DID 인증 방법 및 시스템에 관한 것으로서, 특히 암호 알고리즘인 링 서명 기법(Ring Signature Scheme)을 활용한 DID 인증 방법 및 시스템에 관한 것이다.

배경 기술

- [0003] 분산아이디 또는 DID(Decentralized Identity)는 기존 신원확인 방식과 달리 중앙 시스템에 의해 통제되지 않으며 개개인이 자신의 정보에 완전한 통제권을 가질 수 있게 하는 기술이고, 분산신원확인 또는 탈중앙화 신원확인이라고도 한다. DID는 국제표준단체인 W3C 주도하에 표준이 제정되고 있으며 자격증, 증명서 관리 등 다양한 기능을 제공한다.
- [0004] 최근에는 블록체인 기반 DID 인증 기술에 대한 연구가 활발히 진행되고 있다. 블록체인 기반 DID 인증 시스템은 사용자가 본인을 증명할 수 있는 DID document를 블록체인에 저장하고, 사용자가 발행자에게 VC(Verifiable Credential) 발급을 요청하면 DID 인증을 수행하여 발행자로부터 VC를 발행받으며, 사용자는 발행받은 VC를 VP(Verifiable Presentation) 형태로 만들어 검증자에게 제출하여 서비스를 요청한다.
- [0005] 기존 블록체인 기반 DID 인증 시스템은 RSA, ECDSA 계열의 암호 알고리즘을 이용한 서명 기법을 지원하여 VC에 대한 VP를 서명할 때 단일 서명만 가능하므로, 그룹 기반 익명 서명 기능을 제공하지 않는다. 이를 해결하기 위한 방법으로 제안된 그룹 서명(Group Signature) 기반 DID 시스템은 그룹 매니저에 의해 익명성을 폐기가 가능하고, 그룹의 멤버 관리를 위한 셋업 과정이 복잡하다는 문제점이 있다.
- [0006] 따라서, 익명성을 폐기할 수 없고, 그룹 매니저가 별도로 존재하지 않으며, 그룹 서명이 가능한 DID 인증 방법 및 시스템이 요구되고 있는 실정이다.

발명의 내용

해결하려는 과제

- [0008] 본 발명은 블록체인 기반 DID 인증 시스템에서 그룹 서명이 가능하면서도 익명성을 폐기할 수 없고, 그룹 매니저가 별도로 존재하지 않는 링 서명을 지원하는 DID 인증 방법 및 시스템을 제공하고자 한다.

과제의 해결 수단

- [0010] 상기 목적을 달성하기 위하여 본 발명은, 서명의 참여자인 복수의 사용자가 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록단계; 복수의 사용자 중 임의 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급단계; 검증자의 증명 요청을 받은 사용자가 VC에 대한 그룹 서명값을 생성하는 링 서명단계; 증명 요청을 받은 사용자가 생성된 그룹 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출단계; 및 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증단계;를 포함하는 것을 일 특징으로 한다.
- [0011] 바람직하게는, 상기 DID 등록단계는, 복수의 사용자가 각각의 공개키쌍(개인키, 공개키)을 생성하고 생성된 공개키를 임의 사용자에게 전달하며, 복수 사용자의 공개키(공개키 리스트)를 전달받은 임의 사용자가 링 서명을 위해 상기 공개키 리스트를 저장하는 DID 문서를 생성할 수 있다.
- [0012] 바람직하게는, 상기 링 서명단계는, 서명하고자 하는 메시지, 그룹의 공개키 리스트, 인덱스, 및 자신의 개인키를 입력으로 하여 그룹 서명값을 생성할 수 있다.
- [0013] 바람직하게는, 상기 검증단계는, 서명된 메시지, 그룹 서명값, 및 공개키 리스트를 입력으로 하고 검증 결과를

참 또는 거짓으로 반환할 수 있다.

- [0014] 또한 본 발명은, 서명의 참여자인 복수의 사용자가 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록부; 복수의 사용자 중 임의 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급부; 검증자의 증명 요청을 받은 사용자가 VC에 대한 그룹 서명값을 생성하는 링 서명부; 증명 요청을 받은 사용자가 생성된 그룹 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출부; 및 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증부;를 포함하는 것을 다른 특징으로 한다.

발명의 효과

- [0016] 본 발명은 링 서명을 활용하여, 익명성을 폐기할 수 없고 그룹 매니저가 별도로 존재하지 않으면서도 그룹 서명이 가능하다는 이점이 있다.
- [0017] 본 발명은 기존 DID 인증의 확장된 구조로서 기존에 구현 및 배포된 DID 인증 시스템에 이식하기 용이하여 실용적이라는 이점이 있다.

도면의 간단한 설명

- [0019] 도 1은 본 발명의 실시예에 따른 DID 인증 방법의 흐름도를 나타낸다.
- 도 2는 본 발명의 실시예에 따른 DID 인증 방법의 블록도를 나타낸다.
- 도 3은 본 발명의 실시예에 따른 DID 등록단계의 순서도를 나타낸다.
- 도 4는 본 발명의 실시예에 따른 VC 발급단계의 순서도를 나타낸다.
- 도 5는 본 발명의 실시예에 따른 VC 제출단계 및 검증단계의 순서도를 나타낸다.
- 도 6은 본 발명의 실시예에 따른 DID 인증 시스템의 구성도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0020] 이하, 첨부된 도면들에 기재된 내용들을 참조하여 본 발명을 상세히 설명한다. 다만, 본 발명이 예시적 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일 참조부호는 실질적으로 동일한 기능을 수행하는 부재를 나타낸다.
- [0021] 본 발명의 목적 및 효과는 하기의 설명에 의해서 자연스럽게 이해되거나 보다 분명해 질 수 있으며, 하기의 기재만으로 본 발명의 목적 및 효과가 제한되는 것은 아니다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이, 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다.
- [0022] 도 1은 본 발명의 실시예에 따른 DID 인증 방법의 흐름도를 나타낸다. 도 1을 참조하면, DID 인증 방법은 DID 등록단계(S110), VC 발급단계(S130), 링 서명단계(S150), VP 제출단계(S170), 및 검증단계(S190)를 포함할 수 있다.
- [0023] DID 인증 방법은 링 서명을 활용하여, 익명성을 폐기할 수 없고 그룹 매니저가 별도로 존재하지 않으면서도 그룹 서명이 가능하다. DID 인증 방법은 기존 DID 인증의 확장된 구조로서 기존에 구현 및 배포된 DID 인증 시스템에 이식하기 용이하다.
- [0024] 도 2는 본 발명의 실시예에 따른 DID 인증 방법의 블록도를 나타낸다. 도 2를 참조하면, DID 인증 방법은 서명하고자 하는 사용자인 Holder들이 각각 개인키와 공개키로 구성되는 공개키 쌍을 생성하는 과정을 거쳐 DID 문서를 생성하고 이를 블록체인에 등록할 수 있다. DID 인증 방법은 Holder 1(사용자 1)이 Issuer(발급자)에게 자격증명을 요청하면, Issuer는 Holder의 DID를 토대로 VC(Verifiable Credential)를 발행할 수 있다. DID 인증 방법은 Holder가 Verifier(검증자)의 요청을 토대로 VP(Verifiable Presentation)를 생성 및 제출하여 Verifier가 Holder의 DID 문서를 바탕으로 VP를 검증할 수 있다.

- [0025] DID 인증 방법은 익명성을 보장할 수 있다. 기존 DID 시스템은 특정 VC에 대한 링 서명을 수행하기 위해 참여자가 VC에 대한 서명을 수행하여 VP를 생성하므로 본인을 밝힌 채 검증이 진행된다. 그러나, 본 발명에 따른 DID 인증 방법은 본인의 그룹만을 공개하고, 본인에 대한 익명성을 유지한 채 서명 및 검증이 가능하다.
- [0026] DID 인증 방법은 위변조를 원천적으로 차단할 수 있다. DID 인증 방법은 그룹 참여자의 개인키가 없는 한 외부에서 서명을 위조하는 행위가 불가능하다.
- [0027] DID 인증 방법은 관리자가 불필요하다. DID 인증 방법은 그룹에 참여하는 참여자들 간의 권한이 동등하고, 제3자가 필요 없기 때문에 탈중앙화되고 참여자의 주권을 향상시킬 수 있다.
- [0028] DID 인증 방법은 DID 인증 매커니즘을 바탕으로 암호 알고리즘 수정만을 통해 설계되어 링 서명이 가능한 방법이다. DID 인증 방법은 운전면허증, 백신 접종 앱 등과 같이 잘 구축된 DID 기반 인증 시스템과 연계될 수 있으며, 보유자 인증이 필요한 모든 종류의 애플리케이션에 활용할 수 있다.
- [0029] DID 인증 방법은 다양하게 활용될 수 있는데, 이사회에서 각 이사진이 익명성을 유지한 채 다수결에 의해 합의된 결정을 실행할 수 있고(의사결정), 익명성을 유지한 채 특정인의 권한을 확인하여 접근을 제어할 수 있으며(접근 제어), 특정 그룹에 소속된 참여자가 본인임을 공개하지 않은 채 그룹의 소속임을 밝히며 채팅을 할 수 있다(익명 채팅).
- [0030] 도 3은 본 발명의 실시예에 따른 DID 등록단계(S110)의 순서도를 나타낸다. 도 3을 참조하면, DID 등록단계(S110)는 서명의 참여자인 복수의 사용자가 DID 문서(DID document)를 생성하여 블록체인에 등록할 수 있다.
- [0031] DID 등록단계(S110)는 복수의 사용자가 각각의 공개키쌍(개인키, 공개키)을 생성하고 생성된 공개키를 임의의 사용자에게 전달하며, 복수 사용자의 공개키(공개키 리스트)를 전달받은 임의의 사용자가 링 서명을 위해 상기 공개키 리스트를 저장하는 DID 문서를 생성할 수 있다.
- [0032] DID 등록단계(S110)는 다음과 같이 진행될 수 있다.
- [0033] DID 등록단계(S110)에서는 참여자 Holder 1, Holder 2, ..., Holder n이 각각의 공개키쌍(sk_i , pk_i)을 생성할 수 있다. DID 등록단계(S110)에서는 각 참여자들이 Holder 1에게 자신의 공개키를 전달할 수 있다. 즉, Holder 2 내지 Holder 5는 본인의 공개키 pk_2 내지 pk_5 를 Holder 1에게 전달할 수 있다. Holder 1은 전달받은 공개키 리스트를 바탕으로 링 서명을 위한 DID 문서를 생성할 수 있다. 여기에서, 생성된 DID 문서는 그룹 참여자들의 공개키가 모두 저장될 수 있다. DID 등록단계(S110)에서는 Holder 1이 생성한 DID 문서를 블록체인에 등록할 수 있다.
- [0034] 도 4는 본 발명의 실시예에 따른 VC 발급단계(S130)의 순서도를 나타낸다. 도 4를 참조하면, VC 발급단계(S130)는 복수의 사용자 중 임의의 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행할 수 있다. VC 발급단계(S130)는 다음과 같은 절차로 진행될 수 있다. 아래의 설명은 참여자가 5인인 경우로 가정하였으나, 이는 실시예일뿐 참여자의 숫자는 제한되지 않는다.
- [0035] VC 발급단계(S130)에서는 VC를 발행하고자 하는 임의의 Holder i가 발급자에게 VC를 발행해줄 것을 요청하면 발급자가 DID 문서를 블록체인으로 부터 얻을 수 있다. VC 발급단계(S130)에서는 발급자가 Holder i에게 DID 인증을 위한 challenge를 보내게 되면 Holder i는 response값을 생성하여 발급자에게 전달할 수 있다. VC 발급단계(S130)는 response 값의 검증 결과가 참이면 발급자가 Holder i에게 VC를 발행할 수 있다.
- [0036] 링 서명단계(S150)는 검증자의 증명 요청을 받은 사용자가 VC에 대한 그룹 서명값을 생성할 수 있다. 링 서명단계(S150)는 서명하고자 하는 메시지, 그룹의 공개키 리스트, 인덱스, 및 자신의 개인키를 입력으로 하여 그룹 서명값을 생성할 수 있다.
- [0037] 즉, 링 서명단계(S150)은 그룹 서명값 $\sigma(\text{Ring-Sign}(m, pk_1, pk_2, \dots, pk_n, i, sk_i))$ 를 생성할 수 있다. 여기에서, m 은 서명하고자 하는 메시지를 의미하고, pk_1 내지 pk_n 은 Holder 1 내지 Holder n의 공개키를 의미하며, i 와 sk_i 는 검증자의 증명 요청을 받은 사용자의 인덱스와 개인키를 의미한다.
- [0038] 도 5는 본 발명의 실시예에 따른 VC 제출단계(S170) 및 검증단계(S190)의 순서도를 나타낸다. 도 5를 참조하면, VC 제출단계(S170)는 증명 요청을 받은 사용자가 생성된 그룹 서명값을 바탕으로 VP(Verifiable Presentatio

n)를 생성하여 검증자에게 제출할 수 있다. 즉, VC 제출단계(S170)는 Holder i가 생성한 VP를 검증자에게 제출하는 절차이다. VC 제출단계(S170)에서는 Holder i가 제출하고자 하는 VC에 대한 그룹 서명값 σ 를 생성하고 이를 바탕으로 VP를 생성하여 검증자에게 전달할 수 있다.

- [0039] 검증단계(S190)는 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증할 수 있다.
- [0040] 검증단계(S190)는 VP에 명시된 증명 요청을 받은 사용자 Holder i의 DID를 통해 블록체인에서 증명 요청을 받은 사용자 Holder i의 DID 문서를 조회할 수 있다. 검증단계(S190)에서는 조회된 DID 문서에 명시되어 있는 공개키를 바탕으로 Holder i가 생성한 VP 서명값을 검증할 수 있다.
- [0041] 검증단계(S190)는 VP 내 VC에 명시되어 있는 발급자의 DID를 바탕으로 발급자의 DID 문서를 조회하여 찾은 발급자의 공개키를 토대로 VC의 서명값이 참인지 검증할 수 있다. 검증단계(S190)는 검증자가 검증 결과를 증명 요청을 받은 Holder i에게 전송할 수 있다.
- [0042] 검증단계(S190)는 서명된 메시지, 그룹 서명값, 및 공개키 리스트를 입력으로 하고 검증 결과를 참 또는 거짓으로 반환할 수 있다.
- [0043] 즉, 검증단계(S190)는 검증 대상인 $\text{Ring-Verify}(m, \sigma, pk_1, pk_2, \dots, pk_n)$ 를 입력받아 참 또는 거짓을 반환할 수 있다. 여기에서, m은 서명하고자 하는 메시지를 의미하고, pk_1 내지 pk_n 은 Holder 1 내지 Holder n의 공개키를 의미하며, σ 는 그룹 서명값을 의미한다.
- [0044] 도 6은 본 발명의 실시예에 따른 DID 인증 시스템(10)의 구성도를 나타낸다. 도 6을 참조하면, 본 발명의 다른 실시예인 DID 인증 시스템(10)은 DID 등록부(100), VC 발급부(300), 링 서명부(500), VP 제출부(700), 및 검증부(900)를 포함할 수 있다.
- [0045] DID 등록부(100)는 서명의 참여자인 복수의 사용자가 DID 문서(DID document)를 생성하여 블록체인에 등록할 수 있다. DID 등록부(100)는 전술한 DID 등록단계(S110)의 동작을 수행할 수 있다.
- [0046] VC 발급부(300)는 복수의 사용자 중 임의의 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행할 수 있다. VC 발급부(300)는 전술한 VC 발급단계(S130)의 동작을 수행할 수 있다.
- [0047] 링 서명부(500)는 검증자의 증명 요청을 받은 사용자가 VC에 대한 그룹 서명값을 생성할 수 있다. 링 서명부(500)는 전술한 링 서명단계(S150)의 동작을 수행할 수 있다.
- [0048] VP 제출부(700)는 증명 요청을 받은 사용자가 생성된 그룹 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출할 수 있다. VP 제출부(700)는 전술한 VP 제출단계(S170)의 동작을 수행할 수 있다.
- [0049] 검증부(900)는 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증할 수 있다. 검증부(900)는 전술한 검증단계(S190)의 동작을 수행할 수 있다.
- [0050] 이상에서 대표적인 실시예를 통하여 본 발명을 상세하게 설명하였으나, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리 범위는 설명한 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 특허청구범위와 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태에 의하여 정해져야 한다.

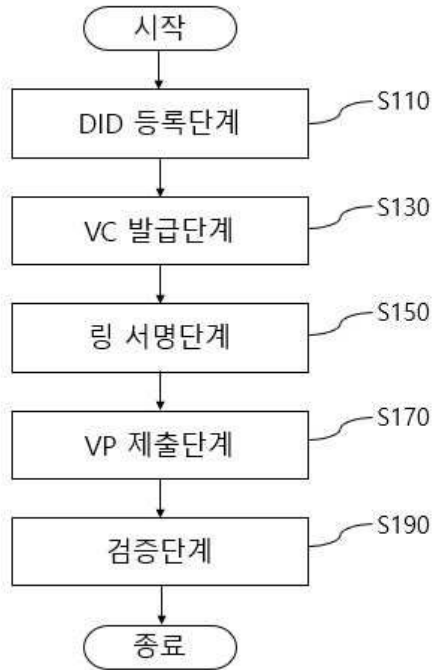
부호의 설명

- [0052] 10 : DID 인증 시스템
- 100 : DID 등록부
- 300 : VC 발급부
- 500 : 링 서명부
- 700 : VP 제출부

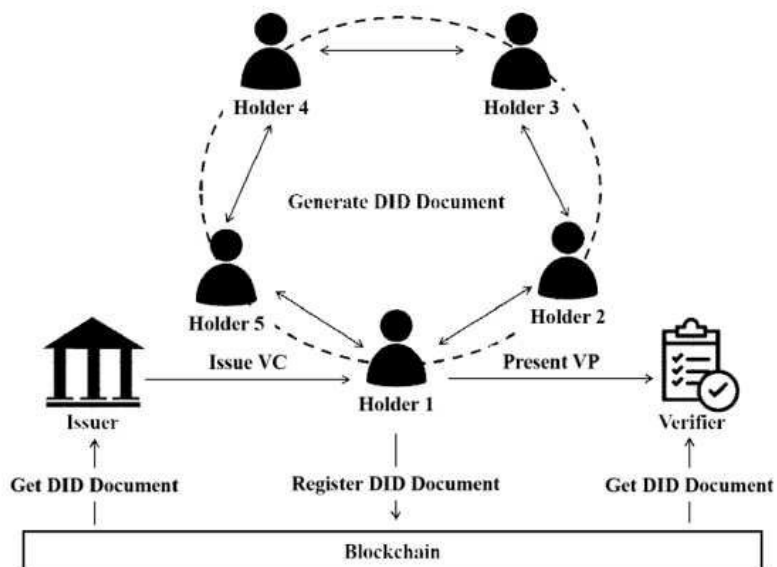
900 : 검증부

도면

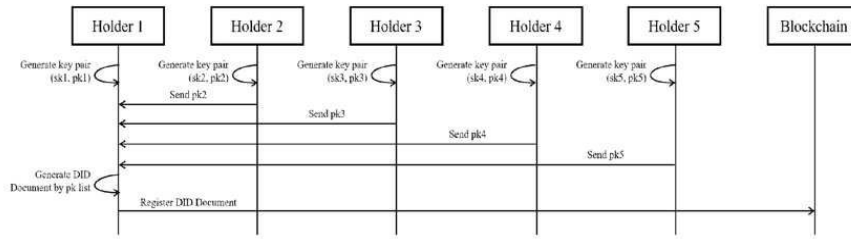
도면1



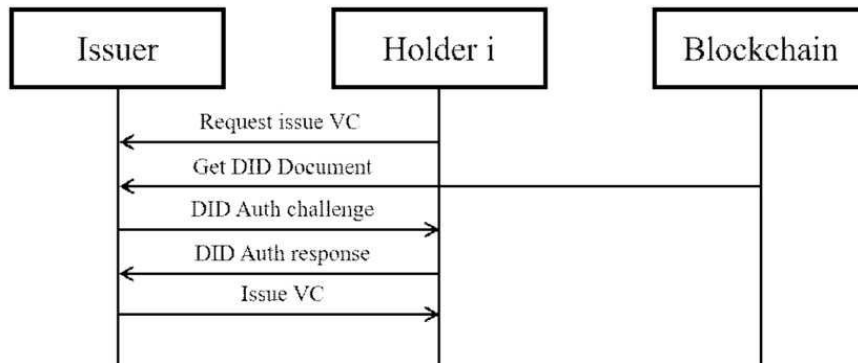
도면2



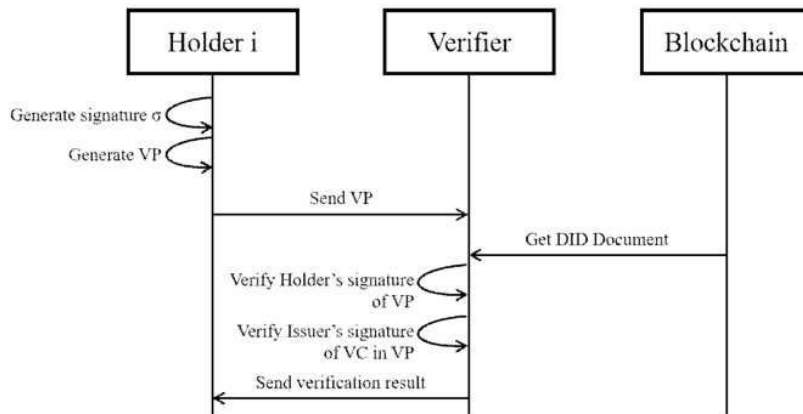
도면3



도면4



도면5



도면6

