(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년03월25일
(11) 등록번호 10-2651448
(24) 등록일자 2024년03월21일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *G06K 19/06* (2006.01)
H04L 65/40 (2022.01)
(52) CPC특허분류
H04L 63/0892 (2013.01)
G06K 19/06037 (2013.01)
(21) 출원번호 10-2021-0033881
(22) 출원일자 2021년03월16일
심사청구일자 2021년03월16일
(65) 공개번호 10-2022-0129245
(43) 공개일자 2022년09월23일
(56) 선행기술조사문헌
US20200296091 A1
KR1020180026751 A
KR1020140084217 A
KR101746745 B1

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
홍상원
서울특별시 노원구 석계로 49, 111동 405호
(74) 대리인
특허법인이상

전체 청구항 수 : 총 12 항 심사관 : 천대식

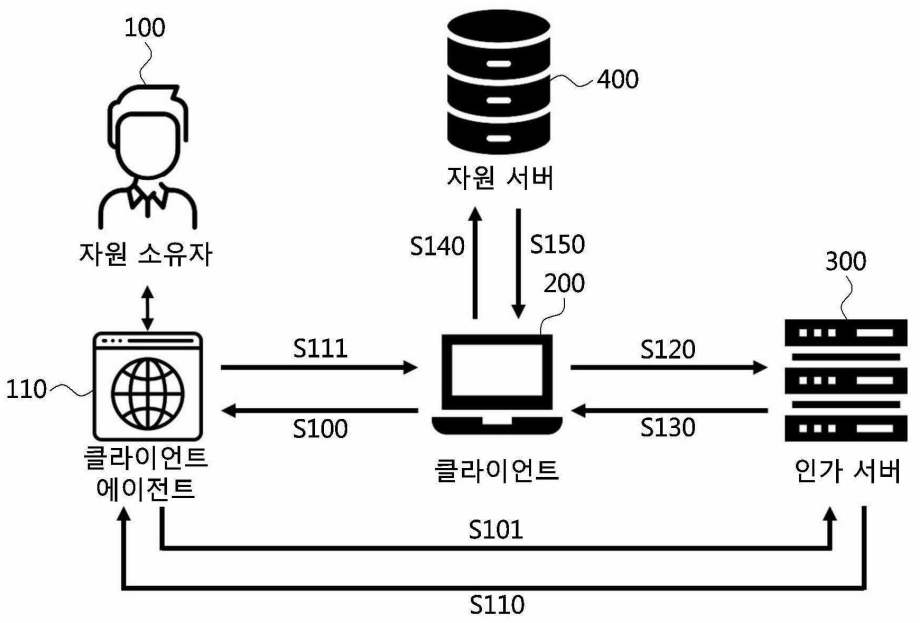
(54) 발명의 명칭 **블록 체인 기반 탈중앙화 인가 프로토콜 방법 및 장치**

(57) 요 약

본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법은, 클라이언트가 자원 소유자에게 인가를 요청하면서 인가 흐름이 시작되는 단계, 자원 소유자의 클라이언트 에이전트가 클라이언트의 요청을 받은 후 인가 서버의 인가 엔드포인트(authorization endpoint)로 리다이렉트(redirect)되는 단계, 자원 소유자가 인가 요청을 승인할 경

(뒷면에 계속)

대 표 도 - 도1



우, 인가 서버는 자원 소유자의 웹 브라우저를 리다이렉션 URI로 리다이렉트하는 단계, 리다이렉트 시, 인가 서버는 리다이렉션 URI에 인가 승인 코드 및 상태 정보를 포함시켜서 클라이언트로 전달하는 단계, 클라이언트는 인가 서버의 토큰 엔드포인트(token endpoint)에 인가 승인 코드 및 리다이렉션 URI 등을 전달하며 액세스 토큰 발급을 요청하는 단계, 인가 서버는 인가 토큰을 검증하여 인가 승인 코드가 유효할 경우, 클라이언트에게 액세스 토큰을 발급해주는 단계, 클라이언트는 액세스 토큰을 통해 자원 서버에 자원에 대한 접근 요청을 하는 단계; 및 자원 서버는 액세스 토큰을 검증하여 액세스 토큰이 유효한 경우, 액세스 토큰에서 허용하는 접근 권한 범위에 해당하는 자원을 클라이언트(200)에게 제공해주는 단계를 포함한다.

(52) CPC특허분류
H04L 63/0815 (2013.01)
H04L 63/083 (2013.01)
H04L 63/10 (2023.05)
H04L 67/563 (2022.05)
H04L 69/08 (2022.05)
H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711125876
과제번호	2020-0-00936-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	블록체인융합기술개발
연구과제명	5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율	1/1
과제수행기관명	포항공과대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

명 세 서

청구범위

청구항 1

블록 체인 기반 탈중앙화 인가 프로토콜 장치에 있어서,

프로세서(processor);

프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory); 를 포함하되,

적어도 하나의 명령은,

인가 서버 대신 블록 체인을 통해 인가를 관리하는 명령을 포함하는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 2

청구항 1에 있어서, 상기 장치는,

자원(resource)에 대한 소유권을 가지며 제3의 클라이언트에게 해당 자원 접근을 승인하거나 거절하는 자원 소유자(resource owner);

소유자 자원을 접근하고자 하는 제 3자 애플리케이션인 클라이언트(client);

클라이언트 에이전트를 통해 인가 요청 메시지를 구성하는 에이전트 사용자(agent user);

인가 프로토콜 과정에서 블록 체인상 스마트 컨트랙트와의 인터페이스를 담당하는 인가 프록시(authorization proxy);

블록 체인 상 인가 스마트 컨트랙트로 구성되며, 인가 자격 증명(authorization credential)을 대체불가능 토큰(NFT) 형태로 생성 및 관리하는 인가 제공자(authorization server); 및

사용자 자원을 호스팅하는 서비스 제공자인 자원 서버(resource server); 를 포함한,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 3

청구항 1에 있어서, 인가 서버의 비즈니스 로직은,

인가 프록시를 통해 블록 체인 상에서 인가 스마트 컨트랙트를 수행하는 동작으로 대체하는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 4

청구항 1에 있어서, 블록 체인 상에서 동작하는 인가 스마트 컨트랙트가,

OAuth 2.0 프로토콜과 호환되는 정보인 인가 자격 증명 정보를 속성으로 하는 대체 불가능 토큰(NFT)을 발행 및 관리하는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 5

청구항 1에 있어서, 블록 체인 상에서 동작하는 인가 스마트 컨트랙트가,

블록 체인 상에 배포된 대체 불가능 토큰(NFT)을 통해 OAuth 2.0 액세스 토큰 소유자를 검증함으로써 액세스 토큰 유효성을 판단하는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 6

청구항 4에 있어서, 인가 자격 증명 정보는,

블록 체인 상에서 유일하게 식별할 수 있는 토큰 ID을 나타내는 id 속성;

대체 불가능 토큰이 보증하는 인가 자격 증명 즉, 인가 승인 코드 또는 액세스 토큰을 나타내는 type 속성;

대체 불가능 토큰의 소유자를 나타내는 owner 속성;

대체 불가능 토큰의 소유권을 변경할 수 있는 권한을 가진 엔티티를 나타내는 approvee 속성;

인가 자격 증명 발급을 발행해주는 주체, 즉 자원 소유자를 나타내는 issuer 속성;

액세스 토큰을 활용하여 자원 접근을 요청하는 주체, 즉 클라이언트를 나타내는 subject 속성;

액세스 토큰을 전달받아, 액세스 토큰을 기반으로 자원을 제공해주는 주체, 즉 자원 서버를 나타내는 audience 속성;

인가 승인 코드를 식별할 수 있는 문자열을 나타내는 code 속성; 접근을 승인하는 자원 범위를 나타내는 scope 속성;

상태 정보를 나타내는 state 속성;

액세스 토큰을 식별할 수 있는 문자열을 나타내는 access_token 속성;

클라이언트로 리다이렉트하는 콜백 URI을 나타내는 redirect_uri 속성;

인가 자격 증명의 발행 시간을 나타내는 issued_at 속성;

인가 자격 증명의 만료 시간을 나타내는 expire_in 속성; 및

대체 불가능 토큰이 폐기되었는지 여부를 나타내는 revoked 속성; 을 포함하고,

대체 불가능 토큰을 배포, 관리 및 인가 자격 증명의 유효성에 대한 검증을 수행하는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 7

청구항 1에 있어서, 자원 소유자에게 사용자 인증 및 인가 승인 요청을 전달하는 방식은,

QR 코드, 문자 메시지, 모바일 앱 푸시 메시지 중 적어도 하나가 채택되는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 8

청구항 1에 있어서, 복수 개의 기관들이 함께 참여하는 컨소시움 환경은,

하이퍼레저 패브릭을 활용하여 컨소시움 블록 체인을 구성하고,

복수 개의 기관들에 의한 공동 인가 서비스를 제공하는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 9

청구항 1에 있어서, 복수 개의 기관들이 함께 참여하는 컨소시움 환경은,

각 기관별 자원 서버들을 통합하는 중계 자원서버를 구성하고,

기관별 자원서버들에 분산 저장된 자원 소유자의 자원에 대한 통합 자원 접근을 제공하는,

블록 체인 기반 탈중앙화 인가 프로토콜 장치.

청구항 10

클라이언트(200)가 자원 소유자(100)에게 인가를 요청하면서 인가 흐름이 시작되는 단계(S100);

자원 소유자(100)의 클라이언트 에이전트(110)가 클라이언트(200)의 요청을 받은 후 인가 서버(300)의 인가 엔드포인트(authorization endpoint)로 리다이렉트(redirect)되는 단계(S101);

자원 소유자(100)가 인가 요청을 승인할 경우, 인가 서버(300)는 자원 소유자(100)의 웹 브라우저(110)를 리다이렉션 URI로 리다이렉트하는 단계(S110);

리다이렉트 시, 인가 서버(300)는 리다이렉션 URI에 인가 승인 코드 및 상태 정보를 포함시켜서 클라이언트(200)로 전달하는 단계(S111);

클라이언트(200)는 인가 서버(300)의 토큰 엔드포인트(token endpoint)에 인가 승인 코드 및 리다이렉션 URI 등을 전달하며 액세스 토큰 발급을 요청하는 단계(S120);

인가 서버(300)는 인가 토큰을 검증하여 인가 승인 코드가 유효할 경우, 클라이언트(200)에게 액세스 토큰을 발급해주는 단계(S130);

클라이언트(200)는 액세스 토큰을 통해 자원 서버(400)에 자원에 대한 접근 요청을 하는 단계(S140); 및

자원 서버(400)는 액세스 토큰을 검증하여 액세스 토큰이 유효한 경우, 액세스 토큰에서 허용하는 접근 권한 범위에 해당하는 자원을 클라이언트(200)에게 제공해주는 단계(S150); 를 포함하는,

블록 체인 기반 탈중앙화 인가 프로토콜 방법.

청구항 11

에이전트 사용자(2000)는 클라이언트에서 제공하는 서비스를 활용하기 위해 먼저 웹 브라우저인 클라이언트 에이전트(2100)를 통해 자원 소유자(1000) 의 자원 접근 인가 요청을 위한 설정을 입력하는 단계(S1000);

클라이언트(3000)는 클라이언트 에이전트(2100)을 통해 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 보내는 단계(S1010, S1011);

인가 제공자(4000)는 자원 소유자(1000)에게 클라이언트(3000)에 대한 사용자 인증 혹은 자원 접근 인가 승인 요청을 보내는 단계(S1020, S1030);

인가 제공자(4000)는 자원 소유자 모바일 폰(1100) 으로부터 승인 처리 결과 응답 메시지를 수신하고, 자원소유자의 유효한 승인 여부를 검증한 후, 클라이언트 에이전트(2100)로 인가 승인 코드(authorization code)를 발급하는 단계(S1050):

클라이언트(3000)는 인가 제공자(4000)로 인가 승인 코드 및 리다이렉션 URI 등을 전달함으로써, 액세스 토큰 발급을 요청하는 단계(S1060, S1070);

클라이언트(3000)는 발급받은 액세스 토큰을 활용하여 자원 서버(5000)에 자원 소유자의 자원에 대한 접근 요청을 하는 단계(S1080):

자원 서버(5000)는 인가 제공자(4000)에게 액세스 토큰에 대한 검증 요청을 보내어 최종적으로 액세스 토큰 유효성을 재차 확인하는 단계(S1090, S1100); 및

자원 서버(5000)가 인가 제공자(4000) 로부터 액세스 토큰이 유효하다는 응답 결과를 받았을 경우, 클라이언트(3000) 에게 액세스 토큰에 표현되어 있는 범위의 자원을 전달하는 단계(S1110); 를 포함하는,

블록 체인 기반 탈중앙화 인가 프로토콜 방법.

청구항 12

청구항 11에 있어서, 상기 방법은,

에이전트 사용자(2000)가 클라이언트 에이전트인 웹 브라우저(2100)를 통해 인가 요청을 위한 설정을 입력한 후(S1000), 클라이언트(3000)가 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 웹 브라우저(2100)를 통해 전달하는 단계(S1010, S1011);

인가 제공자(4000)는 웹 브라우저(2100) 에서 리다이렉트 정보와 자원 접근 범위 및 권한 정보를 포함하는 QR 코드를 생성하고 웹 브라우저(2100)에 표시되도록 전달하는 단계(S1050);

자원 소유자(1000)는 본인의 모바일 폰(1100)으로 에이전트 사용자(2000)의 웹 브라우저(2100)에 로드된 QR 코드를 스캔하는 단계(S2000); 및

자원 소유자(1000)의 모바일 폰(1100)은 QR 코드 내 자원 접근 범위 및 권한 정보를 확인하고, 승인할 경우에는 생체 인증 등 다양한 사용자 인증 처리를 하고 승인 결과를 인가제공자(4000)로 전달하는 과정을 리다이렉트 기능을 활용하여 진행하는 단계(S3000); 를 더 포함하는,

블록 체인 기반 탈중앙화 인가 프로토콜 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록 체인 기반 탈중앙화 인가 프로토콜 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 인증(authentication)이란 사용자의 신원을 증명하는 것을 의미하고, 인가(authorization)란 사용자가 소유한 자원(resource)에 대한 접근 권한을 부여하는 것을 의미한다. 따라서, 인가 과정은 사용자 인증 과정을 거친 후 진행된다.

[0003] 인가 과정은 주로 사용자가 제 3의 클라이언트 애플리케이션에게 사용자 자원(resource)에 대한 접근 권한을 부여하고자 할 때 진행된다. 일반적으로 사용자 자원 호스팅 서비스를 제공하는 애플리케이션을 가정하며, 사용자 자격 증명 정보(즉, 사용자 계정 및 비밀번호)를 제 3의 클라이언트 애플리케이션에 전달하면, 클라이언트 애플리케이션은 사용자 자격 증명 정보를 통해 사용자 자원 호스팅 서비스 제공 애플리케이션을 통해 사용자 인증을 한 후, 원하는 사용자 자원에 접근하게 된다. 그러나 사용자 자격 증명 정보가 클라이언트 애플리케이션에 그대로 노출되면, 서비스 제공 애플리케이션은 사용자 자격 증명 정보를 제시하는 요청자가 사용자인지 클라이언트 애플리케이션인지 구분할 수 없기 때문에, 사용자가 공유를 원하지 않는 사용자 자원이라고 할지라도 클라이언트 애플리케이션은 사용자 자격 증명 정보를 활용하여 임의로 해당 사용자 자원에 접근할 수 있게 된다.

[0004] 이러한 인가 과정은 사용자를 대신하여 제 3의 클라이언트 애플리케이션이 사용자 자원을 접근하게 할 필요성으로 인해 매우 빈번하게 발생하므로, 효과적인 인가 과정을 위해 개방형 표준 프로토콜인 OAuth 2.0이 등장하였다. OAuth 2.0은 제 3의 클라이언트 애플리케이션에게 사용자 자격 증명 정보를 직접 노출시키지 않으며, 대신 사용자 신원 인증 증거로서 액세스 토큰(access token)을 발급한다. 또한, 액세스 토큰에는 사용자 신원 인증 증거 이외 추가적으로 사용자가 제3의 클라이언트 애플리케이션에게 접근을 허용하는 사용자 자원에 대한 접근 권한 범위(scope) 정보를 포함한다. 즉, 사용자는 본인이 소유한 다양한 자원들에 대해 선택적으로 제 3의 클라이언트에게 접근을 승인하며, 제3의 클라이언트에서는 발급받은 액세스 토큰을 사용자 자원을 관리하는 서버에 제공하고, 사용자 자원 관리 서버에서는 액세스 토큰이 보증하는 사용자 신원 증명 및 접근 권한 범위 정보를 확인한 후, 최종적으로 승인한 범위 내의 사용자 자원을 제3의 클라이언트 애플리케이션에게 제공한다.

[0005] OAuth 2.0은 사용자가 제 3의 클라이언트 애플리케이션에 사용자 자원을 접근할 수 있도록 허용해주는, 인가를 위한 개방형 표준 프로토콜이다. OAuth 2.0은 애플리케이션 간의 사용자 자원 공유를 위해 널리 활용되고 있다. 사용자 자원 호스팅 서비스를 제공하는 애플리케이션은 사용자 자원을 API로 제공하여, 클라이언트 애플리케이션들이 사용자에게 인가를 받은 후 API 호출을 통해 사용자 자원에 접근할 수 있게 한다.

[0006] OAuth 2.0에는 자원 소유자(resource owner), 클라이언트(client), 인가 서버(authorization server), 자원 서버(resource server)로 총 네 가지 엔티티(entity)가 존재한다. 자원 소유자는 자원 서버에서 호스팅하는 자원에 대한 소유권을 가진 사용자이다. 자원 소유자는 클라이언트가 본인의 자원에 대한 접근 권한을 요청하면 승인 또는 거절한다. 클라이언트는 사용자 자원을 접근하고자 하는 제 3의 애플리케이션이다. 자원 서버는 사용자 자원을 호스팅하는 서비스 제공 애플리케이션이다. 인가 서버는 인가 승인 코드(authorization code), 액세스 토큰(access token), 갱신 토큰(refresh token) 등 인가 자격 증명(authorization credential)을 발급 및 관리하는 인가 제공자이다.

[0007] OAuth 2.0의 인가 흐름은 다음과 같다. 클라이언트가 자원 소유자에게 인가를 요청한다. 자원 소유자는 클라이언트에게 권한 부여 타입(grant type)에 따라 직접 혹은 인가 서버를 통해 간접적으로 인가 그랜트(authorization grant)를 발급한다. 가장 일반적으로 활용되는 권한 부여 타입인 인가 승인 코드 권한 부여 타입 기반 인가 흐름에서는 자원 소유자가 인가 서버를 통해 인가 그랜트인 인가 승인 코드를 발급받은 후, 해당

인가 승인 코드를 클라이언트에게 전달한다. 인가 그랜트는 자원 소유자가 클라이언트의 인가 요청을 승인했다는 것을 보증해주는 임시적인 인가 자격증명(temporary authorzation credential)이다. 클라이언트는 인가 그랜트를 통해 인가 서버에 액세스 토큰 발행을 요청한다. 인가 서버는 클라이언트 인증을 한 후, 클라이언트에게 액세스 토큰을 발행한다. 만약 갱신 토큰 발행이 허용되었다면 갱신 토큰도 액세스 토큰과 함께 발행한다. 액세스 토큰은 자원 소유자가 본인의 자원에 대한 제한된 접근 권한을 허용했다는 것을 증명하는 인가 자격 증명이다. 액세스 토큰은 접근 권한 범위(scope), 만료 시간(expiration time) 등의 여러 정보를 포함하고 있다. 갱신 토큰은 액세스 토큰이 만료되면 클라이언트가 인가 서버에 액세스 토큰을 재발급받을 수 있도록 해주는 인가 자격 증명이다. 클라이언트는 액세스 토큰을 통해 자원 서버로부터 자원 소유자의 자원 접근을 요청한다. 자원 서버는 접근 토큰의 접근 권한 범위를 확인한 후, 접근 권한 범위에 해당하는 제한된 자원만 반환해준다.

[0008] 블록 체인(blockchain)은 트랜잭션(transaction)들의 집합으로 구성된 블록이 이전 블록의 해시(hash)값을 담아 모든 블록을 체인 형식으로 연결하는 데이터 구조로서, 블록 체인 네트워크에 참여하는 모든 노드(node)가 상기 데이터 구조를 동일하게 유지하고, 합의 알고리즘을 기반으로 새로운 블록을 생성하여 연결하는 분산 원장 기술(distributed ledger technology)이다. 특정 노드의 블록 체인 데이터가 임의로 조작되더라도 블록 간에 이전 블록의 해시값을 가지고 있으므로 데이터 조작을 바로 탐지할 수 있으며, 조작된 데이터는 노드 간에 합의된 것이 아니기 때문에 블록 체인에 반영되지 않는다. 이처럼 블록 체인은 데이터를 임의로 위변조하는 것이 불가능하여 데이터의 무결성 및 투명성을 보장해준다.

[0009] 블록 체인은 무허가형 블록 체인(permissionless blockchain)과 허가형 블록 체인(permissioned blockchain)으로 구분된다. 무허가형 블록 체인은 사용자 및 노드가 아무런 제약 없이 블록 체인 네트워크에 참여할 수 있는 블록 체인이다. 대표적인 무허가형 블록 체인으로는 이더리움(Ethereum)이 있다. 허가형 블록 체인은 허가된 사용자 및 노드들만 블록 체인 네트워크에 참여할 수 있는, 비즈니스 환경에서 활용하기에 적합한 블록 체인이다. 대표적인 허가형 블록 체인으로는 하이퍼레저 패브릭(Hyperledger Fabric)이 있다.

[0010] 블록 체인 상에서 실행되는 프로그램인 스마트 컨트랙트(smart contract)에 비즈니스 로직을 구성하여 분산 애플리케이션(distributed application: dApp)을 개발 및 운영할 수 있다. 스마트 컨트랙트는 제 3자의 개입 없이 각 요청을 비즈니스 로직에 따라 자동으로 실행한다는 장점을 갖고 있다. 대표적인 dApp으로 토큰(token)이 있다.

[0011] 토큰은 디지털 자산(digital asset)을 블록 체인 상에 표현한 것이다. 블록 체인에 디지털 자산을 토큰화하면 디지털 자산의 소유권 증명, 투명성 및 유동성 보장 등의 장점을 확보할 수 있다. 토큰은 대체 가능 토큰(fungible token)과 대체 불가능 토큰(non-fungible token)으로 구분된다. 대체 가능 토큰은 쪼개질 수 있는 디지털 자산을 표현한 토큰이고, 대체 불가능 토큰은 쪼개질 수 없는 디지털 자산을 표현한 토큰이다.

[0012] 개방형 표준 프로토콜 OAuth 2.0은 통합 사용자 인증, 사용자 정보 공유 제어 등에 광범위하게 사용되고 있으나, 기본적으로 다음과 같은 문제점을 가진다.

[0013] 첫째, OAuth 2.0 액세스 토큰은 사용자 신원 증명과 함께 접근이 허용된 자원 범위 정보를 담고 있다. 액세스 토큰은 클라이언트에게 발급되고 저장되는데, 공격자가 다양한 공격 방법을 통해 액세스 토큰을 획득하는 경우, 공격자는 액세스 토큰을 활용하여 사용자 자원에 접근할 수 있다.

[0014] 둘째, OAuth 2.0 액세스 토큰을 클라이언트에게 발급하기 위하여, 사용자 인증을 해야 한다. 사용자 인증은 사용자 자격 증명 정보를 유지/관리하는 중앙 집중식 서버(본 발명에서는 이 서버를 인가 서버로 부르기로 함)에서 진행되며, 따라서 중앙 집중식 인가 서버 관리자의 악의적 행위 혹은 중앙집중식 인가 서버 해킹을 통해 사용자 동의 없이도 OAuth 2.0 액세스 토큰 발행이 가능하다.

[0015] 셋째, OAuth 2.0 액세스 토큰은 사용자 자원 접근을 희망하는 클라이언트 별로 발급된다. 그러나, 클라이언트는 사용자에게 웹브라우저(클라이언트 에이전트) 형태로 인터페이스되므로, 웹브라우저 상 크로스 사이트 공격이 가능하다. 따라서, 액세스 토큰은 클라이언트 별이 아닌 클라이언트 에이전트 별로 발급되어야 한다.

[0016] 넷째, OAuth 2.0 액세스 토큰은 사용자 자원 접근을 희망하는 클라이언트 별로 각각 발급된다. 액세스 토큰 발급에는 OAuth 2.0 프로토콜의 전체적 실행이 필요하며, 이에 따른 오버헤드가 발생한다. 이는 액세스 토큰을 재사용하지 못하기 때문이다.

[0017] 다섯째, OAuth 2.0 프로토콜은 기본 스펙(RFC 6749)만을 따라 구현될 경우, 액세스 토큰 폐기에 대한 과정을 정의하지 않으므로, 발급된 액세스 토큰을 중간에 폐기하는 것이 불가능하다. 이를 해결하기 위해 액세스 토큰 발행시 유효기간을 짧게 설정하고, 갱신 토큰을 통해 액세스 토큰을 재발행하는 과정을 효과적으로 정의하고

있다. 그러나, 액세스 토큰 재발행 관련 오버헤드는 여전히 존재한다.

발명의 내용

해결하려는 과제

[0018] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 블록 체인으로 인가를 관리하도록 하는 OAuth 2.0과 상호 연동 가능한 블록 체인 기반 탈중앙화 인가 프로토콜 방법 및 장치를 제공하는 것에 있다.

과제의 해결 수단

[0019] 제안된 발명의 일 양상에 따르면, 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 장치는, 블록 체인 기반 탈중앙화 인가 프로토콜 장치에 있어서, 프로세서(processor); 프로세서를 통해 실행되는 적어도 하나의 명령이 저장된 메모리(memory); 를 포함하되, 적어도 하나의 명령은, 인가 서버 대신 블록 체인을 통해 인가를 관리하는 명령을 포함할 수 있다.

[0020] 상기 장치는, 자원(resource)에 대한 소유권을 가지며 제3의 클라이언트에게 해당 자원 접근을 승인하거나 거절하는 자원 소유자(resource owner); 소유자 자원을 접근하고자 하는 제 3자 애플리케이션인 클라이언트(client); 클라이언트 에이전트를 통해 인가 요청 메시지를 구성하는 에이전트 사용자(agent user); 인가 프로토콜 과정에서 블록 체인상 스마트 컨트랙트와의 인터페이스를 담당하는 인가 프록시(authorization proxy); 블록 체인 상 인가 스마트 컨트랙트로 구성되며, 인가 자격 증명(authorization credential)을 대체불가능 토큰(NFT) 형태로 생성 및 관리하는 인가 제공자(authorization server); 및 사용자 자원을 호스팅하는 서비스 제공자인 자원 서버(resource server); 를 포함할 수 있다.

[0021] 인가 서버의 비즈니스 로직은, 인가 프록시를 통해 블록 체인 상에서 인가 스마트 컨트랙트를 수행하는 동작으로 대체할 수 있다.

[0022] 블록 체인 상에서 동작하는 인가 스마트 컨트랙트가, OAuth 2.0 프로토콜과 호환되는 정보인 인가 자격 증명 정보를 속성으로 하는 대체 불가능 토큰(NFT)을 발행 및 관리할 수 있다.

[0023] 블록 체인 상에서 동작하는 인가 스마트 컨트랙트가, 블록 체인 상에 배포된 대체 불가능 토큰(NFT)을 통해 OAuth 2.0 액세스 토큰 소유자를 검증함으로써 액세스 토큰 유효성을 판단할 수 있다.

[0024] 인가 자격 증명 정보는, 블록 체인 상에서 유일하게 식별할 수 있는 토큰 ID을 나타내는 id 속성; 대체 불가능 토큰이 보증하는 인가 자격 증명 즉, 인가 승인 코드 또는 액세스 토큰을 나타내는 type 속성; 대체 불가능 토큰의 소유자를 나타내는 owner 속성; 대체 불가능 토큰의 소유권을 변경할 수 있는 권한을 가진 엔티티를 나타내는 approvee 속성; 인가 자격 증명 발급을 발행해주는 주체, 즉 자원 소유자를 나타내는 issuer 속성; 액세스 토큰을 활용하여 자원 접근을 요청하는 주체, 즉 클라이언트를 나타내는 subject 속성; 액세스 토큰을 전달받아, 액세스 토큰을 기반으로 자원을 제공해주는 주체, 즉 자원 서버를 나타내는 audience 속성; 인가 승인 코드를 식별할 수 있는 문자열을 나타내는 code 속성; 접근을 승인하는 자원 범위를 나타내는 scope 속성; 상태 정보를 나타내는 state 속성; 액세스 토큰을 식별할 수 있는 문자열을 나타내는 access_token 속성; 클라이언트로 리다이렉트하는 콜백 URI을 나타내는 redirect_uri 속성; 인가 자격 증명의 발행 시간을 나타내는 issued_at 속성; 인가 자격 증명의 만료 시간을 나타내는 expire_in 속성; 및 대체 불가능 토큰이 폐기되었는지 여부를 나타내는 revoked 속성; 을 포함하고, 대체 불가능 토큰을 배포, 관리 및 인가 자격 증명의 유효성에 대한 검증을 수행할 수 있다.

[0025] 자원 소유자에게 사용자 인증 및 인가 승인 요청을 전달하는 방식은, QR 코드, 문자 메시지, 모바일 앱 푸시 메시지 중 적어도 하나가 채택될 수 있다.

[0026] 복수 개의 기관들이 함께 참여하는 컨소시움 환경은, 하이퍼레저 패브릭을 활용하여 컨소시움 블록 체인을 구성하고, 복수 개의 기관들에 의한 공동 인가 서비스를 제공할 수 있다.

[0027] 복수 개의 기관들이 함께 참여하는 컨소시움 환경은, 각 기관별 자원 서버들을 통합하는 중계 자원서버를 구성하고, 기관별 자원서버들에 분산 저장된 자원 소유자의 자원에 대한 통합 자원 접근을 제공할 수 있다.

[0028] 제안된 발명의 다른 일 양상에 따르면, 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법은, 클라이언트가 자원 소유자에게 인가를 요청하면서 인가 흐름이 시작되는 단계; 자원 소유자의 클라이언트 에이전트가 클라이언트의 요청을 받은 후 인가 서버의 인가 엔드포인트(authorization endpoint)로 리다이렉트(redirect)되는

단계; 자원 소유자가 인가 요청을 승인할 경우, 인가 서버는 자원 소유자의 웹 브라우저를 리다이렉션 URI로 리다이렉트하는 단계; 리다이렉트 시, 인가 서버는 리다이렉션 URI에 인가 승인 코드 및 상태 정보를 포함시켜서 클라이언트로 전달하는 단계; 클라이언트는 인가 서버의 토큰 엔드포인트(token endpoint)에 인가 승인 코드 및 리다이렉션 URI 등을 전달하며 액세스 토큰 발급을 요청하는 단계; 인가 서버는 인가 토큰을 검증하여 인가 승인 코드가 유효할 경우, 클라이언트에게 액세스 토큰을 발급해주는 단계; 클라이언트는 액세스 토큰을 통해 자원 서버에 자원에 대한 접근 요청을 하는 단계; 및 자원 서버는 액세스 토큰을 검증하여 액세스 토큰이 유효한 경우, 액세스 토큰에서 허용하는 접근 권한 범위에 해당하는 자원을 클라이언트에게 제공해주는 단계; 를 포함할 수 있다.

[0029] 제안된 발명의 다른 일 양상에 따르면, 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법은, 에이전트 사용자는 클라이언트에서 제공하는 서비스를 활용하기 위해 먼저 웹 브라우저인 클라이언트 에이전트를 통해 자원 소유자의 자원 접근 인가 요청을 위한 설정을 입력하는 단계; 클라이언트는 클라이언트 에이전트를 통해 인가 제공자로 에이전트 사용자의 요구사항을 포함한 인가 요청을 보내는 단계; 인가 제공자는 자원 소유자에게 클라이언트에 대한 사용자 인증 혹은 자원 접근 인가 승인 요청을 보내는 단계; 인가 제공자는 자원 소유자 모바일 폰으로부터 승인 처리 결과 응답 메시지를 수신하고, 자원소유자의 유효한 승인 여부를 검증한 후, 클라이언트 에이전트로 인가 승인 코드(authorization code)를 발급하는 단계: 클라이언트는 인가 제공자로 인가 승인 코드 및 리다이렉션 URI 등을 전달함으로써, 액세스 토큰 발급을 요청하는 단계; 클라이언트는 발급받은 액세스 토큰을 활용하여 자원 서버에 자원 소유자의 자원에 대한 접근 요청을 하는 단계: 자원 서버는 인가 제공자에게 액세스 토큰에 대한 검증 요청을 보내어 최종적으로 액세스 토큰 유효성을 재차 확인하는 단계; 및 자원 서버가 인가 제공자로부터 액세스 토큰이 유효하다는 응답 결과를 받았을 경우, 클라이언트에게 액세스 토큰에 표현되어 있는 범위의 자원을 전달하는 단계; 를 포함할 수 있다.

[0030] 제안된 발명의 다른 일 양상에 따르면, 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법은, 에이전트 사용자가 클라이언트 에이전트인 웹 브라우저를 통해 인가 요청을 위한 설정을 입력한 후, 클라이언트가 인가 제공자로 에이전트 사용자의 요구사항을 포함한 인가 요청을 웹브라우저를 통해 전달하는 단계; 인가 제공자는 웹 브라우저에서 리다이렉트 정보와 자원 접근 범위 및 권한 정보를 포함하는 QR 코드를 생성하고 웹 브라우저에 표시되도록 전달하는 단계; 자원 소유자는 본인의 모바일 폰으로 에이전트 사용자의 웹 브라우저에 로드된 QR 코드를 스캔하는 단계; 및 자원 소유자의 모바일 폰은 QR 코드 내 자원 접근 범위 및 권한 정보를 확인하고, 승인할 경우에는 생체 인증 등 다양한 사용자 인증 처리를 하고 승인 결과를 인가제공자로 전달하는 과정을 리다이렉트 기능을 활용하여 진행하는 단계; 를 더 포함할 수 있다.

발명의 효과

[0031] 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법 및 장치는, 기존 OAuth 2.0 프로토콜의 문제점을 해결하는 블록 체인 기반 인가 프로토콜 방법 및 장치로 기존의 OAuth 2.0 프로토콜과 상호 연동 가능하며 실용성을 높이는 인가 프로토콜을 제공할 수 있다.

[0032] 첫째, 공격자가 클라이언트 해킹을 통해 액세스 토큰을 탈취하더라도, 자원 서버에서 블록 체인 상 대체 불가능 토큰을 통해 액세스 토큰의 소유자가 유효한 사용자인지 검증하기 때문에, 유효하지 않은 공격자는 사용자 자원에 접근할 수 없다.

[0033] 둘째, 중앙 집중식 인가 서버의 경우 관리자의 악의적 공격을 통해 사용자 동의 없이도 액세스 토큰 발급이 가능하지만, 본 발명의 경우 사용자 인증은 블록 체인 DID 컨트랙트를 통해 진행되므로, 반드시 사용자 동의에 의해서만 액세스 토큰이 발급된다.

[0034] 셋째, 중앙 집중식 인가 서버 경우 사용자 인증 정보를 서버에서 관리하므로 해킹시 대규모로 사용자 인증 정보가 유출될 수 있다. 본 발명에서 사용자 인증은 블록 체인 DID로 사용자 직접 관리하기 때문에, 수많은 사용자 계정들이 한 번에 유출되지 않는다.

[0035] 넷째, 블록 체인 상 대체 불가능 토큰 전송 혹은 생성을 통해 인가 프로토콜 전과정을 재실행하지 않고도 필요한 클라이언트들에게 액세스 토큰을 발행할 수 있다.

[0036] 다섯째, 액세스 토큰을 클라이언트에서 관리한다고 하더라도, 블록 체인 상 대체 불가능 토큰의 폐기를 통해 발급된 액세스 토큰의 만료 전 폐기가 가능하다.

[0037] 본 발명은 OAuth 2.0 프로토콜과 동일하게 OpenID Connect(OIDC)와 같이 사용자 인증 프로토콜을 사용할 수 있

다. 특히 본 발명은 사용자 인증이나 장치 신원 증명에 블록 체인에서 관리하는 탈중앙 신원 정보 DID(Decentralized Identifier) 를 기반하고 있어 어떤 환경에서도 사용자 인증이 적용 가능하며, 더욱이 접근 자원 범위 및 권한을 제어하는 기능을 활용하면 사용자 정보 공유를 제어하는 서비스에도 광범위하게 적용할 수 있다.

[0038] 최근 시행되는 마이데이터 서비스의 경우에 개인 프라이버시 보호를 위해 개인이 직접 정보 공유 범위에 대하여 승인하고 제어할 수 있어야 하므로, 마이데이터 서비스에도 반드시 필요한 프로토콜을 제공할 수 있다.

도면의 간단한 설명

[0039] 도 1은 가장 널리 사용되고 있는 권한 부여 타입인 인가 승인 코드 권한 부여 타입 기반 OAuth 2.0의 인가 흐름을 보여주는 도면이다.

도 2는 OAuth 2.0 프로토콜과 상호 연동 가능한 블록 체인 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 도면이다.

도 3은 OAuth 2.0 기반 탈중앙화 인가 프로토콜의 인가 흐름의 한 예로서, QR 코드를 활용한 OAuth 2.0 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 도면이다.

도 4는 블록 체인 기반 인가 제공자의 구조를 나타내는 도면이다. 인가 제공자는 인가 프록시와 내부 블록 체인으로 구성된다.

도 5는 블록 체인 상에 배포되는 대체 불가능 토큰(NFT)의 한 가지 예를 나타내는 도면이다.

도 6은 OAuth 2.0 기반 탈중앙화 인가 프로토콜을 구성하는 방식의 한 가지 예로서, 여러 기관들이 참가하는 컨소시움 환경에서 OAuth 2.0과 연동 가능한 블록 체인 기반 탈중앙화 인가 프로토콜을 보여주는 도면이다.

도 7은 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법의 일 실시예에 따른 권한 부여 타입인 인가 승인 코드 권한 부여 타입 기반 OAuth 2.0의 인가 흐름을 보여주는 순서도이다.

도 8은 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법의 일 실시예에 따른 OAuth 2.0 프로토콜과 상호 연동 가능한 블록 체인 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 순서도이다.

도 9는 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법의 일 실시예에 따른 OAuth 2.0 기반 탈중앙화 인가 프로토콜의 인가 흐름의 한 예로서, QR 코드를 활용한 OAuth 2.0 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0040] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 예시를 가질 수 있는바, 특정 예시를 도면을 통해 상세하게 설명하고자 한다.

[0041] 그러나 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해해야 한다.

[0042] 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 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0043] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0044] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부

품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0045] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술이 문맥상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않아야 한다.

[0046] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0048] OAuth 2.0 프로토콜에서는 사용자 자원을 관리하는 자원 서버, 사용자 인증 과정을 수행하고 액세스 토큰을 발행하는 인가 서버, 제3의 클라이언트, 사용자 등으로 구성된 환경을 가정한다. 본 발명에서는 인가 서버 기능을 블록 체인 기반 서비스로 구성하고, 요구에 따라 기능을 확장할 수 있다. 또한, 클라이언트, 자원 서버, 사용자와 블록 체인 간의 통신을 담당하는 인가 프록시를 정의함으로써, 기존 OAuth 2.0 프로토콜과 상호 연동을 지원한다.

[0049] 인가 서버 기능을 제공하는 블록 체인 기반 서비스는 스마트 컨트랙트(smart contract)로 구성하며, 여기에는 사용자 신원 정보를 관리하는 DID(Decentralized Identifier, 탈중앙 신원) 컨트랙트와 OAuth 2.0 액세스 토큰을 관리하는 인가 컨트랙트로 구성한다.

[0050] 본 발명에서는 DID 컨트랙트는 따로 정의하지 않고, 마이크로소프트 ION, Sovrin, W3C DID, 하이퍼레저 인디(Hyperledger Indy), DID Alliance, Initial DID, MyID 등과 같은 기존 블록 체인 기반 탈중앙 신원 관리 기법과 연동하는 것을 가정한다. 사용자는 DID 컨트랙트를 통해 사용자 신원 인증을 진행하며, DID 컨트랙트에서 사용자 신원 인증 후 랜덤 인가 승인 코드를 사용자에게 전달한다. 인가 승인 코드는 현재 진행중인 인가 프로토콜 과정이 유효함을 증명하는 데 활용한다. 사용자는 인가 승인 코드를(사용자 자원 접근을 요청하는) 클라이언트에게 전달하고, 클라이언트는 인가 승인 코드를 인가 컨트랙트로 전송함으로써 액세스 토큰 발급을 요청한다. 인가 컨트랙트는 클라이언트에서 전송한 인가 승인 코드가 유효한지 먼저 확인하고, 해당 코드가 유효할 경우, 인가 승인 코드에 따른 액세스 토큰을 발행하고 클라이언트에게 전송한다. 액세스 토큰을 클라이언트에게 전송하는 이유는 기존 OAuth 2.0 프로토콜과의 상호 연동을 가능하게 하기 위함이다. 액세스 토큰은 인가 컨트랙트에서 관리하는 대체 불가능 토큰(Non-fungible Token) 형태로 블록 체인 상에서 발행되고 관리되며, 액세스 토큰 속성(attributes)들은 기존 OAuth 2.0에서 정의하는 액세스 토큰 속성을 포함하고 필요시 확장 가능하다.

[0051] 본 발명에서 액세스 토큰은 하나의 대체불가능 토큰으로 블록 체인 상에서 관리되므로, 액세스 토큰 생성/폐기 등 전주기 관리가 용이하며, 또한 클라이언트 에이전트 별 고유 정보를 저장함으로써 발급된 액세스 토큰이 특정 클라이이언트 에이전트를 통해 발급되었음을 확인할 수 있다. 블록 체인 상 관리되는 액세스 토큰은 투명성, 불변성 등을 보장하고, 또한 인가 프로토콜 전 과정에서 필요한 경우 블록 체인 상 검증 과정을 추가할 수 있다.

[0052] 본 발명에서는 자원 서버가 클라이언트에게 사용자 자원을 전달하기 전, 블록 체인 상 액세스 토큰의 유효성을 다시 한번 검증하는 과정을 추가하는 것을 일 실시예로 제안한다.

[0054] 도 1은 가장 널리 사용되고 있는 권한 부여 타입인 인가 승인 코드 권한 부여 타입 기반 OAuth 2.0의 인가 흐름을 보여주는 도면이다.

[0055] 도 1을 참조하면, 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법 은, 클라이언트(200)가 자원 소유자(100)에게 인가를 요청하면서 인가 흐름이 시작된다(S100).

[0056] 자원 소유자(100)의 클라이언트 에이전트(보통 웹브라우저 형식으로 제공되므로 이하 웹브라우저로 표기하기로 함)(110)는 클라이언트(200)의 요청을 받은 후 인가 서버(300)의 인가 엔드포인트(authorization endpoint)로 리다이렉트(redirect)된다(S101). 리다이렉트 시, 인가 서버(300)에 클라이언트 ID, 접근 권한 범위(scope), 상태 정보(state), 리다이렉션 URI(uniform Resource Identifier) 등이 함께 전달된다. 자원 소유자(100)는 웹브라우저(110)를 통해 인가 서버(300)에서 사용자 인증을 한 후, 클라이언트(200)에게 접근 권한 범위에 해당하는 자원에 대한 접근 권한을 승인 또는 거절한다(S101).

[0057] 만약 자원 소유자(100)가 인가 요청을 승인할 경우, 인가 서버(300)는 자원 소유자(100)의 웹 브라우저(110)를

리다이렉션 URI로 리다이렉트한다(S110).

[0058] 리다이렉트 시, 인가 서버(300)는 리다이렉션 URI에 인가 승인 코드 및 상태 정보 등을 포함시켜서 클라이언트(200)로 전달한다(S111).

[0059] 클라이언트(200)는 인가 서버(300)의 토큰 엔드포인트(token endpoint)에 인가 승인 코드 및 리다이렉션 URI 등을 전달하며 액세스 토큰 발급을 요청한다(S120). 이때, 인가 서버(300)에서 클라이언트(200) 인증도 수행한다.

[0060] 인가 서버(300)는 인가 토큰을 검증하여 인가 승인 코드가 유효할 경우, 클라이언트(200)에게 액세스 토큰을 발급해준다(S130). 이때, 필요할 경우 갱신 토큰도 함께 발급해준다. 액세스 토큰은 일반적으로 만료 기간을 짧게 하여 발급하기 때문에, 클라이언트(200)가 앞선 흐름(S100, S101, S110, S111, S120, S130)을 거치지 않고 액세스 토큰을 재발급 받는 것을 허용해주기 위해 갱신 토큰을 발급해줄 수 있다. 클라이언트(200)는 갱신 토큰을 통해서 인가 서버(300)에게 곧바로 액세스 토큰을 재발급 받을 수 있다(S120, S130).

[0061] 클라이언트(200)는 액세스 토큰을 통해 자원 서버(400)에 자원에 대한 접근 요청을 한다(S140).

[0062] 자원 서버(400)는 액세스 토큰을 검증하여 액세스 토큰이 유효한 경우, 액세스 토큰에서 허용하는 접근 권한 범위에 해당하는 자원을 클라이언트(200)에게 제공해준다(S150).

[0064] 도 2는 OAuth 2.0 프로토콜과 상호 연동 가능한 블록 체인 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 도면이다.

[0065] 도 2를 참조하면, 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜은 OAuth 2.0의 인가 승인 코드 권한 부여 타입 기반 인가 흐름을 기본적으로 포함한다. 다만, 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜은 OAuth 2.0의 인가 흐름에 추가적인 동작 흐름(S1090, S1100)을 포함하며, 클라이언트 서비스 사용자(에이전트 사용자(2000)와 자원 소유자(1000)가 다를 수도 있는 환경에서의 인가 프로토콜 과정을 대상으로 한다.

[0066] 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 장치를 구성하는 엔티티 중 인가 제공자(4000)를 제외한 모든 엔티티, 즉 자원 소유자(1000), 에이전트 사용자(2000), 클라이언트 에이전트(2100), 클라이언트(3000), 자원 서버(5000)는 블록 체인 기반 인가 제공자(이하 인가 제공자)(4000) 내에서 유지/관리하는 신원 증명 정보 DID(Decentralized ID)를 소유하고 있다.

[0067] 1. 동작(S1000): 에이전트 사용자(2000)는 클라이언트에서 제공하는 서비스를 활용하기 위해 먼저 웹 브라우저, 즉 클라이언트 에이전트(2100)를 통해 자원 소유자(1000) 의 자원 접근 인가 요청을 위한 설정을 입력한다. 설정 정보로는 접근하고자 하는 자원 소유자의 자원 범위뿐 아니라 접근 권한 등을 포함한다.

[0068] 2. 동작(S1010, S1011): 클라이언트(3000)는 클라이언트 에이전트(2100)을 통해 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 보낸다(S1010, S1011).

[0069] 3. 동작(S1020, S1030): 인가 제공자(4000)는 자원 소유자(1000)에게 클라이언트(3000)에 대한 사용자 인증 혹은 자원 접근 인가 승인 요청을 보낸다. 자원 소유자(1000)는 클라이언트에 대한 인가 승인 요청 내용, 즉 접근하고자 하는 자원 범위 그리고 접근 권한 등을 확인한 후, 인가 승인 요청에 동의하는 경우에는 본인의 모바일 폰(1100)을 통해 생체 인증, 개인 식별 고유 번호/패턴 입력 등 다양한 방법으로 클라이언트(3000)에 대한 인가 승인 요청을 승인 처리한다. 만일 인가 승인 요청을 거절하는 경우에는 승인 처리 과정을 진행하지 않는다. 자원 소유자 모바일 폰(1100) 에서의 승인 처리 결과는 인가 제공자(4000)으로 전송된다.

[0070] 4. 동작(S1050): 인가 제공자(4000)는 자원 소유자 모바일 폰(1100) 으로부터 승인 처리 결과 응답 메시지를 수신하고, 자원소유자의 유효한 승인 여부를 검증한 후, 클라이언트 에이전트(2100)로 인가 승인 코드(authorization code)를 발급한다. 인가 승인 코드 발급시 인가 제공자(4000)는 클라이언트 에이전트인 웹 브라우저(2100)를 클라이언트(3000)의 리다이렉션 URI로 설정한다. 웹 브라우저(2100)는 리다이렉션 URI에 인가 승인 코드 및 상태 정보 등을 포함시켜서 클라이언트(3000)로 전달한다.

[0071] 5. 동작(S1060, S1070): 클라이언트(3000)는 인가 제공자(4000)로 인가 승인 코드 및 리다이렉션 URI 등을 전달함으로써, 액세스 토큰 발급을 요청한다. 인가 제공자(4000)는 클라이언트(3000)로부터 액세스 토큰 발급 요청을 받으면, 먼저 인가 승인 코드의 유효성을 검증하고, 유효한 경우에는 액세스 토큰을 발급하고, 클라이언트(3000) 에게 전송한다.

[0072] 6. 동작(S1080): 클라이언트(3000)는 발급받은 액세스 토큰을 활용하여 자원 서버(5000)에 자원 소유자의 자원에 대한 접근 요청을 한다.

[0073] 7. 동작(S1090, S1100): 자원 서버(5000)는 인가 제공자(4000)에게 액세스 토큰에 대한 검증 요청을 보내어 최종적으로 액세스 토큰 유효성을 한번 더 확인한다. 인가 제공자(4000)는 관리하고 있는 액세스 토큰 정보를 기반으로 요청 받은 액세스 토큰 유효성을 확인한 후 결과를 자원 서버(5000)로 전달한다.

[0074] 8. 동작(S1110): 자원 서버(5000)가 인가 제공자(4000) 로부터 액세스 토큰이 유효하다는 응답 결과를 받았을 경우, 클라이언트(3000) 에게 액세스 토큰에 표현되어 있는 범위의 자원을 전달한다.

[0076] 도 3은 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜의 인가 흐름의 한 예로서, QR 코드를 활용한 OAuth 2.0 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 도면이다.

[0077] 도 3을 참조하면, 자원 소유자의 모바일 폰(1100)으로 사용자 인증 혹은 자원 접근 인가 승인 요청 메시지를 보내기 위해서 QR 코드를 활용한다.

[0078] 에이전트 사용자(2000)가 클라이언트 에이전트인 웹 브라우저(2100)를 통해 인가 요청을 위한 설정을 입력한 후(S1000), 클라이언트(3000)가 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 웹 브라우저(2100)를 통해 전달한다(S1010, S1011).

[0079] 인가 제공자(4000)는 웹 브라우저(2100) 에서 리다이렉트 정보와 자원 접근 범위 및 권한 정보를 포함하는 QR 코드를 생성하고 웹 브라우저(2100)에 표시되도록 전달한다(S1050).

[0080] 자원 소유자(1000)는 본인의 모바일 폰(1100)으로 에이전트 사용자(2000)의 웹 브라우저(2100)에 로드된 QR 코드를 스캔한다(S2000).

[0081] 자원 소유자(1000)의 모바일 폰(1100)은 QR 코드 내 자원 접근 범위 및 권한 정보를 확인하고, 승인할 경우에는 생체 인증 등 다양한 사용자 인증 처리를 하고 승인 결과를 인가제공자(4000)으로 전달하는 과정을 리다이렉트 기능을 활용하여 진행한다. 이후의 흐름은 도2의 인가 흐름과 동일하다.

[0082] 자원 소유자(1000)의 모바일 폰(1100)으로 사용자 인증 및 자원 접근 인가 승인 요청 메시지를 보내는 방식은 도 3과 같이 QR 코드를 활용하는 방법 이외에도 다양한 방법을 채택할 수 있다. 예를 들면, 인가 제공자(4000)가 자원 소유자(1000)의 모바일 폰(1100)로 사용자 인증 및 인가 승인 과정을 진행할 수 있는 URL을 문자 메시지로 보내면, 자원 소유자(1000)가 모바일 폰(1100)을 통해 해당 URL 을 접근하는 방법을 채택할 수 있다. 또는 본 프로토콜의 사용자 인증 및 인가 승인 과정을 처리할 수 있는 모바일 앱이 자원 소유자(1000)의 모바일 폰(1100)에 설치되어 있는 경우, 인가 제공자(4000)는 자원 소유자(1000)에게 해당 앱을 통해 푸시(push) 메시지를 보내 사용자 인증 및 인가 승인 과정을 진행하는 방법을 채택할 수 있다.

[0084] 도 4는 블록 체인 기반 인가 제공자(이하, 인가 제공자)(4000) 의 구조를 나타내는 도면이다.

[0085] 도 4를 참조하면, 인가 제공자(4000)는 인가 프록시(4100)와 내부 블록 체인(4200)으로 구성된다. 인가 프록시(4100)는 내부 블록 체인(4200) 동작에 대한 RESTful API 와 같은 외부 인터페이스를 담당하며, 인가 제공자(4000) 기능을 활용하기 위해서는 인가 프록시(4100)에게 요청을 전송한다. 인가 프록시(4100) 는 외부에서 받은 요청을 내부 블록 체인(4200)으로 전달하고, 처리 결과를 받은 후, 다시 외부로 응답을 전달한다. 블록 체인(4200) 은 두 가지 스마트 컨트랙트들을 실행하는데, DID 스마트 컨트랙트(4220)와 인가 스마트 컨트랙트(4210)이다.

[0086] DID 스마트 컨트랙트(4220)는 자원 소유자(1000), 에이전트 사용자(2000), 클라이언트 에이전트(2100), 클라이언트(3000), 자원 서버(5000) 등 인가 제공자(4000)로 요청을 보내는 모든 장치들의 신원을 인증할 수 있도록 신원 증명 정보 DID(Decentralized ID)를 블록 체인 상에 유지/관리한다. 본 발명에서는 DID 정보를 관리하는 엔티티로 DID 스마트 컨트랙트를 정의함으로써, 다양한 표준안들이 제시되어 있는 기존 DID 표준 방법들과의 연동을 고려할 수 있도록 한다.

[0087] 인가 스마트 컨트랙트(4210)는 클라이언트 에이전트(2100) 에서의 인가 승인 코드 생성 요청(S1011) 과정에서부터 관여하게 되며, 인가 코트 생성 요청은 인가 스마트 컨트랙트(4210)에서 대체 불가능 토큰(non-fungible token, NFT)을 생성하고 여기에 발급하는 인가 승인 코드 정보를 속성으로 관리한다. 발급된 NFT를 기반으로 인가 프록시(4100)는 인가 승인 코드를 발급하고 회신한다. 인가 승인 코드 발급 요청시 새롭게 생성한 블록 체인 상 NFT는 이후 액세스 토큰 발급에 사용된다. 인가 프록시(4100)가 클라이언트(3000)로부터 액세스 토큰 발급 요청을 전달받으면, 이를 인가 스마트 컨트랙트(4210)에 전달한다. 인가 스마트 컨트랙트(4210) 는 액세스 토큰 발급 요청의 유효성을 해당 인가 승인 코드를 속성으로 저장하고 있는 NFT를 통해 검증한다. 모두 유효한 경우, 관련된 대체 불가능 NFT 속성에 액세스 토큰 정보를 추가 저장한다. 이 후, 인가 스마트 컨트랙트(4210)는 해당

NFT을 기반으로 액세스 토큰을 발급하고, 인가 프록시(4100)는 해당 액세스 토큰을 OAuth 2.0 액세스 토큰 형식에 맞추어 구성한 후 클라이언트(3000)로 액세스 토큰을 전달한다.

[0089] 도 5는 블록 체인 상에 배포되는 대체 불가능 토큰(NFT)의 한 가지 예를 나타내는 도면이다.

[0090] 도 5를 참조하면, 대체 불가능 토큰(Non-Fungible Token, NFT)은 다양한 속성(attribute) 들로 정의할 수 있다.

[0091] id 속성은 블록 체인(4200) 상에서 NFT를 유일하게 식별할 수 있는 토큰 ID를 나타낸다.

[0092] Type 속성은 NFT가 인가 승인 코드 발급 단계인지 액세스 토큰 발급 단계인지를 나타낸다. 즉, type 속성값을 기반으로 NFT은 인가 승인 코드 또는 액세스 토큰 검증에 사용한다.

[0093] Owner 속성은 대체 불가능 토큰의 소유자를 나타낸다. NFT가 처음 생성될 때, 즉 인가 승인 코드 발급될 때, owner 속성값은 자원 소유자로 설정된다. 이후 클라이언트 에서 해당 인가 승인 코드에 기반하여 액세스 토큰 발행을 요청할 때, 클라이언트 자격 검증과 인가 승인 코드 유효성이 검증된 후 owner 속성값은 자원 소유자에서 클라이언트로 변경된다.

[0094] Approvee 속성은 NFT의 소유권을 변경할 수 있는 권한을 가진 엔티티를 의미한다. 인가 승인 코드를 발급하기 위해 대체 불가능 토큰이 처음 생성될 때, approvee 속성값은 인가 승인 코드 발급 요청한 클라이언트로 설정되며, 이후 액세스 토큰 발급 시에는 approvee 속성값은 자원 소유자로 설정된다. 이는 액세스 토큰을 발급받은 클라이언트가 NFT 속성을 임의로 변경하지 못하게 하며, 어떤 경우든 자원 소유자의 동의를 받아야 함을 강제할 수 있다.

[0095] Issuer 속성은 인가 자격 증명 발급을 발행해주는 주체, 즉 자원 소유자를 나타낸다.

[0096] Subject 속성은 액세스 토큰을 활용하여 자원 접근을 요청하는 주체, 즉 클라이언트를 나타낸다.

[0097] Audience 속성은 액세스 토큰을 전달받아, 액세스 토큰을 기반으로 자원을 제공해주는 주체, 즉 자원 서버를 나타낸다.

[0098] Code 속성은 인가 승인 코드를 표현하는 문자열을 나타낸다.

[0099] Scope 속성은 NFT로 승인된 자원 접근 범위를 나타낸다.

[0100] State 속성은 NFT 상태 정보를 나타낸다.

[0101] Access_token 속성은 액세스 토큰을 표현하는 문자열을 나타낸다.

[0102] Redirect_uri 속성은 클라이언트로 리다이렉트하는 콜백 URI을 나타낸다.

[0103] Issued_at 속성은 인가 자격 증명의 발행 시간을 나타낸다.

[0104] Expire_in 속성은 인가 자격 증명의 만료 시간을 나타낸다.

[0105] Revoked 속성은 대체 불가능 토큰이 폐기되었는지 여부를 나타낸다.

[0106] 대체 불가능 토큰을 구성하는 속성들은 위에서 언급된 속성들 이외에도 필요에 의해 확장되어 구성될 수 있다.

[0108] 도 6은 OAuth 2.0 기반 탈중앙화 인가 프로토콜을 구성하는 방식의 한 가지 예로서, 여러 기관들이 참가하는 컨소시움 환경에서 OAuth 2.0과 연동 가능한 블록 체인 기반 탈중앙화 인가 프로토콜을 보여주는 도면이다.

[0109] 도 6을 참조하면, OAuth 2.0 기반 탈중앙화 인가 프로토콜을 구성하는 방식의 4개 기관들이 참가하는 컨소시움 환경을 보여준다. 컨소시움 환경에서는 각 기관별로 관리하는 자원 서버들(5110, 5120, 5130, 5140)과 인가 제공자(4000)를 구성하는 블록 체인(4200) 구성을 고려해야 한다. 자원 소유자(1000), 모바일 디바이스(1100), 에이전트 사용자(2000), 웹 브라우저(2100), 클라이언트(3000), 자원 서버(5100, 5110, 5120, 5130, 5140) 들의 신원 자격 증명은 블록 체인 상 DID 로 관리하므로, 특정 기관에서 관리하는 계정에 의존할 필요 없이 컨소시움 환경에서 효과적인 신원 인증이 가능하다.

[0110] 컨소시움 환경에서의 블록 체인 구성은 하이퍼레저 패브릭 등 컨소시움 블록 체인 플랫폼을 활용하여 구성할 수 있으며, 이 경우, 각 기관별로 블록 체인 노드(4310, 4320, 4330, 4340)로 참여함으로써 블록 체인(4200)을 구성한다. 컨소시움 환경에서의 자원 서버 구성에서는 기관별로 관리하는 자원 서버들(5110, 5120, 5130, 5140)을 하나로 통합시켜 처리하는 중계 자원서버(5100)을 둘 수 있다.

[0111] 중계 자원서버(5100)는 각 기관별 자원 관리 방식 및 표현 양식이 상이할 수 있으므로, 이를 처리하는 기능을 담당하며, 또한 자원 소유자(1000) 의 자원들이 여러 기관들에 분산되어 저장된 경우에도 클라이언트에게 하나의 액세스 토큰으로 처리하는 기능도 담당한다. 다시 설명하자면, 클라이언트(3000)에서 기관 별 자원 서버(5110, 5120, 5130, 5140)에 분산 저장된 자원 소유자(1000)의 자원을 접근하기 위해서는, 각 기관 별 자원 서버당 액세스 토큰을 개별적으로 발급받아야 한다. 즉, 기관 1 자원 서버를 위한 액세스 토큰, 기관 2 자원 서버를 위한 액세스 토큰, 기관 3 자원 서버를 위한 액세스 토큰, 기관 4 자원 서버를 위한 액세스 토큰을 각각 발급 받아야 한다.

[0112] 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 장치의 예시에서, 클라이언트(3000)는 중계 자원 서버(5100)에게 자원 접근 요청을 보내고, 중계 자원 서버(5100)가 각각의 기관 별 자원 서버(5110, 5120, 5130, 5140)에 자원들을 요청하는 방식으로 구성할 경우, 클라이언트(3000)는 한 개의 액세스 토큰만 발급받더라도 여러 기관들에서 호스팅하는 자원들을 한꺼번에 제공받을 수 있다.

[0113] 중계 자원 서버(5100)는 클라이언트(3000)로부터 전달받은 액세스 토큰을 분석한 후, 액세스 토큰에서 허용한 기관 별 자원들을 기관 별 자원 서버에 요청하여 전달받은 후, 해당 자원들을 클라이언트에게 반환하게 된다.

[0115] 도 7은 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법의 일 실시예에 따른 권한 부여 타입인 인가 승인 코드 권한 부여 타입 기반 OAuth 2.0의 인가 흐름을 보여주는 순서도이다.

[0116] 도 7을 참조하면, 본 발명의 일 실시예에서 블록 체인 기반 탈중앙화 인가 프로토콜 방법은, S100 내지 S150 단계를 포함할 수 있다.

[0117] S100 단계는 클라이언트(200)가 자원 소유자(100)에게 인가를 요청하면서 인가 흐름이 시작되는 단계이다.

[0118] S101 단계는 자원 소유자(100)의 클라이언트 에이전트(110)가 클라이언트(200)의 요청을 받은 후 인가 서버(300)의 인가 엔드포인트(authorization endpoint)로 리다이렉트(redirect)되는 단계이다.

[0119] S110 단계는, 자원 소유자(100)가 인가 요청을 승인할 경우, 인가 서버(300)는 자원 소유자(100)의 웹 브라우저(110)를 리다이렉션 URI로 리다이렉트하는 단계이다.

[0120] S111 단계는, 리다이렉트 시, 인가 서버(300)는 리다이렉션 URI에 인가 승인 코드 및 상태 정보를 포함시켜서 클라이언트(200)로 전달하는 단계이다.

[0121] S120 단계는, 클라이언트(200)는 인가 서버(300)의 토큰 엔드포인트(token endpoint)에 인가 승인 코드 및 리다이렉션 URI 등을 전달하며 액세스 토큰 발급을 요청하는 단계이다.

[0122] S130 단계는, 인가 서버(300)는 인가 토큰을 검증하여 인가 승인 코드가 유효할 경우, 클라이언트(200)에게 액세스 토큰을 발급해주는 단계이다.

[0123] S140 단계는, 클라이언트(200)는 액세스 토큰을 통해 자원 서버(400)에 자원에 대한 접근 요청을 하는 단계이다.

[0124] S150 단계는, 자원 서버(400)는 액세스 토큰을 검증하여 액세스 토큰이 유효한 경우, 액세스 토큰에서 허용하는 접근 권한 범위에 해당하는 자원을 클라이언트(200)에게 제공해주는 단계이다.

[0126] 도 8은 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법의 일 실시예에 따른 OAuth 2.0 프로토콜과 상호 연동 가능한 블록 체인 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 순서도이다.

[0127] 도 8을 참조하면, 본 발명의 일 실시예에서 블록 체인 기반 탈중앙화 인가 프로토콜 방법은, S1000 내지 S1110 단계를 포함할 수 있다.

[0128] S1000 단계는 에이전트 사용자(2000)는 클라이언트에서 제공하는 서비스를 활용하기 위해 먼저 웹 브라우저인 클라이언트 에이전트(2100)를 통해 자원 소유자(1000) 의 자원 접근 인가 요청을 위한 설정을 입력하는 단계이다.

[0129] S1010, S1011 단계는, 클라이언트(3000)는 클라이언트 에이전트(2100)을 통해 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 보내는 단계이다.

[0130] S1020, S1030 단계는 인가 제공자(4000)는 자원 소유자(1000)에게 클라이언트(3000)에 대한 사용자 인증 혹은 자원 접근 인가 승인 요청을 보내는 단계이다.

[0131] S1050 단계는 인가 제공자(4000)는 자원 소유자 모바일 폰(1100) 으로부터 승인 처리 결과 응답 메시지를 수신하고, 자원소유자의 유효한 승인 여부를 검증한 후, 클라이언트 에이전트(2100)로 인가 승인 코드(authorization code)를 발급하는 단계이다.

[0132] S1060, S1070 단계는 클라이언트(3000)는 인가 제공자(4000)로 인가 승인 코드 및 리다이렉션 URI 등을 전달함으로써, 액세스 토큰 발급을 요청하는 단계이다.

[0133] S1080 단계는 클라이언트(3000)는 발급받은 액세스 토큰을 활용하여 자원 서버(5000)에 자원 소유자의 자원에 대한 접근 요청을 하는 단계이다.

[0134] S1090, S1100 단계는 자원 서버(5000)는 인가 제공자(4000)에게 액세스 토큰에 대한 검증 요청을 보내어 최종적으로 액세스 토큰 유효성을 재차 확인하는 단계이다.

[0135] S1110 단계는 자원 서버(5000)가 인가 제공자(4000) 로부터 액세스 토큰이 유효하다는 응답 결과를 받았을 경우, 클라이언트(3000) 에게 액세스 토큰에 표현되어 있는 범위의 자원을 전달하는 단계이다.

[0137] 도 9는 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법의 일 실시예에 따른 OAuth 2.0 기반 탈중앙화 인가 프로토콜의 인가 흐름의 한 예로서, QR 코드를 활용한 OAuth 2.0 기반 탈중앙화 인가 프로토콜의 인가 흐름을 보여주는 순서도이다.

[0138] 도 9를 참조하면, 본 발명의 일 실시예에서 블록 체인 기반 탈중앙화 인가 프로토콜 방법은, S1010 내지 S3000 단계를 S1000 내지 S1110 단계에 더 포함할 수 있다.

[0139] S1010, S1011 단계는, 에이전트 사용자(2000)가 클라이언트 에이전트인 웹 브라우저(2100)를 통해 인가 요청을 위한 설정을 입력한 후(S1000), 클라이언트(3000)가 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 웹브라우저(2100)를 통해 전달하는 단계이다.

[0140] S1050 단계는 인가 제공자(4000)는 웹 브라우저(2100) 에서 리다이렉트 정보와 자원 접근 범위 및 권한 정보를 포함하는 QR 코드를 생성하고 웹 브라우저(2100)에 표시되도록 전달하는 단계이다.

[0141] S2000 단계는 자원 소유자(1000)는 본인의 모바일 폰(1100)으로 에이전트 사용자(2000)의 웹 브라우저(2100)에 로드된 QR 코드를 스캔하는 단계이다.

[0142] S3000 단계는 자원 소유자(1000)의 모바일 폰(1100)은 QR 코드 내 자원 접근 범위 및 권한 정보를 확인하고, 승인할 경우에는 생체 인증 등 다양한 사용자 인증 처리를 하고 승인 결과를 인가제공자(4000)로 전달하는 과정을 리다이렉트 기능을 활용하여 진행하는 단계이다.

[0144] 본 발명의 블록 체인 기반 탈중앙화 인가 프로토콜 방법 및 장치는, 기존 OAuth 2.0 프로토콜의 문제점을 해결하는 블록 체인 기반 인가 프로토콜 방법 및 장치로 기존의 OAuth 2.0 프로토콜과 상호 연동 가능하며 실용성을 높이는 인가 프로토콜을 제공할 수 있다.

[0145] 첫째, 공격자가 클라이언트 해킹을 통해 액세스 토큰을 탈취하더라도, 자원 서버에서 블록 체인 상 대체 불가능 토큰을 통해 액세스 토큰의 소유자가 유효한 사용자인지 검증하기 때문에, 유효하지 않은 공격자는 사용자 자원에 접근할 수 없다.

[0146] 둘째, 중앙 집중식 인가 서버의 경우 관리자의 악의적 공격을 통해 사용자 동의 없이도 액세스 토큰 발급이 가능하지만, 본 발명의 경우 사용자 인증은 블록 체인 DID 컨트랙트를 통해 진행되므로, 반드시 사용자 동의에 의해서만 액세스 토큰이 발급된다.

[0147] 셋째, 중앙 집중식 인가 서버 경우 사용자 인증 정보를 서버에서 관리하므로 해킹시 대규모로 사용자 인증 정보가 유출될 수 있다. 본 발명에서 사용자 인증은 블록 체인 DID로 사용자 직접 관리하기 때문에, 수많은 사용자 계정들이 한 번에 유출되지 않는다.

[0148] 넷째, 블록 체인 상 대체 불가능 토큰 전송 혹은 생성을 통해 인가 프로토콜 전과정을 재실행하지 않고도 필요한 클라이언트들에게 액세스 토큰을 발행할 수 있다.

[0149] 다섯째, 액세스 토큰을 클라이언트에서 관리한다고 하더라도, 블록 체인 상 대체 불가능 토큰의 폐기를 통해 발급된 액세스 토큰의 만료 전 폐기가 가능하다.

[0150] 본 발명은 OAuth 2.0 프로토콜과 동일하게 OpenID Connect(OIDC)와 같이 사용자 인증 프로토콜을 사용할 수 있

다. 특히 본 발명은 사용자 인증이나 장치 신원 증명에 블록 체인에서 관리하는 탈중앙 신원 정보 DID(Decentralized Identifier) 를 기반하고 있어 어떤 환경에서도 사용자 인증이 적용 가능하며, 더욱이 접근 자원 범위 및 권한을 제어하는 기능을 활용하면 사용자 정보 공유를 제어하는 서비스에도 광범위하게 적용할 수 있다.

[0151] 최근 시행되는 마이데이터 서비스의 경우에 개인 프라이버시 보호를 위해 개인이 직접 정보 공유 범위에 대하여 승인하고 제어할 수 있어야 하므로, 마이데이터 서비스에도 반드시 필요한 프로토콜을 제공할 수 있다.

[0152] 본 발명의 실시예들에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있 는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0153] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만 들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇 몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0154] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그래머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방 법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다. 이상 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0155] 100 : 자원 소유자

110 : 클라이언트 에이전트

200 : 클라이언트

300 : 인가 서버

400 : 자원 서버

1000 : 자원 소유자

1100 : 자원 소유자 모바일 폰

2000 : 에이전트 사용자

2100 : 클라이언트 에이전트

3000 : 클라이언트

4000 : 블록 체인 기반 인가 제공자

4100 : 인가 프록시

4200 : 내부 블록 체인

4210 : 인가 스마트 컨트랙트

4220 : DID 스마트 컨트랙트

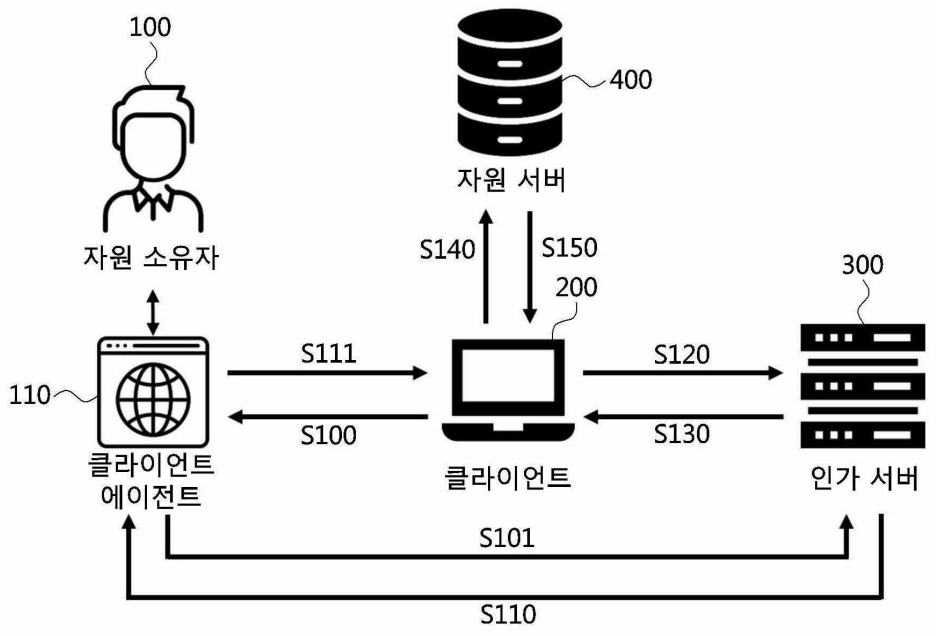
5000 : 자원 서버

5100 : 중계 자원서버

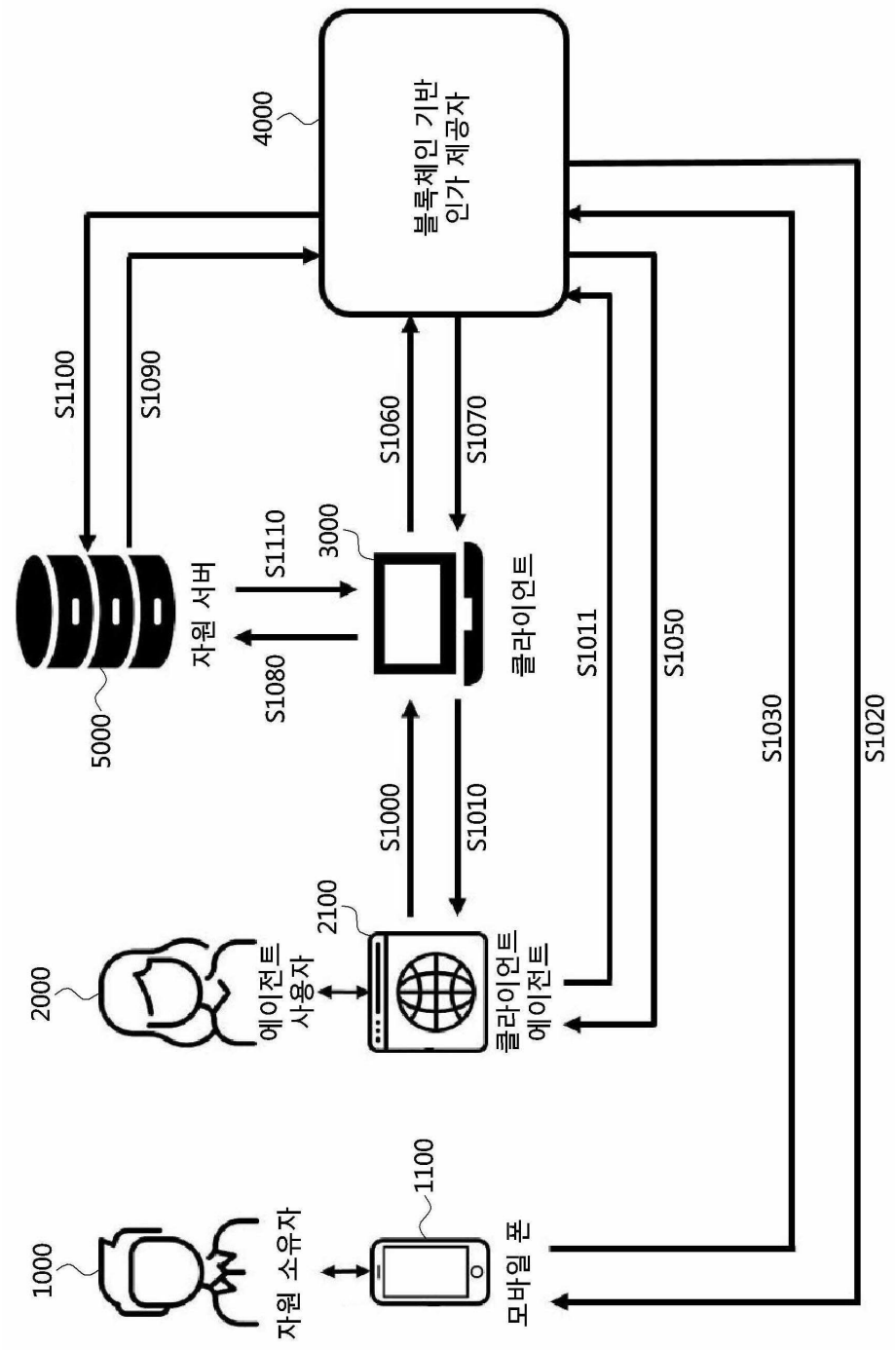
5110, 5120, 5130, 5140 : 자원 서버들

도면

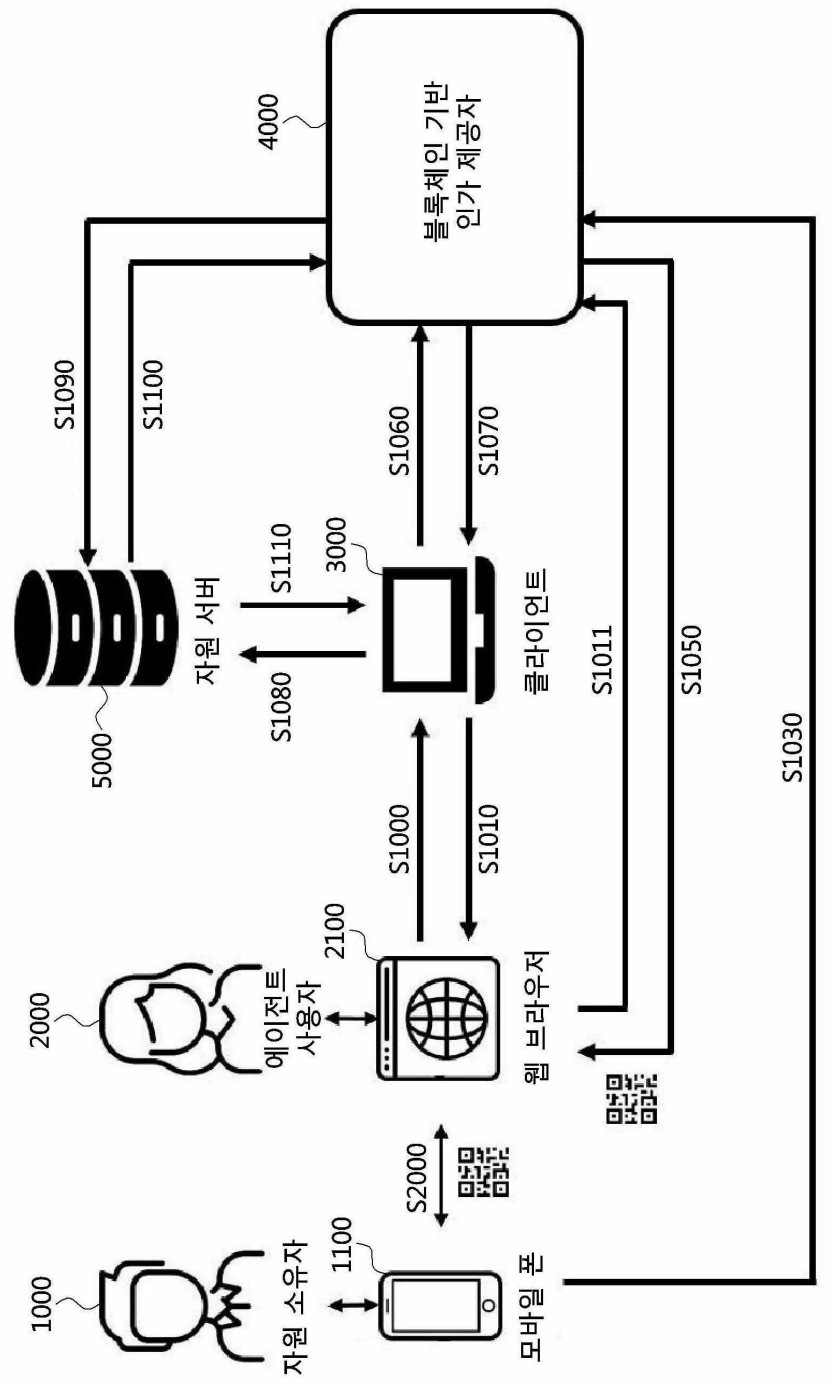
도면1



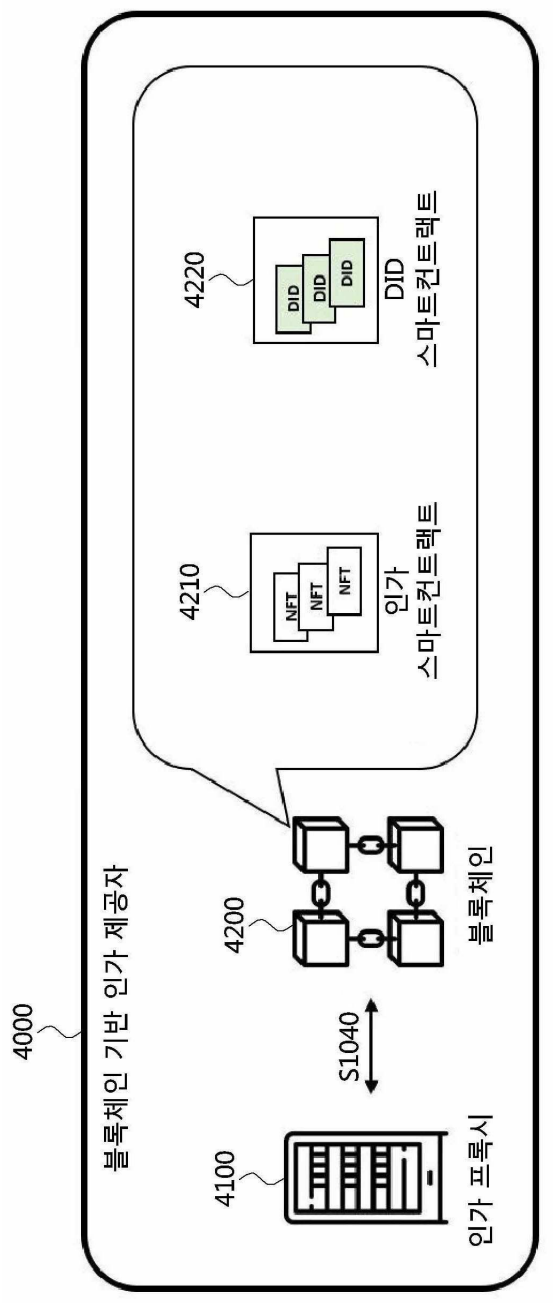
도면2


4000
블록체인 기반
인가 제공자
S1100
S1090
S1060
S1070
S1110
3000
자원 서버
클라이언트
S1080
S1011
S1050
5000
S1000
S1010
S1030
S1020
2100
2000
에이전트
사용자
클라이언트
에이전트
1100
1000
자원 소유자
모바일 폰

도면3


4000
블록체인 기반
인가 제공자
S1090
S1100
S1060
S1070
S1110
3000
자원 서버
클라이언트
S1080
S1011
S1050
5000
S1030
S1000
S1010
2100
2000
에이전트
사용자
웹 브라우저
S2000
1100
1000
자원 소유자
모바일 폰

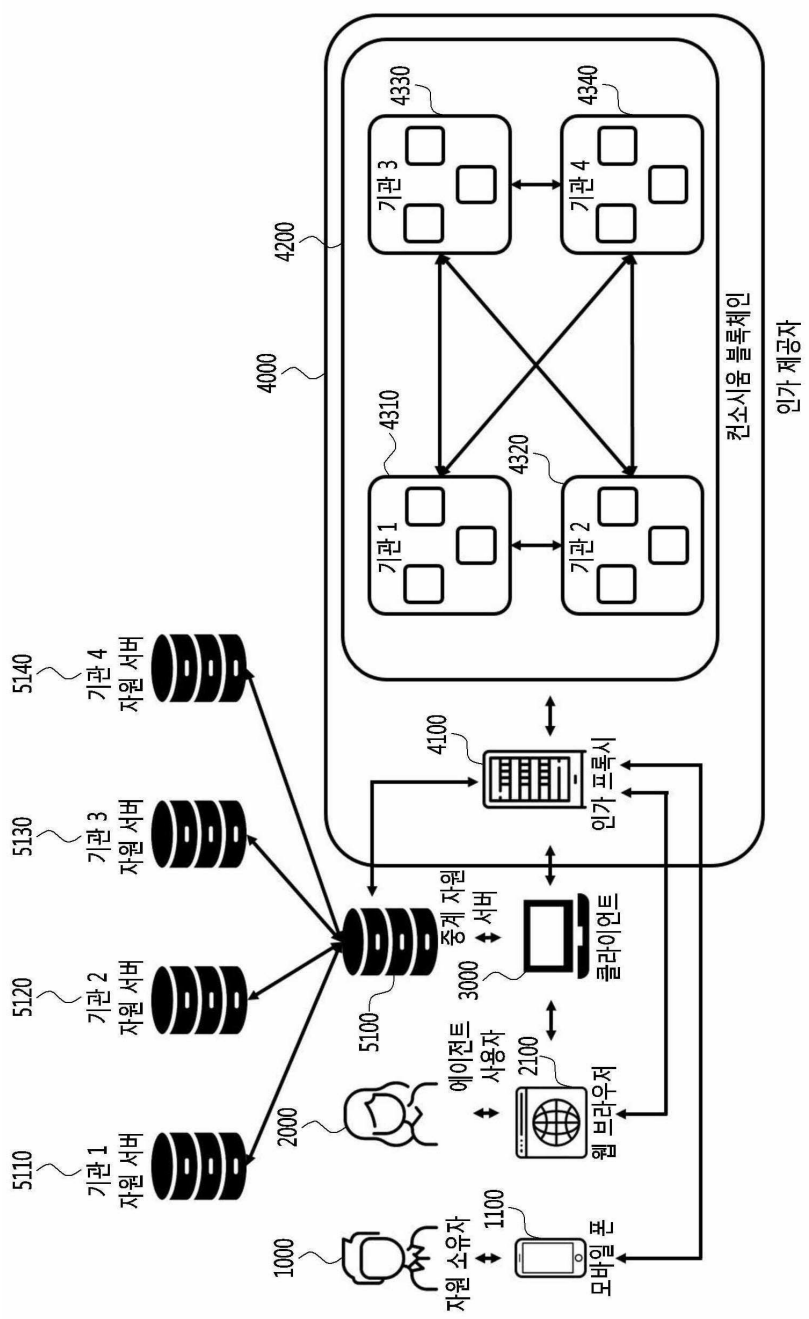
도면4


4000
블록체인 기반 인가 제공자
4100
인가 프록시
S1040
4200
블록체인
4210
NFT
NFT
NFT
인가
스마트컨트랙트
4220
DID
DID
DID
DID
스마트컨트랙트

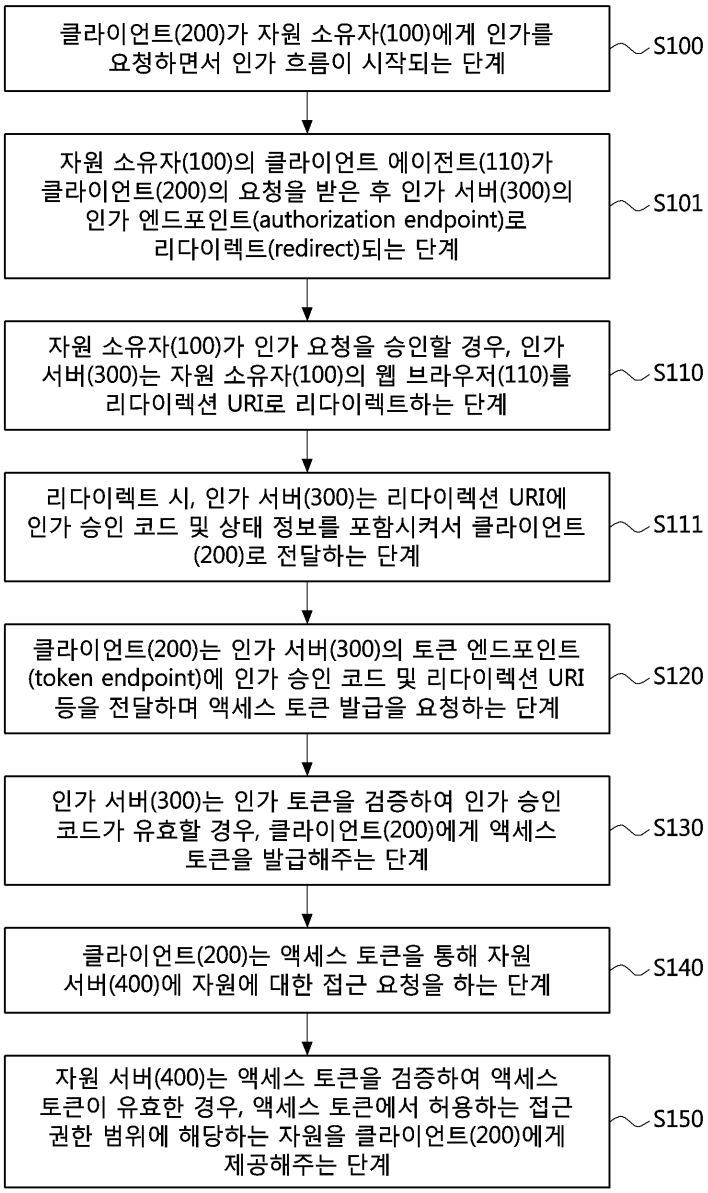
도면5

대체 불가능 토큰 Non-Fungible Token NFT	
id	code
type	scope
owner	state
approvee	access_token
issuer	redirect_uri
subject	issued_at
audience	expire_in
	revoked

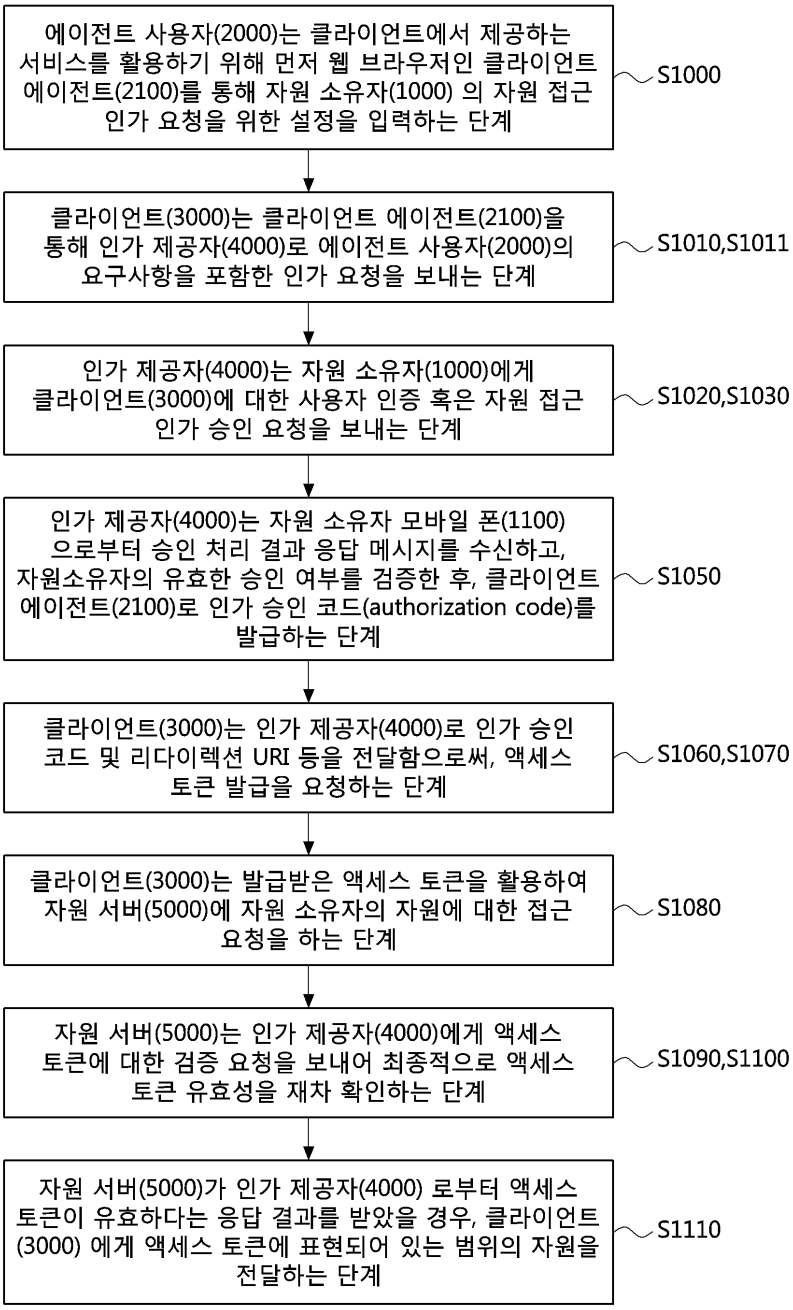
도면6


4000
4200
4330
4340
기관 3
기관 4
4310
4320
기관 1
기관 2
컨소시움 블록체인
인가 제공자
4100
인가 프록시
5140
기관 4 자원 서버
5130
기관 3 자원 서버
5120
기관 2 자원 서버
5110
기관 1 자원 서버
중계 자원 서버
5100
3000
클라이언트
에이전트 사용자
2000
2100
웹 브라우저
1000
자원 소유자
1100
모바일 폰

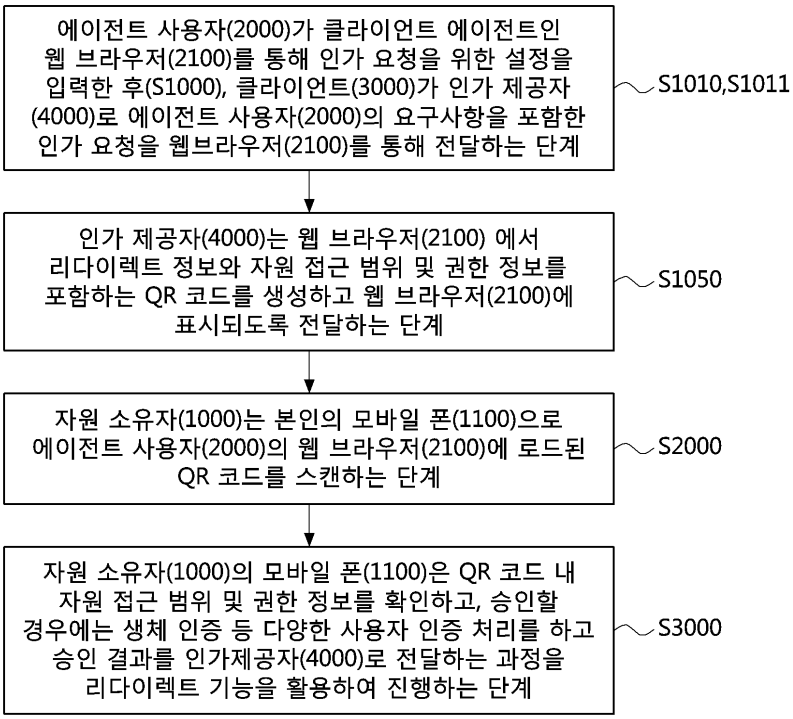
도면7


클라이언트(200)가 자원 소유자(100)에게 인가를 요청하면서 인가 흐름이 시작되는 단계
S100
자원 소유자(100)의 클라이언트 에이전트(110)가 클라이언트(200)의 요청을 받은 후 인가 서버(300)의 인가 엔드포인트(authorization endpoint)로 리다이렉트(redirect)되는 단계
S101
자원 소유자(100)가 인가 요청을 승인할 경우, 인가 서버(300)는 자원 소유자(100)의 웹 브라우저(110)를 리다이렉션 URI로 리다이렉트하는 단계
S110
리다이렉트 시, 인가 서버(300)는 리다이렉션 URI에 인가 승인 코드 및 상태 정보를 포함시켜서 클라이언트(200)로 전달하는 단계
S111
클라이언트(200)는 인가 서버(300)의 토큰 엔드포인트(token endpoint)에 인가 승인 코드 및 리다이렉션 URI 등을 전달하며 액세스 토큰 발급을 요청하는 단계
S120
인가 서버(300)는 인가 토큰을 검증하여 인가 승인 코드가 유효할 경우, 클라이언트(200)에게 액세스 토큰을 발급해주는 단계
S130
클라이언트(200)는 액세스 토큰을 통해 자원 서버(400)에 자원에 대한 접근 요청을 하는 단계
S140
자원 서버(400)는 액세스 토큰을 검증하여 액세스 토큰이 유효한 경우, 액세스 토큰에서 허용하는 접근 권한 범위에 해당하는 자원을 클라이언트(200)에게 제공해주는 단계
S150

도면8


에이전트 사용자(2000)는 클라이언트에서 제공하는 서비스를 활용하기 위해 먼저 웹 브라우저인 클라이언트 에이전트(2100)를 통해 자원 소유자(1000) 의 자원 접근 인가 요청을 위한 설정을 입력하는 단계
S1000
클라이언트(3000)는 클라이언트 에이전트(2100)을 통해 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 보내는 단계
S1010,S1011
인가 제공자(4000)는 자원 소유자(1000)에게 클라이언트(3000)에 대한 사용자 인증 혹은 자원 접근 인가 승인 요청을 보내는 단계
S1020,S1030
인가 제공자(4000)는 자원 소유자 모바일 폰(1100)으로부터 승인 처리 결과 응답 메시지를 수신하고, 자원소유자의 유효한 승인 여부를 검증한 후, 클라이언트 에이전트(2100)로 인가 승인 코드(authorization code)를 발급하는 단계
S1050
클라이언트(3000)는 인가 제공자(4000)로 인가 승인 코드 및 리다이렉션 URI 등을 전달함으로써, 액세스 토큰 발급을 요청하는 단계
S1060,S1070
클라이언트(3000)는 발급받은 액세스 토큰을 활용하여 자원 서버(5000)에 자원 소유자의 자원에 대한 접근 요청을 하는 단계
S1080
자원 서버(5000)는 인가 제공자(4000)에게 액세스 토큰에 대한 검증 요청을 보내어 최종적으로 액세스 토큰 유효성을 재차 확인하는 단계
S1090,S1100
자원 서버(5000)가 인가 제공자(4000) 로부터 액세스 토큰이 유효하다는 응답 결과를 받았을 경우, 클라이언트(3000) 에게 액세스 토큰에 표현되어 있는 범위의 자원을 전달하는 단계
S1110

도면9


에이전트 사용자(2000)가 클라이언트 에이전트인 웹 브라우저(2100)를 통해 인가 요청을 위한 설정을 입력한 후(S1000), 클라이언트(3000)가 인가 제공자(4000)로 에이전트 사용자(2000)의 요구사항을 포함한 인가 요청을 웹브라우저(2100)를 통해 전달하는 단계
S1010,S1011
인가 제공자(4000)는 웹 브라우저(2100) 에서 리다이렉트 정보와 자원 접근 범위 및 권한 정보를 포함하는 QR 코드를 생성하고 웹 브라우저(2100)에 표시되도록 전달하는 단계
S1050
자원 소유자(1000)는 본인의 모바일 폰(1100)으로 에이전트 사용자(2000)의 웹 브라우저(2100)에 로드된 QR 코드를 스캔하는 단계
S2000
자원 소유자(1000)의 모바일 폰(1100)은 QR 코드 내 자원 접근 범위 및 권한 정보를 확인하고, 승인할 경우에는 생체 인증 등 다양한 사용자 인증 처리를 하고 승인 결과를 인가제공자(4000)로 전달하는 과정을 리다이렉트 기능을 활용하여 진행하는 단계
S3000