(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월13일
(11) 등록번호 10-2442874
(24) 등록일자 2022년09월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/10* (2013.01)
G06F 21/34 (2013.01) *G06F 21/60* (2013.01)
G06F 21/64 (2013.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/6218 (2013.01)
G06F 21/10 (2013.01)
(21) 출원번호 10-2021-0068089
(22) 출원일자 2021년05월27일
심사청구일자 2021년05월27일
(56) 선행기술조사문헌
권민호 외 1인, 'InfoDID: A robust user information management serivce based on Decentralized Identifiers', 한국컴퓨터 정보학회논문지 제26권 제4호, 2021.04.03.,*
US20190230092 A1
US10708060 B2
KR102132118 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
울산대학교 산학협력단
울산광역시 남구 대학로 93(무거동)
(72) 발명자
이명준
울산광역시 중구 평동3길 1, 108동 2001호(유곡동, 울산 유곡 푸르지오)
김혜원
부산광역시 사하구 다대로 328, 101동 402호(장림동, 사하 리버팰리스)
(뒷면에 계속)
(74) 대리인
특허법인 무한

전체 청구항 수 : 총 20 항 심사관 : 구대성

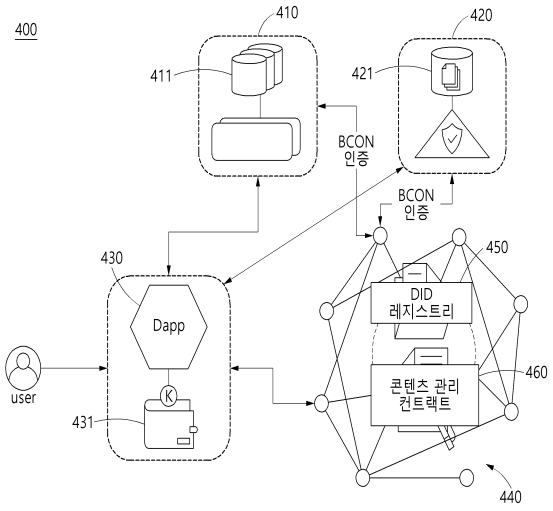
(54) 발명의 명칭 **블록체인 기반의 콘텐츠 서비스 구현 방법 및 시스템**

(57) 요 약

블록체인 기반의 콘텐츠 서비스 구현 방법 및 시스템이 개시된다. 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 방법은, 블록체인 네트워크에서 사용자 단말에 할당한 분산식별자(DID)를 포함한 DID 문서를 작성하여, DID 레지스트리에 기록하는 단계와, 상기 사용자 단말로부터 콘텐츠 파일의 업로드 요청이 발생함에

(뒷면에 계속)

대 표 도 - 도4



따라, 상기 블록체인 네트워크 내 검증 서버에서, 상기 업로드 요청을 발생시킨 사용자 단말의 분산식별자(DID)를 이용해 상기 DID 레지스트리로부터 DID 문서를 로딩하는 단계와, 상기 검증 서버에서, 상기 로딩한 DID 문서를 이용하여, 상기 사용자 단말의 신원 및 사용권한을 확인하는 BCON 인증을 실시하여, 상기 사용자 단말에 자격증명정보를 발급하는 단계와, 상기 블록체인 네트워크 내 제1 스토리지 서버에서, 상기 자격증명정보를 검증하여, 상기 사용자 단말에 업로드 토큰을 부여하는 단계, 및 상기 제1 스토리지 서버에서, 상기 업로드 토큰을 입력하는 사용자 단말로부터의 콘텐츠 파일을 저장하는 단계를 포함한다.

(52) CPC특허분류
G06F 21/34 (2013.01)
G06F 21/602 (2013.01)
G06F 21/64 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/50 (2022.05)

(72) 발명자
이영은
울산광역시 북구 명촌로 91, 216동 504호(명촌동, 평창리비에르2차아파트)

권민호
울산광역시 중구 오산3길 51-7(태화동)

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

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

블록체인 네트워크에서, 사용자 단말에 할당한 분산식별자(DID)를 포함한 DID 문서를 작성하여, DID 레지스트리에 기록하는 단계;

상기 사용자 단말로부터 콘텐츠 파일의 업로드 요청이 발생함에 따라,

상기 블록체인 네트워크 내 검증 서버에서, 상기 업로드 요청을 발생시킨 사용자 단말의 분산식별자(DID)를 이용해 상기 DID 레지스트리로부터 DID 문서를 로딩하는 단계;

상기 검증 서버에서, 로딩한 DID 문서를 이용하여, 상기 사용자 단말의 신원 및 사용권한을 확인하는 BCON 인증을 실시하여, 상기 사용자 단말에 자격증명정보를 발급하는 단계;

상기 블록체인 네트워크 내 제1 스토리지 서버에서, 상기 자격증명정보를 검증하여, 상기 사용자 단말에 업로드 토큰을 부여하는 단계; 및

상기 제1 스토리지 서버에서, 상기 업로드 토큰을 입력하는 사용자 단말로부터의 콘텐츠 파일을 저장하는 단계

를 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 2

제1항에 있어서,

상기 블록체인 네트워크에서, 블록체인 기반의 콘텐츠 서비스를 위해 제작된 분산 앱을 상기 사용자 단말에 배포하는 단계

를 더 포함하고,

상기 분산 앱의 배포에 따라, 상기 블록체인 네트워크는,

상기 제1 스토리지 서버를 포함하는 복수의 스토리지 서버와, 상기 검증 서버, 및 상기 분산 앱이 배포된 사용자 단말, 상기 DID 레지스트리 및 콘텐츠 관리 컨트랙트를 포함하여 구성되는

블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 3

제2항에 있어서,

상기 콘텐츠 파일을 저장하는 단계는,

상기 제1 스토리지 서버에서, 상기 업로드 토큰을 입력하는 사용자 단말의 상기 분산 앱을 통해 전송되는 콘텐츠 파일을, 상기 제1 스토리지 서버에 마련된 복수의 분산 DB 중 어느 하나의 DB에 저장하는 단계

를 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 4

제2항에 있어서,

상기 업로드 요청의 발생 시,

상기 사용자 단말의 분산 앱에서, 상기 콘텐츠 파일의 사이즈값, 타입값, 저장상태값, 소유자값, 생성시간값 및 해시값을 기재한 콘텐츠 메타 정보를 생성하여, 상기 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 저장하는 단계; 및

상기 사용자 단말의 분산 앱에서, 상기 콘텐츠 메타 정보를 사용자의 비밀키로 암호화해 생성한 서명값, 사용자

의 분산식별자, 및 사용자의 공개키 아이디를 포함한 정보를, 상기 검증 서버로 전송하여, 콘텐츠 업로드를 위한 상기 자격증명정보의 발급을 요청하는 단계

를 더 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 5

제4항에 있어서,

상기 검증 서버에서, 상기 사용자 단말의 분산 앱에서 전송된 상기 정보로부터, 사용자의 분산식별자 및 사용자의 비밀키로 암호화된 서명값을 추출하는 단계;

상기 검증 서버에서, 상기 추출한 분산식별자에 의해 식별되는 사용자의 DID 문서를, 상기 DID 레지스트리로부터 로딩하는 단계; 및

상기 검증 서버에서, 로딩한 DID 문서에 포함된 공개키 아이디로부터 추출되는 공개키로, 상기 추출한 서명값의 유효성을 검증하여, 상기 BCON 인증을 실시하는 단계

를 더 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 6

제4항에 있어서,

상기 제1 스토리지 서버에서, 상기 콘텐츠 파일을 저장 완료함에 따라, 상기 콘텐츠 파일의 다운로드 권한을 증명하는 다운증명정보를, 상기 사용자 단말에 발급하는 단계; 및

상기 사용자 단말의 분산 앱에서, 상기 사용자 단말에 발급된 다운증명정보를, 상기 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 더 저장하는 단계

를 더 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 7

제6항에 있어서,

상기 사용자 단말로부터, 상기 제1 스토리지 서버에 저장한 콘텐츠 파일의 다운로드 요청이 발생하면,

상기 제1 스토리지 서버에서, BCON 인증을 실시하여, 상기 사용자 단말에 발급된 다운증명정보를 검증하는 단계;

상기 다운증명정보가 검증되면, 상기 제1 스토리지 서버에서, 상기 사용자 단말에 다운로드 토큰을 부여하는 단계; 및

상기 제1 스토리지 서버에서, 설정된 유효시간 이내에 상기 다운로드 토큰을 입력하는 사용자 단말로 상기 콘텐츠 파일을 제공하는 단계

를 더 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 8

제7항에 있어서,

상기 제1 스토리지 서버에서, 상기 콘텐츠 파일을 상기 유효시간 이내에 다운로드 할 수 있는 임시 경로를 생성하여, 상기 다운로드 토큰과 함께 상기 사용자 단말에 부여하는 단계; 및

상기 콘텐츠 파일이 다운로드 완료되거나, 상기 유효시간이 경과됨에 따라, 상기 제1 스토리지 서버에서, 상기 임시 경로를 무효화 하는 단계

를 더 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 9

제6항에 있어서,

상기 사용자 단말로부터, 상기 제1 스토리지 서버에 저장한 콘텐츠 파일의 소유권 확인 요청이 발생할 경우,

상기 사용자 단말의 분산 앱에서, 상기 블록체인 네트워크의 콘텐츠 관리 컨트랙트에서 상기 콘텐츠 메타 정보 및 상기 다운증명정보를 로딩하는 단계; 및

상기 사용자 단말의 분산 앱에서, 상기 콘텐츠 메타 정보에 기재된 상기 콘텐츠 파일의 소유자값, 생성시간값 및 해시값과, 상기 다운증명정보를, 소유권 근거자료로서 사용자 단말의 화면에 출력하는 단계

를 더 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 10

제4항에 있어서,

상기 사용자 단말의 분산 앱에서, 로그인 요청하는 사용자 단말로부터 입력된 로그인 정보가, 상기 블록체인 네트워크의 지갑 프로그램에 유지된 계정 정보와 일치하면, 상기 사용자 단말을 로그인 처리하는 단계;

상기 사용자 단말의 분산 앱에서, 상기 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 저장된 상기 콘텐츠 메타 정보 중, 저장상태값이 'Saved'인 모든 콘텐츠 파일을 식별하여, 저장 콘텐츠 목록을 사용자 단말의 화면에 출력하는 단계; 및

상기 사용자 단말의 분산 앱에서, 상기 업로드 요청의 발생에 따라 상기 제1 스토리지 서버에 상기 콘텐츠 파일이 저장 완료되면, 해당 콘텐츠 파일을 포함하도록 상기 화면을 갱신하는 단계

를 더 포함하는 블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 11

제1항에 있어서,

상기 제1 스토리지 서버를 포함하는 복수의 스토리지 서버의 각각은, 단일의 상기 검증 서버와 분리된 구조인

블록체인 기반의 콘텐츠 서비스 구현 방법.

청구항 12

사용자 단말에 할당한 분산식별자(DID)를 포함한 DID 문서를 작성하여, DID 레지스트리에 기록하는 블록체인 네트워크;

상기 사용자 단말로부터 콘텐츠 파일의 업로드 요청이 발생함에 따라,

상기 업로드 요청을 발생시킨 사용자 단말의 분산식별자(DID)를 이용해 상기 DID 레지스트리로부터 DID 문서를 로딩하고, 로딩한 DID 문서를 이용해 상기 사용자 단말의 신원 및 사용권한을 확인하는 BCON 인증을 실시하여, 상기 사용자 단말에 자격증명정보를 발급하는 상기 블록체인 네트워크 내 검증 서버; 및

상기 자격증명정보를 검증하여, 상기 사용자 단말에 업로드 토큰을 부여하고, 상기 업로드 토큰을 입력하는 사용자 단말로부터의 콘텐츠 파일을 저장하는 상기 블록체인 네트워크 내 제1 스토리지 서버

를 포함하는 블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 13

제12항에 있어서,

상기 블록체인 네트워크는, 블록체인 기반의 콘텐츠 서비스를 위해 제작된 분산 앱을 상기 사용자 단말에 배포하고,

상기 분산 앱의 배포에 따라, 상기 블록체인 네트워크는,

상기 제1 스토리지 서버를 포함하는 복수의 스토리지 서버와, 상기 검증 서버, 및 상기 분산 앱이 배포된 사용자 단말, 상기 DID 레지스트리 및 콘텐츠 관리 컨트랙트를 포함하여 구성되는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 14

제13항에 있어서,

상기 제1 스토리지 서버는,

상기 업로드 토큰을 입력하는 사용자 단말의 상기 분산 앱을 통해 전송되는 콘텐츠 파일을, 상기 제1 스토리지 서버에 마련된 복수의 분산 DB 중 어느 하나의 DB에 저장하는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 15

제13항에 있어서,

상기 업로드 요청의 발생 시, 상기 사용자 단말의 분산 앱은,

상기 콘텐츠 파일의 사이즈값, 타입값, 저장상태값, 소유자값, 생성시간값 및 해시값을 기재한 콘텐츠 메타 정보를 생성하여, 상기 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 저장하고,

상기 콘텐츠 메타 정보를 사용자의 비밀키로 암호화해 생성한 서명값, 사용자의 분산식별자, 및 사용자의 공개키 아이디를 포함한 정보를, 상기 검증 서버로 전송하여, 콘텐츠 업로드를 위한 상기 자격증명정보의 발급을 요청하는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 16

제15항에 있어서,

상기 검증 서버는,

상기 사용자 단말의 분산 앱에서 전송된 상기 정보로부터, 사용자의 분산식별자 및 사용자의 비밀키로 암호화된 서명값을 추출하고,

상기 추출한 분산식별자에 의해 식별되는 사용자의 DID 문서를, 상기 DID 레지스트리로부터 로딩하고,

로딩한 DID 문서에 포함된 공개키 아이디로부터 추출되는 공개키로, 상기 추출한 서명값의 유효성을 검증하여, 상기 BCON 인증을 실시하는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 17

제15항에 있어서,

상기 제1 스토리지 서버는,

상기 콘텐츠 파일을 저장 완료함에 따라, 상기 콘텐츠 파일의 다운로드 권한을 증명하는 다운증명정보를, 상기 사용자 단말에 발급하고,

상기 사용자 단말의 분산 앱은,

상기 사용자 단말에 발급된 다운증명정보를, 상기 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 더 저장하는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 18

제17항에 있어서,

상기 사용자 단말로부터, 상기 제1 스토리지 서버에 저장한 콘텐츠 파일의 다운로드 요청이 발생하면,

상기 제1 스토리지 서버는,

BCON 인증을 실시하여, 상기 사용자 단말에 발급된 다운증명정보를 검증하고,

상기 다운증명정보가 검증되면, 상기 사용자 단말에 다운로드 토큰을 부여하고,

설정된 유효시간 이내에 상기 다운로드 토큰을 입력하는 사용자 단말로 상기 콘텐츠 파일을 제공하는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 19

제18항에 있어서,

상기 제1 스토리지 서버는,

상기 콘텐츠 파일을 상기 유효시간 이내에 다운로드 할 수 있는 임시 경로를 생성하여, 상기 다운로드 토큰과 함께 상기 사용자 단말에 부여하고,

상기 콘텐츠 파일이 다운로드 완료되거나, 상기 유효시간이 경과됨에 따라, 상기 임시 경로를 무효화 하는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

청구항 20

제17항에 있어서,

상기 사용자 단말로부터, 상기 제1 스토리지 서버에 저장한 콘텐츠 파일의 소유권 확인 요청이 발생할 경우,

상기 사용자 단말의 분산 앱은,

상기 블록체인 네트워크의 콘텐츠 관리 컨트랙트에서 상기 콘텐츠 메타 정보 및 상기 다운증명정보를 로딩하고,

상기 콘텐츠 메타 정보에 기재된 상기 콘텐츠 파일의 소유자값, 생성시간값 및 해시값과, 상기 다운증명정보를, 소유권 근거자료로서 사용자 단말의 화면에 출력하는

블록체인 기반의 콘텐츠 서비스 구현 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 분산신원증명(DID, Decentralized Identity) 기술을 이용한 블록체인 기반의 콘텐츠(Blockchain-based CONtents, BCON) 서비스 구현 방법에 연관되며, 보다 특정하게는 콘텐츠 제작자의 결과물을 신원 인증을 통해 안전하게 보관하고, 콘텐츠 소유권도 보장하는 BCON 서비스의 제공에 연관된다.

배 경 기 술

[0002] 콘텐츠 서비스를 안전하게 사용하기 위해선 사용자의 신원인증절차가 필요하다. 공인인증서의 독점적 지위가 폐지되면서, 새로운 전자서명 기술들이 등장하고, 특히, 차세대 신원확인 기술로 분산신원증명(DID)이 주목받고 있다.

[0003] DID 기술은 블록체인 기반으로 탈중앙화된 신원확인 서비스를 제공하며, 사용자가 서비스 기업에 필요한 정보만 선택적으로 전달할 수 있어 데이터 주권을 강화할 수 있는 기술이다.

[0004] 여러 기업이 DID를 이용한 서비스를 시작하고 있으며, 현재 DID 기술은 W3C(World Wide Web Consortium)에서 표준화를 진행하고 있다.

[0005] 국내에서는 한국정보통신기술협회(TTA)가 ICT 기반 탈중앙화 대면 분야 표준화 포럼에 DID를 포함했으며, 여러 기업이 서비스 상용화를 적극적으로 추진하고 있다.

[0006] 이에 따라, 사용자 스스로 신원 인증하여 자신의 콘텐츠를 안전하게 보관하고, 콘텐츠에 대한 소유권을 신뢰성 있게 보장받을 수 있는 기술 개발이 요구된다.

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예는 사용자 스스로 신원 인증을 통해 자신의 콘텐츠를 안전하게 보관하고, 보관한 콘텐츠에 대한 자신의 소유권을 신뢰성 있게 보장할 수 있는 블록체인 기반의 콘텐츠(BCON) 서비스를 구현하는 것을 목적으로 한다.

[0008] 본 발명의 실시예는 DID 기술을 이용하여 사용자가 서비스에 필요한 정보만 선택적으로 제공하여 신원 인증을 수행하고, 액세스 토큰을 통해 콘텐츠에 대한 사용자의 접근 권한을 체계적으로 제어하는 BCON 서비스를 구현하는 것을 목적으로 한다.

[0009] 본 발명의 실시예는 블록체인 네트워크의 DID 레지스트리에 기록된 사용자 단말의 DID 문서를 이용해 신원 및 사용권한을 확인하는 종래 보다 간략화된 BCON 인증을 실시하여, 콘텐츠 업로드/다운로드 서비스를 구현하는 것을 목적으로 한다.

[0010] 본 발명의 실시예는 사용자 단말에 의한 콘텐츠 파일의 업로드 요청 발생 시, 스토리지 서버와 분리된 검증 서버에서 BCON 인증을 실시해 콘텐츠 업로드 가능을 나타내는 자격증명정보를 사용자 단말에 발급함으로써, 스토리지 서버에서 상기 자격증명정보의 검증에 의해 콘텐츠 파일을 저장(보관)하는 서비스를 간단히 제공할 수 있게 하는 것을 목적으로 한다.

[0011] 본 발명의 실시예는 스토리지 서버에서 콘텐츠 파일을 저장 완료 시 해당 콘텐츠 파일의 다운로드 가능을 나타내는 다운증명정보를 사용자 단말에 발급함으로써, 이후, 상기 다운증명정보의 검증 만으로, 저장된 콘텐츠 파일을 이용(다운로드)할 수 있게 하는 것을 목적으로 한다.

[0012] 본 발명의 실시예는 스토리지 서버에서 상기 자격증명정보의 검증과, 상기 다운증명정보의 발급 및 검증을 수행할 때 마다 상기 BCON 인증을 실시해 사용자 단말의 신원 및 사용권한을 확인함으로써, 블록체인 기반 콘텐츠 서비스의 보안성을 보다 강화하는 것을 목적으로 한다.

[0013] 본 발명의 실시예는 콘텐츠 파일을 스토리지 서버에 업로드하기 전에, 해당 콘텐츠 파일을 설명하는 콘텐츠 메타 정보(소유자값, 생성시간값, 해시값 등)를 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 저장하고, 콘텐츠 파일을 스토리지 서버에 업로드한 후에, 스토리지 서버에 의해 발급된 다운증명정보를, 콘텐츠 관리 컨트랙트에 더 저장함으로써, 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 안전하게 유지된 콘텐츠 메타 정보와 다운증명정보를 이용해, 사용자 단말의 해당 콘텐츠 파일의 소유권 근거자료로서 활용할 수 있게 하는 것을 목적으로 한다.

[0014] 본 발명의 실시예는 하나의 검증 서버를 이용하여, 콘텐츠 크기/콘텐츠 종류 별로 마련된 다수의 스토리지 서버의 콘텐츠 서비스를 구현함으로써, 콘텐츠 파일의 용량이나 종류에 관계없이 빠른 속도로 콘텐츠 서비스를 제공하고, 다수의 스토리지 서버를 효율적으로 운영할 수 있게 하는 것을 목적으로 한다.

과제의 해결 수단

[0015] 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 방법은, 블록체인 네트워크에서 사용자 단말에 할당한 분산식별자(DID)를 포함한 DID 문서를 작성하여, DID 레지스트리에 기록하는 단계와, 상기 사용자 단말로부터 콘텐츠 파일의 업로드 요청이 발생함에 따라, 상기 블록체인 네트워크 내 검증 서버에서, 상기 업로드 요청을 발생시킨 사용자 단말의 분산식별자(DID)를 이용해 상기 DID 레지스트리로부터 DID 문서를 로딩하는 단계와, 상기 검증 서버에서, 로딩한 DID 문서를 이용하여, 상기 사용자 단말의 신원 및 사용권한을 확인하는 BCON 인증을 실시하여, 상기 사용자 단말에 자격증명정보를 발급하는 단계와, 상기 블록체인 네트워크 내 제1 스토리지 서버에서, 상기 자격증명정보를 검증하여, 상기 사용자 단말에 업로드 토큰을 부여하는 단계, 및 상기 제1 스토리지 서버에서, 상기 업로드 토큰을 입력하는 사용자 단말로부터의 콘텐츠 파일을 저장하는 단계를 포함할 수 있다.

[0016] 또한, 본 발명의 실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템은, 사용자 단말에 할당한 분산식별자(DID)를 포함한 DID 문서를 작성하여, DID 레지스트리에 기록하는 블록체인 네트워크와, 상기 사용자 단말로부터 콘텐츠 파일의 업로드 요청이 발생함에 따라, 상기 업로드 요청을 발생시킨 사용자 단말의 분산식별자(DID)를 이용해 상기 DID 레지스트리로부터 DID 문서를 로딩하고, 로딩한 DID 문서를 이용해 상기 사용자 단말의 신원 및 사용권한을 확인하는 BCON 인증을 실시하여, 상기 사용자 단말에 자격증명정보를 발급하는 상기 블록체인 네트워크 내 검증 서버, 및 상기 자격증명정보를 검증하여, 상기 사용자 단말에 업로드 토큰을 부여하고, 상기 업로드 토큰을 입력하는 사용자 단말로부터의 콘텐츠 파일을 저장하는 상기 블록체인 네트워크 내 제1 스토리지 서버를 포함할 수 있다.

발명의 효과

[0017] 본 발명에서 제안하는 블록체인 기반의 콘텐츠 서비스(BCON service)에서는, 분산신원증명(DID) 기술을 이용해 사용자 스스로 필요한 정보만을 선택적으로 제공하여 신원 인증함으로써 콘텐츠 파일을 스토리지 서버에 안전하게 보관할 수 있다.

[0018] 또한, 본 발명에 의하면, 각 스토리지 서버 내에 대용량 콘텐츠 파일의 저장이 가능한 분산 DB(예, '카산드라 데이터베이스')를 마련함으로써, 빠른 속도의 콘텐츠 서비스를 구현할 수 있다.

[0019] 또한, 본 발명에 의하면, 콘텐츠 파일의 업로드 권한을 나타내는 액세스 토큰/다운로드 권한을 나타내는 액세스 토큰을 사용자 단말에 부여함으로써, 액세스 토큰을 통한 사용자의 콘텐츠 접근 권한을 체계적으로 제어할 수 있다.

[0020] 또한, 본 발명에 의하면, 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 유지한 콘텐츠 메타 정보와 다운증명정보를 스토리지 서버에 보관한 콘텐츠 파일에 대한 소유권을 주장하는데 활용할 수 있다.

[0021] 따라서, 본 발명에 의하면, 콘텐츠 제작자의 결과물을 안전하고 신뢰성 있게 보관할 수 있고, 콘텐츠 제작자의 소유권을 확실하게 보장할 수 있게 된다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템의 구성을 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, DID 문서를 DID 레지스트리에 기록하는 일례를 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, BCON 인증을 실시하는 과정을 도시한 도면이다.

도 4는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템의 서비스 구조를 도시한 도면이다.

도 5는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 스토리지 서버의 내부 구성의 일례를 도시한 도면이다.

도 6은 본 발명의 다른 실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 단일의 검증 서버로 복수의 스토리지 서버의 콘텐츠 서비스를 제공하는 서비스 구조를 도시한 도면이다.

도 7a 및 도 7b는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 저장되는 콘텐츠 메타 정보 및 다운증명정보를 도시한 도면이다.

도 8은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 블록체인 네트워크를 통한 콘텐츠 업로드 과정을 도시한 도면이다.

도 9는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 콘텐츠 메타 정보, 자격증명정보, 다운증명정보, 업로드 토큰 및 다운로드 토큰의 데이터 구조를 도시한 도면이다.

도 10은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 콘텐츠 업로드를 요청 시 분산 앱의 화면 일례를 도시한 도면이다.

도 11은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 블록체인 네트워크를 통한 콘텐츠 다운로드 과정을 도시한 도면이다.

도 12은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 콘텐츠 다운로드를 요청 시 분산 앱의 화면 일례를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 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.

[0024] 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.

[0025] 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.

[0026] 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.

[0027] 도 1은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템의 구성을 도시한 도면이다.

[0028] 도 1을 참조하면, 본 발명의 블록체인 기반의 콘텐츠 서비스 구현 시스템(100)은, 블록체인 네트워크(110), 스토리지 서버(120), 검증 서버(130), 및 분산 앱(140)을 포함하여 구성할 수 있다. 블록체인 네트워크(110)에는, DID 레지스트리(150) 및 콘텐츠 관리 컨트랙트(160)가 포함될 수 있다.

[0029] 블록체인 네트워크(110)는, 블록체인 기반의 콘텐츠 서비스를 위해 제작된 분산 앱(140)을 사용자 단말에 배포한다.

[0030] 분산 앱(140)의 배포에 따라, 블록체인 네트워크(110)는, 제1 스토리지 서버를 포함하는 복수의 스토리지 서버(120)와, 검증 서버(130), 및 분산 앱(140)이 배포된 사용자 단말, DID 레지스트리(150) 및 콘텐츠 관리 컨트랙트(160)를 포함하여 구성될 수 있다.

[0031] 복수의 스토리지 서버(120)와 검증 서버(130)는, 각각 별도의 노드에서 동작하며, 분산 앱(140)도 별도의 사용자 단말 노드에서 동작할 수 있다.

[0032] 즉, 복수의 스토리지 서버(120)와 검증 서버(130) 및 분산 앱(140)은 각각 블록체인 노드가 아닌 개별 노드들에서 동작하고, DID 레지스트리(150)와 콘텐츠 매니지먼트 컨트랙트(160)만이 블록체인 네트워크(110)에 배포하여 관리되고, BCON 및 권한 검증이 필요할 때 각 노드들이 블록체인 네트워크(110)와 상호작용하는 구조로 동작할 수 있다.

[0033] 상기 제1 스토리지 서버를 포함하는 복수의 스토리지 서버(120)의 각각은, 단일의 검증 서버(130)와 분리(이격)된 구조일 수 있다.

[0034] 즉, 여러 종류의 스토리지 서비스에 대한 각각의 검증 서버(130)를 구비할 필요 없이, 하나의 검증 서버(130)를 각 스토리지 서버(120)들과 분리된 구조로 마련하여, 스토리지 서비스에 특화된 클라우드 서비스들이 운영하는 다수의 스토리지 서버의 콘텐츠 서비스를 구현할 수 있다.

[0035] 블록체인 네트워크(110)로는, '클레이튼' 블록체인(Klaytn Blockchain)을 예시할 수 있다. '클레이튼' 블록체인은, 스마트 컨트랙트를 통해 분산 앱(분산 어플리케이션)(140)을 개발하고 실행할 수 있는 블록체인 플랫폼이다.

[0036] '클레이튼'의 스마트 컨트랙트는, 특정 주소에 배포되어 블록에 저장된 프로그램 코드로 특정 조건에 따라 자동으로 계약을 수행하고, 배포된 컨트랙트 주소에 트랜잭션을 보내 계약을 실행하고, 실행된 결과를 블록체인에 저장해 분산된 모든 노드의 동의 없는 임의 수정을 불가능하게 함으로써, 저장된 데이터의 무결성을 보장할 수 있다.

[0037] 특히 '클레이튼'은 Istanbul BFT 합의 알고리즘을 채택하여 임의의 노드들만 암호학적으로 랜덤하게 선출해 합의를 진행하고 빠른 속도로 블록의 완결성을 보장할 수 있다.

[0038] 이에 따라, 트랜잭션 양이 증가하더라도, 속도의 병목현상으로 비싼 거래 수수료를 내는 이더리움과 달리, '클레이튼'은 초당 4000 트랜잭션을 처리하고 1초 남짓한 시간 안에 블록을 생성할 수 있어 즉각적인 트랜잭션 처리가 가능하기 때문에, 효율적인 합의 방법과 빠른 트랙잭션 처리 속도로 고성능의 서비스 친화적인 블록체인으

로 사용되고 있다.

[0039] 블록체인 네트워크(110)에는, DID 레지스트리(150) 및 콘텐츠 관리 컨트랙트(160)가 포함될 수 있다.

[0040] DID 레지스트리(150)는, 블록체인 네트워크(110) 내의 사용자 단말에 분산식별자(DID)를 할당하고, 상기 분산식별자(DID)와 사용자 단말의 자격증명을 검증하는데 필요한 데이터(예, 공개키, 인증정보와 상호작용 가능한 서비스의 리스트 등)를 포함하여 사용자 단말의 DID 문서를 작성해 기록하는 기능을 한다.

[0041] 분산신원증명(DID)이란, 기존 신원 제공자, 인증 기관 등 제3의 중앙기관으로부터 독립되어 사용자 본인이 자신의 신원을 증명 가능한 분산 디지털 신원 확인 기술로서, DID는, 블록체인 기반 인증으로 비대칭 암호화 알고리즘 방식을 사용하여 자신을 설명할 수 있는 DID 문서를 직접 소유 및 관리하여 스스로 신원 데이터의 통제, 신원 증명 권한을 가진다.

[0042] 이하 도 2를 참조하여 DID 레지스트리(150)를 설명한다.

[0043] 도 2는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, DID 문서를 DID 레지스트리에 기록하는 일례를 도시한 도면이다.

[0044] 도 2를 참조하면, DID 레지스트리(150)는 DID의 생성, 확인, 업데이트 및 비활성화를 담당하게 되고, 사용자 단말의 자격증명을 검증할 수 있는 데이터(공개키, 인증정보와 상호작용 가능한 서비스의 리스트)를 포함해서 DID 문서를 기록하고, DID 문서 작성에 필요한 상기 데이터를 사용자 단말에 반환한다.

[0045] 이에 따라 DID 레지스트리(150)를 통해 DID를 갖게 되는 사용자 단말은 블록체인 네트워크(110) 상에서 신뢰할 수 있는 기법을 통해 손쉽게 신원을 검증 받는 것이 가능해진다.

[0046] 콘텐츠 관리 컨트랙트(160)는 신뢰성 있는 콘텐츠 관리 서비스에 필요한 증명서(자격증명정보, 다운증명정보, 콘텐츠 메타 정보 등)들을 블록체인 네트워크(110)에 저장하는 스마트 컨트랙트이며, 사용자 단말에서는 분산 앱(140)을 통해서 콘텐츠 관리 서비스를 이용할 수 있다.

[0047] 이처럼 블록체인 구성부(110)에서 복수의 스토리지 서버(120)와 검증 서버(130) 및 사용자 단말에 배포된 분산 앱(140)을 포함한 블록체인 네트워크(110)가 구성되고, 블록체인 네트워크(110)에서 사용자 단말의 분산식별자(DID)를 포함한 DID 문서를 작성해 DID 레지스트리(150)에 기록한 후에는, 스토리지 서버(120)와 검증 서버(130)에서, DID 레지스트리(150)의 상기 DID 문서를 이용한 BCON 인증을 실시해 사용자 단말의 신원 및 사용권한을 확인함으로써, 콘텐츠 파일의 업로드/다운로드 서비스가 구현될 수 있다.

[0048] 먼저, 콘텐츠 파일의 스토리지 서버(120)로의 업로드 요청이 사용자 단말로부터 발생하면, 스토리지 서버(120)와 분리된 검증 서버(130)에서, 상기 업로드 요청하는 사용자 단말의 분산식별자(DID)를 이용해 DID 레지스트리(150)로부터 로딩한 DID 문서를 이용하여, 사용자 단말의 신원 및 사용권한을 확인하는 BCON 인증을 실시하고, 상기 BCON 인증의 결과로 상기 사용자 단말에 업로드 가능을 나타내는 자격증명정보를 발급한다.

[0049] 상기 업로드 요청을 발생 시 사용자 단말의 분산 앱(140)에서는, 업로드할 콘텐츠 파일을 설명하는 콘텐츠 메타 정보를 생성하여, 블록체인 네트워크(110)의 콘텐츠 관리 컨트랙트(160)에 저장한다.

[0050] 도 7a 및 도 7b는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 저장되는 콘텐츠 메타 정보 및 다운증명정보를 도시한 도면이다.

[0051] 도 7a를 참조하면, 콘텐츠 메타 정보(ContentMeta)(710)에는, 업로드할 콘텐츠 파일의 이름(Content Name)과 사이즈값(Content Size), 콘텐츠 파일의 종류에 따른 타입값(Content Type), 콘텐츠 파일의 스토리지 서버(120) 저장 여부를 나타내는 저장상태값(Content State), 콘텐츠 파일의 소유자값(Content Owner), 콘텐츠 파일의 생성시간값(Content Created time), 및 해시값(Content Hash)이 기재될 수 있다.

[0052] 상기 사용자 단말의 분산 앱(140)은, 콘텐츠 메타 정보(710)를 콘텐츠 관리 컨트랙트(160)에 저장한 후에, 콘텐츠 메타 정보(710)를 사용자의 비밀키로 암호화해 생성한 서명값, 사용자의 분산식별자, 및 사용자의 공개키 아이디를 포함한 정보를, 검증 서버(130)로 전송하여, 콘텐츠 업로드를 위한 상기 자격증명정보의 발급을 요청할 수 있다.

[0053] 이에 따라, 검증 서버(130)는 분산 앱(140)에서 보내온 상기 정보를 이용하여 BCON 인증을 실시하고, 상기 BCON 인증의 결과로 사용자 단말에 업로드 가능을 나타내는 자격증명정보를 발급할 수 있다.

[0054] 일례로, 검증 서버(130)는 사용자 단말의 분산 앱(140)에서 전송된 상기 정보로부터, 사용자의 분산식별자 및

사용자의 비밀키로 암호화된 서명값을 추출하고, 추출한 분산식별자에 의해 식별되는 사용자의 DID 문서를, DID 레지스트리(150)로부터 로딩하고, 로딩한 DID 문서에 포함된 공개키 아이디로부터 추출되는 공개키로, 추출한 서명값의 유효성을 검증하여, BCON 인증을 실시할 수 있다.

[0055] 이하에서는 도 3을 참조하여 BCON 인증을 실시하는 과정을 설명한다.

[0056] 도 3은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, BCON 인증을 실시하는 과정을 도시한 도면이다.

[0057] 도 3을 참조하면, 사용자 단말의 분산 앱(140)에서 사용자의 DID, 공개키 ID, 서명값을 포함한 정보를 검증 서버(130)로 보내오면, 검증 서버(130)는, 사용자의 DID를 이용해 DID 레지스트리(150)로부터 사용자의 DID 문서를 로딩하고, 로딩한 DID 문서로부터 공개키를 추출하고, 추출한 공개키를 이용해 상기 분산 앱(140)에서 보내온 정보 내 서명값을 검증하고, 서명값이 유효한 것으로 검증될 때 사용자의 신원을 인증하는 종래의 분산신원 인증보다 간략화된 BCON 인증을 실시할 수 있다.

[0058] 이처럼 본 발명은 DID 이용해 사용자의 신원인증절차를 구축하여 사용자 스스로 필요한 정보만을 선택적으로 제공하여 신원 인증함으로써, 사용자의 정보 주권을 강화하고, 콘텐츠 파일을 스토리지 서버에 안전하게 보관할 수 있다.

[0059] 상기 BCON 인증의 결과로 사용자 단말에 발급되는 자격증명정보(920)에는, 도 9에 도시된 것처럼, 자격증명정보(920)의 발급을 위해 분산 앱(140)에서 보내온 모든 정보(서명값, 분산식별자, 공개키 아이디)가 'user' 파트에 기재되고, 자격증명정보(920)를 발급하는 검증 서버(130)의 DID와, 자격증명정보(920)의 유효성을 스토리지 서버(120)에서 검증하기 위한 검증 서버(130)의 공개키 아이디, 검증 서버(130)의 접근 위치, 스토리지 서버(120)의 접근 위치, 사용자의 서비스 권한, 자격증명정보(920)의 발급 시간과 유효시간, 및 이 모든 정보를 검증 서버(130)의 공개키와 대칭되는 비밀키로 서명하여 만든 자격증명서명이 기재될 수 있다.

[0060] 복수의 스토리지 서버(120) 중 어느 하나의 제1 스토리지 서버에서, 상기 사용자 단말에 발급된 자격증명정보를 검증하고, 검증이 완료되면, 사용자 단말에 제1 스토리지 서버로의 업로드 권한을 나타내는 업로드 토큰을 부여한다.

[0061] 이때 제1 스토리지 서버에서도 상기 BCON 인증을 실시하여, 사용자 단말에 발급된 자격증명정보를 검증할 수 있고, 상기 BCON 인증 결과로 사용자 단말에 도 9에 도시된 것과 같은 업로드 토큰(940)을 부여할 수 있다.

[0062] 즉, 사용자 단말의 분산 앱(140)에서, 사용자 단말에 발급된 자격증명정보를 제1 스토리지 서버로 전송하면, 제1 스토리지 서버는, 사용자 단말의 분산 앱(140)에서 보내온 자격증명정보의 'user' 파트에서 사용자의 분산식별자 및 사용자의 비밀키로 암호화된 서명값을 추출하고, 추출한 분산식별자에 의해 식별되는 사용자의 DID 문서를, DID 레지스트리(150)로부터 로딩하고, 로딩한 DID 문서에 포함된 공개키 아이디로부터 추출되는 공개키로, 추출한 서명값의 유효성을 검증하여, BCON 인증을 실시할 수 있다.

[0063] 사용자 단말은 분산 앱(140)을 통해 업로드 토큰(940)을 입력한 후, 업로드할 콘텐츠 파일을 전송할 수 있다.

[0064] 이 때에도, 상기 제1 스토리지 서버는 카산드라 데이터베이스에서 비밀키를 가져와서, 사용자 단말이 분산 앱(140)을 통해 입력한 업로드 토큰(940)의 유효성을 검증할 수 있다.

[0065] 이후, 상기 제1 스토리지 서버는, 사용자 단말이 입력한 업로드 토큰(940)의 유효성이 확인되면, 분산 앱(140)을 통해 전송된 콘텐츠 파일을 상기 제1 스토리지 서버에 마련된 복수의 분산 DB 중 어느 하나의 DB에 저장한다.

[0066] 여기서 제1 스토리지 서버에 마련된 각각의 DB는, '카산드라(Cassandra)'로 예시할 수 있다. '카산드라'는, 대규모 확장 가능한 아파치 오픈소스 기반의 분산 데이터베이스로서, 기존의 관계형 데이터베이스와 달리 SQL을 사용하지 않는 NoSQL 데이터베이스이기 때문에, 대용량의 트랜잭션에 대해 빠른 처리가 가능한 장점이 있다.

[0067] '카산드라'의 데이터 모델을 설명하면, 키스페이스(Keyspace)라는 논리적 데이터 저장소가 최상위에 존재하고, 아래에 다수의 Row로 구성된 Table이 존재한다. 하나의 Row는 키값(Key-Value)으로 이루어진 다수의 컬럼(Column)들로 구성되며, Row Key 데이터의 해시값을 기준으로 데이터가 분산 저장되고, 데이터가 저장된 노드들은 Gossip 프로토콜을 통해 모든 노드가 동등한 Ring 구조를 이룬다. '카산드라'는 노드들이 주기적으로 서로 정보를 주고받는 Gossip 프로토콜을 이용하기 때문에 새 노드의 추가가 용이하므로 수평적인 용량 확장이 손쉽게 이루어지는 장점이 있다.

[0068] 따라서 본 발명에 의하면, 각 스토리지 서버 내에 대용량 콘텐츠 파일의 저장이 가능한 분산 DB(예, '카산드라 데이터베이스')를 이용해, 빠른 속도의 콘텐츠 서비스를 구현할 수 있다.

[0069] 이하에서는 사용자 단말에 의해 전송된 콘텐츠 파일이 제1 스토리지 서버(120)에 새롭게 저장됨에 따라, 사용자 단말의 분산 앱(140)에서 제공하는 피드 화면이 자동으로 갱신 처리되는 과정을 설명한다.

[0070] 도 10은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 콘텐츠 업로드를 요청 시 분산 앱의 화면 일례를 도시한 도면이다.

[0071] 도 10을 참조하면, 사용자 단말의 분산 앱(140)은, 로그인 요청하는 사용자 단말로부터 입력된 로그인 정보가, 블록체인 네트워크(110)의 지갑 프로그램(예, '카이카스(Kaikas)')에 유지된 계정 정보와 일치함에 따라, 사용자 단말을 로그인 처리하고, 블록체인 네트워크(110)의 콘텐츠 관리 컨트랙트(160)에 저장된 콘텐츠 메타 정보(710) 중, 저장상태값이 'Saved'인 모든 콘텐츠 파일을 식별하여, 저장 콘텐츠 목록을 사용자 단말의 피드 화면에 출력할 수 있다.

[0072] 즉, 사용자 단말의 분산 앱(140)은, 사용자 단말이 로그인하면, 로그인 시점까지 스토리지 서버(120)에 보관된 모든 콘텐츠 파일 목록을 표시할 수 있다.

[0073] 이후, 화면(1010)을 통해 새로운 콘텐츠 파일의 업로드가 요청되어, 제1 스토리지 서버에 해당 콘텐츠 파일이 저장 완료되면, 콘텐츠 관리 컨트랙트(160)에 저장된 해당 콘텐츠 파일의 콘텐츠 메타 정보(710) 내 저장상태값이 'Saved'로 변경되고, 이에 따라, 분산 앱(140)은 새로 저장된 콘텐츠 파일을 포함한 갱신된 피드 화면(1020)을 출력할 수 있다.

[0074] 또한, 상기 제1 스토리지 서버는, 사용자 단말에 의해 전송된 콘텐츠 파일을 저장 완료함에 따라, 콘텐츠 파일의 다운로드 권한을 증명하는 다운증명정보를, 사용자 단말에 발급할 수 있다.

[0075] 사용자 단말의 분산 앱(140)은, 발급된 다운증명정보를, 블록체인 네트워크(110)의 콘텐츠 관리 컨트랙트(160)에 저장하여, 백업할 수 있다.

[0076] 도 7b를 참조하면, 다운증명정보(DownloadCert)(720)에는, 자격증명정보(920)를 통해 획득한 콘텐츠 메타 정보(910)와 다운증명정보(720)의 생성시간, 사용자의 DID, 스토리지 서버(120)의 DID가 기재되며, 이 모든 값을 스토리지 서버(120)의 비밀키로 사인한 서명값이 포함된다.

[0077] 이후, 사용자 단말로부터, 상기 제1 스토리지 서버에 저장한 콘텐츠 파일의 다운로드 요청이 발생하면, 상기 제1 스토리지 서버는, 사용자 단말에 발급된 다운증명정보(720)를 검증하여, 사용자 단말에 다운로드 토큰을 부여할 수 있다.

[0078] 도 12은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 콘텐츠 다운로드를 요청 시 분산 앱의 화면 일례를 도시한 도면이다.

[0079] 도 12를 참조하면, 사용자 단말의 분산 앱(140)은, 화면(1210)을 통해, 사용자 단말에 발급된 다운증명정보(720)를 제1 스토리지 서버로 전송하면서 콘텐츠 파일의 다운로드를 요청할 수 있다.

[0080] 제1 스토리지 서버는, 상기 BCON 인증을 실시하여 사용자 단말의 분산 앱(140)에서 보내온 다운증명정보(720)를 검증하고, 상기 BCON 인증 결과로 사용자 단말에 도 9에 도시된 것과 같은 다운로드 토큰(950)을 부여할 수 있다.

[0081] 제1 스토리지 서버는, 설정된 유효시간 이내에 다운로드 토큰(950)을 입력하는 사용자 단말로 상기 콘텐츠 파일을 제공할 수 있다.

[0082] 이때에도, 상기 제1 스토리지 서버는 사용자 단말에서 분산 앱(140)을 통해 다운로드 토큰(950)을 입력하면, 카산드라 데이터베이스에서 비밀키를 가져와서, 사용자가 보낸 다운로드 토큰(950)의 유효성을 확인한 후에, 상기 콘텐츠 파일을 제공할 수 있다.

[0083] 이처럼 본 발명에 의하면, 콘텐츠 파일의 업로드 권한을 나타내는 액세스 토큰/다운로드 권한을 나타내는 액세스 토큰을 사용자 단말에 부여해, 액세스 토큰을 통한 사용자의 콘텐츠 접근 권한을 체계적으로 제어할 수 있다.

[0084] 또한, 상기 제1 스토리지 서버는 상기 콘텐츠 파일을 상기 유효시간 이내에 다운로드 할 수 있는 임시 경로를 생성하여, 다운로드 토큰(950)과 함께 상기 사용자 단말에 부여함으로써, 상기 사용자 단말에서 상기 임시 경로

에 접근해 콘텐츠 파일을 이용하도록 할 수도 있다.

[0085] 이후, 제1 스토리지 서버는 상기 콘텐츠 파일이 다운로드 완료되거나, 상기 유효시간이 경과됨에 따라, 상기 제1 스토리지 서버에서 상기 임시 경로를 무효화함으로써, 상기 콘텐츠 파일의 저장 경로가 노출되지 않게 할 수 있다.

[0086] 실시예에 따라, 사용자 단말로부터 제1 스토리지 서버에 저장한 콘텐츠 파일의 소유권 확인 요청이 발생할 경우, 사용자 단말의 분산 앱(140)은, 블록체인 네트워크(110)의 콘텐츠 관리 컨트랙트(160)에 저장된 콘텐츠 메타 정보(710) 및 다운증명정보(720)를 로딩하고, 콘텐츠 메타 정보(710)에 기재된 콘텐츠 파일의 소유자값, 생성시간값 및 해시값과, 다운증명정보(720)를, 소유권 근거자료로서 사용자 단말의 화면에 출력할 수 있다.

[0087] 이처럼, 본 발명에서 제안하는 BCON 서비스에 의하면, 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 유지한 콘텐츠 메타 정보와 다운증명정보를 스토리지 서버에 보관한 콘텐츠 파일에 대한 소유권을 주장하는데 활용할 수 있으므로, 콘텐츠 제작자의 결과물을 안전하고 신뢰성 있게 보관할 뿐만 아니라, 콘텐츠 제작자의 소유권을 확실하게 보장할 수 있게 된다.

[0088] 도 4는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템의 서비스 구조를 도시한 도면이다.

[0089] 도 4를 참조하면, 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템(400)은 스토리지 서버(410), 검증 서버(420), 분산 앱(Dapp)(430), 클레이튼 네트워크(440)의 DID 레지스트리(450) 및 콘텐츠 관리 컨트랙트(460)를 포함하여 구성할 수 있다.

[0090] 스토리지 서버(410)는 사용자의 콘텐츠를 유지하고, 콘텐츠에 접근하는 모든 권한을 관리하는 서비스 제공자의 역할을 한다.

[0091] 스토리지 서버(410)는 사용자의 대용량 콘텐츠를 분산 저장하기 위해 3개 이상의 카산드라 데이터베이스(411)를 구비할 수 있다.

[0092] 검증 서버(420)는 DID 기반으로 사용자의 신원 및 권한을 관리하며, BCON 인증 과정에 필요한 DID 문서를 가지고 있는 DID 레지스트리(450)를 관리하는 BCON 서비스 검증자의 역할을 한다.

[0093] 검증 서버(420)는 DID 레지스트리(450)에 기록된 사용자의 DID 문서를 이용해 BCON 인증을 실시하여, 사용자에게 콘텐츠 파일의 업로드 가능을 나타내는 자격증명정보 발급해 준다.

[0094] 검증 서버(420)는 사용자 분산식별자(DID), 사용자의 서비스 권한, 콘텐츠 파일을 업로드할 스토리지 서버(410)의 접근 위치 등을 저장하는 LDAP 기반의 스토리지(421)를 구비할 수 있다.

[0095] 여기서, LDAP(Lightweight Directory Access Protocol)는, 네트워크 상에서 분산 디렉터리 서비스에 접근하고 사용하기 위해 공개된 표준 애플리케이션 프로토콜이며, LDAP는 트리 구조로 된 사용자, 시스템 등의 정보를 저장할 중앙 서버 위치를 제공하고, 다양한 애플리케이션과 서비스를 LDAP 서버에 연결하여 손쉽게 조회 및 관리할 수 있다.

[0096] 분산 앱(Dapp)(430)은 BCON 서비스 제공을 위해 제작되어 사용자 단말에 배포되는 사용자 앱으로서, 리액트와 리덕스를 기반으로 개발된 웹 분산 애플리케이션(Dapp)이다.

[0097] Dapp(430)은 클레이튼 네트워크(440)의 웹 브라우저 확장 프로그램 형태의 지갑인 카이카스(Kaikas)(431)를 이용해 사용자의 로그인 및 계정 관리를 수행한다.

[0098] Dapp(430)은 스토리지 서버(410)와 검증 서버(420) 및 클레이튼 네트워크(440)와 상호작용하여, 편리하고 신뢰성 있는 BCON 서비스를 사용자에게 제공할 수 있다.

[0099] 클레이튼 네트워크(440)에는, 사용자의 BCON 인증에 필요한 DID 문서를 기록, 관리하는 DID 레지스트리(450)와, 신뢰성 있는 콘텐츠 관리를 위해 서비스에 필요한 증명서들을 블록체인에 저장하는 콘텐츠 관리 컨트랙트(460)가 포함된다.

[0100] BCON 서비스 사용자는 Dapp(430)을 통해 BCON 서비스에 필요한 증명서와 정보들은 블록체인(440)에 저장하고, 실제 콘텐츠는 스토리지 서버(410)의 카산드라 데이터베이스(411)에 저장하는 방식으로, 블록체인(440)의 용량 한계를 해결하고 신뢰성 있게 콘텐츠 관리를 수행할 수 있다.

[0101] 본 발명에서 BCON 서비스는 기존의 DID 인증 과정을 간략화하여 필요한 정보를 선택적으로 제공하는 BCON 인증

을 통해 구현된다. 따라서 BCON 인증은 사용자의 정보 주권을 강화하는데 도움이 된다.

[0102] BCON 인증은 사용자의 신원 인증과 더불어 사용권한을 증명하는 문서(자격증명정보, 다운증명정보)에 대한 발급자의 신원을 확인할 때 각각 실시되기 때문에, 그 때마다 BCON 인증을 실시하는 주체는 검증 서버(420)와 스토리지 서버(410)로 바뀔 수 있다.

[0103] BCON 서비스에서는 검증 서버(420)와 스토리지 서버(410)에서 BCON 인증 과정이 일어나며, 해당 과정에서 필요한 DID 문서는 검증 서버(420)에서 관리하는 DID 레지스트리(450)에 포함되어 있다.

[0104] 도 3에 도시된 BCON 인증 절차에 따르면, 사용자는 BCON 인증을 위해 필요한 정보를 보내고, BCON 인증의 대상이 될 주체(subject)의 DID를 이용하여 클레이튼 네트워크(440)의 DID 레지스트리(450)에서 주체의 DID 문서를 가져오고, 가져온 DID 문서와 사용자가 보내온 주체의 공개키 아이디를 이용하여 공개키를 추출하고, 대칭키 암호의 복호화 과정을 거쳐 사용자로부터 받은 서명값이(signature) 유효한지 검증하여 사용자가 보낸 문서에 대한 사용자의 신원 또는 해당 문서 발급자의 신원을 인증한다.

[0105] 검증 서버(420)에서 BCON 인증의 결과로 사용자에게 업로드 가능을 나타내는 자격증명정보를 발급하면, 도 8과 같은 콘텐츠 업로드 과정이 진행된다.

[0106] 스토리지 서버(410)에서 콘텐츠 업로드 후에 다운증명정보를 발급하면, 도 11과 같은 콘텐츠 다운로드 과정이 진행된다.

[0107] 도 5는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 스토리지 서버의 내부 구성의 일례를 도시한 도면이다.

[0108] 도 5를 참조하면, 하나의 스토리지 서비스(410)는 3개의 카산드라 데이터베이스 노드(node 1, 2, 3)로 구성되어, 사용자가 업로드 요청하는 콘텐츠 파일을, 3개의 노드에 분산 복제 저장하여 콘텐츠 파일의 가용성 및 견고성을 제고할 수 있다.

[0109] 사용자가 업로드 요청을 발생하면, 검증 서버(420)는 콘텐츠 업로드를 위한 BCON 인증을 실시해 신원 인증된 사용자에게 자격증명정보를 발급하고, 스토리지 서버(410)는 상기 자격증명정보의 검증 및 업로드 토큰을 부여해, 클러스터링 되어 있는 3개의 카산드라 데이터베이스 중 어느 하나의 DB에 콘텐츠 파일의 업로드를 진행하고, 업로드 완료 후 사용자에게 다운증명정보를 발급해 응답한다.

[0110] 사용자가 다운로드 요청을 발생하면, 스토리지 서버(410)는 콘텐츠 다운로드를 위한 BCON 인증을 실시해 사용자의 신원을 인증하고, 상기 다운증명정보를 검증하여, 다운로드 토큰을 부여해, DB에 업로드한 콘텐츠 파일의 다운로드를 진행하여, 다운로드 완료된 콘텐츠 파일로 응답한다.

[0111] 본 발명에서 제안하는 BCON 서비스에서는 체계적인 인증 과정을 거쳐 콘텐츠를 안전하게 업로드와 다운로드를 구현할 수 있으며, 모든 과정을 진행하는 동안 콘텐츠 용량에 관계없는 적절한 속도로 서비스 제공이 가능하다.

[0112] 도 6은 본 발명의 다른 실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 단일의 검증 서버로 복수의 스토리지 서버의 콘텐츠 서비스를 제공하는 서비스 구조를 도시한 도면이다.

[0113] 도 6을 참조하면, 검증 서버(600)는, 여러 제1 내지 제3 스토리지 서버(610~630)와 분리되어 구성될 수 있다.

[0114] 예를 들어, 제1 스토리지 서버(610)는 콘텐츠 보관 서비스를 제공하고, 제2 및 제3 스토리지 서버(620, 630)에서 콘텐츠 보관 서비스 외 다른 서비스를 제공하는 경우, 하나의 검증 서버(600)에서 서로 다른 서비스를 제공하는 여러 서버를 관리할 수 있는 장점이 있다.

[0115] 따라서, 콘텐츠 보관 서비스를 제공하는 제1 스토리지 서버(610)에서는 사용자 관리를 위한 작업을 할 필요 없이 콘텐츠를 관리하는 서비스에만 집중할 수 있다.

[0116] 이와 같이 본 실시예에 의하면, 하나의 검증 서버(600)를 이용하여, 스토리지 서비스에 특화된 클라우드 서비스들이 운영하는 다수의 스토리지 서버(610~630)의 콘텐츠 서비스를 효율적으로 운영할 수 있다.

[0117] 도 9는 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 콘텐츠 메타 정보, 자격증명정보, 다운증명정보, 업로드 토큰 및 다운로드 토큰의 데이터 구조를 도시한 테이블이다.

[0118] 도 9에 도시된 테이블(900)을 참조하면, 먼저, 사용자 단말(user)에서 업로드할 콘텐츠 파일을 설명하는 콘텐츠 메타 정보(910)에는, 업로드할 콘텐츠 파일의 이름(Content Name), 콘텐츠 파일의 종류에 따른 타입값(Content Type), 콘텐츠 파일의 사이즈값(Content Size), 해시값(Content Hash)이 기재되고, 이 외에, 콘텐츠 파일의 스

토리지 서버 저장 여부를 나타내는 저장상태값(Content State), 콘텐츠 파일의 소유자값(Content Owner), 콘텐츠 파일의 생성시간값(Content Created time)이 더 기재되어, 블록체인의 콘텐츠 관리 컨트랙트에 저장될 수 있다.

[0119] 또한, 검증 서버(verifier)에서 발급하는 자격증명정보(920)에는, 1)자격증명정보(920)의 발급을 요청하는 사용자 단말(user)의 분산 앱에서 보내온 모든 정보, 즉, 분산식별자(DID), 공개키 ID, 콘텐츠 메타 정보(910), 서명값이 기재되고, 2)검증 서버의 DID, 공개키 ID, 접근 위치(access point)가 기재되고, 3)사용자 단말에 이용을 허가할 스토리지 서버의 접근 위치(end point)와 서비스 권한(privilege), 4)자격증명정보(920)의 발급 시간(issued time), 유효시간(valid time), 및 각 정보를 검증 서버(verifier)의 공개키와 대칭되는 비밀키로 서명하여 만든 자격증명서명이 기재될 수 있다.

[0120] 또한, 콘텐츠 파일의 업로드 후에 스토리지 서버에서 발급하는 다운증명정보(930)에는, 자격증명정보(920)를 통해 획득한 콘텐츠 메타 정보(content meta info)(910), 다운증명정보(930)의 생성시간, 사용자의 DID, 스토리지 서버의 DID, 이 모든 값을 스토리지 서버의 비밀키로 사인한 서명값 등이 기재될 수 있다.

[0121] 또한, 검증 서버에서 콘텐츠 파일의 업로드를 요청한 사용자 단말의 자격증명정보(920)를 검증한 후에 발급하는 업로드 토큰(940)에는, 업로드 토큰 정보에 관한 옵션(option), 만료시간(expiresln), 업로드 토큰(940)을 발급한 검증 서버(issuer), 페이로드(payload), 비밀키(secretKey)가 기재되며, 여기서, 옵션에, 토큰 발급자인 스토리지 서버의 DID 및 토큰 발급 대상자인 사용자의 DID가 업로드 토큰 정보에 관한 기재되고, 페이로드에, 사용자 단말의 콘텐츠 메타 정보(content meta info)(910)가 기재될 수 있다. 검증 서버는 헥사바이트로 256 길이의 임의의 문자열의 형태로 상기 비밀키를 생성하고, 추후 업로드 토큰(940)의 검증 시 필요하므로 카산드라 데이터베이스에 비밀키를 저장해 둘 수 있다. 검증 서버는 옵션, 페이로드, 비밀키를 사인한 형태로 업로드 토큰(940)을 사용자에게 발급할 수 있다.

[0122] 또한, 스토리지 서버에서 콘텐츠 파일의 다운로드를 요청한 사용자 단말의 다운증명정보(930)를 검증한 후에 발급하는 다운로드 토큰(950)에는, 만료시간(expiresln), 다운로드 토큰(950)을 발급한 스토리지 서버의 DID(issuer), 페이로드, 비밀키(secretKey)가 기재되고, 상기 페이로드에는 다운증명정보(download certificate)(930)가 기재될 수 있다.

[0123] 도 8은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 블록체인 네트워크를 통한 콘텐츠 업로드 과정을 도시한 도면이다.

[0124] 도 8을 참조하면, 사용자(user)는 콘텐츠를 업로드하기 위해 Dapp(830)을 통해 업로드할 콘텐츠의 메타정보를 먼저 블록체인(840)의 콘텐츠 관리 컨트랙트(860)에 저장한다(step 1).

[0125] 이후 사용자(user)는 콘텐츠 관리 컨트랙트(860)에 저장한 정보를 가지고 검증 서버(820)에 자격증명정보의 발급을 요청하고, 그러면 검증 서버(820)는 블록체인(840)의 DID 레지스트리(850)에서 사용자의 DID 문서를 가져와 BCON 인증을 실시하여, 사용자의 신원 및 사용권한을 확인한 후 자격증명정보를 발급한다(step 2).

[0126] 이후 사용자(user)는 발급받은 자격증명정보를 스토리지 서버(810)로 보내 콘텐츠 업로드 요청을 하고, 그러면 스토리지 서버(810)는 블록체인(840)의 DID 레지스트리(850)에서 사용자의 DID 문서를 가져와 BCON 인증을 실시하여, 사용자가 보내온 자격증명정보를 검증하고, 콘텐츠를 업로드할 수 있는 권한을 사용자에게 부여하기 위해 업로드 토큰을 발급한다(step 3). 여기서, 업로드 토큰은 추가 저장소가 필요 없고 위변조 방지가 보장된 JWT를 사용하여 생성될 수 있다.

[0127] 이후 사용자(user)는 발급받은 업로드 토큰과 실제 콘텐츠를 함께 스토리지 서버(810)로 보내 업로드 요청하고. 그러면 스토리지 서버(810)는 카산드라 데이터베이스에서 비밀키를 가져와서 사용자가 보낸 업로드 토큰의 유효성을 검증한 후, 실제 콘텐츠를 카산드라 데이터베이스에 저장하고, 업로드 완료에 따라 해당 콘텐츠의 다운증명정보를 발급한다(step 4).

[0128] 사용자(user)는 스토리지 서버(810)에서 발급받은 다운증명정보를 Dapp(830)을 통해 블록체인(840)의 콘텐츠 관리 컨트랙트(860)에 저장하고, 콘텐츠의 업로드 완료를 기록하기 위해, 앞서 블록체인(840)의 콘텐츠 관리 컨트랙트(860)에 저장한 콘텐츠 메타정보의 Content State의 값을 'Saved'로 변경한다(step 5).

[0129] Dapp(830)은 사용자(user)가 로그인하면, 콘텐츠 관리 컨트랙트(860)에 저장한 콘텐츠 메타정보의 Content State의 값을 이용해 스토리지 서버(810)에 업로드 완료된 콘텐츠들의 목록을 피드 화면(Feed Page)에 출력하게 되는데, 새로운 콘텐츠의 업로드 완료 후에는, 콘텐츠 메타정보의 Content State 값이 Saved인 콘텐츠 해시값과

일치하는 다운증명정보를 컨트랙트에서 조회하여, 새롭게 업로드 완료된 콘텐츠를 포함하여 피드 화면을 업데이트 한다.

[0130] 사용자(user)는 업데이트 된 피드 화면에서 업로드 완료된 콘텐츠의 아이콘을 클릭하면, 도 12의 화면(1210)과 같이, 업로드된 콘텐츠에 대해 발급받은 다운증명정보를 확인할 수 있고, 'Download' 버튼 클릭을 통해 업로드된 콘텐츠의 다운로드를 요청할 수 있다. 발급받은 다운증명정보를 이용하여 업로드된 콘텐츠를 다운로드 하는 과정은 도 11에 도시된다.

[0131] 이와 같이, 본 발명은 사용자 단말에 의한 콘텐츠 파일의 업로드 요청 발생 시, 스토리지 서버와 분리된 검증 서버에서 BCON 인증을 실시해 콘텐츠 업로드 가능을 나타내는 자격증명정보를 사용자 단말에 발급함으로써, 스토리지 서버에서 상기 자격증명정보의 검증에 의해 콘텐츠 파일을 저장(보관)하는 서비스를 제공할 수 있다.

[0132] 또한 본 발명은 콘텐츠 파일의 업로드 전에, 해당 콘텐츠 파일을 설명하는 콘텐츠 메타 정보(소유자값, 생성시간값, 해시값 등)를 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 저장하고, 콘텐츠 파일의 업로드 후에, 스토리지 서버에 의해 발급된 다운증명정보를, 콘텐츠 관리 컨트랙트에 더 저장함으로써, 블록체인 네트워크의 콘텐츠 관리 컨트랙트에 안전하게 유지된 콘텐츠 메타 정보와 다운증명정보를 이용해, 사용자 단말의 해당 콘텐츠 파일의 소유권을 주장할 수 있게 지원한다.

[0133] 도 11은 본 발명의 일실시예에 따른 블록체인 기반의 콘텐츠 서비스 구현 시스템에서, 블록체인 네트워크를 통한 콘텐츠 다운로드 과정을 도시한 도면이다.

[0134] 도 11을 참조하면, 사용자(user)는 자신이 업로드한 콘텐츠를 스토리지 서버(1110)에서 다운로드 하기 위해, Dapp(1130)을 통해, 도 8에서 발급받은 다운증명정보를 스토리지 서버(1110)로 보내 콘텐츠 다운로드 요청을 하고, 그러면 스토리지 서버(1110)는 블록체인(1140)의 DID 레지스트리(1150)에서 사용자의 DID 문서를 가져와 BCON 인증을 실시하여 사용자가 보내온 다운증명정보를 검증하고, 콘텐츠를 다운로드할 수 있는 권한을 사용자에게 부여하기 위해 다운로드 토큰을 발급한다(step 1).

[0135] 이때, 스토리지 서버(1110)는 사용자가 요청한 콘텐츠를 카산드라 데이터베이스에서 미리 꺼내 두고, 콘텐츠를 다운로드할 수 있는 임시 경로를 생성해 다운로드 토큰과 함께 줄 수 있다. 임시 경로는 헥사바이트 형태의 중복되지 않는 랜덤한 문자열로 생성되며 콘텐츠 다운로드 완료 시 삭제된다.

[0136] 사용자가 발급받은 다운로드 토큰을 설정된 유효시간 이내에 Dapp(1130)을 통해 스토리지 서버(1110)로 보내면, 스토리지 서버(1110)는 카산드라 데이터베이스에서 비밀키를 가져와서, 사용자가 보낸 다운로드 토큰의 유효성을 검증하고, 유효한 토큰이면 사용자는 상기 임시 경로를 통해 콘텐츠를 다운로드할 수 있다(step 2)

[0137] 이때, 스토리지 서버(1110)는 다운로드 토큰을 보내온 사용자가 해당 콘텐츠에 대한 다운로드 권한을 가진 사람이 맞는지 먼저 BCON 인증을 통해 신원을 확인하고, 신원 확인이 완료되면, 카산드라 데이터베이스에서 비밀키를 가져와서 사용자가 보낸 다운로드 토큰의 유효성을 검증한다. 유효한 다운로드 토큰이라면 사용자는 임시 경로를 통해 콘텐츠를 다운로드할 수 있다.

[0138] 이와 같이, 본 발명은 스토리지 서버에서 콘텐츠 파일의 저장 완료 시 콘텐츠 다운로드 가능을 나타내는 다운증명정보를 사용자 단말에 발급함으로써, 이후, 상기 다운증명정보의 검증 만으로, 저장된 콘텐츠 파일을 이용 가능하게 한다.

[0139] 또한 본 발명은 스토리지 서버에서 자격증명정보의 검증과, 다운증명정보의 발급 및 검증을 수행할 때 마다 DID 레지스트리에 기록된 사용자의 DID 문서를 이용해 BCON 인증을 실시하여, 사용자 단말의 신원 및 사용권한을 확인함으로써, 블록체인 기반 콘텐츠 서비스의 보안성을 보다 강화할 수 있다.

[0140] 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.

[0141] 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.

[0142] 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.

[0143] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.

부호의 설명

[0144] 400: 블록체인 기반의 콘텐츠 서비스 구현 시스템

410: 스토리지 서버

420: 검증 서버

430: 분산 앱(Dapp)

440: 클레이튼 네트워크

450: DID 레지스트리

460: 콘텐츠 관리 컨트랙트

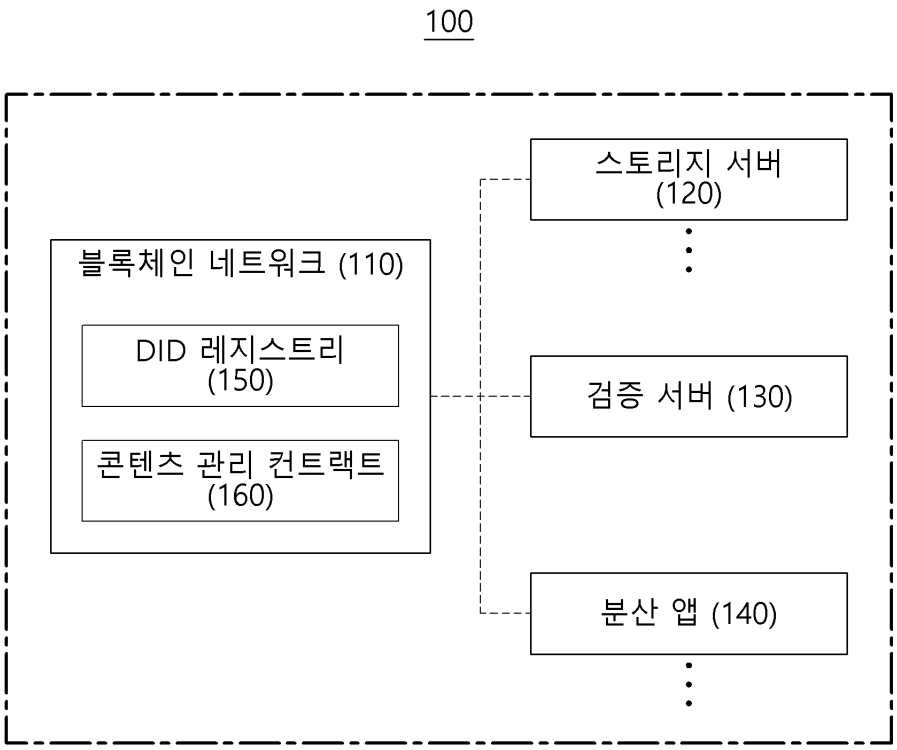
411: 카산드라 데이터베이스

421: LDAP 기반의 스토리지

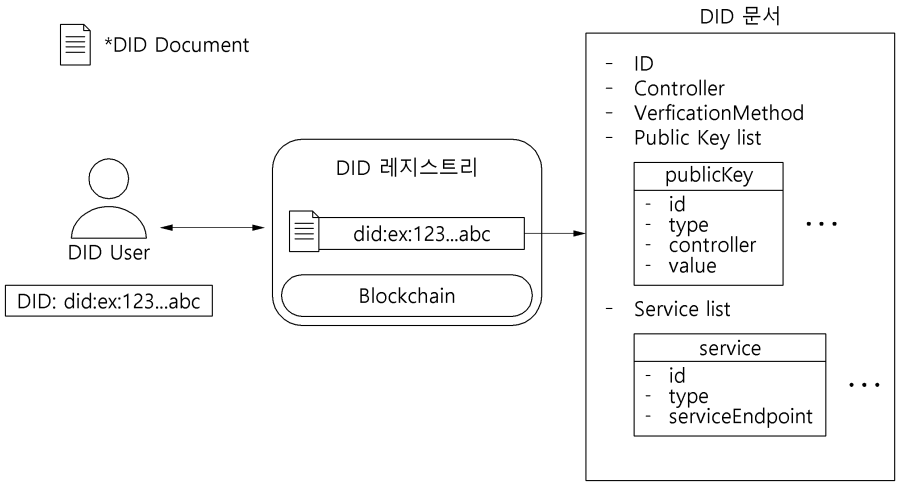
431: 카이카스

도면

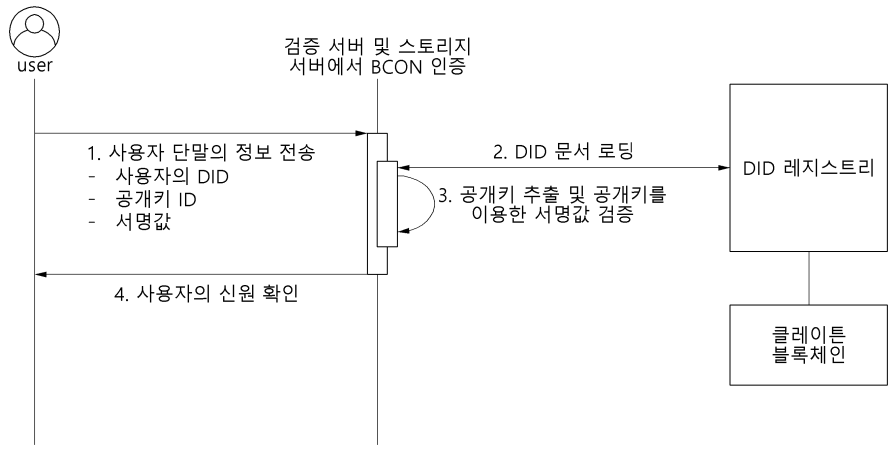
도면1


100
스토리지 서버 (120)
블록체인 네트워크 (110)
DID 레지스트리 (150)
콘텐츠 관리 컨트랙트 (160)
검증 서버 (130)
분산 앱 (140)

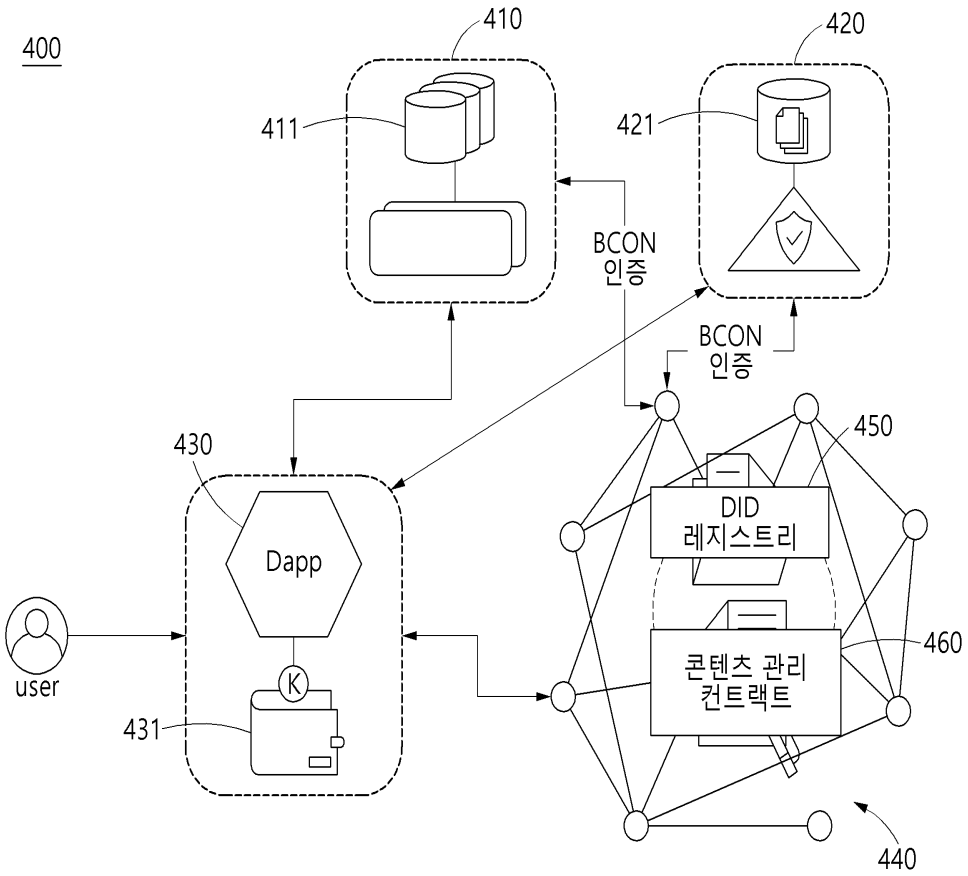
도면2


*DID Document
DID 문서
- ID
- Controller
- VerficationMethod
- Public Key list
publicKey
- id
- type
- controller
- value
DID 레지스트리
did:ex:123...abc
Blockchain
DID User
DID: did:ex:123...abc
- Service list
service
- id
- type
- serviceEndpoint

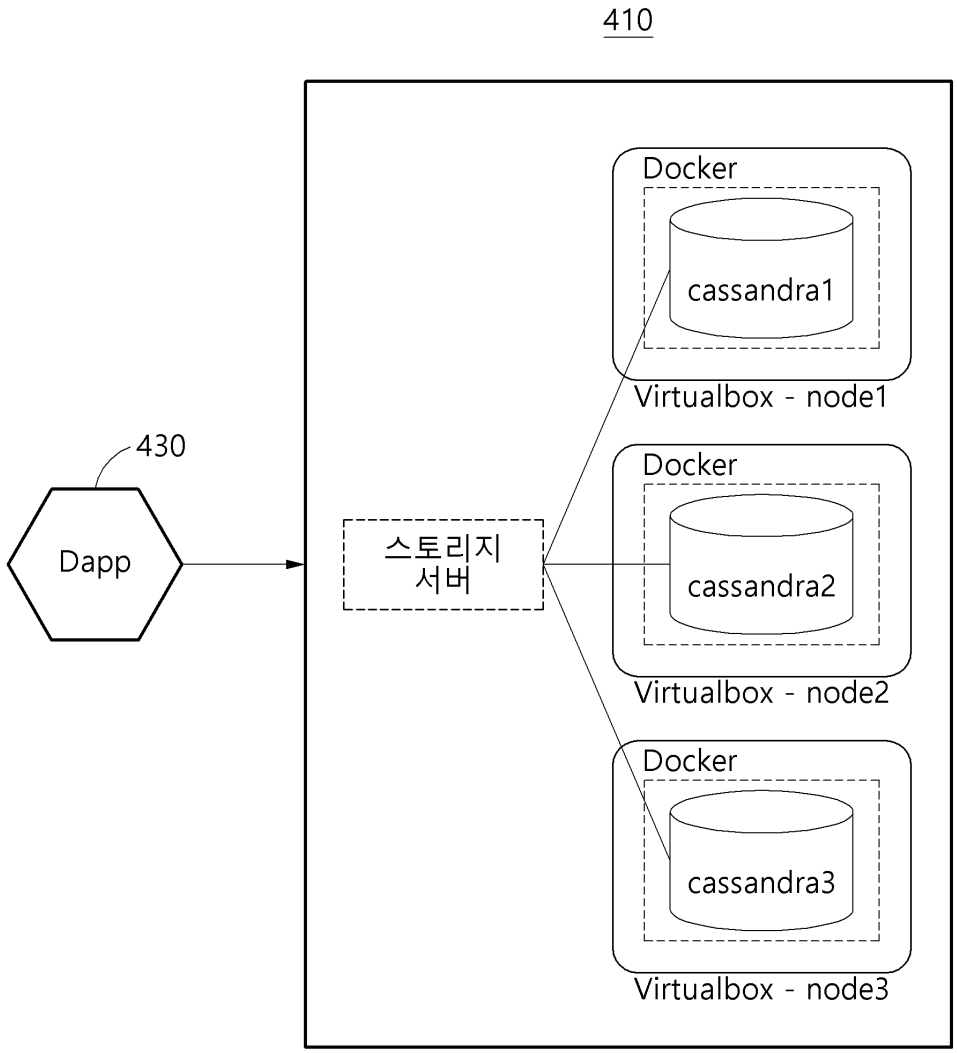
도면3


user
검증 서버 및 스토리지
서버에서 BCON 인증
1. 사용자 단말의 정보 전송
- 사용자의 DID
- 공개키 ID
- 서명값
2. DID 문서 로딩
3. 공개키 추출 및 공개키를
이용한 서명값 검증
4. 사용자의 신원 확인
DID 레지스트리
클레이튼
블록체인

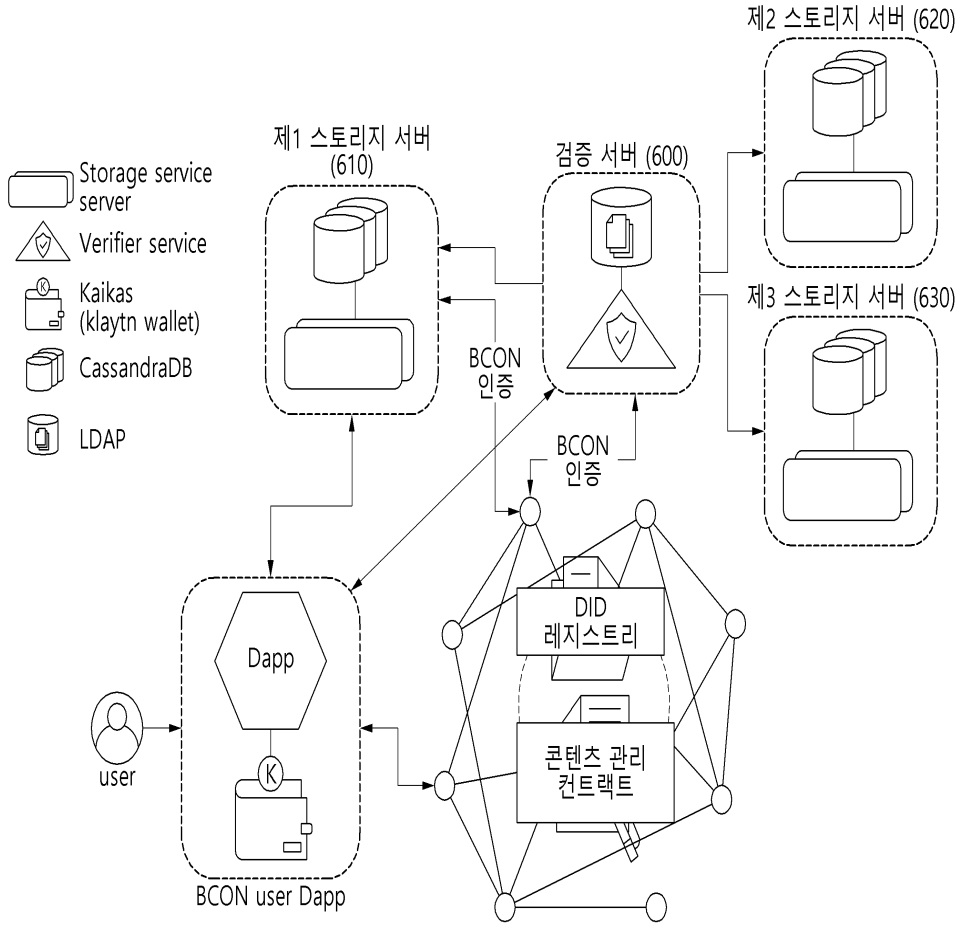
도면4


400
410
411
420
421
BCON
인증
BCON
인증
430
Dapp
K
431
user
450
DID
레지스트리
콘텐츠 관리
컨트랙트
460
440

도면5


410
Docker
cassandra1
Virtualbox - node1
430
Dapp
스토리지
서버
Docker
cassandra2
Virtualbox - node2
Docker
cassandra3
Virtualbox - node3

도면6



도면7a

710

ContentMeta

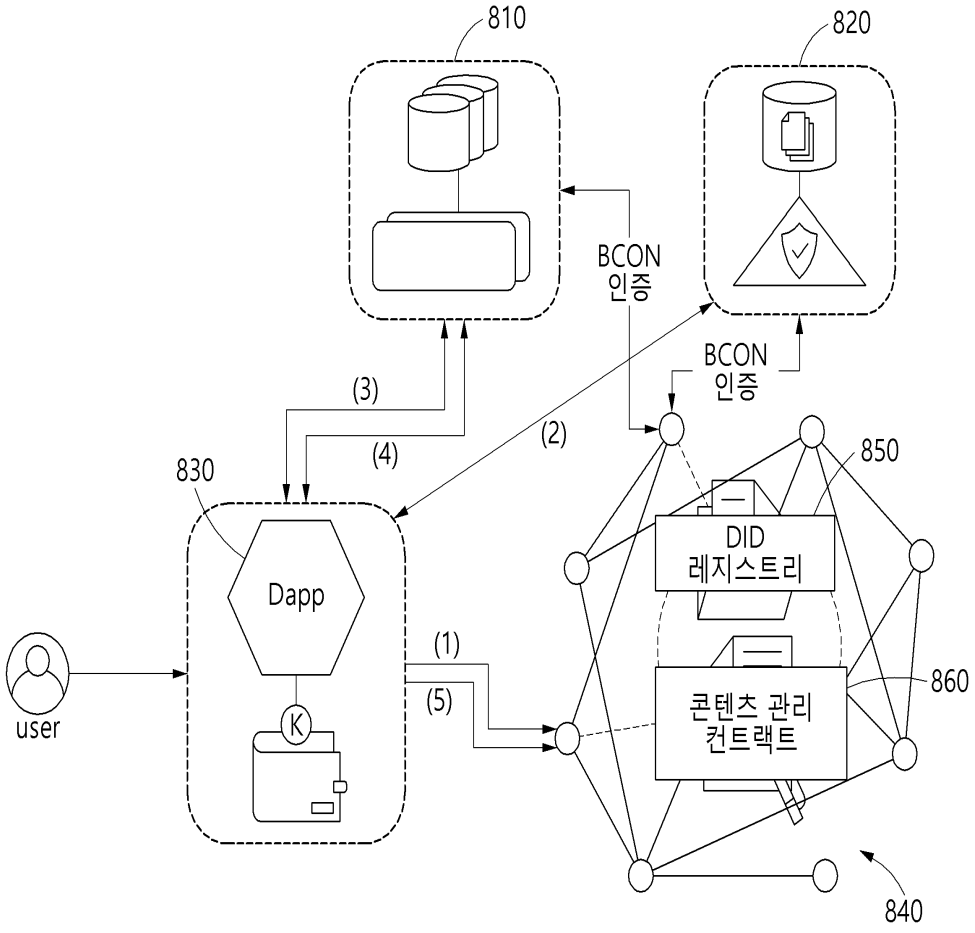
- File Type
- Content Name
- Content Type
- Content Size
- Content Hash
- Content Description
- Content Owner
- Content Created time
- Content State

도면7b

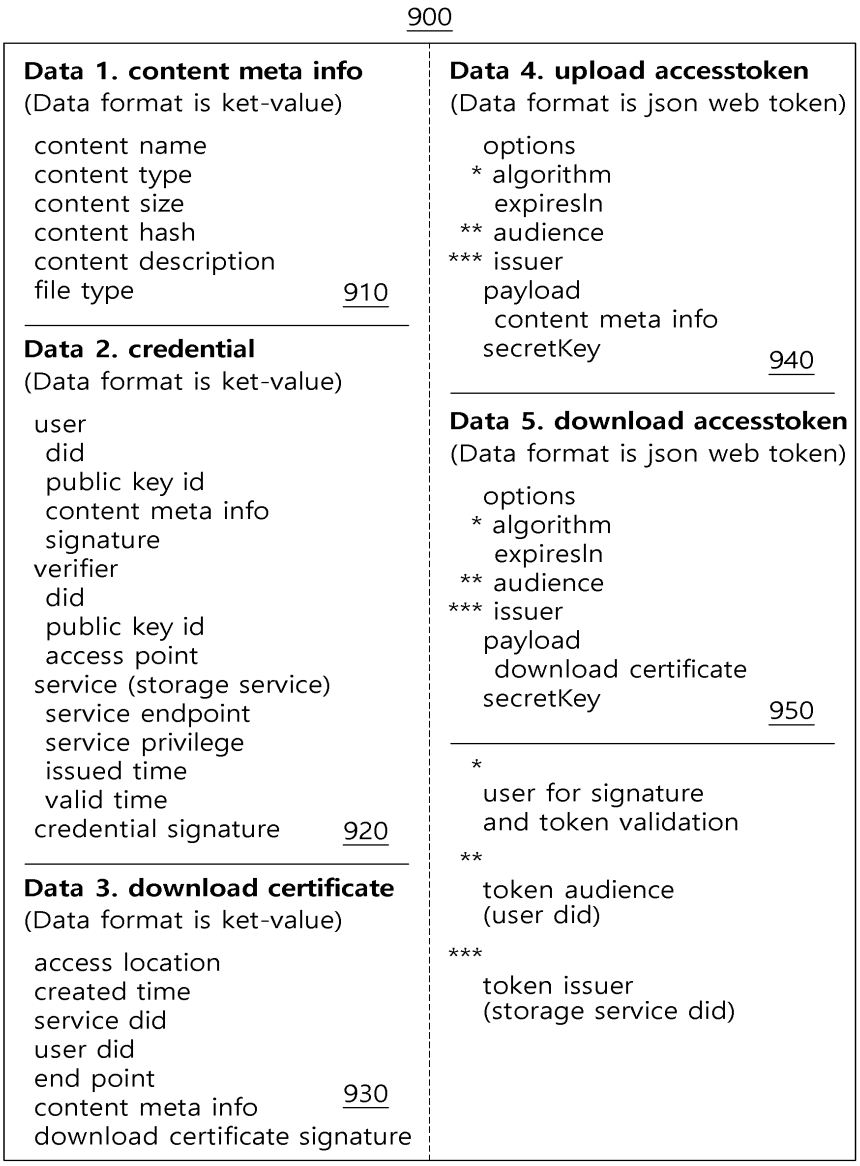
720

DownloadCert
- File Type
- Content Name
- Content Type
- Content Size
- Content Hash
- Content Description
- Access Location
- DownloadCert Created time
- Storage Service DID
- User DID
- Endpoint
- Storage Service Signature

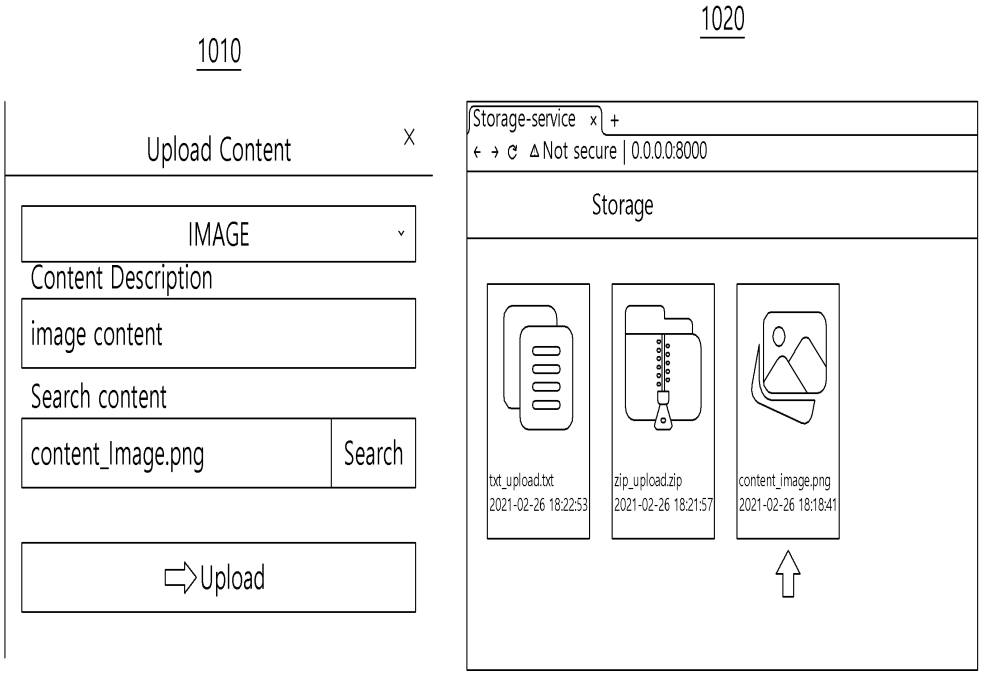
도면8



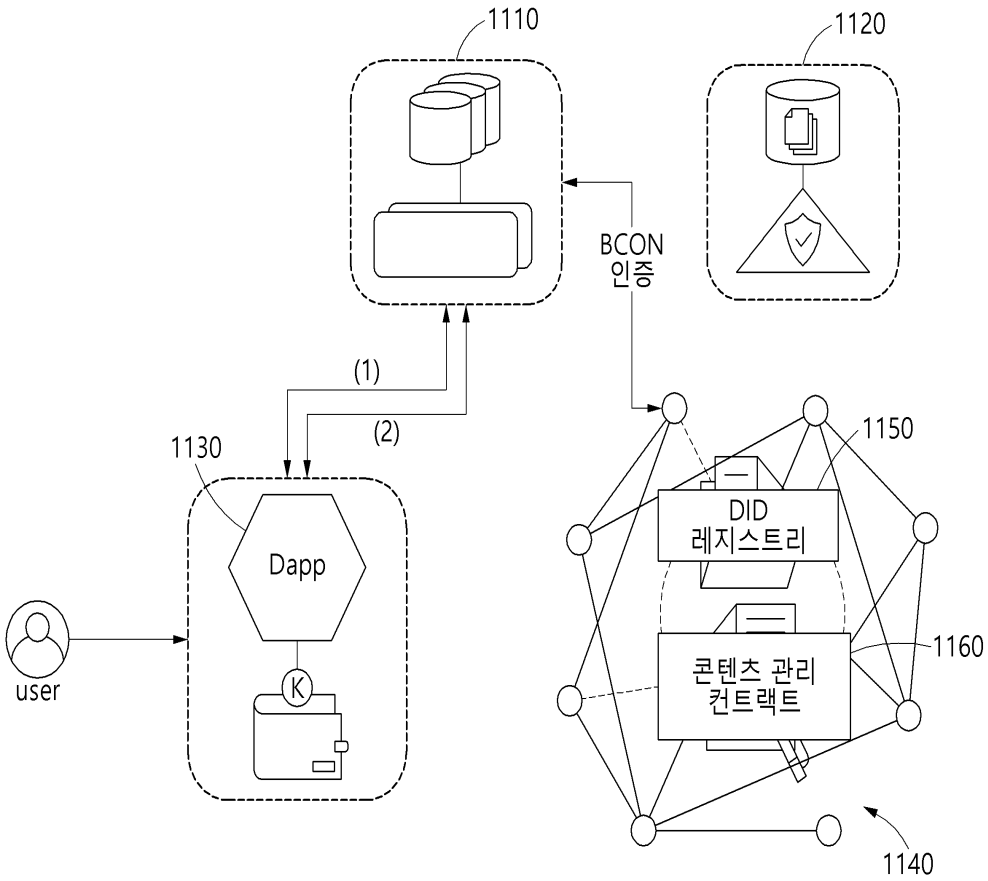
도면9


900
Data 1. content meta info
(Data format is ket-value)
content name
content type
content size
content hash
content description
file type
910
Data 2. credential
(Data format is ket-value)
user
did
public key id
content meta info
signature
verifier
did
public key id
access point
service (storage service)
service endpoint
service privilege
issued time
valid time
credential signature
920
Data 3. download certificate
(Data format is ket-value)
access location
created time
service did
user did
end point
content meta info
download certificate signature
930
Data 4. upload accesstoken
(Data format is json web token)
options
* algorithm
expiresIn
** audience
*** issuer
payload
content meta info
secretKey
940
Data 5. download accesstoken
(Data format is json web token)
options
* algorithm
expiresIn
** audience
*** issuer
payload
download certificate
secretKey
950
*
user for signature
and token validation
**
token audience
(user did)
***
token issuer
(storage service did)

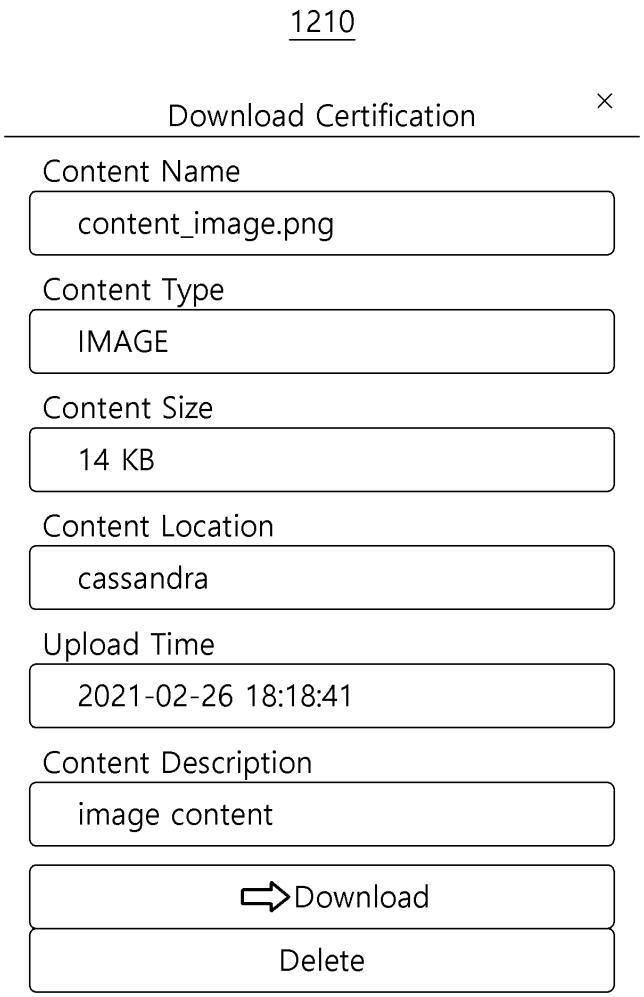
도면10


1010
1020
Upload Content
X
IMAGE
Content Description
image content
Search content
content_Image.png
Search
Upload
Storage-service
Not secure | 0.0.0.0:8000
Storage
txt_upload.txt
2021-02-26 18:22:53
zip_upload.zip
2021-02-26 18:21:57
content_image.png
2021-02-26 18:18:41

도면11


1110
1120
BCON
인증
(1)
(2)
1130
Dapp
user
1150
DID
레지스트리
콘텐츠 관리
컨트랙트
1160
1140

도면12


1210
Download Certification
×
Content Name
content_image.png
Content Type
IMAGE
Content Size
14 KB
Content Location
cassandra
Upload Time
2021-02-26 18:18:41
Content Description
image content
Download
Delete