JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 6, pp. 97-105, June 2021
https://doi.org/10.9708/jksci.2021.26.06.097

BCON : Blockchain-based Content Management Service Using DID

Hye-Won Kim*, Young-Eun Lee*, Min-Ho Kwon*, Myung-Joon Lee**

*Student, Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan, Ulsan, Korea
*Student, Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan, Ulsan, Korea
*Student, Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan, Ulsan, Korea
**Professor, School of IT Convergence, University of Ulsan, Ulsan, Korea

[Abstract]

In this paper, we propose BCON, a service that allows individuals to store personal contents safely, and reliably guarantee their ownership of contents, certifying their identities with DIDs(Decentralized identifiers). DID technology, which supports decentralized identification service based on a blockchain that cannot forgery or alter data, allows users to selectively provide their information, controlling personal information and reinforcing their sovereignty over their identity. BCON stores information about the content specified by a user on the blockchain and Authenticates the user's identity based on DID technology. It also provides functions for the user to safely upload and download the user's content to a distributed database. BCON consists of the content service verifier, the content storage service, the content management contract, and the user application, administrating rhe DID registry for Authority management.

▸ **Key words**: Content Management, Blockchain Service, DID, Content Storage Service, Content Service Certifier

[요 약]

본 논문에서는 개인 스스로가 자신의 신원을 인증하여 개인 콘텐츠를 안전하게 보관, 콘텐츠에 대한 자신의 소유권을 신뢰성 있게 보장받을 수 있는 서비스인 BCON을 제안한다. 데이터 위변조가 불가능한 블록체인을 기반으로 탈중앙화된 신원확인 서비스를 지원하는 DID 기술은 사용자가 자신의 정보를 선택적으로 제공하여 자신의 신원정보에 대한 주권을 강화하고 스스로 개인 정보에 대한 통제가 가능하다. BCON은 블록체인에 사용자가 지정한 콘텐츠에 대한 정보를 저장하고 DID 기술을 기반으로 사용자 신원을 인증하여, 사용자가 개인 콘텐츠를 안전하게 분산 데이터베이스에 업로드하고 다운로드하는 기능을 제공한다. BCON은 콘텐츠 서비스 검증자, 콘텐츠 보관 서비스, 콘텐츠 매니지먼트 컨트랙트 및 사용자 어플리케이션으로 구성되며, 서비스 권한 관리를 위한 DID 레지스트리를 운영한다.

▸ **주제어**: 콘텐츠 관리, 블록체인 서비스, DID, 콘텐츠 보관 서비스, 콘텐츠 서비스 검증자

• First Author: Hye-Won Kim, Corresponding Author: Myung-Joon Lee
*Hye-Won Kim (alsldjcjstk@cicweb.ulsan.ac.kr), Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan
*Young-Eun Lee (lyoung828@cicweb.ulsan.ac.kr), Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan
*Min-Ho Kwon(alsgh458@gmail.com), Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan
**Myung-Joon Lee (mjlee@ulsan.ac.kr), School of IT Convergence, University of Ulsan
• Received: 2021. 04. 14, Revised: 2021. 05. 25, Accepted: 2021. 05. 25.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

많은 콘텐츠가 디지털 형태로 생산 및 가공되어 유통되면서 디지털 콘텐츠의 불법복제와 유통 체계의 혼란, 소유권 관리의 어려움 등 문제점으로 인해 소유권의 중요성이 대두되고 있다. 콘텐츠 거래의 투명성과 소유권을 보장하기 위한 해결책으로 데이터 위변조 불가의 특성을 가진 블록체인 기술이 제시되고 있으며[1], 실제로 중국에서 블록체인 기술을 통해 개인의 소유권이 보장된 사례도 나타났다[2]. 현재 많은 블록체인 기업들이 콘텐츠의 소유권 보장을 위해 블록체인 기반의 신원관리 및 인증 시스템을 개발하고 있다. 대표적인 사례로 미디어체인은[3] 콘텐츠에 대한 메타정보를 게시, 검색 및 협업할 수 있는 플랫폼으로 특정 미디어 자산의 소유권에 관한 타임스탬프와 데이터를 접목하는 방안을 제시하였다.

콘텐츠 서비스를 안전하게 사용하기 위해선 사용자의 신원인증절차가 필요하다. 공인인증서의 독점적 지위가 폐지되면서, 새로운 전자서명 기술들이 등장했다. 특히 차세대 신원확인 기술로 분산신원증명(DID, Decentralized Identity)이 주목받고 있다[4]. DID 기술은 블록체인 기반으로 탈중앙화된 신원확인 서비스를 제공하며, 사용자가 서비스 기업에 필요한 정보만 선택적으로 전달할 수 있어 데이터 주권을 강화할 수 있는 기술이다. 여러 기업이 DID를 이용한 서비스를 시작하고 있으며[5], 현재 DID 기술은 W3C(World Wide Web Consortium)에서 표준화를[6] 진행하고 있다. 국내에서는 한국정보통신기술협회(TTA)가 ICT 기반 탈중앙화 대면 분야 표준화 포럼에 DID를 포함했으며[7], 여러 기업이 서비스 상용화를 적극적으로 추진하고 있다.

본 논문에서는 개인 스스로가 자신의 신원을 인증하여 자신의 콘텐츠를 안전하게 보관하며, 콘텐츠에 대한 소유권을 신뢰성 있게 보장받을 수 있는 서비스인 BCON (Blockchain-based CONtents management service)에 대해서 소개한다. BCON은 카카오 블록체인 플랫폼인 클레이튼에서[8] 동작하며 콘텐츠 서비스 검증자, 콘텐츠 보관 서비스, 콘텐츠 매니지먼트 컨트랙트, 콘텐츠 서비스 사용자 앱으로 구성된다. 콘텐츠 서비스 검증자는 DID 기반으로 사용자의 신원 및 권한을 관리하는 서비스이다. 콘텐츠 보관 서비스는 사용자가 콘텐츠에 접근하는 권한과 콘텐츠를 유지 및 관리한다. 콘텐츠 매니지먼트 컨트랙트는 콘텐츠 관리에 필요한 정보를 클레이튼 블록체인에 저장함으로써 콘텐츠에 대한 신뢰성 있는 관리를 가능하게 한다. 콘텐츠 서비스 사용자 앱은 3개의 독립적인 서비스들과 상호작용하여 사용자가 BCON 서비스를 보다 편리하게 이용할 수 있게 개발된 클레이튼 분산 어플리케이션이다.

본 논문의 구성은 다음과 같다. 1장 및 2장에서는 서론과 배경지식을 다룬다. 3장에서는 DID를 이용한 블록체인 기반 콘텐츠 서비스(BCON)를 제안하고 이와 더불어 4장에서는 BCON 서비스를 여러 용량의 콘텐츠를 이용하여 실험하고 그 결과에 관하여 기술한다. 마지막으로 5장에서는 본 논문의 결론에 관하여 서술한다.

II. Background Knowledge

1. Klaytn Blockchain and Smart Contract

카카오의 블록체인 기술 관련 자회사 Ground X가 개발한 클레이튼은 스마트 컨트랙트를 통해 분산 애플리케이션을 개발하고 실행이 가능한 블록체인 플랫폼이다. 클레이튼의 스마트 컨트랙트는 특정 주소에 배포되어 블록에 저장된 프로그램 코드로 특정 조건에 따라 자동으로 계약을 수행한다. 배포된 컨트랙트 주소에 트랜잭션을 보내 계약을 실행하고 실행된 결과는 블록체인에 저장되어 분산된 모든 노드의 동의 없인 임의의 수정이 불가하므로 데이터의 무결성을 보장한다. 클레이튼은 Istanbul BFT 합의 알고리즘을[9] 채택하여 임의의 노드들만 암호학적으로 랜덤하게 선출해 합의를 진행하고 빠른 속도로 블록의 완결성을 보장한다. 이에 트랜잭션 양이 증가하면 속도의 병목현상으로 비싼 거래 수수료를 내는 이더리움과[10] 달리 클레이튼의 성능은 초당 4000 트랜잭션을 처리하고 블록 생성이 1초에 남짓한 시간 안에 이루어져 즉각적인 트랜잭션 처리가 가능하다. 클레이튼은 효율적인 합의 방법과 빠른 트랜잭션 처리를 지원하여 고성능의 서비스 친화적인 블록체인으로 사용하기에 적합하다.

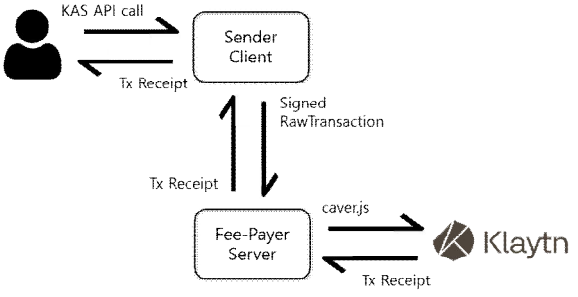

Fig. 1. Klaytn Fee Delegation

클레이튼은 트랜잭션 전처리 비용을 줄이기 위해 사용자가 트랜잭션을 보낼 때 트랜잭션 타입을 명시적으로 지정하

게 한다. 클레이튼의 트랜잭션 타입을 Fee Delegate 타입으로 지정하면 기본적인 트랜잭션들에 대해 수수료를 대신 납부하는 기능(Fig. 1, Klaytn Fee Delegation)을 제공한다.

2. DID

DID(Decentralized Identifier)는 기존 신원 제공자, 인증 기관 등 제3의 중앙기관으로부터 독립되어 사용자 본인이 자신의 신원을 증명 가능한 분산 디지털 신원 확인 기술이다. DID는 블록체인 기반 인증으로 비대칭 암호화 알고리즘 방식을 사용하며 자신을 설명할 수 있는 DID Document(Fig. 2, DID Document)를 직접 소유하면서 관리하여 스스로 신원 데이터의 통제, 신원 증명 권한을 가진다. DID Document는 자격증명을 검증할 수 있는 데이터를 담은 문서로 신원을 검증할 수 있는 공개키, 인증 정보와 상호작용 가능한 서비스의 리스트가 포함되어 있다.

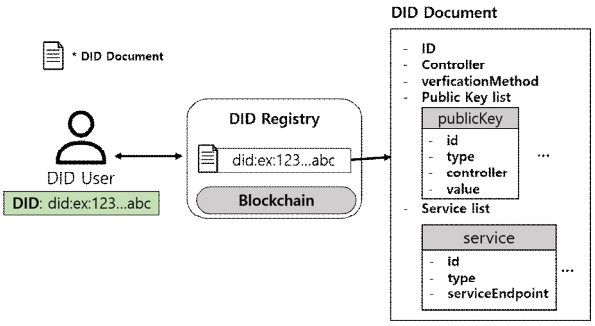

Fig. 2. Structure of DID Registry

DID의 생성, 확인, 업데이트 및 비활성화를 담당하는 블록체인 기반의 시스템인 DID Registry(Fig. 2, DID Registry)는 DID Document 확인을 위해 DID를 기록하고 DID Document 작성에 필요한 데이터를 반환한다. DID Registry를 통해 DID를 가진 개인은 블록체인 상에서 신뢰할 수 있는 기법을 통해 손쉽게 개인의 신원을 검증받는 것이 가능하다.

3. LDAP

LDAP(Light weight Directory Access Protocol)는 [11] 네트워크상에서 분산 디렉터리 서비스에 접근하고 사용하기 위해 공개된 표준 애플리케이션 프로토콜이다. 도메인을 통해 IP 주소에 접근 가능한 DNS(Domain Name System)와 같이 어떠한 정보를 기준으로 대상을 조회하고 편집 가능한 서비스를 디렉터리 서비스라고 한다. LDAP는 트리 구조로 된 사용자, 시스템 등의 정보를 저장할 중앙 서버 위치를 제공하고 다양한 애플리케이션과 서비스를 LDAP 서버에 연결하여 손쉽게 조회하고 관리할 수 있다.

4. Cassandra

카산드라는 대규모 확장 가능한 아파치 오픈소스 기반의 분산 데이터베이스이다. 기존 관계형 데이터베이스와 달리 SQL을 사용하지 않는 NoSQL 데이터베이스로서 대용량 데이터 트랜잭션에 대해 빠른 처리가 가능하다. 카산드라의 데이터 모델에는 Keyspace 라는 논리적 데이터 저장소가 최상위에 존재하고, 아래 다수의 Row로 구성된 Table이 있다. 하나의 Row는 Key-Value로 이루어진 여러 Column들로 구성된다. Row Key 데이터의 해시값을 기준으로 데이터는 분산되며, 데이터가 저장된 노드들은 Gossip 프로토콜을[12] 통해 모든 노드가 동등한 Ring 구조를 이루고 있다. 노드들이 주기적으로 서로 정보를 주고받는 Gossip 프로토콜을 통하여 새 노드를 추가하기 용이하며 수평적으로 쉽게 용량 확장이 가능하다.

III. Architecture and Implementation of BCON

본 장에서는 사용자 개인 스스로 신원을 인증하여 자신의 콘텐츠를 안전하게 보관하며, 콘텐츠에 대한 자신의 소유권을 신뢰성 있게 보장받을 수 있는 서비스인 BCON의 구조와 구현 기법에 관하여 기술한다.

1. BCON service architecture

BCON은 콘텐츠 서비스 검증자, 콘텐츠 보관 서비스, 콘텐츠 매니지먼트 컨트랙트, 콘텐츠 서비스 사용자 앱으로 구성되어 있다.

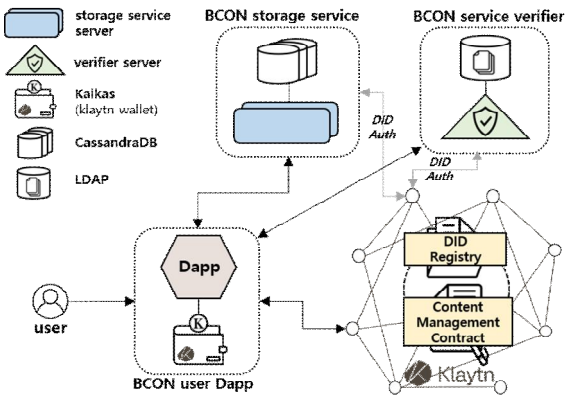

Fig. 3. BCON Service Architecture

콘텐츠 서비스 검증자는 DID 기반으로 사용자의 신원 및 권한을 관리하며, BCON 각 서비스에서 일어나는

BCON Service Authorization 과정에(Fig. 4. BCON Auth Process) 필요한 DID 문서를 가진 DID 레지스트리를 이용한다. 해당 검증자는 사용자에게 자격증명을 발급해주는 검증자 서버와 사용자 DID, 사용자의 서비스 권한, 콘텐츠 보관 서비스의 접근 위치 등을 저장하는 LDAP 기반의 스토리지로 구성된다. 콘텐츠 보관 서비스는 사용자의 콘텐츠와 콘텐츠에 접근하는 모든 권한을 유지하고 관리하는 서비스이다. 해당 서비스는 콘텐츠를 분산화하여 저장하기 위한 카산드라 데이터베이스와 콘텐츠 관리에 대한 서비스를 제공하는 서버로 구성된다. 콘텐츠 매니지먼트 컨트랙트는 신뢰성 있는 콘텐츠 관리를 위해 서비스에 필요한 증명서들을 블록체인에 저장하는 클레이튼 스마트 컨트랙트이다. BCON 사용자는 콘텐츠 서비스 사용자 앱을 통해 해당 서비스를 이용할 수 있다. 콘텐츠 서비스 사용자 앱은 리액트와 리덕스[13] 기반으로 개발된 웹 분산 애플리케이션(DApp)으로 사용자는 카이카스(Kaikas)를 [14] 이용해 DApp 로그인 및 계정 관리가 가능하다. DApp은 3개의 컴포넌트와 상호작용하여 사용자의 편리하고 신뢰성 있게 BCON 서비스를 이용할 수 있도록 한다.

2. BCON Authorization process

BCON 서비스는 서비스를 위한 DID 기반의 신원 및 권한 인증방식으로 기존의 DID Auth 과정을 간략화하여 개발한 *BCON Auth*를 사용한다. 사용자의 신원 인증과 더불어 권한을 증명하는 문서에 대한 발급자의 신원을 확인할 때 사용하므로 BCON Auth의 주체는 상황에 따라 바뀔 수 있다. BCON 서비스에서는 콘텐츠 서비스 검증자와 콘텐츠 보관 서비스에서 BCON Auth 과정이 일어나며, 해당 과정에서 필요한 DID 문서는 콘텐츠 서비스 검증자가 이용하는 DID 레지스트리에 포함되어 있다.

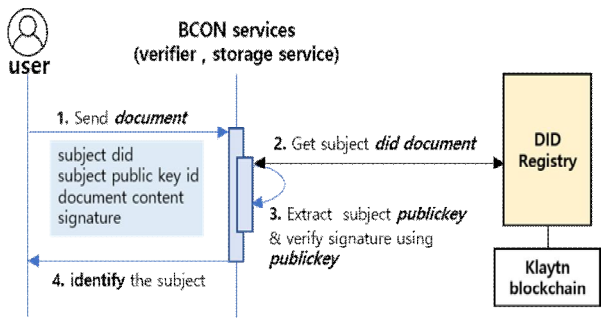

Fig. 4. BCON Auth Process

다음 그림 4는 BCON Authorization 절차를 설명한다. 사용자는 BCON 서비스에 BCON Auth를 위해 필요한 정보를 보낸다. 해당 서비스는 BCON Auth의 대상이 될 주체의(subject) DID를 이용하여 클레이튼에 배포된 DID 레지스트리에서 주체의 DID의 문서를 가져온다. 해당 서비스는 가져온 DID 문서와 사용자가 보내온 주체의 공개키 아이디를 이용하여 공개키를 추출한다. 대칭키 암호의 복호화 과정을 거쳐 사용자로부터 받은 서명 값이(signature) 유효한지 검증하여 사용자가 보낸 문서에 대한 사용자의 신원 또는 해당 문서 발급자의 신원을 인증한다.

3. Content Upload process

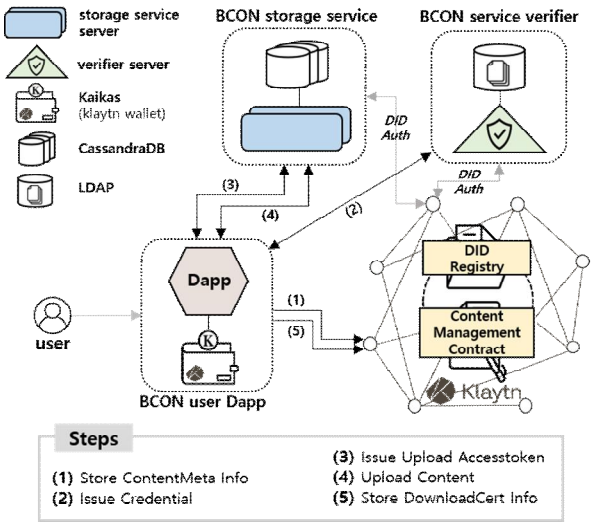

Fig. 5. Content Upload Process

사용자는 콘텐츠 서비스 사용자 앱 이용을 위한 로그인 시 사용자의 지갑 정보를 로컬에 저장하는 대신 보안을 위해 클레이튼 네트워크의 웹 브라우저 확장 프로그램 형태의 지갑인 카이카스를 사용한다. 카이카스를 통해 편리하게 사용자의 계정 관리가 가능하며 BCON 서비스에 로그인하면 자신이 업로드한 콘텐츠의 목록인 *피드 화면* (Fig. 9, Feed Page)을 볼 수 있다.

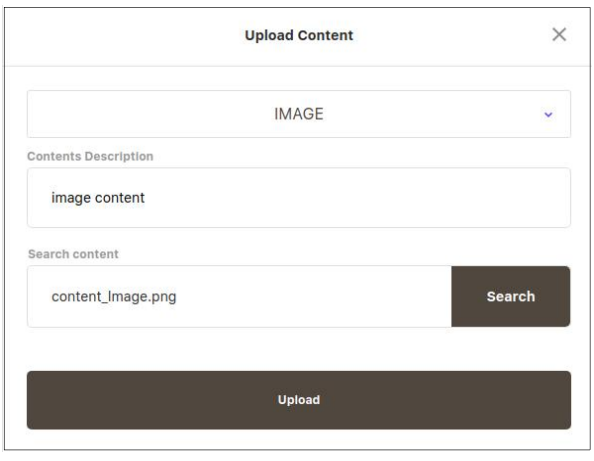

Fig. 6. Content Upload Page (BCON User DApp)

[step(1) in fig. 5] 사용자가 콘텐츠 서비스 사용자 앱에서 업로드할 콘텐츠와 콘텐츠에 대한 설명을 첨부하여 콘텐츠 업로드를 요청(Fig. 6, Upload Button)하면 먼저 업로드할 콘텐츠에 대한 신뢰성 있는 관리를 위해 클레이튼 스마트 컨트랙트에 *콘텐츠 메타정보*(Fig. 7, ContentMeta)를 저장한다.

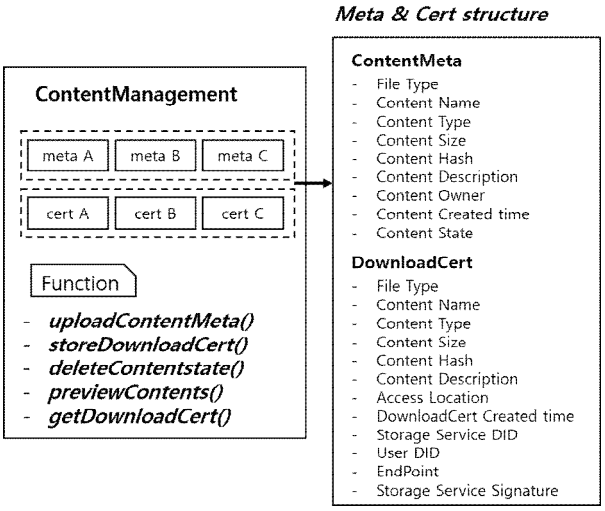

Fig. 7. Structure of ContentManagement Contract

[step(2) in fig. 5] 본 단계는 콘텐츠 서비스 검증자가 사용자의 콘텐츠 업로드를 위한 자격증명을 사용자에게 발급하는 단계로 다음과 같은 순서로 이루어진다.

1. 사용자의 신원과 서비스 사용 권한을 증명해주는 *자격증명*을 콘텐츠 서비스 검증자에게 요청한다. 이때 서비스 검증자에게 전송하는 정보는 사용자 DID, 업로드할 콘텐츠의 메타 정보(fig 8, content meta info), 사용자의 비밀키로 콘텐츠 파일의 메타정보를 서명하여 만든 서명값 및 이를 복호화하여 신원 인증 시 필요한 사용자 DID 문서에서의 공개키 아이디이다. 데이터의 무결성 검증을 위해, 콘텐츠 해시 값에 대한 사용자 서명이 콘텐츠 메타정보에 포함되어있다.

2. 사용자로부터 자격증명 발급 요청을 받으면 검증자 서버는 사용자 DID를 이용하여 LDAP 스토리지에서 해당 사용자가 있는지 확인한 뒤 BCON Auth 과정을 통해 사용자의 신원을 확인한다. 신원이 인증되면 사용자에게 자격증명을(Fig. 8, credential) 발급한다. 자격증명의 구조에는 그림 8과 같이 사용자가 자격증명을 받기 위하여 검증자에게 보내온 모든 정보(fig 8, credential user part), 자격증명을 발급하는 검증자의 DID, 자격증명의 유효성을 콘텐츠 보관 서비스에서 검증하기 위한 검증자의 공개키 아이디, 검증자의 접근 위치, 콘텐츠 보관 서비스의 접근 위치, 사용자의 서비스 권한, 자격증명의 발급 시간과 유효시간 그리고 위의 모든 정보를 검증자의 공개키와 대칭되는 비밀키로 서명하여 만든 자격증명 서명이 있다.

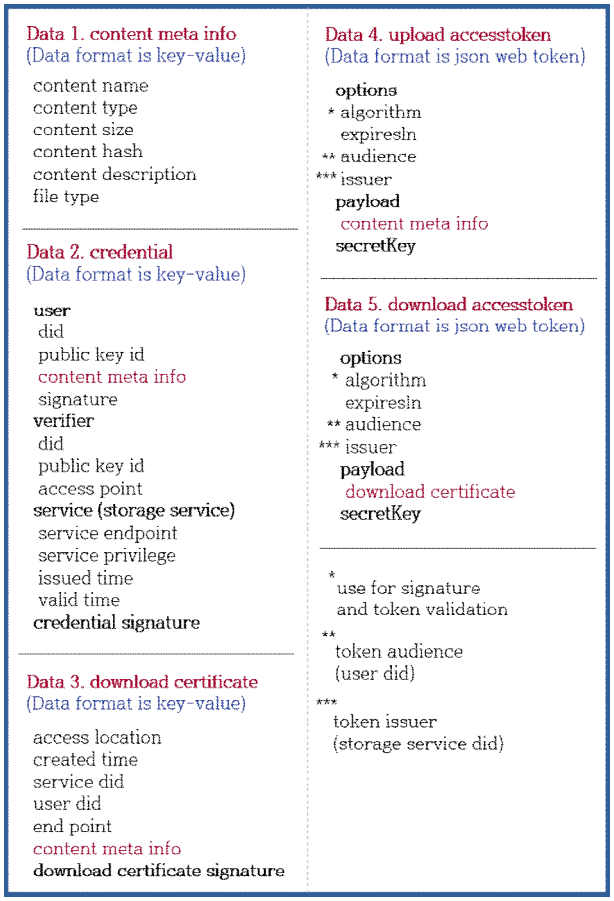

Fig. 8. Structure of Data

[step(3) in fig. 5] 본 단계는 발급받은 자격증명으로 콘텐츠 보관 서비스에게 콘텐츠 업로드를 위한 액세스 토큰을 요청하고, 콘텐츠 보관 서비스는 BCON Auth 과정으로 사용자의 신원을 확인 후 액세스 토큰을 발급하는 것으로서 세부 내용은 다음과 같다.

1. 사용자는 콘텐츠 업로드를 위한 권한을 요청하기 위하여 발급받은 자격증명의 콘텐츠 보관 서비스 접근 위치와 콘텐츠 서비스 사용자 앱을 통해 콘텐츠 보관 서비스에 자격증명을 보낸다. 콘텐츠 보관 서비스는 사용자로부터 받은 자격증명을 발급한 발급자의 신원이 확실하고 자격증명이 유효한지 검증하기 위하여, 자격증명의 유효시간을 검사하고 자격증명의 검증자 DID를 통해 검증자의 DID, 자격증명 내용, 검증자 DID 문서에 저장된 공개키에 대한 아이디와 자격증명 속 서명 값 그리고 자격증명의 검증자 공개키 아이디를 통해 BCON Auth 과정을 진행한다.

2. 자격증명이 유효하고 발급자의 신원이 확인되면 사

용자가 콘텐츠를 BCON 서비스에 업로드할 수 있는 권한으로 액세스 토큰(fig 8, upload accesstoken)을 생성한다. 액세스 토큰은 추가 저장소가 필요 없고, 위변조 방지를 보장하는 JWT를[15] 사용한다. 옵션(fig 8, upload accesstoken options)에는 토큰에 대한 정보를 가지는데 토큰 발급자와 토큰 대상자는 각각 콘텐츠 보관 서비스 DID와 사용자 DID로 표현된다. 페이로드(fig 8, upload accesstoken payload)는 콘텐츠 메타정보를 가진다. 비밀키(fig 8, upload accesstoken secretKey)는 헥사바이트로 256 길이의 임의의 문자열의 형태이며 액세스토큰 검증 시 필요하므로 생성 후 카산드라 데이터베이스에 저장한다. 이렇게 세 값이 사인된 형태로 액세스토큰을 사용자에게 발급한다.

[step(4) in fig. 5] 사용자는 발급받은 액세스토큰과 업로드할 콘텐츠를 FormData 객체 형태로 콘텐츠 보관 서비스에게 전달하여 업로드 요청을 한다. 콘텐츠 보관 서비스는 카산드라 데이터베이스에서 비밀키를 가져와서 사용자가 보낸 액세스토큰을 검증한다. 유효한 액세스토큰이라면 자격증명을 통해 받아온 콘텐츠 메타정보와 업로드할 콘텐츠와 자격증명을 통해 받아온 해당 콘텐츠의 메타정보를 카산드라 데이터베이스에 업로드한다. 업로드가 완료되면 사용자가 콘텐츠를 다운받을 수 있는 권한을 증명하는 *다운로드 증명서*(fig 8, download certificate)를 사용자에게 발급한다. 자격증명을 통해 얻은 콘텐츠 메타정보와 다운로드 증명서가 생성된 시간, 사용자와 콘텐츠 보관 서비스의 DID가 포함되며 이 모든 값을 콘텐츠 보관 서비스의 비밀키로 사인한 서명 값이 포함된다.

[step(5) in fig. 5] 콘텐츠 저장 서비스로부터 발행받은 다운로드 증명서는 안전하게 보관하기 위해 콘텐츠 매니지먼트 컨트랙트를 통해 클레이튼 블록체인에 저장한다. 콘텐츠 업로드가 완료되었음을 기록하기 위해 앞서 블록체인에 저장된 콘텐츠 메타정보(Fig. 7, ContentMeta) 중 Content State의 값을 Saved로 변경한다. 이 상태 값을 이용해 BCON User DApp에서 콘텐츠 저장 서비스에 업로드가 완료된 콘텐츠들의 목록(Fig. 9, Feed Page)을 불러온다.

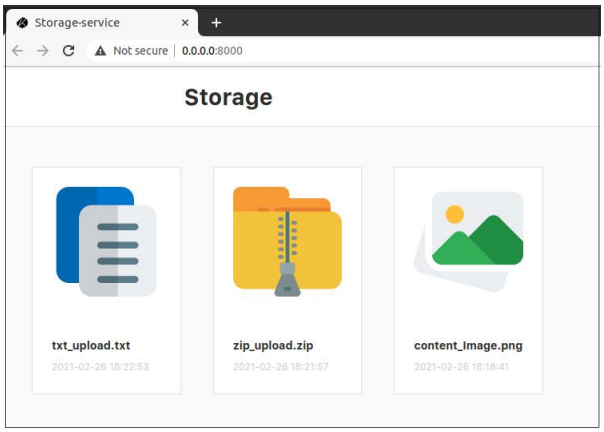

Fig. 9. BCON User DApp (Feed Page)

콘텐츠 메타정보의 Content State 값이 Saved인 콘텐츠 해시값과 일치하는 다운로드 증명서를 조회하여 업로드가 완료된 콘텐츠 목록을 BCON User DApp의 피드 화면에 그림 9와 같이 업데이트한다.

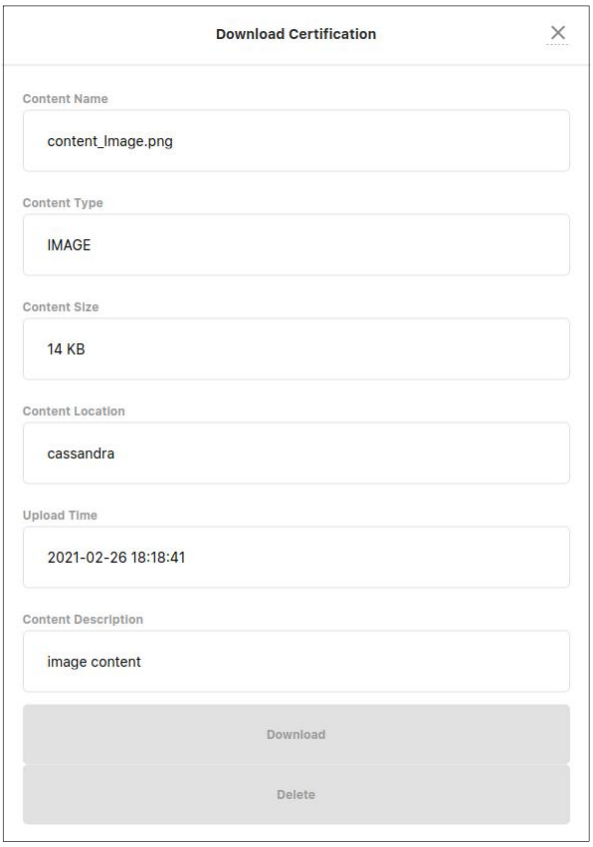

Fig. 10. Download Cert Page

그림 9의 업데이트 된 피드 화면에서 업로드가 완료된 콘텐츠의 아이콘을 클릭하면 업로드된 콘텐츠에 대해 발급받은 다운로드 증명서(Fig 10, Download Certification)를 확인할 수 있다.

4. Content Download process

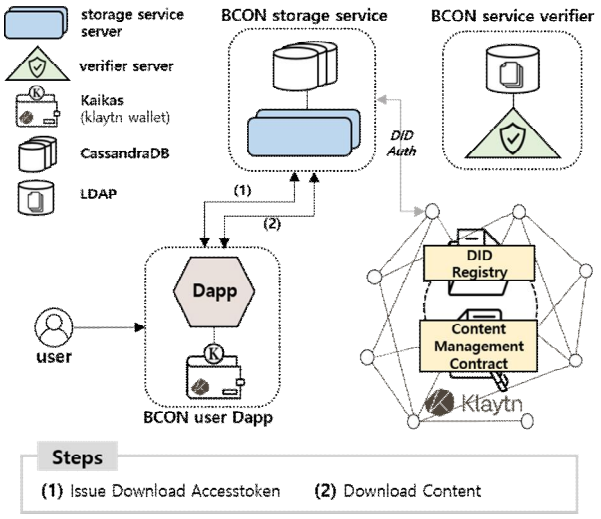

Fig. 11. Content Download Process

[step(1) in fig. 11] 본 단계는 콘텐츠 업로드 후 발급받은 다운로드 증명서를 가지고 콘텐츠 보관 서비스에 다운로드를 위한 액세스 토큰을 요청하는 과정으로 다음과 같은 순서로 진행된다.

1. 사용자가 BCON 서비스에 업로드한 자신의 콘텐츠를 다운받기 위해 업로드 시 콘텐츠 보관 서비스에게 발급받은 다운로드 증명서가 필요하다. 다운로드 증명서를 통해 콘텐츠 보관 서비스에 해당 콘텐츠에 대한 다운로드 권한을 요청(Fig. 10, Download Button)한다. 요청을 받은 콘텐츠 보관 서비스는 사용자가 보내온 다운로드 증명서가 유효한지 검증하기 위해 다운로드 증명서의 유효시간을 검사하고 서명을 제외한 다운로드 증명서에 포함된 모든 정보를 콘텐츠 보관 서비스의 비밀키로 재 서명하여 다운로드 증명서의 서명이 유효한지 검사한다.

2. 다운로드 증명서가 유효하다면 사용자가 BCON 서비스에 업로드한 자신의 콘텐츠를 다운로드할 수 있는 권한으로 액세스 토큰(fig. 8, download accesstoken)을 생성한다. 액세스 토큰을 생성한 뒤 콘텐츠 보관 서비스는 사용자가 다운로드를 위해 접근할 임시경로를 생성한다. 해당 임시경로는 헥사 바이트 형태의 중복되지 않는 랜덤한 문자열로 생성되며 다운로드가 완료되면 삭제된다. 해당 콘텐츠를 카산드라 데이터베이스에서 임시경로 안에 미리 꺼내둔다. 다운로드 준비가 완료되면 사용자에게 콘텐츠를 다운로드할 수 있는 임시경로와 함께 액세스 토큰을 발급한다.

[step(2) in fig. 11] 사용자는 발급받은 액세스 토큰과 함께 다운로드 경로로 콘텐츠 보관 서비스에 다운로드 요청을 보낸다. 이 요청을 받은 콘텐츠 보관 서비스는 액세스 토큰을 보내온 사용자가 해당 콘텐츠에 대한 권한을 가진 사람이 맞는지 BCON Auth를 통해 신원을 확인한다. 신원확인이 완료되면 콘텐츠 보관 서비스는 카산드라 데이터베이스에서 비밀키를 가져와서 사용자가 보낸 액세스 토큰을 검증하고 유효한 액세스 토큰이라면 사용자는 다운로드 경로를 통해 콘텐츠를 다운로드할 수 있다. 다운로드가 완료되면 임시경로를 삭제한다.

IV. Test

다양한 용량을 가진 콘텐츠를 어느 정도로 서비스에서 처리할 수 있는지 검증하기 위하여, BCON 서비스에 다섯 종류의 용량을 가진 콘텐츠를 용량별로 10개씩 업로드와 다운로드하는데 소요된 시간을 측정하였다. 그림 12는 콘텐츠 보관 서비스의 환경을 나타내며 전체적인 아키텍처는 그림 3과 같다. BCON 콘텐츠 보관 서비스 및 콘텐츠 서비스 검증자는 Intel i7-8700 6코어 PC의 Ubuntu 20.04 운영체제 하에서 동작하며, 카산드라 분산 데이터베이스는 세 개의 VM노드에서 실행된다. 콘텐츠 서비스 사용자 앱은 같은 환경에서 Node 10.16.0 버전에서 실행된다. 콘텐츠 매니지먼트 컨트랙트는 클레이튼 노드에서 동작하는 솔리디티 0.5.6 버전으로 개발되었으며 클레이튼 테스트넷인 Baobab에 배포되어 실행된다.

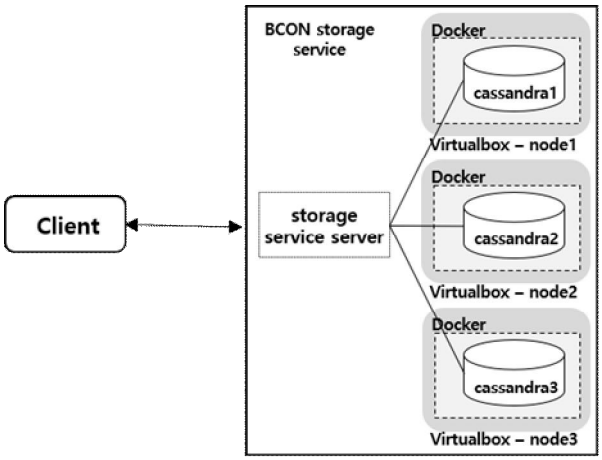

Fig. 12. Test Environment for BCON Storage Service

스토리지 서비스는 1개의 서버와 3개의 카산드라 데이터베이스 노드로 구성된다. 사용자가 요청을 보내면 3개의 노드에 데이터를 분산 복제 저장하여 데이터의 가용성 및 견고성을 높인다.

(1) 사용자는 각 콘텐츠 용량 당 10번의 업로드 또는 다운로드 요청을 BCON 서비스에게 보낸다.

(2) 사용자 요청을 받은 BCON 서비스는 콘텐츠 업로드 또는 다운로드를 위한 인증 과정을(§3.3, 3.4) 거치게 된다.

(3) 인증이 완료되면 스토리지 서버는 클러스터링 되어 있는 3개의 카산드라 데이터베이스 중 1개에 콘텐츠 파일 업로드 또는 다운로드를 진행한다.

(4) 업로드 또는 다운로드가 완료되면 사용자에게 다운로드 증명서 또는 콘텐츠로 응답하고 소요시간을 기록한다.

테스트 결과는 표1에서 업로드 테스트와 다운로드 테스트로 구별되어 제공된다.

Table 1. Test Result

	average upload(s)	average download(s)
500MB	55.55	48.11
100MB	21.30	11.63
50MB	18.41	7.24
10MB	13.76	3.70
1MB	13.41	2.91

업로드 테스트는 사용자가 업로드를 요청한 시점부터 각 인증 과정을 거쳐 콘텐츠가 카산드라 데이터베이스에 업로드된 뒤 다운로드 증명서를 받은 시점까지의 시간을 측정한다. 다운로드 테스트는 사용자가 다운로드를 요청한 시점부터 카산드라 데이터베이스에서 콘텐츠를 가져온 후 사용자가 콘텐츠를 브라우저를 통해 다운로드를 받은 시점까지의 시간을 측정한다. 업로드 테스트 결과에서 10MB까지는 용량에 따라 업로드 시간이 크게 달라지지 않으며 50MB부터 용량에 따른 소요 시간의 차이가 발생한다. 다운로드 테스트 결과에서도 마찬가지로 10MB까지는 용량에 따라 다운로드 시간이 크게 달라지지 않으며 50MB부터 용량에 따른 소요 시간의 차이가 있고, 500MB부터는 시간 차이가 크게 발생한다. 테스트 결과를 통해 BCON 서비스는 체계적인 인증 과정을 거쳐 콘텐츠를 안전하게 업로드와 다운로드를 할 수 있으며, 모든 과정을 진행하는데 필요한 시간 또한 적절하여 서비스 실용화에 문제가 없음을 보여준다.

V. Conclusions

본 논문에서는 개인이 자신의 신원을 인증하여 자신의 콘텐츠를 안전하게 보관하며, 콘텐츠에 대한 자신의 소유권을 신뢰성 있게 보장받을 수 있는 서비스인 BCON에 대해서 소개하였다. BCON 서비스는 콘텐츠 서비스 검증자, 콘텐츠 서비스 사용자 앱, 콘텐츠 매니지먼트 컨트랙트, 콘텐츠 서비스 사용자 앱으로 구성되어 있으며, 대용량 콘텐츠 저장을 위해 카산드라 데이터베이스를 연동하여 사용한다. BCON 서비스는 DID 기법을 사용하여 사용자가 서비스에 필요한 정보만 선택적으로 제공하여 사용자 인증이 이루어지고, 액세스 토큰을 통해 체계적으로 콘텐츠에 대한 사용자의 접근 권한을 제어한다. 이를 통하여 콘텐츠 제작자의 결과물을 안전하고 신뢰성 있게 보관할 수 있으며 소유권 또한 확실하게 보장받을 수 있다는 장점이 있다. 앞으로 BCON 서비스를 이용한 콘텐츠 경매 서비스 등 콘텐츠 소유권 및 거래의 투명성이 절대적으로 요구되는 다양한 서비스를 개발할 예정이다.

ACKNOWLEDGEMENT

This research was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(No. 2019R1I1A3A01052970)

REFERENCES

[1] Korea copyright commision,, https://www.copyright.or.kr/kcc/tmis/information/notice/view.do?pageIndex=1&brdctsno=45009&portalcode=&brdclasscode=&nationcode=&searchText=&servicecode=05&searchTarget=ALL&brdctsstatecode=&pageIndex=1

[2] Korea copyright commision, https://www.copyright.or.kr/information-materials/trend/the-copyright/download.do?brdctsno=43147&brdctsfileno=14329

[3] Mediachain, https://github.com/mediachain

[4] D.S. Kwon, et al. "Digital Identity Trend for Digital Trust Society", Electronic communication trend analysis, v.34 no.3, pp.114-124, June. 2019. DOI: 10.22648/ETRI.2019.J.340312

[5] DID Alliance, https://www.didalliance.or.kr/

[6] Drummond Reed, Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/

[7] KISA, https://www.kisa.or.kr/main.jsp

[8] Ground X, https://www.klaytn.com

[9] R. Saltini, "IBFT Liveness Analysis," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 245-252, July. 2019. DOI: 10.1109/Blockchain.2019.00039.

[10] D. Mohanty, "Ethereum Use Case," Ethereum for Architects and

Developers, pp. 203-243, 2018. DOI: 10.1007/978-1-4842-4075-5_9.

[11] N. R, A. B. S and R. Kumar P, "Users Sync Authentication using External Ldap in Organizations," 2020 IEEE International Conference for Innovation in Technology (INOCON), pp. 1-4, Nov. 2020. DOI: 10.1109/INOCON50539.2020.9298432.

[12] A. Demers, et al. "Epidemic algorithms for replicated database maintenanc," In Proc. 6th ACM Symp. on Principles of Distributed Computing, pp. 1−12, Jan, 1987, DOI:10.1145/41840.41841

[13] Netlify, React Redux, https://react-redux.js.org

[14] Klaytn, Kaikas Docs, https://docs.kaikas.io

[15] Introduction to JSON Web Tokens, https://jwt.io/introduction

Authors

Hye-Won Kim received the B.S degrees in IT convergence from University of Ulsan, Korea, in 2021. She is currently an M.S student in Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan. She is interested in blockchain technology, distributed computing, and Artificial Intelligence technology.

Young-Eun Lee received the B.S degrees in IT convergence from University of Ulsan, Korea, in 2021. She is currently an M.S student in Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan. She is interested in blockchain technology, distributed computing, and Artificial Intelligence technology.

Min-Ho Kwon received the B.S/B.A degrees in IT convergence/Economics from University of Ulsan, Korea, in 2020. He is currently an M.S student in Dept. of Electrical/Electronic and Computer Engineering, University of Ulsan. He is interested in blockchain technology, distributed computing, and cloud computing.

Myung-Joon Lee received the B.S. degree in Mathematics from Seoul National University in 1980, and the M.S. and Ph.D. degrees in Computer Science from KAIST in 1982 and 1991, respectively.

Dr. Lee joined the faculty of the Department of Computer Science at University of Ulsan, Ulsan, Korea, in 1982. He is currently a Professor in the School of IT Convergence, University of Ulsan. He is interested in blockchain technology, distributed computing, and mobile/cloud service.