산업융합연구 제20권 제9호 pp. 47-58, 2022
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2022.20.9.047

저작권자의 주권 강화를 위한 DID 기반 검증 프로토콜 설계

김호윤[1], 신승수[2*]
[1]동명대학교 컴퓨터미디어공학과 학생, [2]동명대학교 정보보호학과 교수

Design of DID-based Verification Protocol for Strengthening Copyright Holders' Sovereignty

Ho-Yoon Kim[1], Seung-Soo Shin[2*]
[1]Student, Dept. of Computers & Media Engineering, Tongmyong University
[2]Professor, Dept. of Information Security, Tongmyong University

요 약 디지털 콘텐츠는 그 특성상 원본과 복제본의 구분이 어렵다. 이 때문에 블록체인 기술을 활용한 NFT 기술은 디지털 콘텐츠 원본에 대한 증빙과 희소성을 보장할 수 있어 주목받고 있다. 그러나 NFT 구매자는 디지털 콘텐츠에 대한 저작권을 가지는 것이 아닌 소유권을 가지는 것이다. 특히 NFT를 발행하는 민팅(Minting) 과정은 누구나 가능하기 때문에 저작권자에 대한 저작권 위협이 있다. 본 연구에서는 저작권자의 디지털 콘텐츠에 대한 저작권 보호를 위해 NFT를 발행하고 거래하는 과정을 DID에 기반 한 검증 프로토콜을 제안한다. 연구 방법으로는 디지털 콘텐츠에 관한 연구 사례의 문제점을 분석하여 안전성에 대해 비교 분석하였다. NFT 발행은 DID를 통해 신원인증이 완료된 저작권자만이 발행할 수 있고 사용자 또한 인증이 완료된 자만 거래에 참여하여 디지털 콘텐츠에 대한 무분별한 도용, 이용을 방지하고 안전하고 투명한 거래 시장을 형성할 수 있다.

키워드 : 탈중앙화 신원증명, 대체 불가 토큰, 저작권, 디지털 콘텐츠, 검증 프로토콜

Abstract Digital content is difficult to distinguish between the original and the replica due to its nature. For this reason, NFT technology using blockchain technology is attracting attention because it can guarantee the proof and scarcity of the original digital content. However, the NFT buyer does not own the copyright to the digital content, but the ownership. In particular, since the minting process of issuing NFTs is possible for anyone, there is a copyright threat to the copyright holder. In this study, we propose a verification protocol based on DID for the process of issuing and transacting NFTs for copyright protection of copyright holders' digital contents. As a research method, the problems of research cases related to digital contents were analyzed and the safety was comparatively analyzed. NFT issuance can only be issued by copyright holders whose identity has been verified through DID, and only users who have completed authentication can participate in the transaction to prevent indiscriminate theft and use of digital content and form a safe and transparent transaction market.

Key Words : Decentralized Identifier, NFT, Copyright, Digital Content, Verification Protocol

1. 서론

저작권은 창작자 자신이 만든 창작물에 대한 법적 권리로써 저작물을 보호한다. 온라인상에서 디지털 콘텐츠 제작과 유통이 활발해짐에 따라 불법 복제 및 보안 위협이 증가하고 있고, 이는 저작권자의 저작권을 위협하며 주권 강화가 필요한 대목이다. 보안을 강화하기 위해 블록체인이 주목받고 있으며, 거래의 투명성과 무결성을 보장할 수 있어 연구가 활발하게 진행되고 있다.

This research was supported by the BB21plus funded by Busan Metropolitan City and Busan Institute for Talent & Lifelong Education(BIT).
*Corresponding Author : Seung-Soo Shin(shinss@tu.ac.kr)
Received June 23, 2022 Revised July 25, 2022
Accepted September 20, 2022 Published September 28, 2022

특히, 블록체인 기술을 활용한 NFT(Non-Fungible Token)는 고유 소유권을 보장할 수 있어 주목받고 있다. NFT는 디지털 콘텐츠에 대한 희소성 보장과 원본성 증빙이 가능하고, 소유자 정보와 거래 이력 등 위·변조가 불가능하여 NFT 형태로 거래되는 경우가 많다. 이 때문에 저작권이 다양한 디지털 콘텐츠 분야에서 NFT는 활용성이 높게 평가되어 시장 규모가 커지고 이용자 또한 증가하고 있다[1].

그러나 NFT 구매자는 디지털 콘텐츠에 대한 저작권을 갖는 것이 아니고, 소유권과 저작권은 분리된 개념이다. 디지털 콘텐츠 소유자라 하더라도 판매 등의 목적으로 전시하거나 활용하면 저작권법상 저작권을 침해할 수 있다. NFT를 구매하여 디지털 콘텐츠에 대한 소유권을 확보했다 하더라도 저작권은 창작자 및 저작권자가 가지고 있기 때문에 디지털 콘텐츠에 대한 복제, 전송 등을 원하면 저작권자의 허락이 필요하다. NFT 구매자는 스마트 계약 조건에 저작물 이용 허락, 저작권 양도가 명시되어 있지 않은 한 저작자 유리한 해석의 원칙에 따라 디지털 콘텐츠 복제, 전송 등을 할 수 없다.

디지털 콘텐츠를 NFT로 만드는 것 또한 디지털 콘텐츠에 대한 권한을 가진 저작권 보유자여야 한다. 저작권자의 권한이 없는 타인이 디지털 콘텐츠를 NFT 형태로 민팅하는 경우 디지털화하는 과정과 마켓플레이스에 업로드 하는 과정 등에서 저작권자의 복제 또는 전송권을 침해하게 된다[2,3]. 디지털 콘텐츠는 누구나 복제가 가능하기 때문에 NFT 기술에서 문제점으로 저작권자, 창작자에 상관없이 디지털 콘텐츠를 NFT로 민팅 할 수 있고, 원본 자산의 소실 가능성이 있다. NFT에 대한 문제점을 해결하기 위해 NFT 마켓 플레이스에서는 창작물에 대한 창작자를 검증하고, 소유권 분쟁 시 법적으로 해결해야 하고, 원본 자산의 소실 가능성을 해결해야 한다.

블록체인 네트워크의 성능 저하를 방지하기 위해 디지털 콘텐츠의 원본 파일은 블록체인 네트워크에 저장하는 대신 파일이 업로드된 Off-Chain 링크로 대체한다. Off-Chain을 안전하지 않은 서버로 이용하게 될 경우 해킹 및 관리 소홀로 인해 디지털 콘텐츠의 원본 파일이 삭제될 가능성이 있기 때문에 IPFS (Inter-Planetary File System)를 이용한 탈중앙화 저장 플랫폼이 대두되고 있다[4].

본 논문에서는 누구나 디지털 콘텐츠를 민팅하여 NFT 발행이 가능하다는 문제점 해결과 저작권자의 주권을 강화하기 위해서 DID에 기반 한 NFT를 발행 함으로써 디지털 콘텐츠 거래의 안전성과 신뢰성을 높일 수 있는 DID 기반 검증 프로토콜을 제안한다.

2. 관련 연구

본 장에서는 디지털 콘텐츠에 대한 관련 기술을 알아보고 기존 시스템에 대한 문제점을 분석한다.

2.1 디지털 콘텐츠

디지털 콘텐츠는 음악, 영상, 이미지 등을 디지털 방식으로 제작한 데이터 또는 정보를 의미한다. 디지털 콘텐츠의 보호기술은 디지털 문서 식별자(DOI : Digital Object Identifier), 디지털 저작권 관리(DRM : Digital Right Management), Watermarking 등이 있다.

DOI 시스템은 1998년 국제 DOI 재단에 의해 시작되었고, ISO 26324를 통해 국제 표준으로 채택되었다. DOI는 인터넷에서 찾을 수 있는 객체의 위치와 그 객체에 관한 정보를 포함하는 객체의 현재 정보에 대한 해석이 가능하고 네트워크 링크를 제공하기 위해 영구적으로 객체에 할당된다. 객체에 대한 정보는 시간이 지남에 따라 변경될 수 있지만, 그 DOI 이름은 변경되지 않는다[5].

DRM은 저작권자를 보호하기 위해 저작권자가 배포한 디지털 콘텐츠의 사용을 제어하고 제한하기 위한 기술 및 시스템이다. 사용자는 사용조건에 따라 디지털 콘텐츠를 이용해야 하며 사용 권한이 수행되어야 하는 핵심 조건과 제한 요소를 포함한다[6].

Watermarking 기술은 사진이나 동영상 등과 같은 디지털 콘텐츠에 저작권자의 비밀 정보를 삽입하여 관리하는 기술이다. 디지털 콘텐츠 원본의 출처 및 정보의 추적이 가능하며 저작권 보호, 불법 복제 및 복사 방지, 사용자 제어 등의 기능이 있다[7].

2.2 DID

탈중앙화 신원증명(DID: Decentralized Identifier)은 분산원장기술을 기반 한 신원증명기술이다[8]. DID는 주체에 대한 식별자의 역할과 동시에 분

산저장소에 저장된 DID document를 참조하는 URI(Uniform Resource Identifier) 역할을 갖고 있다[9]. DID는 분산 시스템으로 기존 중앙 집중적인 시스템에서 사용자의 정보와 데이터를 완전히 통제하지 못했던 것을 사용자에게 완전한 통제권을 갖도록 한다. 사용자가 분산저장소에 연동되어있는 디지털지갑에 사용자 자신의 정보를 담아 필요할 때마다 사용자만이 가지고 있는 개인키를 입력해 자신을 증명하는 방식이다[10].

DID는 자기주권 신원증명(SSI: Self-Sovereign Identity)을 가능하게 하는 기술이다. 자기주권 신원증명은 탈중앙화 시스템을 기반으로 사용자가 직접 자신의 ID를 관리하고, 데이터의 주권을 ID 주체에게 부여한다. 자기주권 신원증명 플랫폼은 DID, DID document, 분산저장소(Verifiable Data Registry), 발행인(Issuer), 사용자(Holder), 검증인(Verifier)이 있다. 그리고 사용자가 보관하는 ID 속성으로 검증 가능한 자격증명(VC: Verifiable Credential), 사용자가 VC를 재가공하여 검증인에게 제출하기 위한 ID 속성으로 검증 가능한 제공 ID 데이터 집합(VP: Verifiable Presentation)이 있다[11].

2.3 NFT

NFT는 분산원장기술(DLT: Distributed Ledger Technology)을 이용하여 이미지, 영상, 게임 아이템 등 디지털 형태의 자산에 대한 권리를 표상하는 일종의 암호화 수단으로서의 디지털 토큰이다. NFT는 비트코인과 같은 암호화폐처럼 대체할 수 있는 것이 아닌 대체 불가능한 유일한 토큰으로 디지털 자산의 소유권과 진정성을 증명할 수 있다[12].

NFT는 표준안을 가지는 블록체인을 이용하여 만들고 거래되는데, 이 중 이더리움의 ERC-721 표준안이 가장 많이 이용된다. ERC-721 표준으로 스마트 컨트랙트를 구현할 수 있으며 NFT를 발행할 뿐만 아니라 생산된 토큰을 추적할 수도 있어 유효성 확인도 가능하다[13]. NFT의 생성은 민팅하여 생성되는데 디지털 콘텐츠에 대한 메타데이터, 민팅한 사람, 민팅 일시 등이 기록되고 이후 거래가 발생하게 되면 거래정보 등이 기록된다[14].

NFT의 거래는 민팅된 NFT를 마켓플레이스에 업로드하여 거래하는데, 마켓플레이스는 최대 규모인 OpenSea를 가장 많이 이용하고 있다. NFT를 구매하면 구매자는 디지털 콘텐츠에 대한 소유권이 부여되고, 세부 내용은 스마트 컨트랙트에 따라 결정된다.

2.4 IPFS

IPFS는 데이터를 분산형으로 저장하고 공유하기 위한 파일 시스템이다. 데이터의 해시값을 이용하여 전 세계 컴퓨터에 분산 저장되어있는 디지털 콘텐츠를 찾아서 가져오기 때문에 속도가 빠르다. IPFS의 디지털 콘텐츠는 git의 버전 모델, 암호화 해시, 머클 트리의 개념을 채택한 자체 기술 데이터 유형인 멀티 해시를 사용하여 고유한 이름과 주소를 지정한다[15]. IPFS는 스토리지 용량 제한이 없으며 높은 처리량을 제공한다. 데이터 추출 시 모든 노드의 데이터 블록을 병렬로 처리하여 읽기 및 쓰기 성능이 우수하다.

디지털 콘텐츠 원본 자체를 블록체인 메인 네트워크에 직접 올리게 되면 성능 저하와 비용이 많이 발생하기 때문에 Off-Chain에 저장하는 것이 효율적이다. IPFS에 디지털 콘텐츠를 저장하는 방식은 NFT 자체에 디지털 콘텐츠가 포함되는 것이 아닌 IPFS 링크를 NFT에 포함한다[16]. IPFS는 분산 시스템으로 모든 노드를 공격하는 것이 불가능하여 DDoS 및 DRDoS 공격으로부터 안전하다[17]. IPFS의 시스템은 Fig. 1과 같다.

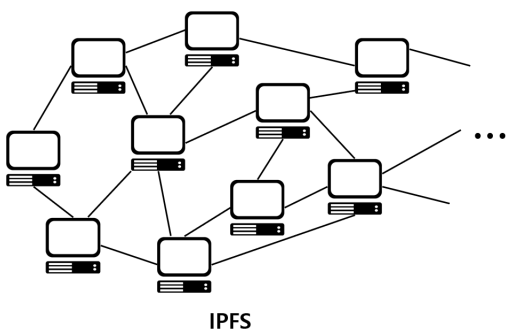

Fig. 1. IPFS System

2.5 디지털 콘텐츠 연구 사례

본 절에서는 기존 디지털 콘텐츠 연구 사례에 대해 분석한다. Jang[18]은 블록체인 기술을 기반 한 디지털 콘텐츠 인증 및 관리 기술을 연구하였다. 디지털 콘텐츠 창작자가 디지털 콘텐츠를 유통 및 관리시스템에 의해 등록되고 관리되며 사용자에게 전달한다. 저작권 등록 관리시스템, 디지털 콘텐츠 유통 관리시스템, 사용자 권한 및 인증을 위한 시스템으로 구성된다. 저작물 등

록은 등록자의 신분을 확인하고 구분하여 저작권을 설정한다. 저작물 자체 정보를 인증 정보로 활용하기 위해 해시값을 생성하여 등록한다. 해시 값을 이용하여 디지털 콘텐츠와 사용자를 인증함으로써 무결성을 제공한다. 그러나 디지털 콘텐츠에 대한 자체 보호를 기술영역에만 집중되어 있고 유통관리 영역은 미흡하다.

Jeon[19] 등은 블록체인을 이용한 모바일 DRM 기반 인증 메커니즘을 설계하였다. 제안 시스템은 Fig. 2와 같고, 시스템 내부는 DRM Server와 Client로 분리되며 디지털 콘텐츠 창작자가 등록한 디지털 콘텐츠를 암호화하는 Packager, 데이터를 저장하고 암호화 및 Right를 발행하는 Rights Issuer, 디지털 콘텐츠를 Server에서 다운로드, WAP Push Message를 이용하여 Rights Issuer로부터 콘텐츠의 권한을 전달받는 Client로 구성된다.

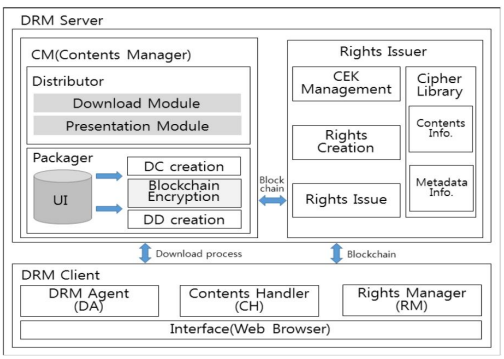

Fig. 2. Mobile DRM-Based Authentication Mechanism Using Blockchain System

Mobile DRM 디지털 콘텐츠 보호 방식 중에서 Separate Deliver 기법을 응용하여 디지털 콘텐츠를 암호화하고 휴대전화 번호 또는 PDA 시리얼 번호, 메타데이터 정보 등을 통하여 DRM 콘텐츠의 인증 권한을 향상시킨다. 그리고 Client 인증을 위해 블록체인을 이용하여 디지털 콘텐츠를 보호한다.

Son[20] 등은 블록체인 기반 자기 주권 콘텐츠 관리 시스템을 제안하였다. 제안 시스템은 Fig. 3과 같으며 자기 주권 콘텐츠 관리 기능을 제공하고, 콘텐츠가 특정 서버나 서비스에 종속되지 않고 사용자가 원하면 언제든지 콘텐츠를 등록, 제공, 접근제어, 그리고 삭제할 수 있다. 중앙 서버를 사용하지 않고 콘텐츠 자체의 종속성을 해결하기 위하여 분산저장소를 이용한다. 블록체인에 기반 한 콘텐츠에 대한 소유권 인증, 접근제어, 사용 이력의 무결성을 제공한다. 콘텐츠에 대한 등록과 관리는 이더리움을 기반 한 스마트 컨트랙트를 이용하고 원본 콘텐츠를 저장하기 위한 분산저장소는 IPFS를 이용한다. 그러나 논문에서는 사용자가 직접 콘텐츠를 등록, 관리, 제어하지만 사용자 등록 시 인증 과정이 없으며 콘텐츠에 대한 사전 검증이 없다. 특히 콘텐츠 저장 시 암호화 과정이 없어 분산 저장하여도 기밀성에 취약하다.

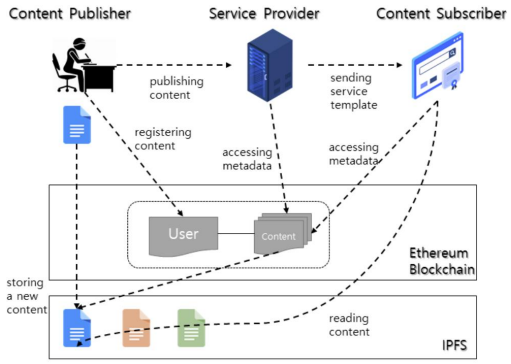

Fig. 3. Blockchain-based Self-Sovereignty Content Management System

Shin[21] 등은 콘텐츠의 안전한 유통을 위한 안드로이드 폰에 기반 한 보안 시스템을 제안하였다. 제안한 시스템은 저작권자, 사용자, 배포권자, 서버로 이루어지며 사용자 단말기의 USIM, IMEI를 이용하여 사용자를 인증한다. 사용자 인증 과정에서 사용자 고유번호와 해시값을 이용하여 서버를 통해 인증 및 무결성을 검증하고 SMS와 난수 값을 이용하여 인증 과정을 거치기 때문에 재전송 공격을 방지한다. 디지털 콘텐츠는 암호화하여 서버에 저장하기 때문에 기밀성을 강화하였고 사용자는 세션키를 발급받아 콘텐츠를 복호화한 후 이용한다. 그러나 중앙 집중형식의 서버를 이용하여 네트워크 장애 시 가용성에 문제가 있으며, 악의적인 내부자 공격에 취약하다. 특히 배포권자라는 제3 자의 개입이 있어 수수료 비용의 증가가 있다.

3. 디지털 콘텐츠 검증 프로토콜

디지털 콘텐츠에 대한 NFT 발행은 저작권자의 권한 없이 무단으로 발급하는 것이 가능하다. 이를 방지하기 위해 디지털 콘텐츠 검증 프로토콜을 제안한다.

3.1 시스템 구성

시스템의 구성요소는 발행기관, 저작권자, 사용자, 분산저장소, IPFS로 이루어진다. 발행기관은 저작권자와 사용자를 인증하고, 디지털 콘텐츠를 검증한다. 검증이 완료된 디지털 콘텐츠에 대해 NFT를 발행하여 분산저장소에 저장하고, 암호화된 디지털 콘텐츠의 원본은 IPFS에 저장한다. 저작권자는 발행기관으로부터 본인인증과 디지털 콘텐츠 검증을 받는다. 그리고 디지털 콘텐츠를 발행기관에게 전송하고 NFT를 발급받은 뒤 사용자와 디지털 콘텐츠 이용에 대한 거래를 진행한다.

사용자는 디지털 콘텐츠 이용을 위해 저작권자에게 일정한 금액을 지불한 뒤 이용을 요청한다. 이용 요청을 하면 저작권자로부터 전송받은 NFT는 분산저장소를 통해 검증하고, 검증이 완료되면 저작권자로부터 마스터키를 발급받는다. 사용자는 발급받은 마스터키로 IPFS에 저장되어있는 암호화된 디지털 콘텐츠의 원본을 불러와 복호화한 뒤 이용한다.

분산저장소는 구성원들의 DID, DID document, NFT를 등록하고 검증한다. IPFS는 디지털 콘텐츠의 원본을 저장한다. 디지털 콘텐츠는 대게 용량이 크기 때문에 블록체인의 메인 네트워크에 저장하는 것은 비효율적이므로 IPFS와 같은 Off-Chain에 저장한다. 시스템 구성요소의 각 역할은 Fig. 4와 같다.

3.2 검증 프로토콜

검증 프로토콜은 발행기관, 저작권자, 그리고 사용자의 등록 및 이용을 위한 신원인증 과정, 저작권자의 디지털 콘텐츠 검증 및 등록 과정, 사용자의 디지털 콘텐츠 요청, 검증, 그리고 이용 과정으로 진행한다. 검증 프로토콜에서 사용되는 시스템 파라미터는 Table 1과 같다.

Table 1. Notations

Notation	Description
DID_U	DID value of member
DID $document_U$	DID document value of member
Cha_U	Challenge value of DID Auth
Res_U	Response value of DID Auth
MK	Master key value
RN_U	A one-time pseudo random number
pub_U	DID document's public key value
pri_U	Owner's private key value

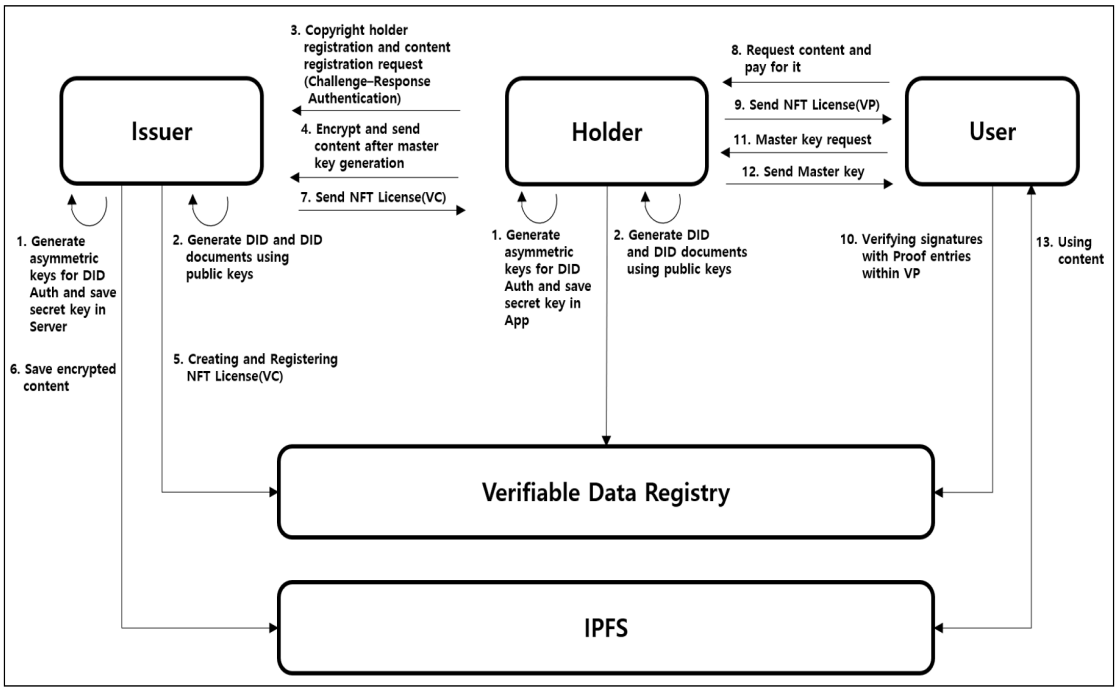

Fig. 4. Proposed Model Scenario

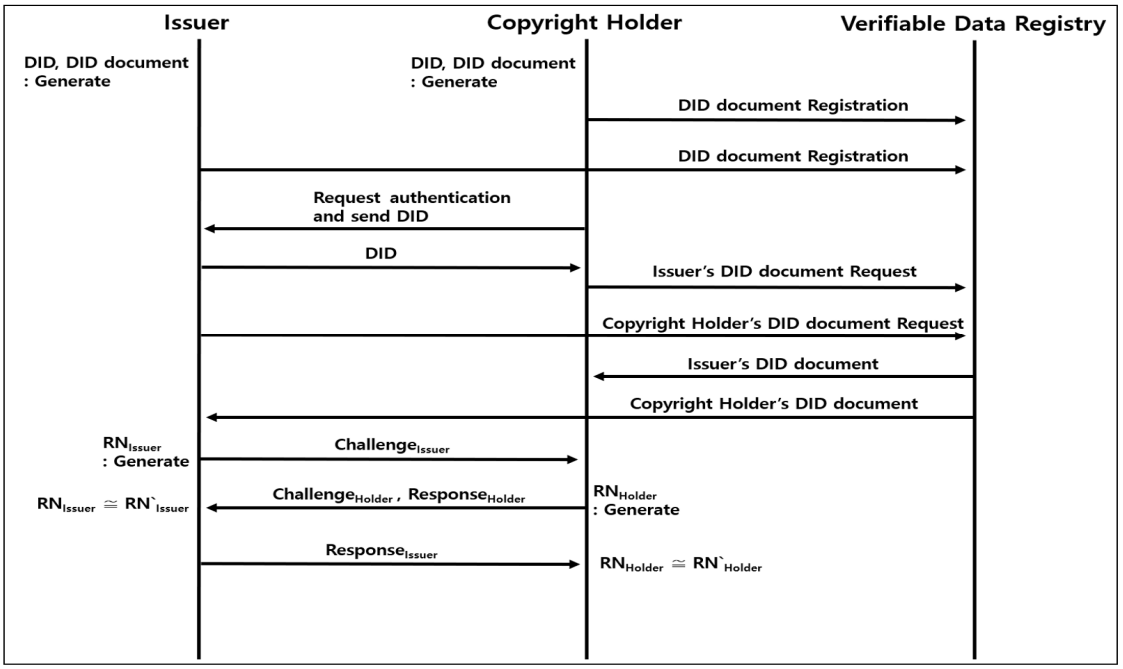

Fig. 5. Identity Authentication

3.2.1 신원인증

발행기관, 저작권자, 그리고 사용자는 디지털 콘텐츠 등록 및 이용을 위해서 신원인증이 필요하다. 신원인증 과정은 동일하기 때문에 저작권자의 신원인증 과정만 기술한다. 발행기관, 저작권자는 신원인증에 필요한 DID 및 DID document를 생성한 후 분산저장소에 등록한다. 저작권자는 신원인증을 위해 발행기관에게 DID를 전송하며 인증을 요청한다. 발행기관은 난수를 이용하여 Challenge를 생성하고 저작권자에게 전송한다.

저작권자 역시 난수를 이용하여 Challenge를 생성하고, Challenge에 해당하는 Response를 생성하여 발행기관에게 전송한다. 발행기관은 자신이 생성한 난수와 비교하여 일치하면 Response를 저작권자에게 전송하고 저작권자 역시 Response를 검증하여 상호 인증한다. 신원인증 과정은 Fig. 5와 같으며 자세한 과정은 아래와 같이 진행된다.

① DID, DID document를 생성한 후 분산저장소 저장: 발행기관, 저작권자는 DID_{Issuer}, DID_{Holder}, DID $document_{Issuer}$, DID $document_{Holder}$를 생성한 후 분산저장소에 저장한다.

② 신원인증 요청: 저작권자는 발행기관에게 신원인증을 요청하고 DID_{Holder}를 전송한다.

③ 신원인증 응답: 발행기관은 신원인증의 응답으로 발행기관의 DID_{Issuer}를 저작권자에게 전송한다.

④ DID document 요청 및 획득: 발행기관과 저작권자는 DID를 이용하여 분산저장소에 등록된 발행기관, 저작권자의 DID document를 요청하고, 분산저장소는 해당하는 DID document를 발행기관, 저작권자에게 전송한다.

⑤ 난수값 생성: 발행기관과 저작권자는 상호 인증 과정인 DID Auth를 위해 RN_{Issuer}, RN_{Holder}를 생성한다.

⑥ 발행기관의 Challenge 생성: 발행기관은 저작권자의 DID $document_{Holder}$에서 publicKey 항목 중 저작권자의 pub_{Holder}값을 가져와 Cha_{Issuer}=(RN_{Issuer}, pub_{Holder})을 저작권자에게 전송한다.

⑦ 저작권자의 Challenge 및 Response 생성: 저작권자는 발행기관으로부터 수신한 Cha_{Issuer}를 이용하여 $RN`_{Issuer}$=($Cha_{Issuer}$, $pri_{Holder}$)을 계산한다. 저작권자는 발행기관의 DID $document_{Issuer}$에서 publicKey 항목 중 발행기관의 $pub_{Issuer}$값을 가져와 $Cha_{Holder}$=($RN_{Holder}$, $pub_{Issuer}$), $Res_{Holder}$=($RN`_{Issuer}$, pri_{Holder})을 발행기관에게 전송한다.

⑧ 발행기관의 Response 생성: 발행기관은 저작권자로부터 Cha_{Holder}, Res_{Holder}을 수신한다. 발행기관은 $RN`_{Issuer}$=($Res_{Holder}$, $pub_{Holder}$)을 계산한 후 $RN_{Issuer} \cong RN`_{Issuer}$을 검증한다. 이후 $RN`_{Holder}$=($Cha_{Holder}$, $pri_{Issuer}$)을 이용하여 $Res_{Issuer}$=($RN`_{Holder}$, pri_{Issuer})를 생성한 후 Res_{Issuer}는 저작권자에게 전송한다.

⑨ 상호인증 완료: 저작권자는 발행기관으로부터 수신한 Res_{Issuer}를 이용하여 $RN`_{Holder}$=($Res_{Issuer}$, $pub_{Issuer}$)를 계산한 후 $RN_{Holder} \cong RN`_{Holder}$로 상호인증 한다.

3.2.2 디지털 콘텐츠 검증 및 등록

저작권자는 마스터키(MK: Master Key)에 해당하는 16자리 난수값을 생성한 후 디지털 콘텐츠를 Rijndael 암호 알고리즘으로 암호화한다. 디지털 콘텐츠 원본에 SHA-2를 이용하여 해시값을 생성한 후 생성된 해시값은 저작권자의 개인키로 암호화한다. 마스터키는 발행기관의 공개키로 암호화 후 암호화된 디지털 콘텐츠, 암호화된 해시값, 암호화된 마스터키를 발행기관에게 전송한다. 발행기관은 저작권자로부터 받은 암호화된 마스터키를 발행기관의 개인키로 복호화하여 마스터키를 획득한다. 획득한 마스터키를 이용하여 암호화된 디지털 콘텐츠를 복호화한 다음 SHA-2를 이용하여 해시값을 생성한다. 또한 암호화된 해시값을 저작권자의 공개키로 복호화해 해시값을 획득한다.

저작권자가 보낸 해시값과 발행기관이 생성한 해시값을 비교하여 디지털 콘텐츠의 무결성을 검증한 후 발행기관은 디지털 콘텐츠에 대한 NFT License (VC)를 생성하여 분산저장소에 등록하고, 암호화된 디지털 콘텐츠의 원본은 IPFS에 저장한다. 그리고 생성한 NFT License(VC)는 저작권자에게 전송한다. 디지털 콘텐츠 검증 및 등록의 과정은 Fig. 6과 같으며 자세한 과정은 아래와 같이 진행된다.

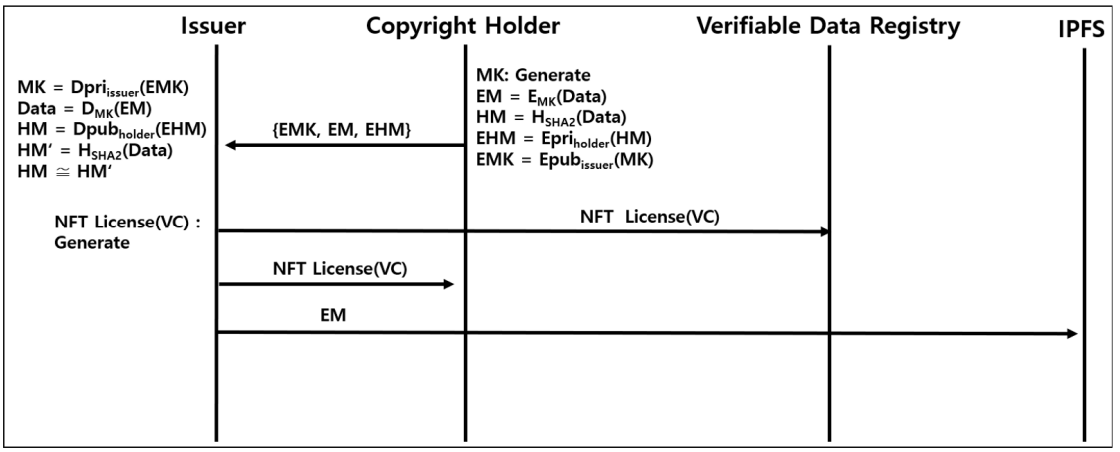

Fig. 6. Verification and Registration of Digital Content

① 마스터키 생성: 저작권자는 MK에 해당하는 16자리 난수값 생성한다.

② 암호화 콘텐츠 생성: 저작권자는 디지털 콘텐츠를 암호화하기 위해 Rijndael 암호 알고리즘과 마스터키를 이용하여 E(M)=E_{MK}(Data)를 생성한다.

③ 콘텐츠 해시값 생성: 저작권자는 디지털 콘텐츠 원본에 SHA-2를 이용하여 H(M)=H_{SHA2}(Data) 생성한다.

④ 암호화된 해시값 생성: 저작권자는 HM에 자신의 개인키를 이용하여 E(HM)=$Epri_{Holder}$(HM)을 생성한다.

⑤ 암호화된 마스터키 생성: 마스터키는 발행기관의 공개키를 이용하여 E(MK)=$Epub_{Issuer}$(MK)를 생성한다.

⑥ 암호화된 데이터 전송: 저작권자는 암호화한 {EMK, EM, EHM}을 발행기관에게 전송한다.

⑦ 발행기관의 마스터키 획득: 발행기관은 개인키를 이용하여 MK=$Dpri_{Issuer}$(EMK)을 획득한다.

⑧ 발행기관의 콘텐츠 획득: 발행기관은 획득한 MK를 이용하여 Data=D_{MK}(EM)을 획득한다.

⑨ 발행기관의 해시값 획득: 발행기관은 저작권자의

공개키를 이용하여 $H(M)=Dpub_{Holder}(EHM)$을 계산한 후 해시값을 얻는다.

⑩ 해시값 비교: 발행기관은 획득한 콘텐츠 원본에 대해 $H(M`)=H_{SHA2}(Data)$을 생성하여 $H(M)\cong H(M`)$을 비교하여 콘텐츠에 대한 무결성을 검증한다.

⑪ NFT License(VC) 생성: 발행기관은 콘텐츠 원본을 민팅하여 NFT License(VC)를 생성한다.

⑫ 발행기관은 생성한 NFT License(VC)를 분산저장소에 등록한다.

⑬ 발행기관은 암호화한 콘텐츠 원본 EM을 IPFS에 저장하고, NFT License(VC)는 저작권자에게 전송한다.

3.2.3 디지털 콘텐츠 요청, 검증, 이용

사용자는 저작권자에게 디지털 콘텐츠 이용을 요청하고 정해진 금액을 지불한다. 저작권자는 요청받은 디지털 콘텐츠에 대한 NFT License(VP)를 사용자에게 전송한다. 사용자가 전송받은 NFT License(VP)는 분산저장소를 통해 저작권자의 디지털 콘텐츠인지 검증하고 완료되면 사용자는 저작권자에게 마스터키를 요청하고 저작권자는 디지털 콘텐츠에 대한 마스터키를 사용자의 공개키로 암호화하여 전송한다. 사용자는 디지털 콘텐츠가 저장된 IPFS의 링크를 통해 암호화된 디지털 콘텐츠 원본을 가져온다. 사용자는 마스터키를 이용하여 암호화된 디지털 콘텐츠를 복호화한 다음 디지털 콘텐츠를 이용한다.

거래가 완료되면 저작권자는 거래정보를 업데이트하기 위해 발행기관에게 요청한다. 발행기관은 업데이트한 NFT(매수인, 매도인, 매매 일시, 매매 금액 등)를 분산저장소에 등록한다. 업데이트된 NFT는 저작권자에게 전송하고 거래 과정을 종료한다. 디지털 콘텐츠 요청, 검증, 그리고 이용 과정은 Fig. 7과 같으며 자세한 과정은 아래와 같이 진행된다.

① 거래요청: 사용자는 저작권자에게 디지털 콘텐츠 이용 요청을 한 후에 정해진 금액을 지불한다.

② NFT License(VP) 전송: 저작권자는 사용자에게 NFT License(VP) 제출을 위해 VC를 VP 형태로 가공한 다음 전송한다.

③ 사용자 NFT 검증: 사용자는 분산저장소를 이용하여 VP내에 있는 proof 값을 이용하여 저작권자의 NFT인지 검증한다.

④ 마스터키 요청: 사용자는 NFT 검증이 완료되면 저작권자에게 마스터키(MK)를 요청한다.

⑤ 마스터키 전송: 저작권자는 사용자의 공개키를 이용하여 $E(MK)=Epub_{User}(MK)$를 생성한 후 사용자에게 전송한다.

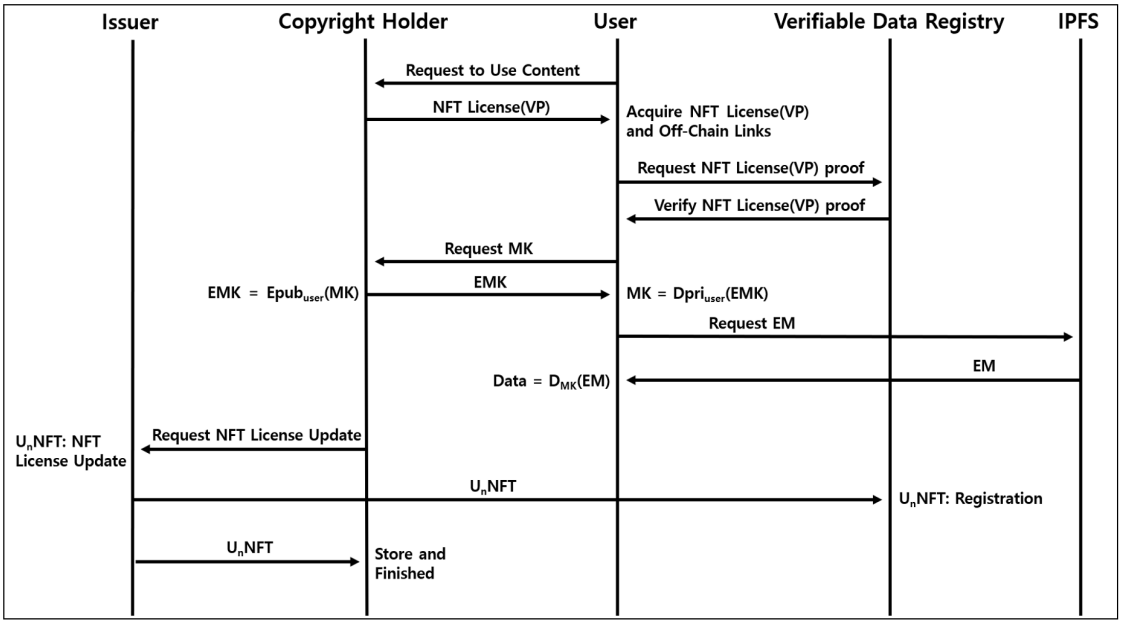

Fig. 7. Request, Verification and Use of Digital Content

⑥ 사용자 마스터키 획득: 사용자는 개인키를 이용하여 $MK=Dpri_{User}(EMK)$를 획득한다.
⑦ 암호화된 디지털 콘텐츠 요청: 사용자는 VP내에 저장된 off-chain Link를 이용하여 IPFS의 저장된 EM을 요청하여 획득한다.
⑧ 디지털 콘텐츠 이용: 사용자는 $Data=D_{MK}(EM)$를 계산하여 디지털 콘텐츠를 획득한 후 이용한다.
⑨ 저작권자는 거래 완료 후 거래 내역과 함께 발행기관에게 NFT 업데이트를 요청한다.
⑩ 발행기관은 NFT를 업데이트한 후 $U_{1.1}$NFT를 생성하여 분산저장소에 등록한다.
⑪ 업데이트된 $U_{1.1}$NFT는 저작권자에게 전송한 후 거래를 종료한다.

4. 분석

본 장에서는 DID 기반 디지털 콘텐츠 검증 프로토콜을 DID 표준 보안 요구사항에 따라 안전성 및 효율성에 대해 분석한다.

4.1 안전성 분석

DID 기반 디지털 콘텐츠 검증 프로토콜에 대한 무결성, 기밀성, 가용성, 인증, 부인방지에 대하여 분석한다.

4.1.1 무결성

저작권자의 디지털 콘텐츠는 발행기관으로부터 검증받은 디지털 콘텐츠만 등록한다. 발행기관은 저작권자로부터 획득한 디지털 콘텐츠 원본에 대해 $H(M`)=H_{SHA2}(Data)$을 생성하여 $H(M)\cong H(M`)$을 비교하여 디지털 콘텐츠에 대한 무결성을 검증한다. 그리고 디지털 콘텐츠의 원본 해시값은 NFT 메타데이터에 기록되어 분산저장소에 저장하기 때문에 디지털 콘텐츠의 위·변조를 검증할 수 있다.

4.1.2 기밀성

저작권자는 디지털 콘텐츠의 암호화 작업 시 필요한 마스터키 MK를 생성하고, 저작권자는 MK를 이용하여 Rijndael 암호 알고리즘으로 디지털 콘텐츠를 암호화한 $E(M)=E_{MK}(Data)$를 생성하여 발행기관에게 보낸다. 중간에서 도청하여 탈취하더라도 비밀키를 알고 있는 자만이 복호화가 가능하다. 이때 비밀키는 $E(MK)=Epub_{Issuer}(MK)$와 같이 전송받는 대상의 공개키로 암호화하여 전송하고 복호화는 $MK= Dpri_{Issuer}(EMK)$와 같이 전송받는 대상자만이 가지고 있는 개인키로만 복호화가 가능하다.

4.1.3 가용성

디지털 콘텐츠에 대한 이용은 접근 권한이 있는 저작권자가 직접 NFT License(VP)와 마스터키를 사용자에게 전달하고 통제한다. NFT License(VC)는 분산저장소에 저장하고 디지털 콘텐츠 원본은 IPFS에 저장하여 네트워크의 부하를 줄이고 효율성을 개선한다. 분산저장소와 IPFS는 분산 시스템으로 모든 노드를 공격하는 것이 불가능하기 때문에 DDoS 및 DRDoS 공격으로부터 안전하다.

4.1.4 인증

구성원들의 인증은 DID Auth를 수행하여 인증한다. DID Auth는 PKI 기반 Challenge-Response Auth를 이용하고, 임의의 난수 RN_{Issuer}, RN_{Holder}를 생성하여 인증한다. 인증 시 매번 다른 값의 난수를 생성하여 Challenge-Response를 수행하기 때문에 재전송 공격으로부터 안전하다. 공개키로 생성한 Challenge에 대한 응답 값 Response는 소유자만이 가지고 있는 개인키로만 생성할 수 있어 중간에서 Challenge 값을 탈취하더라도 공격자는 Response 값을 만들어 내지 못하므로 중간자 공격으로부터 안전하다.

4.1.5 부인방지

디지털 콘텐츠 원본의 해시값을 발행기관에게 전송할 때 저작권자만이 가지고 있는 개인키로 해시값을 암호화하여 전송하기 때문에 저작권자의 공개키로만 복호화가 가능하다. 이는 저작권자만이 가지고 있는 개인키로 암호화하여 전송하기 때문에 부인방지가 가능하다.

4.1.6 저작권 침해성

분산저장소에 등록된 NFT License(VC)에는 디지털 콘텐츠 원본에 대한 해시값과 저작권자의 인증 정보 등이 기록되어 있어 디지털 콘텐츠에 대한 원본 검증이 가능하고, 불법적인 배포·유통으로 인한 저작권 침해로부터 보호받을 수 있다.

4.2 효율성 분석

Son[20] 등은 블록체인 기반 자기 주권 콘텐츠 관리 시스템을 제안하여 자기 주권 콘텐츠 관리 기능을 제공

하고, 콘텐츠가 특정 서버나 서비스에 종속되지 않고 사용자가 원하면 언제든지 콘텐츠의 등록, 제공, 접근제어 및 삭제가 가능하게 한다. 중앙 집중형식의 SPoF(Single Point of Failure)문제점을 해결하고 신뢰기관(TTP) 없이 시스템의 신뢰성을 확보한다. 또한, 블록체인을 기반한 디지털 콘텐츠에 대한 사용자의 무결성을 제공한다. 특히 디지털 콘텐츠는 분산저장소인 IPFS을 이용하여 접근성을 용이하게 한다. 그러나 일반 사용자가 디지털 콘텐츠를 발행하는 역할과 구독하는 역할 모두 할 수 있다. 사용자 등록 시 인증 과정이 없어 검증되지 않은 디지털 콘텐츠를 발행할 수 있다는 문제점이 있고, 디지털 콘텐츠에 자체에 대한 검증 또한 없다. 특히 디지털 콘텐츠를 저장할 때 암호화하지 않고 저장하기 때문에 기밀성에 문제점이 있다. 이는 악의적인 사용자로 인해 저작권자의 저작권 침해가 가능하다.

Shin[21] 등은 콘텐츠의 안전한 유통을 위한 안드로이드 폰에 기반 한 보안 시스템을 제안하였다. 사용자 단말기의 USIM, IMEI를 이용하고, 인증 과정에서 사용자 고유번호와 해시값을 이용하여 서버를 통해 인증 및 무결성을 검증한다. SMS와 난수 값을 이용하여 인증 과정을 거치기 때문에 재전송 공격을 방지할 수 있다. 디지털 콘텐츠는 암호화하여 서버에 저장하기 때문에 기밀성을 강화하였고 사용자는 세션키를 발급받아 디지털 콘텐츠를 복호화한 후 이용한다. 그러나 중앙 집중형식의 서버를 이용하여 네트워크 장애 시 가용성에 문제가 있으며, 악의적인 내부자 공격에 취약하다. 또한, 배포권자라는 제3자의 개입으로 수수료 비용의 증가가 있다.

본 논문에서 제안하는 검증 프로토콜은 DID를 이용하여 인증 과정을 거치기 때문에 인증된 저작권자만이 디지털 콘텐츠를 등록한다. 디지털 콘텐츠는 발행기관으로부터 해시값을 이용하여 무결성을 검증받고 디지털 콘텐츠의 원본 해시값, 저작권자의 인증 정보 등의 메타데이터가 기록된 NFT를 발행한다. 디지털 콘텐츠를 이용하는 사용자 또한 인증 과정을 거친 사용자만이 이용하고 분산저장소를 이용하여 디지털 콘텐츠에 대한 NFT를 검증한다.

IPFS의 해시 링크를 포함한 NFT는 분산저장소에 저장하고 네트워크의 부하를 줄이기 위해 디지털 콘텐츠의 원본은 IPFS에 저장하여 효율성을 개선한다. 디지털 콘텐츠를 이용하기 위해 제안하는 검증 프로토콜을 이용하여 거래하면 배포권자, 유통업자 등 제3 자의 개입 없이 저작권자와 사용자가 직접 거래하기 때문에 수수료 비용 절감 효과가 있고, 안전하고 투명한 거래를 할 수 있다. Son[20], Shin[21]과 제안 프로토콜의 비교는 Table 2와 같다.

Table 2. A comparison between the existing system and the proposed protocols

Classification	Son[20]	Shin[21]	Proposal
User Authentication	X	O	O
Verification of digital content	X	O	O
Confidentiality	X	O	O
Integrity	O	O	O
Availability	O	X	O
Distributed system	O	X	O
Transaction fee	Lowness	Height	Lowness

5. 결론

디지털 콘텐츠는 배포와 이용이 편리하고 쉬운 만큼 원본과 복사본의 구별이 불가능하다. 저작자의 노력에도 불구하고 무단으로 복사하거나 도용할 시, 저작자는 의욕이 감소할 뿐만 아니라 디지털 콘텐츠 시장의 위협을 초래한다. 특히, NFT는 디지털 콘텐츠에 대한 저작권자의 권한 없이 누구나 무단으로 민팅하여 발급할 수 있고 배포, 소유하는 등의 문제점이 있다. 본 논문에서는 이를 해결하기 위해 DID를 기반으로 하여 인증된 저작권자만이 디지털 콘텐츠에 대한 NFT를 발행하게 하고 배포하게 함으로써 저작권자의 주권을 강화하였다. 특히 디지털 콘텐츠는 데이터 용량이 크기 때문에 디지털 콘텐츠 자체를 블록체인 메인 네트워크에 올려 저장하게 되면 네트워크 부하를 초래할 수 있어 Off-Chain인 IPFS를 이용하고, NFT 자체에는 IPFS의 해시 링크를 포함하여 효율성을 높였다. NFT의 시장이 커지는 만큼 저작권자의 저작권 보호를 강화해야 하며, 안전하고 투명한 거래를 위해 제안 프로토콜이 활용될 수 있다.

향후 연구로는 디지털 콘텐츠 종류에 따른 저작권자를 분류 및 검색하고, 효율적으로 접근하여 이용할 수 있는 플랫폼 구축이 필요하다.

REFERENCES

[1] D. H. Kim, H. J. Song, W. J. Zhang, H. J. Jo, Y. H. Choi & J. Y. Hyun. (2022). NFT, Shouts Original in the Digital World. *Architectural institute of korea, 66(3),* 83-86.

[2] Y. S. Park. (2021). *Copyright in the NFT Digital Art Market.* Business, Law & Technology. Available online: https://blt.kr/news/

[3] H. D. Lee. (2021). *NFT legal status, hot potato...On the surface of the copyright debate.* Electronic Times Internet. Available online: https://m.etnews.com/

[4] E. K. Jeon, S. H. Oh, D. H. Son, S. H. Lee, H. Y. Yoo & K. S. Lim. (2022). Effects of Game Changer NFT on Metabuses. *The Journal of The Korean Institute of Communication Sciences, 39(2),* 57-63.

[5] Korea DOI Center. Available online: https://www.doi.or.kr/wordpress/about_doi/

[6] J. O. Jeon & B. M. Seo. (2021). Design and implementation of improved authentication mechanism base on mobile DRM using blockchain. *Journal of Digital Convergence, 19(4),* 133-139. DOI : 10.14400/JDC.2021.19.4.133

[7] S. M. Jung. (2020). Image watermarking technique applying multiple encryption techniques. *The Journal of Korea Institute of Information, Electronics, and Communication Technology, 13(6),* 503-510.

[8] W3C Decentralized Identifiers (DIDs) v1.0. (2021). *DID.* Available online: https://www.w3.org/TR/did-core/

[9] G. H. Kim. (2021). A Design of Self-sovereign Data Distribution Platform for a Reliable Data Economy. *Journal of Digital Contents Society, 22(3),* 483-490. DOI : 10.9728/dcs.2021.22.3.483

[10] H. Y. Kim, K. H. Han & S. S. Shin. (2021). A Model for Self-Authentication Based on Decentralized Identifier. *Journal of Convergence for Information Technology, 11(11),* 66-74. DOI : 10.22156/CS4SMB.2021.11.11.066

[11] W3C Verifiable Credentials Data Model v1.1. (2022). *W3C.* Available online: https://www.w3.org/TR/vc-data-model/

[12] A. Mekacher, A. Bracci, M. Nadini, M. Martino, L. Alessandretti, L. M. Aiello & A. Baronchelli. (2022). *How rarity shapes the NFT market.* arXiv. DOI : 10.48550/arXiv.2204.10243

[13] D. Piyadigama. & G. Poravi. (2022). *An Analysis of the Features Considerable for NFT Recommendations.* arXiv. DOI : 10.48550/arXiv.2205.00456

[14] D. H. Kim, H. J. Song, W. J. Zhang, H. J. Jo, Y. H. Choi & J. Y. Hyun. (2022). NFT, Shouts Original in the Digital World. *Review of Architecture and Building Science, 66(3),* 83-86.

[15] T. V. Doan, Y. Psaras, J. Ott. & V. Bajpai. (2022). *Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Considerations.* arXiv. DOI : 10.48550/arXiv.2202.06315

[16] J. Y. Kim. (2021). *If I buy NFT, will I have the copyright on digital content?.* Hankyung economy. Available online: https://www.hankyung.com/economy/article

[17] H. Lin, X. Li, H. Gao, J. Li & Y. S. Wang. (2022). ISC-MTI: *An IPFS and smart contract-based framework for machine learning model training and invocation.* Multimedia Tools and Applications.

[18] E. G. Jang. (2021). Digital Content Certification and Management Technology Based on Blockchain Technology. *Journal of The Korea Society of Computer and Information, 26(11),* 121-128. DOI : 10.9708/jksci.2021.26.11.121

[19] J. O. Jeon & B. M. Seo. (2021). Design and implementation of improved authentication mechanism base on mobile DRM using blockchain. *Journal of Digital Convergence, 19(4),* 133-139. DOI : 10.14400/JDC.2021.19.4.133

[20] M. S. Son & H. Y. Kim. (2021). A Self Sovereign Contents Management System based on Blockchain. *The transactions of The Korean Institute of Electrical Engineers, 70(5),* 784-790.

[21] S. S. Shin & Y. Y. Kim. (2012). A Study on Multi-Media Contents Security Using Android Phone for Safety Distribution. *Journal of Digital Convergence, 10(6),* 231-239.

김 호 윤(Ho-Yoon Kim) [학생회원]

· 2021년 2월 : 동명대학교 정보보호학과(공학사)
· 2021년 3월~현재 : 동명대학교 컴퓨터미디어공학과 석사과정

· 관심분야 : Blockchain, DID, 암호 프로토콜, IoT
· E-Mail : miask376@gmail.com

신 승 수(Seung-Soo Shin) [정회원]

· 2001년 2월 : 충북대학교 수학과(이학박사)
· 2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)
· 2005년 3월~현재 : 동명대학교 정보보호학과 교수

· 관심분야 : 암호프로토콜, Blockchain, DID, IoT, 데이터분석
· E-Mail : shinss@tu.ac.kr