JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 11, pp. 121-128, November 2021
https://doi.org/10.9708/jksci.2021.26.11.121

Digital Content Certification and Management Technology Based on Blockchain Technology

Eun-Gyeom Jang*

*Professer, Dept. of Software Convergence, Jangan University, Hwaseong, Korea

[Abstract]

After entering the 4th Industrial Revolution, the digital content market, which was only dependent on existing contents supply enterprises, is providing various digital content through the participation of users like YouTube. Accordingly, it activated the digital content market, but it causes a negative influence on the digital content market due to the copyright of the creator and the indiscriminate illegal use and usage of the content. This study researched digital content management technology based on blockchain technology to protect digital content and the copyright of the creator. The suggested technology protects the digital content and the copyright holder and discerns the users and prevents the indiscriminate approach and illegal use of digital content. For the safe management of digital content, hash function applied as the certification technology of blockchain is used to certify the users and manage the digital content and provide integrity and authentication service.

▸ **Key words**: Block Chain, Authentication, Integrity, Access Control, Digital Contents

[요 약]

4차 산업혁명시대에 접어들면서 기존의 콘텐츠 제공 업체에만 의존했던 디지털콘텐츠 시장이 유투브와 같이 사용자의 참여로 다양한 디지털콘텐츠를 제공하고 있다. 이로 인해 디지털콘텐츠 시장의 활성화를 가져왔지만, 저작자의 저작권과 콘텐츠의 무분별한 도용 및 사용으로 디지털콘텐츠 시장에 악영향을 미치고 있다.

본 논문은 디지털콘텐츠를 보호하고 저작자의 저작권을 보호하기 위해 블록체인 기술을 기반으로 디지털콘텐츠 관리 기술을 연구하였다. 제안 기술은 디지털콘텐츠와 저작권자를 보호하고 사용자를 식별하여 무분별한 디지털콘텐츠 접근과 도용을 방지한다. 디지털콘텐츠의 안전한 관리를 위해 블록체인의 인증기술로 활용되는 해쉬 함수를 활용하여 사용자를 인증하고 디지털콘텐츠를 관리하여 무결성과 인증 서비스를 제공한다.

▸ **주제어**: 블록 체인, 인증, 무결성, 접근제어, 디지털콘텐츠

• First Author: Eun-Gyeom Jang, Corresponding Author: Eun-Gyeom Jang
*Eun-Gyeom Jang (jangeg@jangan.ac.kr), Dept. of Software Convergence, Jangan University
• Received: 2021. 10. 07, Revised: 2021. 11. 02, Accepted: 2021. 11. 03.

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

I. Introduction

디지털콘텐츠는 유·무선 전기통신망에서 부호, 영상, 이미지, 음향 등을 디지털 방식으로 제작하여 유통, 제어하는 자료 또는 정보를 의미한다. 이러한 디지털 정보 매체는 단순한 자료 및 정보 문서, 음향과 영상 등의 콘텐츠 개체, 시스템에서 기능을 제공하는 소프트웨어 등의 여러 유형의 매체로 존재한다.

디지털콘텐츠는 누구나 접근하고 활용할 수 있는 콘텐츠, 활용영역에 따른 접근성, 가공성을 제공하기도 하며 저작자의 권리를 보호하기 위한 보호 기법을 활용하여 저작자의 권익을 보호하기도 한다. 디지털콘텐츠의 지적재산권을 보호하기 위한 기법으로 워터마크를 활용한 기법과 인가된 사용자만 접근할 수 있는 접근통제 및 암호화 기법이 대표적이다.

미국의 디지털 밀레니엄 저작권법(Digital Millennium Copyright Act)은 WIPO(세계 지식 재산 기구 : World Intellectual Property Organization) 저작권조약의 규정을 많은 부분 입법화하고이고, 유럽연합(EU)는 2001년 5월에 정보사회에서의 저작권 및 저작인접권의 특정분야의 통일에 관한 지침을 통해 WIPO 저작권조약을 비준 및 가입에 대비하고 있다. 우리나라 또한 온라인디지털콘텐츠산업발전법, 컴퓨터프로그램보호법, 저작권법으로 저작권을 보호하고 있다[1,2].

이러한 법안은 디지털콘텐츠에 대한 저작자의 저작권을 보호하여 지적재산권을 보호하고 디지털콘텐츠 시장을 안전성 있게 유지 및 활성화하는데 목적이 있다고 할 수 있다. 그러나 법적 보호는 디지털콘텐츠의 침해가 발생한 후에 보호하기 위한 대응 방안으로서 침해가 발생한 콘텐츠의 중요도에 따른 의미 없는 대처 방안이 될 수 있다. 예를 들어, 기업의 핵심기술의 누출의 경우, 기업의 사활이 걸린 핵심기술이라면 법적 조치의 의미가 무색할 것이다. 본 논문에서는 이러한 디지털콘텐츠의 침해 예방과 대응방안을 제시하기 위해 2장에서는 디지털콘텐츠 보호를 위한 환경과 기술에 대해 분석하고, 제안 기술은 3장에서 제시한다. 4장에서는 제시한 기술은 분석하고 5장에서는 제안 기술에 대한 결론으로 논문을 구성하였다.

II. Digital content protection and certification

1. Digital content protection

디지털콘텐츠를 보호하기 위한 기술은 로컬 영역에서의 보호 기술이 초기 디지털콘텐츠 시장에서는 활성화되었으나 네트워크 통신의 발달로 실시간 인증서비스를 통한 인증 기술이 각광을 받고 있는 추세이다. 디지털콘텐츠 보호를 위한 기술로는 워터마크, DOI(Digital Object Identifier), INDECS(Interoperability of Data in E-Commerce System), DRM(Digital Rights Management) 기술들이 있다[2].

디지털콘텐츠의 저작자 인증을 위한 워터마크 기술은 콘텐츠 자체에 저작자의 정보를 삽입하는 기술로서 콘텐츠 복제 및 변경시 원 저작자의 저작권을 보호하고 있다. 워터마크 기술은 콘텐츠 공급자로부터 사용자에게 디지털 콘텐츠를 제3자가 알아볼 수 없도록 암호화하는 프론트-앤드 기술과는 달리 저작권을 확증해 주는 백-앤드 기술이다. 워터마크 기술은 콘텐츠에 삽입된 워터마크가 압축이나 복제시 손상이 되지 않고 저작자 정보가 검출되어야 하고, 워터마크의 삽입으로 원 콘텐츠의 품질에 영향이 없어야 하며 저작권 보호에 적은 비용이 소비되어야 한다는 요구사항을 가지고 있다.

국제표준도서번호(ISBN:International Standard Book Number)과 같이 디지털콘텐츠에도 고유번호를 부여할 수 있는 것이 DOI이다. DOI는 디지털콘텐츠 소유 및 제공자를 비롯한 콘텐츠에 대한 정보를 포함하고 있어서 콘텐츠의 위치가 바뀌어도 쉽게 찾을 수 있도록하여 저작자를 보호하고 유통경로를 자동으로 쉽게 추적할 수 있도록 한다. DOI의 메타데이터를 활용하여 디지털콘텐츠 거래에 투명성을 제공하고, DOI 구성은 등록기관이 부여하는 코드와 콘텐츠 번호를 나타내는 코드가 결합되어 하나의 DOI 코드를 형성한다[2,3].

DOI가 미국출판협회에서 개발되었다면 INDECS는 유럽연합의 Info2000 프로젝트로 개발된 시스템이다. INDECS는 정형화된 포맷을 활용하여 콘텐츠 식별에 기반하여 메타데이터를 활용한 상호 호환성에 높은 전자상거래에 초점을 맞추고 있다.

DRM은 디지털콘텐츠의 안전한 유통을 위한 기본 환경을 구축하고 불법 복제 방지 및 인증 사용자에게만 서비스를 제공함으로써 저작자의 저작권과 콘텐츠 자체 보호를 위한 기술이다. DRM은 다양한 채널을 통해 사용자를 인증하고 콘텐츠 유료화를를 가능하게 하고 저작권 승인 관

리, 권리와 승인 처리 및 관리, 인증 환경과 서비스 인프라를 제공한다. 디지털콘텐츠 자체가 유출 및 복제되었다 하더라도 기밀성 유지를 위한 접근제어 및 보호 기술이 적용되어 안전하게 콘텐츠를 보호한다.

DOI, 워터마킹, INDECS 기술을 활용하여 디지털콘텐츠를 보호하고 있지만, 최근 콘텐츠 제공 서비스는 광범위하게 포괄적 개념으로 DRM을 적용하고 있다. 이러한 현황은 사용자의 저작권인증은 콘텐츠 자체에 침해가 발생한 이후에 대한 대응으로써 원천적 디지털콘텐츠 침해 후 대응 영역이고, DRM은 콘텐츠 자체에 대한 접근제어부터 활용 및 유통까지 관리하는 침해 방지 기술을 포함하고 있기 때문이다.

2. Certification technology

인증 기술은 콘텐츠 및 시스템 접근자에 대한 인증영역과 매체 자체 검증을 위한 인증영역으로 구분할 수 있다. 시스템 및 콘텐츠 활용을 위한 접근자의 인증은 사용자의 접근제어 정책에 의해 이루어진다. 사용자 인증 정보를 활용하여 접근을 허용하고 활용영역에 대한 권한이 부여된다. 사용자 인증은 고유 식별코드를 활용한다. 주민번호 인증, PIN(Personal Identification Number) 인증, PKI(Public Key Infrastructure) 인증, 생체인증 등의 고유 정보를 활용하여 사용자의 실체를 인증한다. Fig 1은 PKI 프로세스로서 CA(Certificate Authority)는 보안 적격 및 메시지 암호화를 위한 공개키 발급과 관리를 담당하는 기관이고 RA(Registration Authority)는 인증기관에서 인증서 발급을 수행하는 등록기관, DS(Directory System)는 생성 인증서 및 폐지 인증서 목록을 관리하는 시스템이다.

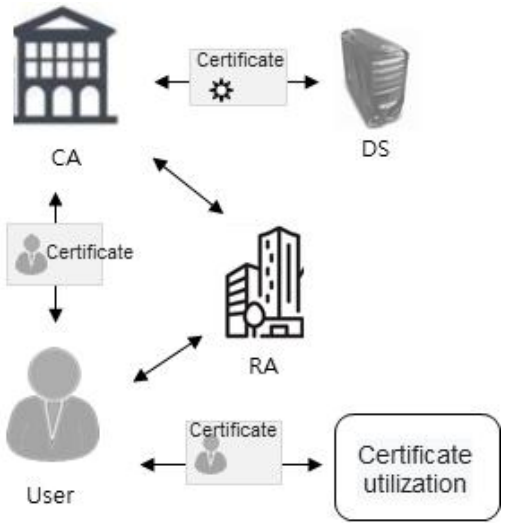


Fig. 1. PKI Process

사용자는 인증서를 발급받기 위해서는 RA에 본인 고유정보를 등록하고 인증서를 발급받을 수 있다. 이렇게 발급받은 인증서는 개인 인증을 필요로하는 업체 및 기관에 제시하여 인증을 받을 수 있다. 이렇게 제시된 인증서는 인증을 요구한 기관 및 업체에서는 DS에 인증 요청하여 사용자를 확인할 수 있다.

3. Blockchain technology

3.1 Block chain introduction

블록체인은 데이터의 변조를 방지하기 위한 기술로서 블록에 데이터를 담고 블록들을 체인 형태로 연결하는 것을 말한다. 블록체인에서 추구하는 보안 서비스는 데이터 인증 서비스로서 기존의 인증 방식과는 많은 차이를 갖는다. 기존 인증 방식의 중앙집중형을 탈중앙화하여 P2P(Peer to Peer)와 같이 개별적인 콘텐츠 관리 방식으로 서비스가 이루어진다. 탈중앙화 서비스는 기존의 중앙집중인증 방식의 프로세스 과중성과 침해시 발생하는 위험성을 감소시킨다. 대표적인 기술 적용 모델로는 가상 암호화폐인 비트코인을 들 수 있다. 비트코인은 2009년 블록체인 기술을 활용하여 가상 세계 및 실생활에서 활용할 수 있도록 기술 및 서비스를 지원하고 있다. 블록체인은 인증 기술로서 데이터를 추적할 수 서비스 기반을 갖는다. 이러한 추적 기술은 택배 추적, 농산물 원산지 추적, 부동산 거래 추적, 의료 기록 등 연계된 정보를 추적할 수 있는 서비스에 적용하여 유용하게 활용될 수 있는 기술이다. 블록체인의 다음과 같은 특성을 갖는다[4,5].

- 중개자가 개입이 필요 없다 : 제 3의 중개 기관 개입 없이도 분산파일관리 시스템을 활용하여 거래가 가능하여 추가적인 시스템 운영이 필요 없어 관리 비용이 적게 든다.
- 블록과 블록을 연결하는 체인 형태로 구성하여 새로운 인증 데이터(블록)이 발생하더라도 체인으로 연결하여 무한하게 데이터를 확장할 수 있다.
- 주요 정보(블록)은 공개되고 오직 데이터의 변경 및 오류로부터 블록을 보호하고 있다. 체인으로 블록을 연견관리하여 중간 블록의 오류를 쉽게 검증할 수 있다.
- 블록체인은 모든 정보를 동일하게 모든 사용자가 관리하여 데이터 오류 및 장애가 발생하여도 블록 전체에 영향을 미치지 않는다.
- 블록을 체인으로 연결하여 불법적으로 변경을 할 수가 없어서 정보의 신뢰성을 제공한다.

블록체인 기술 활용 대표적인 분야로 디지털 저작권 보호, 물류유통, 헬스케어, 환경분야를 들 수 있다. KodacCoin은 이미지를 효율적으로 관리할 수 있도록 사진 중심의 블록체인 기반 암호화 기술을 적용하는 방안을 적용하고 모색하고 있다. 사진 이미지 유통에 따른 과정을 기록하여 관리하고 있다. 물류 유통에서는 물류의 유통과정을 기록하여 물류의 생산부터 목적지까지의 과정을 관리하여 투명한 유통과정을 관리한다. 또한 헬스케어 영역에서도 환자의 최초 정보부터 현재까지의 정보 및 의료 과정을 관리하여 의료사고를 방지하는데 유용할 것으로 본다. 환경분야에서도 폐기물이나 기후 변화 등 과거 데이터를 활용하여 미래지향적인 모델을 설계할 수 있도록 기술을 제공할 수 있다.

3.2 Blockchain certification

(1) Blockchain type

블록체인은 공공 블록체인(Public Blockchain), 사적 블록체인(Private Blockchain), 컨소시엄 블록체인(Cons-ortium Blockchain)으로 구분할 수 있다[4,5].

공공 블록체인은 암호 화폐인 비트코인에 적용된 기술로서 탈중앙화 구조로 모든 블록을 모든 참여자가 확인할 수 있고, 거래 속도가 느린 특성을 갖는다. 또한 PoW, Pos에 의해 거래증명자가 결정되고 확장성이 없다. 대표적인 서비스로는 비트코인, 리플, 라이트코인, 이더리움과 같은 암호 화폐이다.

사적 블록체인은 폐쇄형 인프라 환경의 그룹영역에서 이루어지는 서비스로서 기존의 중앙집중식 구조를 갖는다. 탈중앙화의 공공 블록체인 환경과는 정반대의 구조로서 블록체인의 특성인 탈중앙화의 장점을 갖지 못하지만, 공공 블록체인의 단점인 거래 속도를 빠르게 하고 확장성이 용이하다는 장점을 갖는다. 대표 서비스 모델로는 Chain, Overstock, NASDAQ가 있다.

컨소시엄 블록체인은 사적 블록체인과 공공 블록체인의 중간 형태로서 여러 기관들이 모여서 하나의 서비스 군으로 연결된 형태이다. 컨소시엄 블록체인은 은행권, 금융권, 증권 등 이러한 기관들이 참여하는 형태로 볼 수 있다. 혼합형의 컨소시엄 블록체인은 빠른 거래 속도와 확장성이 용이한다는 장점은 갖는다. 대표적인 서비스로는 Citi Barclays, R3 CEV, Goldman Sashs, HSBC, BoA 등이 있다.

(2) Blockchain structure

블록체인은 블록과 블록을 체인처럼 연결하여 블록 인증 서비스를 제공한다. 블록은 고유 코드로 구분하고 콘텐츠 내용, 블록의 정보를 포함하는 헤더 정보를 갖는다. 블록의 유통 경로와 같은 정보를 관리하는 트랜젝션 정보를 포함한다. Fig 2는 블록의 구조를 나타낸다[4,6].

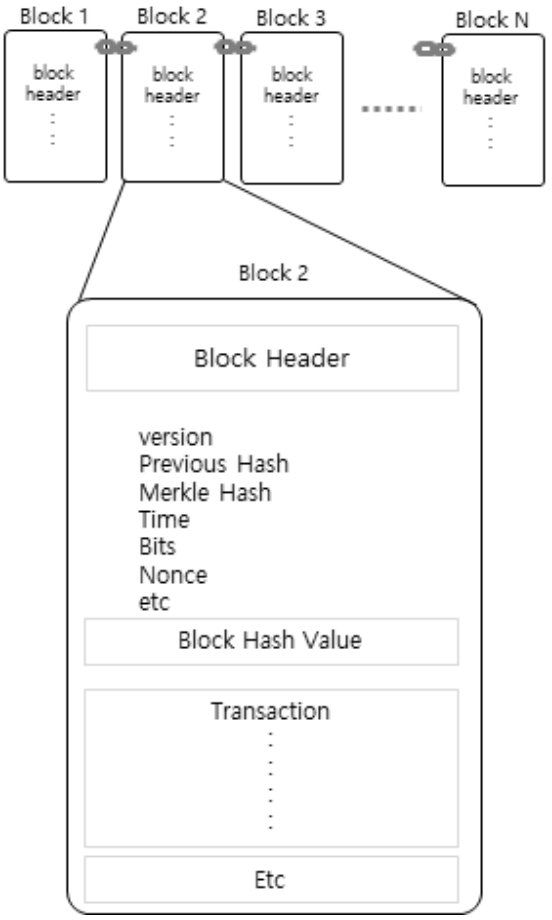


Fig. 2. Blockchain Structure

블록체인은 블록의 고유 번호(Block Number)단위로 크게 3개의 영역으로 구분할 수 있다. 첫 번째는 Block Header이다. Block Header은 블록의 전반적인 정보를 포함하고 있다[4,7,8]. 구성정보로는 프로토콜 버전(Protocol version), 소프트웨어(Software version), Merle Hash (Tree root 위치 해쉬), Bits(난이도), Time (블록 생성시간), Nonce(해쉬 검색 계산 값)가 있다. 두 번째로 Block Hash Value는 이전 블록의 해쉬값을 갖는다. 첫 번째 블록의 Bllock Hash Value는 이전 블록이 없으므로 디폴트 값을 갖는다. Transactin은 추적정보로서 예를 들어 입금과 출금 등과 같은 값을 갖는다. Etc는 기타 정보로서 해쉬값 생성에 포함되지 않는다는 특성을 갖는다. 일반적으로 안정적인 해쉬값을 유지하기 위해 SHA256을 2라운드 운영하여 32byte 크기의 해쉬값을 갖는다[8,9].

블록체인 유형 중에 블록체인의 가장 큰 특성을 갖는 것은 공공 블록체인이다. 속도는 상대적으로 느리지만 정보 인증과 무결성, 탈중앙화라는 블록체인의 특성을 모두 반영하고 있기 때문이다. 본 연구에서는 이러한 탈중앙화 기반 서비스를 제공하고 있는 공공 블록체인 기법과 DRM 보호 기술을 융합한 디지털콘텐츠 보호 기법을 제안한다.

III. Digital content protection and management techniques

3.1 System Configuration and Introduce

유통 및 보관을 위한 디지털콘텐츠 보호 시스템 구조는 그림 3과 같다. 디지털콘텐츠는 전자문서, 음악 및 영상 콘텐츠, 사진과 같은 이미지를 포함하는 디지털 제작 콘텐츠를 총칭한다. 이러한 디지털콘텐츠는 콘텐츠 생산 및 개발자에 의해 제작되어 사용자에게 전달된다. 물론 모든 콘텐츠가 유료화를 의미하지는 않는다. 단순한 개인과 개인과의 콘텐츠 전달과 처리, 유료화에 따른 유통 등 다양한 콘텐츠의 유통구조를 포함한다.

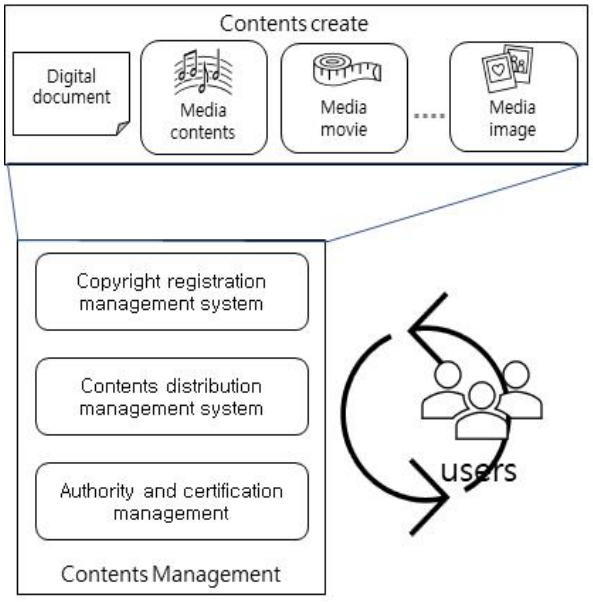


Fig. 3. System structure

제안 시스템은 콘텐츠 개발 및 생산자가 완성한 콘텐츠를 유통 및 관리시스템에 의해 등록되고 관리되어 사용자에게 전달된다. 전달된 콘텐츠 관리는 3개의 영역으로 구분되어 관리된다. 저작권 등록 관리시스템, 콘텐츠 유통관리 시스템, 사용자의 권한과 인증을 위한 시스템으로 시스템은 구성된다.

개발자의 지적 재산권 보호가 필요한 콘텐츠는 저작권 등록 관리시스템에 등록되어 관리되고 추후 저작권 분쟁 시 활용될 수 있다. 또한 콘텐츠의 접근 권한 제어를 위한 인증 시스템과 인증 여부 및 권한에 의한 유통관리 시스템으로 콘텐츠의 안전한 관리를 할 수 있다.

3.2 Digital content registration management

저작물 생산자의 지적재산권을 보호받기 위해서는 원생산자의 정보가 포함되어야 한다. 간이 문서도 저작자의 고유 정보를 포함해야 하므로 등록정보는 반드시 필요하다. 저작물 등록정보는 필수와 선택영역으로 구분되어 저작물의 특성에 따라 다르다. 표 1은 저작물 등록정보이다.

Table 1. Copyright registration information

No	Field name	Qualified	etc
1	Contents name	mandatory	
2	Version	mandatory	
3	Contents size	mandatory	
4	Hash Value	mandatory	
5	Registration date	mandatory	
6	Copyright holder	mandatory	copyright holder code
7	Registran	mandatory	
8	Hash algorism	mandatory	
9	License level	mandatory	User authority
10	Registration code	mandatory	
11	Copiable number	voluntary	
12	Copy limit	voluntary	
13	Present condition	voluntary	

디지털콘텐츠 저작물에 대한 정보는 표1과 같이 13개 항으로 등록 관리한다. 항목은 필수와 선택으로 구분하여 저작물을 관리한다. 콘텐츠 이름은 콘텐츠의 고유 식별이름이고 콘텐츠의 버전관리를 통해 각 버전별로 라이센스를 관리한다. 각 항목에 대한 설명은 다음과 같다.

- Contents name : 콘텐츠를 구분하는 고유 이름
- Version : 콘텐츠 버전
- Contents size : 원본 콘텐츠 전체 크기
- Hash Value : 콘텐츠에 대한 해쉬 코드 값
- Registration date : 등록 년월일
- Copyright holder : 자작권자명
- Registran : 등록자명
- Hash algorism : “Hash Value” 값 생성에 활용된

알고리즘, SHA256 / MD5, etc

- License level : 콘텐츠에 대한 사용자 이용 권한
- Registration code : 콘텐츠 관리를 위한 등록 코드
- Copiable number : 콘텐츠 유통시 발생하는 라이센스 카피 수
- Copy limit : 콘텐츠 카피 제한 수
- Present condition : 콘텐츠 사용 및 활용 현황

그림 4는 저작권자 및 저작물 등록자가 저작물을 등록하는 과정을 도시화 한 것이다. 저작물 등록은 등록자의 신분을 확인하고 저작물의 유형과 저작물 보호 등급을 구분하여 저작권을 설정한다. 설정된 저작물은 저작물 자체 정보를 인증정보로 활용하기 위해 해쉬 값을 생성하여 등록한다. 또한, 기존 등록된 저작물의 침해를 방지하기 위해 새로운 저작물임을 확인하고 최종 저작권자 및 저작물 인증정보를 저작물 관리시스템에 등록한다.

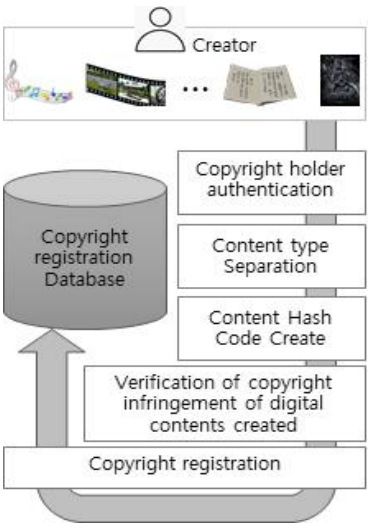


Fig. 4. Copyright registration management system

3.3 Digital content distribution management

(1) Digital content distribution overview

디지털콘텐츠 보호를 위한 시스템 구조는 그림 5와 같다. 기능 모듈 영역으로 보았을 때, 디지털콘텐츠 개발자는 지적재산권인 저작권을 보호하기 위해 저작권을 등록할 수 있다.

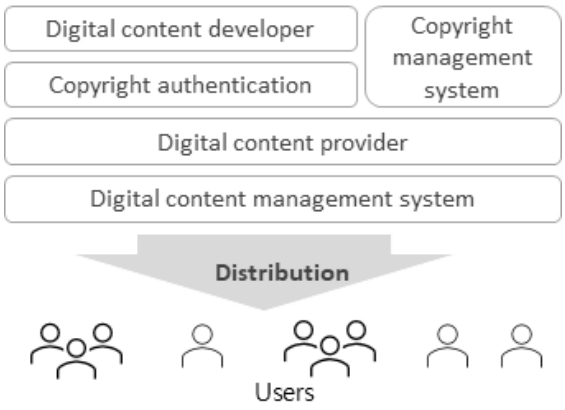


Fig. 5. Digital content distribution overview

저작권이 등록된 콘텐츠는 유통을 위해 콘텐츠 공급자에게 권한을 부여하여 사용자에게 배포할 수 있다. 저작권은 제3의 신뢰하는 공인 기관을 통해 인증되어야 한다. 등록은 기존 디지털콘텐츠의 침해가 없음의 사실성 검증과 저작자 인증 절차를 거쳐야 한다.

(2) Digital content distribution

디지털콘텐츠는 콘텐츠 자체에 대한 인증 코드값($Content_{Code}$)과 사용자에게 유포를 위한 콘텐츠 유포 코드값($User_{Code}$)을 갖는다(그림 6). $Content_{Code}$과 $User_{Code}$은 콘텐츠 관리 및 식별을 위한 코드값이다.

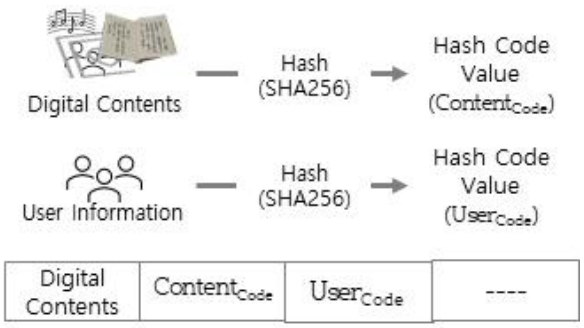


Fig. 6. Unique code Create

새롭게 생성된 디지털콘텐츠는 사용자 영역과 콘텐츠 영역으로 구분하여 관리한다. 콘텐츠 영역은 $Content_{Code}$ Block, 사용자 영역은 $User_{Code}$ Block에서 관리된다(그림 7).

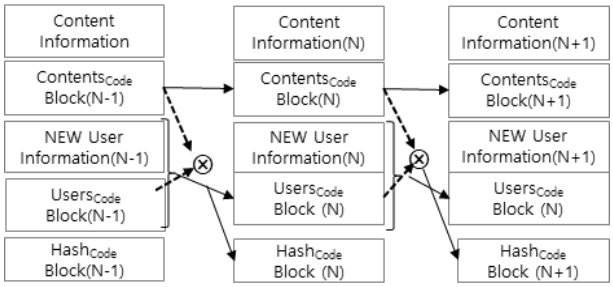


Fig. 7. Code Block

- Content Information = 콘텐츠 정보
- Content$_{Code}$ Block(N) = N 번째 콘텐츠 블록
- NEW User Information(N) : N 번째 새로운 사용자
- User$_{Code}$ Block(N) : N 번째 사용자 코드 블록
- Hash$_{Code}$ Block(N) : 유통 콘텐츠 전체 해쉬 코드 블록(Hash[Content$_{Code}$ Block⊗Use$_{rCode}$ Block])

Hash$_{Code}$(N)은 N-1 번째 사용자 코드 블록과 새로운 사용자의 정보가 해쉬 함수(SHA256)에 의해 만들어진 해쉬 값이고, 사용자가 추가될수록 Content Information에 사용자 정보가 추가된다. 유통되는 전체 콘텐츠는 User$_{code}$ Block와 Contents$_{Code}$ Block의 XOR 해쉬 값(Hash$_{Code}$ Block(N))이 저장된다.

IV. Analysis of the performance of the proposed system

제안 시스템은 디지털콘텐츠의 생성자, 저작권자, 사용자, 유통관리자 영역별로 구분하여 저작권자의 권익을 보호하고 사용자의 편의성과 접근 권한의 유연성을 분석한다.

(1) Copyright registration

생산자에 의해 생성된 디지털콘텐츠 또는 디지털콘텐츠 저작권자는 저작권을 보호받기 위해 콘텐츠 등록 시스템에 저작자의 정보를 포함한 인증 데이터를 등록한다. 등록정보로 콘텐츠 및 저작자의 기본 정보 이외에 콘텐츠 해쉬값(Content Hash Value), 해쉬 알고리즘, 사용 허용권한 정보를 포함한다. 이러한 등록정보는 RA에 등록요청을 하고 인증 및 검증된 콘텐츠에 대해서는 최종 CA 관리 서버에 등록되어 저작권을 보호받을 수 있다. 콘텐츠 해쉬 값은 콘텐츠의 불법 수정을 포함한 무결성 서비스를 제공한다. 그림 6에서와 같이 디지털콘텐츠와 사용자 정보는 SHA$_{256}$[Content] + SHA$_{256}$[User Information]와 같이 등록된다.

(2) Digital content distribution

유통되는 디지털콘텐츠는 사용자별로 사용등록 관리를 위해 콘텐츠의 인증정보를 생성한다. 콘텐츠 인증정보는 다음과 같이 생성된다.

$$Contents_{code}\,Block_{(N)} = \sum_{i=0}^{N}[\,Content\,information_{(N-1)} + Contents_{code}\,Block_{(N-1)}] + [Contentsininformation_{(N)}]$$

$$Users_{code}\,Block_{(N)} = \sum_{i=0}^{N}[\,New\,Userinformation_{(N-1)} + Users_{code}\,Block_{(N-1)}]$$

$$Hash_{code}\,Block_{(N)} = \sum_{i=0}^{N}[\,Contents_{code}\,Block_{(N-1)} \otimes Users_{code}\,Block_{(N-1)}]$$

블록 인증 정보($Contentcode\,Block_{(N)}$)은 이전 블록의 콘텐츠 정보($Contentcode\,information_{(N-1)}$)와 콘텐츠 정보($Contentcode\,Block_{(N-1)}$)의 연산으로 생성하고, 사용자 인증 블록($User_{code}\,Block_{(N)}$)은 이전의 인증블록($User_{code}\,Block_{(N-1)}$)과 추가되는 사용자의 인증정보($User_{code}\,Block_{(N)}$)가 추가되어 생성된다. 유통 자체의 콘텐츠 정보를 포함하는 $Hash_{code}\,Block$은 이전에 생성된 콘텐츠 인증 블록($Contentcode\,Block_{(N-1)}$)과 사용자 인증 블록($User_{code}\,Block_{(N-1)}$)의 XOR 연산하여 해쉬값(SHA$_{256}$)으로 변환되어 관리된다.

(3) Performance analysis and evaluation

- 디지털콘텐츠 무결성 : 배포 콘텐츠는 단계별 배포시에 이전 콘텐츠 정보와 이전콘텐츠의 해쉬 값으로 새로운 해쉬 콘텐츠 블록을 생성하여 배포된다. 이렇게 배포된 콘텐츠는 해쉬값으로 검증하여 콘텐츠의 오류 및 불법 수정시 대응할 수 있다.
- 사용자 접근성 : 배포 콘텐츠에 포함되는 사용자 정보는 이전 블록의 사용자 정보와 결합하여 해쉬값을 생성하여 관리된다. 이렇게 생성된 해쉬값에 의해 사용자를 인증한다.
- 저작권 침해 : 최종 CA에 등록된 디지털콘텐츠와 저작자 인증정보는 원본과 해쉬값으로 콘텐츠의 무결성

을 검증할 수 있다. 등록된 정보는 불법적인 접근에 의한 침해 발생시 저작권을 보호받을 수 있다.

V. Conclusions

본 논문은 디지털콘텐츠 자체에 대한 보호와 저작권을 보호하기 위해 블록체인 기법을 활용하여 유통관리 시스템을 제안하였다. 콘텐츠 보호를 위해 해쉬값을 활용하여 콘텐츠와 사용자를 인증하고 무결성 서비스를 제공하였다.

제안 시스템은 기존 유통시스템의 클라우드 인증 방식과 다운로드 인증 방식에서 같은 콘텐츠 배포에서 발생하는 문제를 보완하여 사용자별 콘텐츠 배포를 통해 사용자와 콘텐츠를 관리하여 인증 및 무결성 서비스를 제공하였다. 제안 기술은 블록체인 기술을 디지털콘텐츠 관리 기술에 적용하여 콘텐츠 및 사용자 인증에 강한 특성을 가질 수 있다. 하지만, 접근통제 영역은 미흡하다 판단한다. 이것은 제안 기술영역을 유통관리 기술영역은 배제하고 콘텐츠 자체에 대한 보호 기술영역으로 제한하였기 때문이다. 추후 유통관리 시스템과 제안 기술을 적용하여 안전한 디지털콘텐츠 유통관리 시스템을 연구할 것이다.

ACKNOWLEDGEMENT

The Work was supported by Jangan University Research Grant in 2021

REFERENCES

[1] Young-Mee Choi, “Digital Rights Management of Education Contents”, Journal of Digital Contents Society 5(3), pp. 192-198, Sep. 2004.

[2] Seok-kyu Kang, Gu Young Oh, Jung Sik Park, Byoung Moon Chin, “The Trend of Standardization for Contents Protection and Distribution”, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 889-892, Nov. 2008.

[3] Dueckyoun Cho, Seogchan Hwang, Gunho Jeong, Hyeongmin Lim, “A Digital Media Service System Supporting Multi-DRM in the Cloud”, Journal of Korea Multimedia Society 19(4), pp. 765-773, 2016.4.

[4] Eun-Gyeom Jang, “User Authentication Technology Using Multi-Blocks in the Cloud Computing Environment”, Journal of the Korea Society of Computer and Information 25(11), pp. 139-146, Apr. 2020.

[5] Ko, Yun Seung, Choi, Heung Seob, “Changing Business Paradigm and Its Application(Focused on the Block Chain Technology”, The Korean Society of Science & Art 27, pp. 13-29, Jan. 2017.

[6] HAN Ho Hyeorn, “Authentication for Blockchain Service”, Communications of the Korean Institute of Information Scientists and Engineers 38(7), pp. 19-24, Jun. 2020.

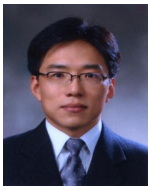
[7] Jung-Sook Kim, “The Future of BlockChain Technology Leading Innovation in the Industrial Ecosystem”, JOURNAL OF THE KOREA CONTENTS ASSOCIATION 18(6), pp. 324-332, Jun. 2018.

[8] Nakhoon Choi, Heey, “Blockchain-based Over-the-Service Copyright Protection and Management System“, The Journal of Korean Institute of Information Technology 19(9), pp. 123-132, Sep. 2021.

[9] Sae Bom Lee, Arum Park, Jae, “Blockchain Technology and Application”, Journal of the Korea Society of Computer and Information 26(2), pp. 89-97, Feb. 2021.

[10] Yeong tae Baek, Youna Min, “Study on Digital content copyright protection and transaction activation method Using block chain Ethereum”, Proceedings of the Korean Society of Computer Information Conference 26(2), pp. 73-75, Jul. 2018.

Authors



Eun-Gyeom Jang received a Ph.D in Daejeon University in 2007. Hi is currently a Professor in the Department of Software Convergence Jangan University. It has an interest in mobile communications, system security and Computer Forensics.