J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

창의적인 아이디어를 등록할 수 있는 블록체인 기반의 저작권 관리시스템

Blockchain-based Copyright Management System Capable of Registering Creative Ideas

황 정 식[1] 김 현 곤[2*]
Jung-sik Hwang Hyun-gon Kim

요 약

최근 웹툰이나 웹소설처럼 저작물로 보호되어야 할 디지털 콘텐츠들이 손쉽게 복제되어 유포되면서 불법 복제가 사회적인 이슈로 떠오르고 있다. 이와 관련하여 본 논문에서는 블록체인을 적용하여 저작물 위변조 방지, 보안성 향상, 거래 속도 향상, 비용 절감, 가시성을 향상시킬 수 있는 저작권 관리시스템을 제안하였다. 시스템은 기존과 같이 공식적으로 저작권을 등록할 수 있고 더불어 단순한 아이디어 수준의 저작물도 시스템에 등록할 수도 있다. 후자의 경우는 창작 아이디어가 떠오르면 언제든지 시스템에 등록하여 추후에 자신의 독자적인 저작물이라는 것을 증명할 수 있는 수단으로 활용할 수 있다. 시스템은 특히, 용량이 큰 콘텐츠의 경우, 트랜잭션에 콘텐츠의 해시 결과 값만을 포함시키고 원본 콘텐츠는 별도로 관리하여, 네트워크 참여 노드들이 처리해야 할 데이터의 양을 줄이고 스토리지 용량을 대폭 감소시킨다.

☞ 주제어 : 콘텐츠, 저작물, 저작권, 블록체인, 저작권 관리시스템

ABSTRACT

Creative works such as webtoon and web novel are part of property rights. However, illegal copies of them are distributed on the internet easily, which raises social issues in today's society. In order to tackle these problems, this paper proposes and presents a blockchain based copyright management system that ensures forgery prevention, robust security features, improving trading performance, cost-effective, and enhanced visibility. The system allows a user to register creative works formally just the same as before registration and also to register simple creative ideas just anytime. In the latter case, if an idea or a thought flashes across through somebody's mind, he or she can register it to the system immediately without formal registration process and afterward, can utilize a way to prove its originality through the system. Regarding large size images and video files of creative works, the system reduces data size and storage volume sharply to be processed by network entities by storing original creative works separately and including only the hash result of creative works to the transactions.

☞ keyword : Contents, Creative Works, Copyright, Blockchain, Copyright Management System

1. 서 론

최근 웹툰이나 웹소설처럼 저작물로 보호해야 할 모바일 저작물들이 손쉽게 복제·유포되면서 관련 업계가 몸살을 앓고 있다. 버튼을 누르기만 하면 현재 보고 있는 스크린을 원본 그대로 갈무리해 누구에게든 보내거나 아예 SNS에 올려 누구나 찾아보게 할 수 있기 때문이다[1]. 한국저작권보호원에 따르면 2017년 전체 불법 복제물 이용량은 약 20억 8천 3백만 건이며 이 중, 온라인 불법복제물 이용량은 약 18억 7천 7백만 건으로 전체의 90.2%를 차지하였다[2]. 콘텐츠별 침해율은 영화, 음악, 게임, 출판, 방송의 순으로 나타났다. 또한, 불법 복제물로 인한 직·간접적인 생산 감소는 약 4조 8천억 원에 이르고, 이에 따른 고용손실은 약 4만 3천 명에 달하는 것으로 분석되었다.

저작물(콘텐츠, creative works)이란 인간의 사상 또는 감정을 표현한 창작물이며, 어문, 음악, 연극, 미술, 건축, 사진, 영상, 도형, 컴퓨터 프로그램, 2차 저작물, 편집 저작물, 공동 저작물 등의 유형으로 분류된다. 최근에는 인

1 Department of Research and Development, Raon Secure, Seoul, 06132, Korea.
2 Department of Information Security, Mokpo National University, Jeonnam, 58554, Korea.
* Corresponding author (hyungon@mokpo.ac.kr)
[Received 07 May 2019, Reviewed 09 May 2019, Accepted 04 September 2019]

공지능, 빅데이터, 블록체인, 사물 인터넷 등 4차 산업혁명을 이끄는 IT 기술들이 쏟아지면서 새로운 유형의 저작물이나 보호해야 할 대상이 급격하게 늘어나고 있다. 하나의 예로, 가상현실과 증강현실의 창작물을 들 수 있다. 또 다른 예로, 인공지능이 인간의 창작물을 모방하여 학습하고, 더 나아가 주체로서 음악, 설계, 디자인, 인테리어 등의 창작물이 등장하고 있다. 인공지능을 창작의 주체로 인정할 것인지, 인공지능에게 저작권을 부여할 것인지 등 새로운 유형의 분류, 저작물에 대한 윤리적인 문제, 제도와 법적인 문제의 해결이 요구된다[3].

저작권을 보호받기 위해서는 자신의 저작물을 '한국저작권위원회'의 '저작권 등록부'에 등록해야 한다. 그러나 현실적으로 등록에 걸리는 시간, 비용, 노력이 요구된다. 특히, 불현듯 떠오르는 아이디어나 새롭게 등장하는 유형의 저작물들은 현 제도로 보호받을 수 있는지를 알기 어려워 등록을 꺼리는 경향도 있다. 또한, 단일 기관에서 저작권을 독점적으로 관리하다 보니 어느 정도 모방이 요구되는 산업의 경우, 저작물에 대한 불확실성, 신뢰성, 정확성을 제공하기가 쉽지 않다. 이와 관련하여 '저작권 위탁관리 제도'나 '불공정이용 규제와 부정경쟁 방지법 시행' 등이 논의되고 있다[4].

한편, 최근에 확산되고 있는 블록체인 기술을 저작권 관리를 위해 사용할 수 있다[5][6][7]. 블록체인에는 거래의 기록이 위·변조가 불가능하게 남아있기 때문에 사용자가 제작한 콘텐츠에 대한 신규성(originality)과 정품 사용(genuine use)의 증거로 활용할 수 있다.

이와 관련하여 본 논문에서는 현재의 저작권 독점관리의 한계를 해소하고, 블록체인의 분산 데이터베이스를 사용하여 저작권 보호와 투명한 저작권 관리를 할 수 있는 저작권 관리시스템을 제안한다. 새로운 유형의 저작물을 수용하고, 창작 아이디어가 떠오르면 언제 어디서나 바로 등록을 할 수 있는 접근의 용이성을 제공한다. 그리고 증강현실이나 가상현실과 같은 새로운 유형의 콘텐츠를 수용할 수 있도록 콘텐츠의 용량이 큰 경우를 고려하였다. 대용량의 콘텐츠가 블록의 트랜잭션에 포함되면 네트워크 참여 노드들이 처리해야 할 데이터의 양과 스토리지 용량이 대폭 늘어나므로 이에 대한 해결방안을 제시한다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 관련 연구로 디지털 저작권 관리(Digital Right Management), 블록체인 개요, 블록체인 기반의 거래 플랫폼, 유럽의 블록체인 기반의 저작권 관리 연구를 소개한다. 3장에서는 새로운 저작권 관리시스템을 제안하고, 이에 대한 아이디어, 구조 및 기능, 사용자 인증, 트랜잭션 구조, 참여 노드의 블록 생성 알고리즘 등을 설계하였다. 4장에서는 제안한 시스템의 구현 구조와 구현한 소프트웨어의 실행결과를 보이고 마지막으로 결론을 맺는다.

2. 관련 연구

2.1 디지털 저작권 관리

DRM은 콘텐츠 제작사, 유통업자 및 최종 사용자가 투명하고 안전하게 사용할 수 있도록 하고, 다양한 디지털 콘텐츠와 관련된 사업 분야 및 기기의 호환성을 지원하는 디지털 콘텐츠 저작권 보호 및 관리 기술 표준이다[8]. 디지털 콘텐츠 안에 고유마크를 삽입하거나 사용권한을 제한하여 저작권을 효과적으로 보호한다. 예를 들어 다운받은 MP3 파일이 제한된 기기에서만 재생할 수 있거나, 공문서에 고유의 기관마크가 찍혀져 나오는 경우들이 모두 디지털 콘텐츠에 DRM을 적용한 사례이다.

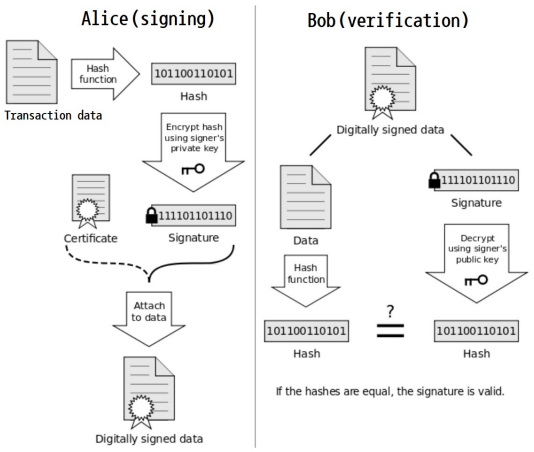
그러나 DRM은 내부 직원이 권한을 남용해 후킹방식으로 암호를 해제할 수 있고, 어플리케이션의 한계, 어플리케이션 버전 업그레이드 시, DRM을 재개발해야 하고 재배포해야 하는 등의 단점이 있다. 또한, 중앙집중식으로 데이터를 관리하기 때문에 '단일 지점 장애(SPOF; Single Point Of Failure)'에 대처하기 어렵다. SPOF는 시스템 내 한 곳의 문제가 전체 시스템의 작동을 멈추게 하는 것을 말하며, 기계의 오작동, 고의 또는 실수에 의한 사람의 행동, 정전 등 다양한 요소가 원인이 될 수 있다.

2.2 블록체인 기술

블록체인은 거래 내역이 담긴 장부(본 논문에서는 콘텐츠로 구성된 트랜잭션)를 거래에 참여하는 모든 구성원에게 분산하여 저장하는 기술로서, 분산원장 기술이라고도 한다. 원장은 주요 자산인 검증된 트랜잭션을 체인으로 연결하여 유지하기 때문에 트랜잭션을 위·변조하기가 매우 어려운 특징을 가지고 있다. 블록체인은 보안성 향상, 거래 속도 향상, 비용 감소, 가시성 극대화의 장점으로 인해 최근 급격하게 확산되고 있으며, 트랜잭션을 교환하는 시스템에서 신뢰성, 추적성, 투명성 그리고 보안성을 제공한다[9].

블록체인에서는 공개키 기반의 전자서명을 적용하여 서명된 트랜잭션에 대해 부인방지(non-repudiation)와 수신자가 트랜잭션의 송신자를 인증하는 기능을 제공한다.

다음은 그림 1을 참고해서 Alice가 트랜잭션을 블록에 포함시켜 전자서명하여 네트워크에 방송하고, 이를 수신한 Bob이 서명 검증하는 과정을 설명한다[10]. 먼저 서명자인 Alice는 트랜잭션의 해시 결과 값을 구한다. 이후 서명용 개인키로 해시 결과 값을 암호화하고, 암호화된 해시 결과 값과 원본 트랜잭션을 블록에 포함시켜 네트워크에 방송한다. 이를 수신한 Bob은 Alice의 공개키로 서명 값의 유효성을 검증한다. 트랜잭션이 변조되었는지와 트랜잭션이 Alice로부터 송신되었다는 사실을 인증한다. Bob은 수신된 트랜잭션의 암호화된 해시 결과 값으로부터 Alice의 공개키로 해시 값을 복구한 후, 수신된 트랜잭션과 자신이 계산한 해시 결과 값이 동일한지 비교한다. 만약 결과 값이 같다면 서명이 유효하고, 수신한 트랜잭션이 변조되지 않았다는 무결성을 검증할 수 있다. 블록체인에서 사용되는 디지털 서명 알고리즘은 RSA[11]와 타원곡선 디지털 서명 알고리즘(ECDSA)[12]을 사용하며 주로 후자가 더 많이 사용된다.



(그림 1) 트랜잭션의 디지털 서명 과정[8]
(Fig. 1) Digitally Signing a Transaction[8]

2.3 블록체인 기술

연구 [5]는 저작권 분야의 블록체인 기반 거래 플랫폼을 소개하였다. 코닥원(Kodakone)은 사진거래 플랫폼으로 코닥 코인을 사용하며, 이미지를 등록하고 스마트계약을 통해 저작권을 관리하며, 웹 크롤링을 통해 저작권 침해 방지 및 이미지를 추적할 수 있다. 우조뮤직(Ujomusic)은 음악 스트리밍 다운로드 플랫폼으로 이더리움을 사용한다. 데이터의 탈중앙화를 위한 웹프로토콜을 사용하며, 하나의 웹사이트 서버를 두지 않고 사용자들의 PC에 분할하여 운영한다. 스팀잇(Steemit)은 글을 작성하는 창작자와 이를 구독하는 구독자에게 암호화폐인 스팀을 보상으로 지급한다. 중앙 집중적 검열시스템이 따로 없고, 콘텐츠는 사용자들의 업투표(upvote)와 다운투표(downvote)로 평가한다. 콘텐츠를 통해 얻은 수익의 75%는 저자가, 나머지 25%는 투표 참여자에게 분배한다.

2.4 브루멘의 블록체인 연구

Bloomen(Blockhains in the new era participatory media experience)는 2020년까지 진행되고 있는 유럽의 연구 프로젝트 중 하나로, 블록체인 기술을 사용하여 작곡가, 작가, 영화 제작자 등이 제작한 디지털 콘텐츠의 저작권을 보호하고, 디지털 콘텐츠 사용에 대한 정당하고 안전한 보상을 제공하는 데 초점을 맞추고 있다[13]. 사용자가 생성한 디지털 콘텐츠나 뉴스를 소셜 미디어와 블록체인을 통하여 공유하면서 저작권을 통하여 수익화시킨다. 그리고 디지털 음악 콘텐츠를 블록체인 기반의 개방형 플랫폼을 통하여 제공한다.

3. 제안한 저작권 관리시스템

제안하는 블록체인 기반의 저작권 관리시스템은 기존의 저작물을 포함하여 단순한 디자인, 웹툰 스토리, 잠깐 떠오른 악상, 기술적인 아이디어 등 다음에 언제라도 저작권을 주장할 수 있는 저작물들을 모두 등록하고 유통·관리할 수 있도록 시스템이다. 단일 지점 장애 문제를 해결하기 위해 다수의 분산 시스템으로 구성된 블록체인 네트워크를 통해 공동으로 관리한다. 그리고 가상현실이나 증강현실의 저작물과 같이 새로운 유형을 수용하고 데이터 사이즈가 큰 콘텐츠를 고려한다.

사용자는 저작권 등록이 필요한 콘텐츠와 그렇지 않은 콘텐츠로 구분하여 시스템에 입력한다. 후자의 경우는 저작권 등록까지는 필요하지 않지만, 추후라도 자신의 독자적인 저작물이라는 것을 증명할 수 있는 증거로 활용할 수 있다. 일례로 연구 노트에 기록된 연구 결과물들은 독자적 증명수단으로 활용되며, 논문, 특허, 영업비밀 등으로 각각의 권리를 확보하는 데 있어서 연구 노트가 중요한 증거로 활용된다. 이러한 관점에서, 저작권 등록이 되어 있지 않지만, 블록체인에 저장되어 있을 때는 독자적 저작물로 인정해 줄 수 있는 기술적인 수단으로

활용할 수 있다.

3.1 블록체인 네트워크의 유형

블록체인 네트워크 유형은 첫째, 누구나 블록체인 네트워크에 참여할 수 있고 블록을 전송하거나 합의 프로세스를 수행할 수 있는 퍼블릭 블록체인 둘째, 법적 책임을 지는 허가 받은 사람만 블록체인 네트워크에 참여할 수 있는 프라이빗 블록체인 셋째, 퍼블릭과 프라이빗 블록체인의 일부 특징을 가지고 있는 세미 프라이빗 블록체인 넷째, 사전에 컨소시엄을 이룬 기업 혹은 그룹과 같은 이해관계자들에 의해 운용되는 컨소시엄 블록체인으로 분류할 수 있다[14].

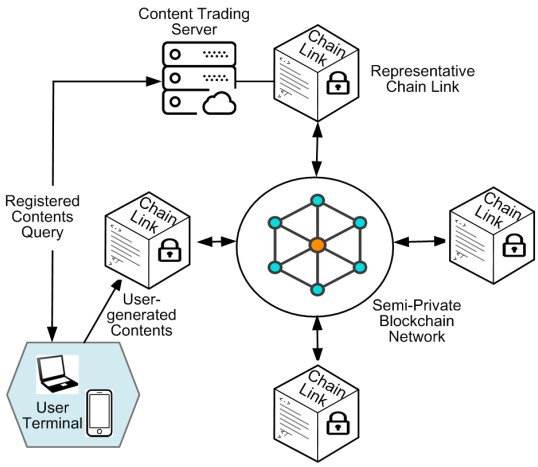
본 논문에서 제안한 저작권 관리시스템은 사용자 인증을 통해 사용자가 식별되고, 블록체인에 참여하는 노드들은 허가받은 노드만 네트워크에 참여할 수 있으므로 세미 프라이빗 블록체인이 적합하다. 이러한 특징으로 인해 세미 블라이빗 블록체인은 정부 응용 분야에 적합하다고 알려져 있다[15].

세미 프라이빗 블록체인은 개인이나 기관이 독자적으로 자신들만의 블록체인을 운영하는 것이므로 보상이 필요 없다. 그러나 콘텐츠를 사용하는 사용자 관점에서는 보상이 필요하다. 다른 저작권 거래 시스템과 동일하게, 개인이나 기관 간에 거래 시 콘텐츠 사용이나 거래에 대해 보상하는 것이다. 예를 들어, 콘텐츠를 등록하는 경우는 보상이 필요 없으나, 타인의 콘텐츠를 사용하거나 거래를 할 경우는 보상할 수 있다.

3.2 시스템 구조

제안한 저작권 관리시스템을 그림 2에 나타내었다. 기존의 저작권 관리시스템은 독립적으로 운영되나, 제안한 저작권 관리시스템은 링크 체인인 분산 서버들로 블록체인 네트워크를 구성하고 공동으로 저작권 원장을 분산 공유한다. 저작권 관리시스템은 크게 사용자 단말의 응용, 다수의 체인 링크, 대표 체인 링크(Representative Chain Link), 저작권 거래 서버(Content Trading Server)로 구성된다. 대표 체인 링크는 별도로 저작권 거래 서버와 직접 연결된다. 저작권 거래 서버는 일반 사용자가 저작권으로 등록된 모든 콘텐츠를 검색하거나 조회할 수 있는 기능을 제공한다. 그리고 개인 간이나 기관 간에 콘텐츠를 거래할 수 있고 그에 따른 보상을 제공한다.

사용자가 자신이 제작한 콘텐츠를 시스템에 등록하고자 할 때는 사용자 단말의 응용을 통해 인접한 체인 링크에 접속하여 콘텐츠 등록을 요청한다. 이를 수신한 체인 링크는 주기적으로 블록을 생성하고 다른 체인 링크들에게 방송하여 해당 블록을 검증하고 검증에 성공하면 블록체인에 등록시킨다. 사용자가 등록된 저작물을 조회하거나 거래하기 위해서는 자신의 터미널(휴대폰, 노트북, 데스크탑 등)의 응용 프로그램을 이용해 콘텐츠 거래 서버에 직접 접속한다.



(그림 2) 제안한 저작권 관리시스템

(Fig. 2) Proposed Copyright Management System

한편, 사용자 단말은 블록체인 참여 노드로 동작하지 않는다. 이유로서 첫째, 사용자는 비주기적이고 간헐적으로 저작권 관리시스템에 접속하므로 주기적으로 합의 프로토콜을 이용한 작업증명을 할 필요가 없다. 둘째, 사용자 단말에 모든 블록체인을 저장하기에는 스토리지 용량의 한계가 있을 수 있고, 컴퓨팅 연산능력도 부족할 수 있기 때문이다. 각 엔티티가 제공하는 주요 기능은 아래와 같다.

- □ 대표 체인 링크: 블록체인 네트워크의 참여 노드로 동작하며, 참여 노드들을 관리한다. 그리고 콘텐츠 거래 서버와 연동한다.
- □ 체인 링크: 블록체인 네트워크의 참여 노드로 동작한다. 사용자로부터 등록 요청받은 콘텐츠가 용량이 클 경우는 해시하여 그 결과 값만을 블록체인의 트랜잭션에 넣는다. 콘텐츠 원본은 자신의 데이터베이스에 저장하고 콘텐츠 거래 서버로도 전송한다.
- □ 콘텐츠 거래 서버: 블록체인 네트워크에 유통되는 모든

콘텐츠를 유형별로 분류하여 관리한다. 사용자에게 콘텐츠 검색 엔진의 기능을 제공하며, 콘텐츠 거래 기능과 그에 따른 보상 기능을 제공한다.

□ 사용자 단말: 응용 프로그램이 탑재되며, 사용자는 응용을 통해 체인 링크에 접속하여 저작물을 등록한다. 그리고 사용자는 필요할 경우, 콘텐츠 거래 서버에 접속하여 저작물을 검색하고 거래한다.

3.3 사용자 인증

사용자는 단말을 통해 콘텐츠를 조회하기 위해 콘텐츠 거래 서버와 접속하거나, 자신이 생성한 콘텐츠를 시스템에 등록하기 위해 인접한 체인 링크와 접속한다. 전자는 저작권 관리시스템에 등록되지 않은 모든 일반 사용자가 접속하여 조회하도록 해야 하므로 사용자 인증이 필요 없다. 그러나 후자의 경우는 체인 링크가 사용자를 식별하기 위해 사용자 인증이 필요하다.

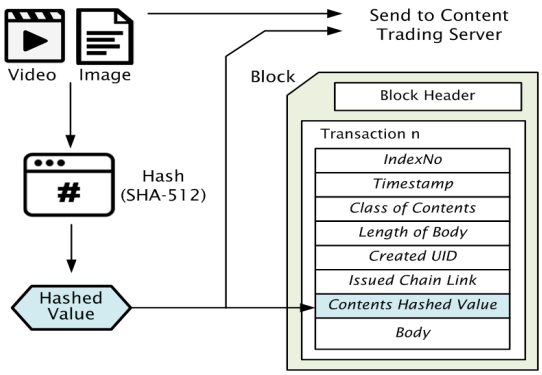
한편, 이와 유사한 사용자 인증 사례로 뱅크 사인에서의 사용자 인증을 들 수 있다[16]. 은행 서버들 간에 블록체인으로 구성하고 있지만, 사용자의 단말과 은행 서버 간에는 공유 비밀키 방식으로 사용자 인증을 한다. 제안한 시스템도 이와 유사하게 공유 비밀키 방식을 적용하며, 보안성을 강화하기 위하여 이중 인증을 적용한다.

3.4 대용량 이미지와 영상 파일

사용자의 저작물은 데이터나 파일의 형태로 블록의 트랜잭션에 포함된다. 그러나 사이즈가 큰 이미지나 동영상을 트랜잭션에 포함하게 되면, 블록의 사이즈가 커지고, 이로 인해 네트워크 참여 노드들이 처리해야 할 데이터의 양이 커지고 더 큰 스토리지가 필요하게 된다. 참고로 비트코인의 경우는 헤더가 80바이트이고 전체 트랜잭션의 크기를 1Mbyte로 제한하고 있다[15].

제안한 저작권 관리시스템에서는 사이즈가 큰 이미지나 동영상을 고려하였다. 사용자로부터 사이즈가 큰 콘텐츠 등록을 요청받으면 체인 링크에서 블록을 생성할 때, 그 콘텐츠의 해시 결과 값만을 추출해서 트랜잭션에 포함해서 전체 블록 사이즈를 줄인다. 그리고 원본은 자신과 콘텐츠 거래 서버에만 저장하도록 한다. 이를 통해 네트워크 참여 노드들이 처리해야 할 데이터의 양을 줄이고 스토리지 용량을 감소시킬 수 있으며, 해시 결과 값이 트랜잭션에 포함되어 있으므로 다음과 같이 무결성을 검증할 수 있다.

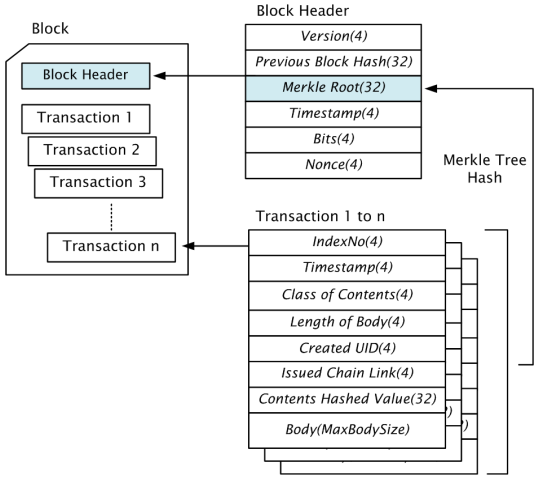
첫째, 콘텐츠 거래 서버에 저장된 콘텐츠와 해시 결과 값을 조회한 다음, 다시 콘텐츠 원본의 해시 결과 값을 계산하고, 두 해시 결과 값을 비교하여 무결성을 검증한다. 둘째, 해당 콘텐츠를 생성한 체인 링크가 원본을 저장하고 있으므로 두 원본을 비교하여 무결성을 검증한다. 사이즈가 큰 이미지나 동영상을 체인 링크가 수신했을 때, 처리 절차를 그림 3에 나타내었다.



(그림 3) 대용량 이미지와 영상 파일 처리
(Fig. 3) Processing of Large Images and Video Files

3.5 블록과 트랜잭션 구조

블록체인에서는 일정한 주기 내에 발생하는 트랜잭션을 모두 결합해 하나의 블록을 생성한다. 예를 들어 비트



(그림 4) 블록과 트랜잭션 구조
(Fig. 4) Block and Transaction Structure

코인은 10분마다, 이더리움은 15초마다 하나의 블록을 생성하며, 3세대로 분류되는 카르다노 등은 더 짧은 주기로 블록을 생성한다. 제안한 시스템도 동일하게 일정한 주기로 블록을 생성하고 사용한다.

다양한 콘텐츠로 구성되는 트랜잭션의 구조를 설계하여 그림 4에 나타내었다. 트랜잭션은 트랜잭션 ID인 *IndexNo*, 트랜잭션이 생성된 *Timestamp*, 콘텐츠의 종류를 나타내는 *Class of Contents*, 트랜잭션 바디 사이즈인 *Length of Body*, 저작물 저자인 *Created UID*(User ID), 저작물을 생성한 *Issued Chain Link*, 해당 트랜잭션의 해시값인 *Contents Hashed Value*, 그리고 트랜잭션 데이터인 *Body*로 구성된다.

3.6 블록 생성 알고리즘

체인 링크에서 블록 생성하는 알고리즘을 그림 5에 나타내었다. 먼저 (1) 트랜잭션(들)을 생성한다. 사용자로부터 저작물 등록을 요청받으면 등록하고자 하는 저작물 단위로 트랜잭션을 생성한다. 트랜잭션 헤더에 *Index No*와 *Timestamp*를 지정하고 저작물의 종류를 분류하여 *Class of Content*를 지정한다. 저작물 내용의 길이를 계산하여 *Length of Body*를 지정하고, 저작권자인 *Created UID*와 트랜잭션을 생성한 *Issued Chain Link*를 지정한다. 저작물의 내용을 해시하여 해시 결과값을 지정하고 저작물을 *Body*에 채운다. 만약, *Body*가 최대 사이즈(*MaxBodySize*)를 초과하면 튜플*(IndexNo, Hashed_Value, Body)*과 원본을 자신의 데이터베이스에 저장하고, 저작권 거래 서버에도 튜플과 원본을 전송한다. 최대 사이즈를 초과하지 않는다면 자신의 데이터베이스에만 저장한다.

트랜잭션이 완성되면 (2) 블록헤더를 생성한다. *Version*, *Previous Block Hash*를 지정한다. 모든 트랜잭션을 대상으로 바이너리 머클 트리를 구성하고, 해시 알고리즘 sha_256으로 머클 루트 값을 구하여 지정한다. 그리고 *Timestmp*, *Bits*, *Nonce*를 지정한다. *Bits*와 *Nonce*는 블록의 작업증명에 사용되는 필드이므로 적용하는 작업증명 알고리즘과 보상의 형태에 맞는 값을 지정한다. (3) 트랜잭션을 AES-256로 암호화하고 RSA 또는 ECDSA 알고리즘으로 전자서명 한다. 그리고 서명 결과 값을 블록에 첨부한다. (4) 완성된 블록을 블록체인 네트워크에 전송한다.

한편, 제안한 시스템에서 어떠한 협의 알고리즘을 적용하여 작업증명을 할 것인지에 대해서는 논외로 한다. 그리고 상용화를 고려한다면 시기적으로 이전에 생성되었던 다수의 저작물을 트랜잭션으로 묶어 배치형태로 블록체인 네트워크에 등록할 필요가 있다.

```
Algorithm: Block Generation
(1) Transaction(s) Generation
    Receive Content Reg. from User Terminal
    for i=0 to TransMax-1 do
        Set IndexNo, Timestamp
        Classify content and set it to Class of Content
        Set Length of Body = len(Body)
        Set Created UID, Issued Chain Link
        Set Hashed_Value = hash_sha256(Body)
        Set Body
        if Length of Body < MaxBodySize
            Store tuple(IndexNo, Hashed_Value, Body)
            Send tuple to Content Trading Server
        else
            Store tuple(IndexNo, Hashed_Value, Body)
        endif
    end for
(2) Block Header Generation
    Set Version, Previous Block Hash
    Calculate Merkle Root using hash_sha256, set it
    Set Timestamp, Bits, Nonce
(3) Encrypt and Signing Transaction
    Encrypt, signing using ASE256, RSA/ECDSA
    Attach Signature to block
(4) Broadcast the Block
```

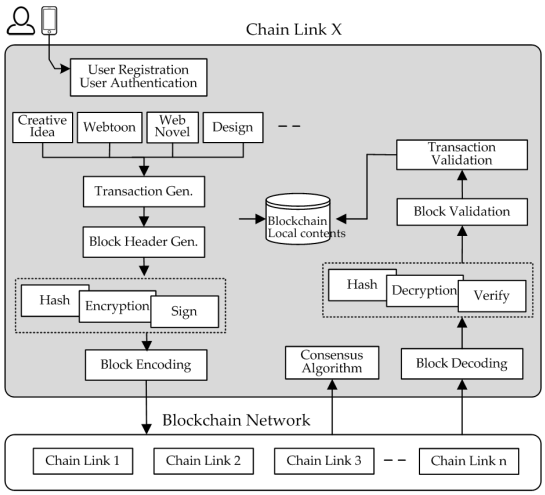
(그림 5) 체인 링크의 블록 생성 알고리즘
(Fig. 5) Block Generation Algorithm of Chain Link

4. 구 현

4.1 체인 링크의 구현 구조 알고리즘

제안한 저작권 관리시스템은 크게 사용자 단말의 응용, 대표 체인 링크, 다수의 체인 링크, 콘텐츠 거래 서버로 구성된다. 이 장에서는 시스템의 핵심인 체인 링크의 주요 기능만을 구현하였다. 체인 링크의 소프트웨어 구조를 유니트 단위로 표현하여 그림 6에 나타내었으며 구현환경을 표 1에 나타내었다.

사용자 등록과 인증, 트랜잭션 생성 및 검증, 블록 헤더 생성, 해시, 암호화 및 복호화, 전자서명 및 서명검증, 블록 엔코딩 및 디코딩, 블록 검증, 트랜잭션, 블록체인과 로컬 콘텐츠를 저장하는 데이터베이스, 합의 알고리즘으로 구성된다.



(그림 6) 체인 링크의 소프트웨어 구현 구조
(Fig. 6) Implementation Software Architecture of Chain Link

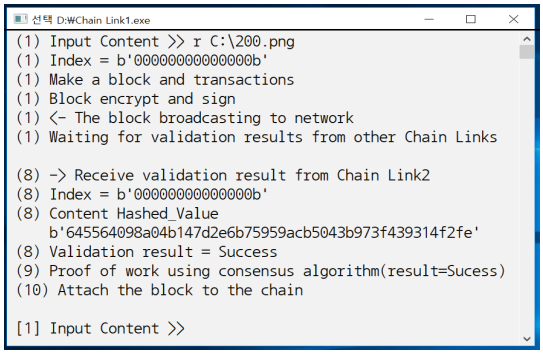
(표 1) 구현 환경
(Table 1) Implementation Environment

CPU	Intel Core i5-6500 3.20GHz
OS	Linux Debian 4.15.11
Language	Python 3.6
Library	PyOpenSSL
Database	LevelDB
Sign & Verify	RSA-2048
Encrypt & Decrypt	AES-256
Hash	SHA3-256

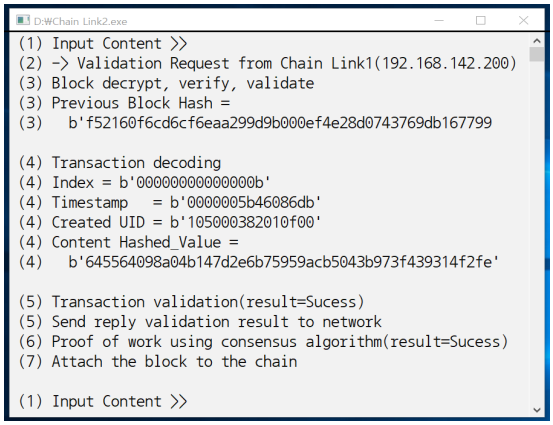
4.2 소프트웨어 실행 결과

구현한 저작권 관리시스템의 주요 기능을 확인하기 위해, 체인 링크 1이 블록을 생성하여 네트워크에 방송하고 체인 링크 2가 이를 검증하고 다시 체인 링크 1에 응답하는 실험 시나리오를 사용하였다. 실행 화면을 그림 7과 그림 8에 나타내었다.

(1) 체인 링크 1에서 저작물인 이미지 파일을 입력받고, 사용자의 저작물을 트랜잭션으로 생성하고, 생성된 트랜잭션에 블록체인 헤더를 추가하고, 블록을 암호화하고 전자서명 한 후, 서명 결과 값을 블록에 첨부한다. 이후, 블록을 엔코딩한 다음 블록체인 네트워크에 전송하고 검증 결과를 기다린다. (2) 이를 수신한 체인 링크 2가 수신한다. (3) 블록의 복호화, 서명 검증, 블록 검증을 하



(그림 7) 체인 링크1의 실행 결과
(Fig. 7) Execution Results of Chain Link1



(그림 8) 체인 링크2의 실행 결과
(Fig. 8) Execution Results of Chain Link2

고, 이전 블록 해시 값과 자신의 데이터베이스 내에 저장된 이전 블록 해시 값과 비교한다.

(4) 트랜잭션을 디코딩한다. (5) 트랜잭션을 검증하고 그 결과를 네트워크에 방송한다. (6) 다른 체인 링크들과 합의 알고리즘을 통해 작업증명을 한다. (7) 성공하면 그 블록을 체인에 연결한다. 실험 결과, 실행화면에서와 같이 주요 기능이 정상적으로 동작함을 확인하였다.

5. 결 언

본 논문에서는 창의적인 아이디어를 바로 등록할 수 있는 블록체인 기반의 저작권 관리시스템을 제안하였다. 세부적으로는 시스템 구조 및 기능, 사용자 인증 방법, 콘텐츠를 수용할 수 있는 블록의 트랜잭션, 참여 노드의

블록 생성 알고리즘 등을 설계하였다. 그리고 주요 기능을 구현하고 정상 동작을 확인함으로써 실용화 가능성을 보였다.

제안한 시스템은 현재의 저작권 독점관리의 한계를 해소하고, 블록체인의 장점인 저작물 위·변조의 어려움, 보안성 향상, 거래 속도 향상, 비용 감소, 가시성 극대화 등을 기할 수 있다. 창작 아이디어가 떠오르면 언제 어디서나 자신의 스마트폰이나 컴퓨터로 시스템에 접속하여 저작물을 등록할 수 있는 접근의 용이성도 제공한다. 특히, 용량이 큰 콘텐츠는 블록의 트랜잭션에 그 콘텐츠의 해시 결과 값만을 사용하여, 네트워크 참여 노드들이 처리해야 할 데이터의 양을 줄이고 스토리지 용량을 대폭 감소시킨다. 추후 연구로는 콘텐츠 거래 서버 설계, 다양한 콘텐츠를 효과적으로 분류하고 검색할 수 있는 기술, 콘텐츠 거래에 따른 보상을 연구하고자 한다.

참고문헌(Reference)

[1] EunJee Lee, "Snapping While Watching Webtoon – Faced with Copyright Infringement," *Kukmin ilbo Newspaper Article*, May 29, 2017.

[2] "2018 Annual Report on Copyright Protection," *Korea Copyright Protection Agency*, June 2018.

[3] YongJoo Kim, "The Possibility to Protect Creative Works of Artificial Intelligence," *Chungnam LawReview*, Vol. 27, No. 3, Dec. 2016.

[4] Research Report, "Research on Institution of Copyright Consignment Management," *Ministry of Culture, Sports and Tourism*, pp.1-167, Aug. 2004.

[5] Mirang Sim, "Copyright Management using Blockchain," *In-depth Analysis Report*, Vol. 2018-16 Nov. 2018.

[6] Michele Finch, Valentina Moscon, "Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0," *International Review of Intellectual Property and Competition Law*, Jan. 2019.

[7] Ma Zhaofeng, HuangWeihua, Gao Hongmin, "A new blockchain-based trusted DRM scheme for built-in content protection, "EURASIP Journal on Image and Video Processing, 19 Sep. 2018.

[8] Market Research Place(MRP), "Global Digital Rights Management (DRM) Market Size, Status and Forecast 2018-2025," *Research Report 833373*, August. 2018.

[9] Ziban Zheng1, etc., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *IEEE 6th International Congress on Big Data*, pp.557-564, 2017.

[10] https://crypto.stackexchange.com/

[11] R. Rivest, A. Shamir, L. Adleman, "A method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol. 21(2), pp.120-126, 1978.

[12] FIPS PUB 186-4, "Digital Signature Standard(DSS)," July 2013.

[13] https://bloomen.io/

[14] William Mougayarm, Vitalik Buterin, "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, " *Wiley*, Sep. 2007.

[15] Mark G., etc., "Blockchain and its Suitability for Government Applications," *2018 Public Private Analytic Exchange Program Report*, pp.1-41, 2018.

[16] KyungYeul Kim, "BankSign Service: Blockchain Certification Platform for Korea's Banks, " *ITFIND*, July. 2018.

◐ 저 자 소 개 ◑

황 정 식(Jung-sik Hwang)
2017년 목포대학교 정보보호학과(공학사)
2019년 목포대학교 대학원 정보보호학과(공학석사)
2019년~현재 라온시큐어 연구원
관심분야 : 모의 해킹, 포렌식
E-mail : rootsik1221@gmail.com

김 현 곤(Hyun-gon Kim)
1992년 금오공과대학교 전자공학과(공학사)
1994년 금오공과대학교 대학원 전자공학과(공학석사)
2003년 충남대학교 대학원 전자공학과(공학박사)
1994년~2005년 한국전자통신연구원 정보보호연구본부 선임연구원
2005년~현재 목포대학교 정보보호학과 교수
관심분야 : 차량통신 보안, 블록체인, 인공지능 보안
E-mail : hyungon@mokpo.ac.kr