

특집논문 (Special Paper)

방송공학회논문지 제24권 제6호, 2019년 11월 (JBE Vol. 24, No. 6, November 2019)

<https://doi.org/10.5909/JBE.2019.24.6.956>

ISSN 2287-9137 (Online) ISSN 1226-7953 (Print)

## 블록체인 및 분산저장시스템을 활용한 음원 및 시그니처 저장 방법

이 경 식<sup>a)</sup>, 김 상 균<sup>a)†</sup>

# Music Source and Signature Storage Method using Blockchain and Distributed Storage System

Kyoung-Sik Lee<sup>a)</sup> and Sang-Kyun Kim<sup>a)†</sup>

### 요 약

유튜브나 트위치와 같은 개인 미디어 시대를 맞아, 개인의 미디어 콘텐츠 제작과 소비가 간편해졌다. 플랫폼 서비스를 통한 엄청난 양의 미디어 콘텐츠가 생성·소비되고 있다. 이와 관련하여 미디어 콘텐츠의 저작권에 대한 관심이 높아지고 있다. 특히, 음원의 경우 거의 모든 미디어 콘텐츠 제작에 있어 없어서는 안 될 중요 요소이다. 본 논문에서는 뮤직 콘텐츠에 대한 저작권을 확인하기 위해 음원과 그의 시그니처를 블록체인과 분산저장시스템을 활용하여 저장할 수 있는 방안을 제안한다. 음원의 오디오 시그니처 추출 결과를 블록체인 트랜잭션 데이터로 포함할 수 있는지의 가능성을 파악한다. 실험을 통해 음원과 그의 시그니처를 분산저장시스템에 저장했을 때의 입출력 속도를 비교 확인한다.

### Abstract

In the age of personal media such as YouTube and Twitch, individual media content creation and consumption have become simpler. A huge amount of media content is created and consumed through platform services. In this regard, interest in copyright of media contents is increasing. In particular, the sound source is an indispensable element in almost all media contents production. In this paper, we propose a method to store the sound source and its signature using blockchain and distributed storage system to verify the copyright of music contents. We identify the possibility of including the audio signature extraction result of the sound source as blockchain transaction data. Through experiments, we compare the input and output speed when the sound source and its signature are stored in the distributed storage system.

Keyword : Blockchain, music copyright, music contents, IPFS, audio signature

---

a) 명지대학교(Myongji University)

† Corresponding Author : 김상균(Sang-Kyun, Kim)

E-mail: [goldmunt@gmail.com](mailto:goldmunt@gmail.com)

Tel: +82-31-330-6443

ORCID: <https://orcid.org/0000-0002-2359-8709>

※ 이 논문의 연구결과 중 일부는 한국방송·미디어공학회 “2019년 하계학술대회”에서 발표한 바 있음.

※ This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (NRF-2019R1F1A1041882).

· Manuscript received August 21, 2019; Revised November 11, 2019; Accepted November 11, 2019.

## I. 서론

4차 산업혁명의 시대를 맞아 기존의 TV, 라디오와 같은 전문적인 대중 매체의 시대가 저물고 1인 미디어 시대가 다가왔다. 이에 따라 최근에는 개인의 PC환경 혹은 모바일 기기를 통해 손쉬운 미디어 콘텐츠의 제작과 소비가 가능하게 되었다. 특히, 1인 미디어의 대표적 플랫폼인 유튜브의 경우, 개인이 제작한 콘텐츠에 광고를 삽입하여 개인 수익 창출이 가능한 서비스를 제공하고 있다<sup>[1]</sup>. 이러한 서비스를 통해 유튜브는 2017년 전체 국내 광고시장의 37%를 차지하였으며, 2018년에는 그 비중이 40%로 증가하였다<sup>[2]</sup>.

이처럼 다양한 플랫폼을 통해 엄청난 양의 콘텐츠가 생성·소비되면서 최근 저작권과 관련된 문제가 대두되고 있다. 특히 음원의 경우, 동영상과 비롯한 거의 모든 미디어 콘텐츠 제작의 필수 요소로 활용되고 있기 때문에 음원의 사용과 관련된 분쟁은 더욱 치열하다. 이를 해결하고자 인터넷 방송 플랫폼인 트위치에서는 콘텐츠 제작에 사용된 음원에 대해 실시간 감시를 진행하며<sup>[3]</sup>, 유튜브에서는 저작권에 반하는 음원을 사용하여 콘텐츠를 제작하는 경우에 대하여 이로 인해 발생한 수익을 창작자가 배분 받지 못하도록 하는 조치를 취하고 있다<sup>[4]</sup>. 하지만 이러한 노력에도 불구하고 생산된 모든 콘텐츠에 대하여 확인이 불가능하기 때문에 보다 근본적인 해결책이 요구된다.

이에 본 논문은 음원의 특징을 담은 오디오 시그니처를 추출하여 각 음원들을 구분할 수 있도록 하고, 이를 블록체

인과 분산저장시스템을 통해 저장함으로써, 음원의 저작권을 검색 및 검증할 수 있는 시스템 구현의 기초 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2 절에서는 디지털 시그니처와 블록체인의 적용 사례와 관련된 동향을 살펴보고, 오디오 시그니처 추출과 관련된 기술에 대해 파악한다. 3 절에서는 음원과 음원에서 추출한 오디오 시그니처를 블록체인 및 분산저장시스템에 저장하는 방안을 제시한다. 4 절에서는 분산저장시스템과 HTTP시스템에 음원 및 시그니처의 입출력 시간을 측정 비교함으로써 음원 저작권 검색 및 검증 활용 가능성에 대하여 살펴본다. 마지막으로, 5 절에서는 본 논문의 결론과 함께 향후 연구의 방향성을 제시한다.

## II. 관련 기술

### 1. Ujo music

Ujo music은 블록체인 기반의 음악 플랫폼 서비스로써, 음원에 대한 권한과 보상을 창작자에게 온전히 돌려주고자 하는 목적을 갖고 있다. 이에 창작자는 자유롭게 자신의 창작물을 판매할 수 있고, 필요에 따라 그 권한과 가격을 책정할 수 있다. 음원 사용 비용의 결제는 이더리움의 스마트 계약을 통해 이루어지는데, 스마트 컨트랙트에 명시된 비

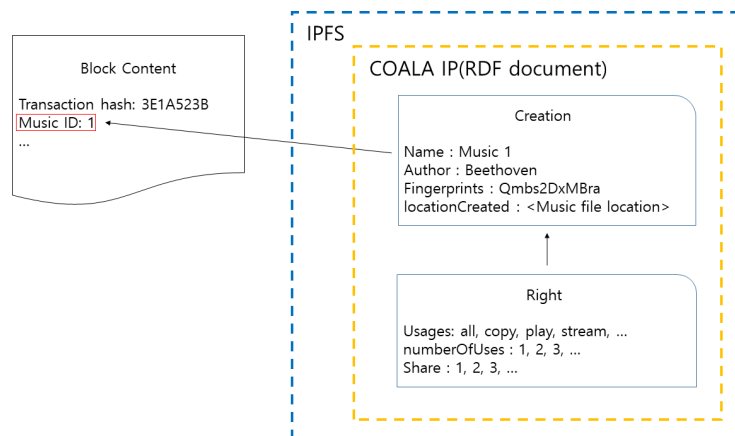


그림 1. Ujo music의 COALA IP를 통한 음원 정보 저장 방법  
 Fig. 1. A method for storing music content information using COALA IP on Ujo music

울에 따라 창작에 참여한 모든 기여자에게 직접 수익이 분배된다<sup>[5]</sup>.

Ujo music의 스마트 컨트랙트는 음원 최초 등록 시 부여한 고유 ID와 거래 관련 사항만을 저장하며, 음원 정보에 대한 메타데이터는 직접 저장하지 않는다. 생성된 음원의 저작권을 비롯한 모든 음원 관련 메타데이터는 COALA IP 프로토콜을 준수한 RDF 형태의 문서로 작성하여 관리한다<sup>[6]</sup>.

[그림 1]은 Ujo music의 저작권 관리 방법의 예시이다. 최초 생성된 음원에 대하여 ‘1’이라는 고유 ID가 생성되며, 이더리움의 스마트 컨트랙트에는 고유 ID ‘1’과 함께 해당 음원의 거래 관련 정보가 등록된다. 생성된 음원의 기본적인 정보는 ‘Creation’ RDF문서를 통해 관리한다. 음원의 이름, 저작자를 비롯한 기본적인 정보와 해당 음원에 대한 fingerprint가 포함되며, 실제 음원이 저장된 위치도 담고 있다. 해당 음원과 관련된 권리 및 권한에 대해서는 ‘Right’ RDF문서를 통해 서술한다. ‘Right’ RDF문서에는 복제, 단순 스트리밍 등의 사용 범위와 사용횟수 및 공유횟수 등의 내용이 포함되어 있다. [그림 1]의 예시에서 설명한 Creation, Right 외에도 User, Group 등 추가적인 RDF문서를 통해 음원과 관련된 메타데이터를 서술할 수 있다.

Ujo music은 복제 음원에 대한 검증이 어렵다는 문제점을 안고 있다. 트랜잭션 데이터에 음원과 관련된 정보를 직접적으로 저장하지 않기 때문에 불법 복제된 음원을 블록체인 네트워크에 등록하거나 사용하였을 때, 이를 검색하거나 차단하기 어렵다.

## 2. JPEG-blockchain Framework

영상 파일 포맷의 표준화를 이끌고 있는 JPEG(Joint Photographic Experts Group)에서는 최근 블록체인을 적용하려는 논의가 활발히 이루어지고 있다. 특히, ISO/IEC 19566-4 JPEG Privacy and Security 프로젝트를 통해 블록체인 기반의 이미지 파일 관리 시스템에 대한 표준화를 진행 중에 있다<sup>[7]</sup>.

JPEG-blockchain framework에서는 이미지 파일의 메타데이터를 블록체인 트랜잭션 데이터로 작성하여 블록에 포함시킨다. 이미지 메타데이터에는 파일명, 파일의 크기 등

기본적인 정보는 물론, 파일의 시그니처 해시 값과 같이 저작권 정보를 나타낼 수 있는 정보들이 포함된다[그림 2].

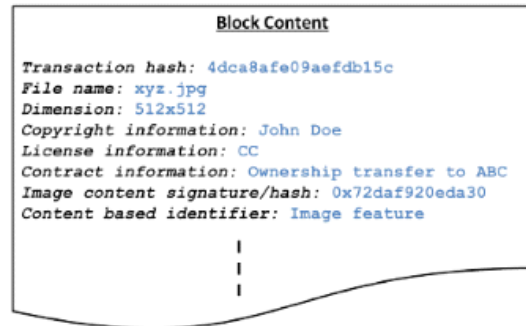


그림 2. JPEG-blockchain 트랜잭션 데이터 예시<sup>[7]</sup>  
Fig. 2. JPEG-blockchain transaction data<sup>[7]</sup>

블록체인의 블록에 올라갈 수 있는 데이터 크기에 제약이 있기 때문에, 원본 이미지 등의 대용량 파일을 블록체인 트랜잭션 데이터로 포함시키기에는 어려움이 따른다. 이를 해결하기 위해 JPEG-blockchain framework에서는 원본 이미지 파일은 별도의 저장소에 저장하고, 이미지 파일이 저장된 저장소의 위치정보를 블록 트랜잭션 데이터에 포함시키도록 하고 있다.

[그림 3]은 JPEG-blockchain framework의 전체 구성 예시를 보여준다. 각 노드는 블록체인에 등록된 블록들을 의미하며, 각 블록의 트랜잭션 데이터에는 원본 이미지 파일을 제외한, 이미지 파일과 관련된 모든 메타데이터들이 담겨있다. 이를 통해 블록체인을 통한 이미지 파일의 검증은 물론 원본 이미지 파일로의 접근 역시 가능하다.

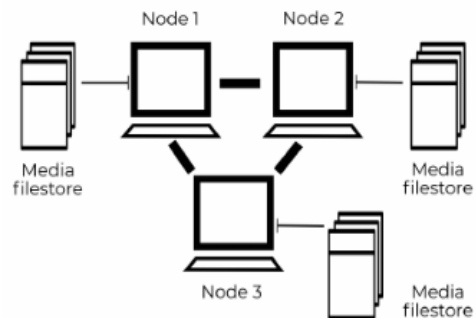


그림 3. JPEG-blockchain 네트워크 구성 예시<sup>[7]</sup>  
Fig. 3. JPEG-blockchain network configuration<sup>[7]</sup>

### 3. Dejavu project

데자뷰(Dejavu)는 파이썬으로 개발된 오픈소스 프로젝트로써, 입력된 음원에 대해 일련의 처리 과정을 거친 후 각 음원만의 특징을 지닌 오디오 시그니처를 추출하도록 한다. 각 음원마다 추출된 오디오 시그니처들의 비교를 통해 서로 동일한 음원인지의 여부 판별이 가능하다<sup>[8]</sup>.

음원의 특징 추출을 위해 데자뷰에 입력된 음원은 고속 푸리에 변환(Fast Fourier Transform)을 통해 파형의 형태를 지닌 스펙트로그램으로 변환된다. [그림 4]는 고속 푸리에 변환 후 음원 파일의 스펙트로그램 추출 예시를 보여준다. 다음으로, 변환된 스펙트로그램에서 각 파형의 피크(최고점)를 검출하여 (시간, 주파수)의 쌍으로 나타낸다. [그림 5]는 스펙트로그램에서 추출한 피크들을 도식적으로 나타낸 결과이다.

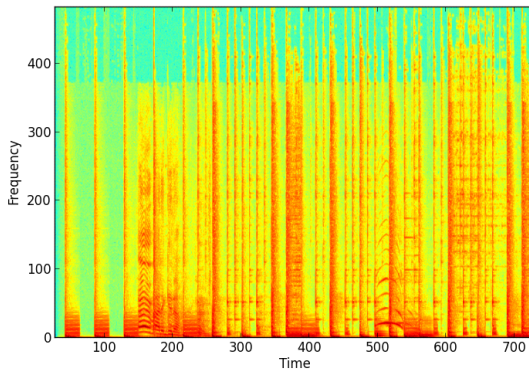


그림 4. 오디오 시그널 스펙트로그램의 예시<sup>[8]</sup>  
 Fig. 4. A spectrogram of an audio signal<sup>[8]</sup>

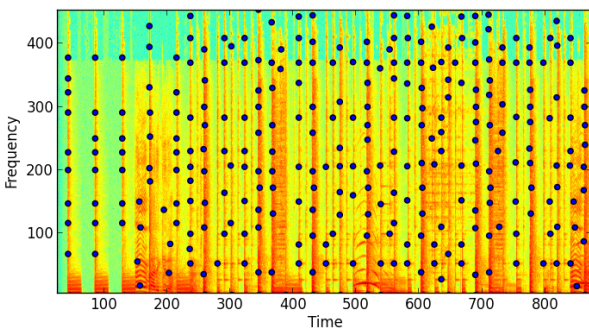


그림 5. 스펙트로그램에서 추출한 peak(최고점)들의 예시<sup>[8]</sup>  
 Fig. 5. Example of peaks extracted from the spectrogram<sup>[8]</sup>

계산된 피크값들을 나열 후, 해쉬함수를 적용하면 해당 음원의 오디오 시그니처를 추출할 수 있다. 데자뷰에서는 이렇게 얻은 해쉬값들에 이진화 과정을 한 번 더 진행함으로써 최종적으로 이전 해쉬값에 비해 크기가 감소된 오디오 시그니처를 추출한다.

## III. 블록체인을 통한 음원 및 오디오 시그니처 데이터 저장 방안

### 1. 블록체인 활용 방안

블록체인의 블록은 헤더와 트랜잭션(Transaction)데이터로 구분된다. 트랜잭션에는 현재 블록의 생성을 위한 모든 변경내역을 저장하며, 블록 헤더에는 이전 블록의 데이터를 암호화하여 그 결과를 포함시킨다. 이전 블록의 데이터 암호화 과정에서 수행하는 해쉬연산은 단방향 연산만을 수행하기 때문에 암호화 결과의 역산을 통해 이전 블록의 데이터를 복호화 하는 것이 어렵도록 설계되어 있다. 또한 블록체인의 모든 참여자(노드)들은 모두 같은 블록 데이터를 공유하게 되어있기 때문에 데이터의 무결성에 대한 보장이 가능하며, 일부 특정 노드나 블록체인 관리자에 의해 무단으로 데이터의 위·변조가 불가능하다.

이러한 블록체인의 특징을 활용하여, 음원의 특징을 추출한 오디오 시그니처가 블록체인 블록의 트랜잭션 데이터로 포함되어 있다면, 추후 생성될 블록들과의 비교를 통해 특정 음원의 저작권에 대하여 검증이 가능하다. 하지만 현재 대부분의 블록체인에서는 포함할 수 있는 블록 트랜잭션 데이터의 크기에 제한을 두고 있다. 비트코인에서는 1MB로 블록 크기를 제한하고 있으며, 이더리움에서 역시 최대 1MB까지로 그 크기를 제한하고 있다.

이에, 추출한 오디오 시그니처 데이터가 블록체인의 블록 생성 제한 크기를 초과하지 않는지에 대한 검증이 먼저 필요하다.

### 2. 오디오 시그니처 추출 결과

먼저, 오디오 시그니처를 직접 추출하여 블록체인의 블

록에 포함시킬 수 있는 가능성에 대해 알아본다. 오디오 시그니처의 추출 대상으로는 mp3 확장자의 10개 음원 파일을 선정하였으며, [표 1]에서 각 음원 파일의 재생 시간과 크기를 보여준다. 음원 파일 확장자의 경우, 가장 대중적으로 사용되는 3개의 확장자(wav, flac, mp3)중 가장 사용 빈도가 높고, 비교적 음원파일의 크기가 작은 mp3를 선택하여 테스트를 진행하였다.

표 1. 음원 파일의 재생 시간, 파일 크기  
Table 1. Play time and file size of music source files

Number of music file	Play time(sec)	Size(MB)	File extension
1	4:59	9.6	.mp3
2	3:11	6.9	.mp3
3	2:45	6.2	.mp3
4	3:45	7.4	.mp3
5	3:44	7.9	.mp3
6	2:59	6.9	.mp3
7	4:01	8.3	.mp3
8	3:23	7.0	.mp3
9	3:52	7.5	.mp3
10	3:58	7.6	.mp3

선정한 mp3 음원 파일에서 추출한 오디오 시그니처의 크기는 아래 [표 2]의 결과와 같다.

표 2. 추출된 오디오 시그니처의 크기  
Table 2. Size of extracted audio signature

Number of music file	Size of audio signature(MB)
1	9.5
2	6.8
3	6.4
4	7.9
5	7.5
6	6.6
7	8.7
8	7.5
9	7.5
10	7.8

[표 2]의 데이터를 분석한 결과, 3번 음원의 오디오 시그니처 크기가 6.4MB로 가장 작았고, 1번 음원의 오디오 시그니처 크기가 9.5MB로 가장 크게 나타났다. 가장 작은 크기인 3번 오디오 시그니처조차 블록체인의 생성 가능한 최대 크기인 1MB를 초과한다.

실험 결과대로, 음원 파일에서 추출한 오디오 시그니처를 블록 트랜잭션 데이터에 직접 포함시키기에는 어려움이 따른다. 이를 해결하기 위해, 추출한 오디오 시그니처를 블록체인 트랜잭션 데이터로 포함시키기에 알맞은 크기로 축소할 수 있는 방안을 살펴본다.

### 3. P2SH(Pay to Script Hash)

비트코인 상의 거래는 트랜잭션에 작성된 스크립트(script)의 실행을 통해 이루어진다<sup>[9]</sup>. 스크립트는 잠금 스크립트(Locking script)와 해제 스크립트(Unlocking script)로 구분할 수 있다. 잠금 스크립트는 거래를 위해 충족되어야 하는 요건들이 작성된 스크립트로서, 거래 대상자의 정보, 실제 진행되어야 하는 거래의 내용 등이 작성되어 있다. 잠금 스크립트에 작성된 거래 조건을 확인하여 실제 거래를 실행하기 위해서는 잠금 스크립트에서 요구하는 알맞은 값을 해제 스크립트에서 제시하여 해당 거래의 소유자인지를 검증해야 한다. 일반적으로 잠금 스크립트에는 거래 대상자의 공개키(public key)를 활용하기 때문에, 거래를 위해서는 개인키(private key)를 활용한 해제 스크립트를 제시하여 상호 검증과정을 거쳐야 한다. 하지만, 이 방법은 거래에 참여한 대상자가 여럿인 경우, 각 참여자의 공개키를 모두 포함하는 잠금 스크립트를 작성해야하기 때문에, 그 크기가 커진다는 단점이 있다.

이를 해결하기 위해 P2SH에서는 먼저 각 참여자의 공개키들을 모아 하나의 교환 스크립트(redeem script)로 생성한다. 이렇게 작성된 교환 스크립트에 해시 과정을 거쳐

```

Redeem Script (M-of-N signature) : OP_M <Public Key 1> <Public Key 2> ..... <Public Key N> OP_N OP_CHECKMULTISIG
Locking Script : OP_HASH160 <Redeem Script hash> OP_EQUAL
Unlocking Script : <Sig-1> <Sig-2> ..... <Sig-M> <Redeem Script>
    
```

그림 6. 교환 스크립트(redeem script)와 잠금, 해제 스크립트  
Fig. 6. Example of a redeem script, a locking and unlocking script

20bytes 고정크기의 잠금 스크립트를 생성한다. 이렇게 생성된 잠금 스크립트는 거래 참여자의 공개키를 모두 나열하는 기존의 방법에 비해 훨씬 효율적인 공간의 활용이 가능하다. [그림 6]에서는 n개의 공개키를 사용하여 작성한 교환 스크립트와 해시를 활용한 잠금 스크립트 및 해제 스크립트의 작성 예시를 보여준다.

앞서 설명한 P2SH에서의 방법을 활용하여 20bytes의 축소된 오디오 시그니처 값을 얻을 수 있다. 축소된 오디오 시그니처는 블록 트랜잭션 데이터로 포함시키기에 충분한 크기를 만족한다.

이를 활용하면 블록체인 트랜잭션 데이터만의 비교를 통해 단순한 형태의 음원 저작권 검증은 가능하다. 하지만, 원본 음원 파일이나 오디오 시그니처에 대한 요청 등을 통한 비교 검증이 어렵기 때문에 음원 저작권의 검증에 필요한 저장 방법이라 할 수 없다. 음원 및 음원의 오디오 시그니처와 같은 원본 파일들에 대한 저장을 위해 다음장에서 분산파일시스템(IPFS)을 통한 해결 방안을 제시한다.

#### 4. IPFS(InterPlanetary File System)

IPFS는 Torrent로 대표되는 P2P기반의 분산파일저장 방법으로써, 하나의 파일을 여러 개의 조각으로 나누어 관리하도록 하는 방법이다<sup>[10]</sup>. IPFS는 먼저 원본데이터 파일의 위·변조가 불가능하도록 일련의 암호화 과정을 거친다. 이후 암호화된 파일은 보다 작은 크기의 여러 개의 샤드(Shard)로 분할하고, IPFS에 연결된 여러 노드들에 분산되어 저장된다.

여러 노드에 분산 저장된 데이터들은 DHT(Distributed Hash Table)라는 구조를 통해 관리된다. 분할된 노드들은 각각 키(key)와 대응값(value) 쌍의 구조를 지니며, 각 노드를 구별할 수 있는 고유의 해시 값을 키로 나타낸다. 대응값에는 해당 노드가 저장된 위치나 자신과 관련이 있는 노드의 정보가 담겨있다.

[그림 7]의 예시에서 70MB크기의 파일을 IPFS를 사용하여 3개의 노드로 분할하였다. 분할된 노드들은 DHT를 통해 관리되기 때문에 각각 키와 대응값을 갖는다. 각 노드들은 원본 파일의 해시 값(9627)에 특정 문자나 숫자를 추가하여(A9627, B9627, C9627) 키로 사용한다. 이는 분할된 각 노드들이 9627의 해시 값을 갖는 원본파일로부터 분할되었다는 것을 의미한다. 분할된 각 노드들은 대응값으로 자신이 저장된 저장소의 위치를 갖고 있기 때문에 원본 파일로의 통합이나 관리가 가능하다.

#### 5. 블록체인과 IPFS를 활용한 오디오 음원 및 시그니처 저장 방법

앞서 살펴본 기술들을 종합하여 본 논문에서는 블록체인과 분산저장시스템을 활용한 음원 및 오디오 시그니처 저장 방법을 제안한다.

P2SH에서 교환 스크립트의 크기를 20bytes의 고정 크기로 축소시킨 해시 함수를 추출한 오디오 시그니처와 원본 음원 파일에 적용한다. 생성된 오디오 시그니처와 음원 파일의 20bytes 해시 값을 블록 트랜잭션 데이터에 추가하여 블록체인에 포함시킨다. 이 때, 해시되기 이전의 오디오 시

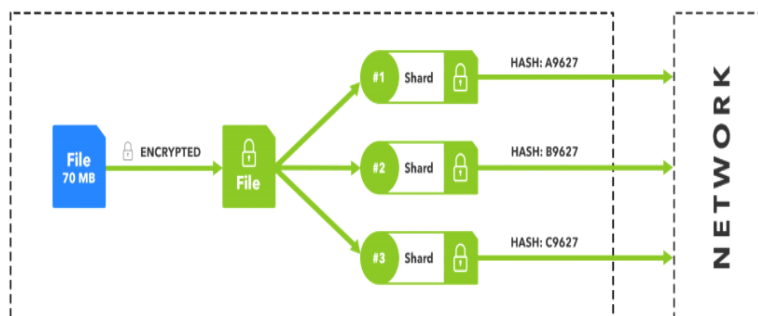


그림 7. IPFS 샤드 분할 및 DHT 적용 예제<sup>[10]</sup>  
 Fig. 7. Example of IPFS shard partitioning and DIT enforcement<sup>[10]</sup>

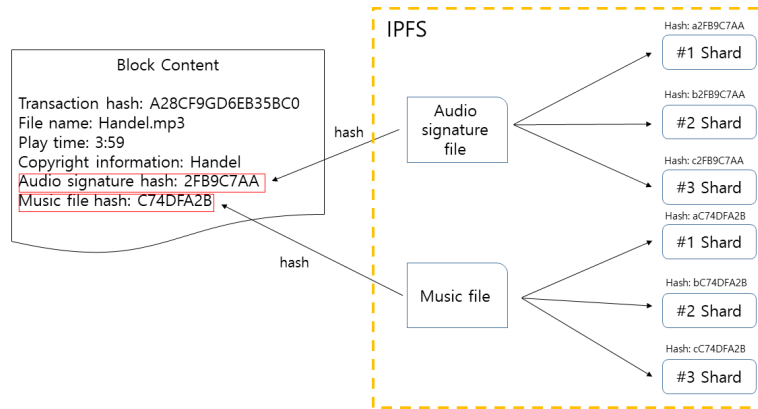


그림 8. 블록체인을 활용한 오디오 시그니처 및 음원파일 저장 방법  
 Fig. 8. Audio signature and music source storage method using blockchain

그니처와 음원 파일은 IPFS를 활용하여 별도의 노드로 분할하여 관리한다. IPFS의 노드들은 DHT구조를 통해 관리되기 때문에, 블록 트랜잭션 데이터에 포함된 오디오 시그니처의 해시 값과 음원 파일의 해시 값을 참조하여 IPFS에 분산 저장된 원본 데이터로의 접근이 가능하다.

[그림 8]은 본 논문에서 제안한 방법의 활용 예시를 보여준다. 추출한 오디오 시그니처와 원본 음원 파일에 해시값을 적용하여 각각 20bytes 크기의 해시 값(2FB9C7AA, C74DFA2B)을 추출한다. 이렇게 얻은 해시 값은 블록 트랜잭션 데이터에 추가되어 블록체인에 포함시킨다. 오디오 시그니처 파일과 원본 음원 파일은 IPFS를 통해 여러 노드로 분할하여 관리한다. 이 때, 블록 트랜잭션 데이터에 포함시킨 각각의 해시 값(2FB9C7AA, C74DFA2B)에 특정 문자나 숫자를 포함시켜 분할된 각 노드의 키값으로 구성한다. [그림 8]의 예에서는 오디오 시그니처 노드의 경우 각각 a2FB9C7AA, b2FB9C7AA, c2FB9C7AA의 해시 값을 키로 갖고, 음원 파일의 노드의 경우 aC74DFA2B, bC74DFA2B, cC74DFA2B의 해시 값을 키로 갖는다. 이를 통해 추후 오디오 시그니처 파일이나 원본 음원 파일에 대한 접근이 가능하다.

제안한 블록체인 데이터에는 오디오 시그니처를 비롯한 음원의 해시 값이 직접적으로 포함된다. 따라서 블록체인 네트워크의 탐색을 통해 트랜잭션 데이터를 비교하여 음원에 대한 저작권 검증이 가능하다. 나아가 P2SH에서 교환 스크립트 작성에 활용한 해시 방법을 적용하여 트랜잭션

데이터에 포함되는 데이터의 크기를 축소시켜 블록 내 포함되는 데이터의 크기를 감소시킬 수 있다.

#### IV. 분산저장시스템 활용을 위한 입출력 비교 실험

특정 음원의 오디오 시그니처를 검증하기 위해서는 IPFS에 저장된 다수의 오디오 시그니처 파일들에 접근하여 서로 비교하여야 한다. 이를 위해 다수의 오디오 시그니처 파일에 대하여 효율적인 탐색과 접근을 통한 빠른 응답이 요구된다. 이에, 본 실험에서는 IPFS와 HTTP 네트워크를 구현하고 파일의 쓰기/읽기 속도를 비교하여 IPFS의 효율성을 검토한다.

##### 1. IPFS와 HTTP네트워크 구성

실험은 IPFS와 HTTP네트워크 모두 동일한 네트워크 상 두 대의 컴퓨터에서 진행하였으며, IPFS의 경우 Unix환경에서 파이썬으로 구현된 오픈소스 라이브러리를 활용하였다. 또한, HTTP네트워크는 windows환경에서 구현하고, MySQL 데이터베이스를 저장소로 사용하였다.

두 가지 환경에서 동일한 크기의 음원 파일에 대하여 각각 쓰기/읽기 속도를 측정 및 비교하여 IPFS의 활용 방안 및 가능성에 대해 검토한다.

## 2. IPFS와 HTTP네트워크 속도 비교 결과

[표 3]은 HTTP 네트워크에서 음원 파일의 쓰기과 읽기에 소요된 시간을 보여준다. 7MB 크기의 음원파일 1개에 대하여 3회의 실험을 한 결과, 쓰기 시간은 평균 0.1초, 읽기 시간은 평균 0.11초로 나타났다. 70MB에 대한 쓰기 시간은 평균 1.18초, 읽기 시간은 평균 1.27초였고, 파일의 크기가 700MB인 경우에는 각각 평균 10.99초, 12.42초로 나타났다.

표 3. HTTP 네트워크에서의 쓰기/읽기 시간  
 Table 3. Writing/reading time on HTTP network

File size \ Try	Writing time(sec)			Reading time(sec)		
	1	2	3	1	2	3
7MB	0.09	0.11	0.10	0.10	0.12	0.11
7MB * 10	1.21	1.23	1.12	1.26	1.30	1.25
7MB * 100	11.01	11.02	10.95	12.02	12.91	12.35

IPFS에 대한 실험결과는 [표 4]의 내용과 같다. 7MB 크기의 음원파일 1개에 대한 쓰기 시간은 평균 0.11초, 읽기 시간은 평균 0.09초로 나타났다. 70MB에 대한 쓰기시간은 평균 1.18초, 읽기 시간은 평균 0.99초였고, 700MB 크기에 대해서는 각각 평균 11.96초, 9.87초로 나타났다.

표 4. IPFS 네트워크에서의 쓰기/읽기 시간  
 Table 4. Writing/reading time on IPFS network

File size \ Try	Writing time(sec)			Reading time(sec)		
	1	2	3	1	2	3
7MB	0.10	0.12	0.11	0.09	0.10	0.09
7MB * 10	1.3	1.4	1.2	1.0	0.99	1.0
7MB * 100	12.0	12.0	11.9	9.89	9.98	9.75

먼저, 쓰기 시간과 읽기 시간을 합친 전체 시간을 비교한 결과, 음원 파일의 크기가 7MB나 70MB로 비교적 작은 경우에는 IPFS와 HTTP 네트워크 간의 속도 차이가 크게 나지 않았다. 하지만, 700MB로 비교적 큰 데이터를 처리할 경우, IPFS가 HTTP 네트워크에 비해 처리속도가 대략 2초 정도 빠른 결과를 얻었다.

쓰기/읽기 시간의 차이를 분석한 결과, HTTP 네트워크

에서는 7MB, 70MB, 700MB인 경우 각각 0.01, 0.09, 1.43초의 차이를 보였다. 또한, 음원 파일의 쓰기에 걸리는 시간보다 읽기에 걸리는 시간이 비슷하거나 조금 더 소요되었다. 이에 비해 IPFS에서는 7MB, 70MB, 700MB인 경우 각각 0.02, 0.19, 2.09초로 HTTP 네트워크에 비해 비교적 값의 차이가 크게 나타났으며, 쓰기 시간에 비해 음원 파일의 읽기에 걸리는 시간이 적게 소요되었다.

이러한 차이는 DHT를 통해 데이터에 접근하는 IPFS의 특징 때문이다. IPFS에서는 데이터를 최초로 저장할 때, 저장된 데이터의 위치를 비롯한 메타데이터를 활용하여 추가로 DHT를 생성한다. 추후 데이터 요청 시, 생성된 DHT를 참조하여 저장된 데이터로의 빠른 접근이 가능하다.

위 실험에서 HTTP 네트워크의 읽기 시간에 비해 IPFS에서의 읽기 시간이 적게 소요되었다. 또한, 음원 파일의 크기가 클수록 HTTP 네트워크와 IPFS 간의 읽기 시간 차이가 크게 나타났다. 이는 데이터의 크기가 커질수록 IPFS의 DHT를 통한 데이터 접근 효율이 증가함을 보여준다. 이러한 IPFS와 DHT의 장점은 블록체인을 통해 생성되는 방대한 양의 데이터와 고용량의 음원 파일을 관리하고 처리하기에 알맞은 대안이 될 수 있다.

## V. 결론 및 향후 연구 과제

최근 비트코인에서는 segwit이라는 방법을 통해 4MB까지 블록의 크기를 확장하려는 시도가 진행되고 있으며, 이더리움도 생성 가능한 블록의 크기를 늘리려는 노력이 진행 중이다. 하지만, 음원이나 그의 시그니처를 블록 내에 포함하기는 불가능하다.

본 논문에서는 1MB 정도의 블록 크기에 음원 및 음원의 오디오 시그니처 정보를 포함시킬 수 있는 방안으로 P2SH에서 활용한 해시연산 방법을 적용하는 가능성을 살펴보았다. 그 결과, 오디오 시그니처의 크기를 20 바이트로 축소시켜 블록체인 블록에 포함시키기에 제약이 없었다.

또한, 오디오 시그니처 파일과 원본 음원 파일의 저장 및 접근에 대하여 효율적인 관리를 위해 IPFS의 활용을 제안하였다. IPFS와 HTTP 네트워크를 통한 음원 및 시그니처



파일의 입출력 비교 실험을 진행하였다. 실험 결과, IPFS의 활용은 블록체인에 저장하는 고용량의 음원 파일 및 관련 메타데이터를 관리 및 저장하기에 보다 효율적인 방안이 될 수 있음을 확인하였다.

향후, 이를 바탕으로 음원의 저작권 검색 및 검증을 위한 실제 서비스를 구현하여, 소요 시간, 비용 등을 비교 분석하는 연구가 필요하다.

### 참 고 문 헌 (References)

- [1] Youtube advertising service, [https://www.youtube.com/intl/ko/ads/?&subid=kr-ko-ha-yt-bk-c-plt!o3~CjwKCAjw0N3nBRBvEiwAHMwvNrmMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc\\_Ad98wAPoh5iTBoCBokQAvD\\_BwE~%7badgroup%7d~kwd-463486203081~1727016377~337034874168&gclid=CjwKCAjw0N3nBRBvEiwAHMwvNrmMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc\\_Ad98wAPoh5iTBoCBokQAvD\\_BwE&gclid=aw.ds](https://www.youtube.com/intl/ko/ads/?&subid=kr-ko-ha-yt-bk-c-plt!o3~CjwKCAjw0N3nBRBvEiwAHMwvNrmMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc_Ad98wAPoh5iTBoCBokQAvD_BwE~%7badgroup%7d~kwd-463486203081~1727016377~337034874168&gclid=CjwKCAjw0N3nBRBvEiwAHMwvNrmMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc_Ad98wAPoh5iTBoCBokQAvD_BwE&gclid=aw.ds) (accessed May. 1, 2019).
- [2] 2018 1st half sector analysis report, <https://www.slideshare.net/MezzoMedia/2018-106564325> (accessed May. 1, 2019).
- [3] Twitch music copyright guide, <https://www.twitch.tv/p/ko-kr/legal/community-guidelines/music/> (accessed May. 1, 2019).
- [4] Youtube music copyright guide, <https://creatoracademy.youtube.com/page/lesson/artist-copyright?hl=ko> (accessed May. 1, 2019).
- [5] Ujo music, <https://www.ujomusic.com> (accessed Jul. 30, 2019).
- [6] COALA IP white paper, <https://github.com/COALAIP/specs> (accessed Jul. 30, 2019).
- [7] D. Bhowmil, A. Natu, T. Ishikawa, T. Feng, C. Abhayaratne, "The Jpeg-Blockchain Framework For Glam Services", 2018 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2018.
- [8] Dejavu project, <https://github.com/worldveil/dejavu> (accessed May. 5, 2019).
- [9] Bitcoin transaction guide, <https://bitcoin.org/en/transactions-guide#introduction> (accessed May. 5, 2019).
- [10] IPFS Documentation, <https://docs.ipfs.io/> (accessed May. 1, 2019).
- [11] K. Lee, S. Kim "Use of blockchain for music content copyright protection", Journal of Broadcast Engineering, Vol.19, No.6, pp.295-299, 2019.

### 저 자 소 개



이 경 식

- 2011년 ~ 2017년 : 명지대학교 컴퓨터공학과 학사
- 2017년 ~ 현재 : 명지대학교 일반대학원 컴퓨터공학과 석사과정
- ORCID : <https://orcid.org/0000-0003-1308-2650>
- 주관심분야 : 4D media, audio contents, VR and Internet of Things, Blockchain



김 상 군

- 1997년 : 아이오와대(Univ. of Iowa)전산과학, B.S.(1991), M.S.(1995), Ph.D(1997)
- 1997년 : 3월 ~ 2007년 2월 : 삼성종합기술원 멀티미디어랩 전문연구원
- 2007년 3월 ~ 2016년 2월 : 명지대학교 컴퓨터공학과 교수
- 2017년 3월 ~ 현재 : 명지대학교 융합소프트웨어학부 데이터테크놀로지전공 교수, 컴퓨터공학과 겸임교수
- ORCID : <https://orcid.org/0000-0002-2359-8709>
- 주관심분야 : digital content(image, video and music) analysis and management, 4D media, Blockchain, VR, Internet of Things and multimedia standardization