

## 유직 콘텐츠 저작권 보호를 위한 블록체인 활용 방안

이경식 \*김상균<sup>1</sup>

명지대학교 \*명지대학교

kyoungsik0702@gmail.com \*goldmunt@gmail.com

### Use of blockchain for music content copyright protection

Kyung - Sik, Lee \*Sang- Kyun , Kim  
Myongji University \*Myongji University

#### 요 약

4 차 산업혁명과 더불어 1 인 미디어 시대를 맞아 개인의 미디어 콘텐츠 제작과 소비가 간편해졌다. 이에, 유튜브, 트위치 등의 플랫폼을 통해 엄청난 양의 미디어 콘텐츠가 생성·소비되고 있다. 이와 관련하여 미디어 콘텐츠의 저작권에 대한 분쟁이 뜨겁다. 특히, 유직(음원)콘텐츠의 경우, 동영상에 비롯한 거의 모든 콘텐츠의 제작에 있어 없어서는 안 될 요소로 자리 잡고 있기 때문에 유직 콘텐츠와 관련된 저작권 분쟁은 더욱 치열하다. 이에, 본 논문에서는 유직 콘텐츠에 대한 저작권 분쟁을 블록체인을 적용하여 해결할 수 있는 방안을 제안한다.

#### 1. 서론

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

이처럼 다양한 플랫폼을 통해 엄청난 양의 콘텐츠가 생성·소비되면서 최근 저작권과 관련된 문제가 대두되고 있다. 특히 음원의 경우, 동영상을 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[3], 유튜브에서는 저작권에 반하는 음원을 사용하여 콘텐츠를 제작하는 경우에 대하여 이로 인해 발생한 수익을 창작자가 배분 받지 못하도록 하는 등의 조치를 취하고 있다[4]. 하지만 이러한 노력에도 불구하고 생산된 모든 콘텐츠에 대하여 확인이 불가능하기 때문에 보다 근본적인 해결책이 요구된다.

이에 음원의 특징을 담은 audio signature 를 추출하여 각 음원들을 구분할 수 있도록 하고, 이를 블록체인을 통해 검증함으로써, 음원의 저작권을 주장할 수 있는 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2 절에서 digital signature 와 블록체인의 적용 사례와 관련하여 동향을 살펴보고, audio signature 추출과 관련된 기술에 대해 파악한다. 3 절에서는 실제 추출한 audio signature 의 결과를 토대로 블록체인을 audio signature 검증에 활용하기 위한 방안에 대해 살펴본다. 4 절에서는 본 논문의 결론과 함께 향후 연구의 방향성을 제시한다.

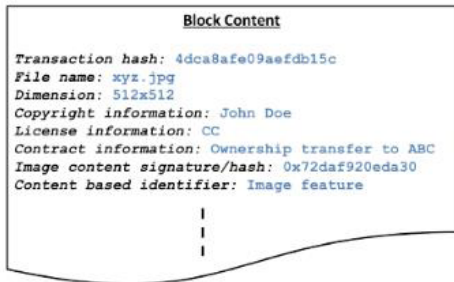
#### 2. 관련 기술

##### 2.1 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 시스템을 구상 중에 있다[5].

JPEG-blockchain framework 에서는 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 정보 역시 포함된다[그림 1].

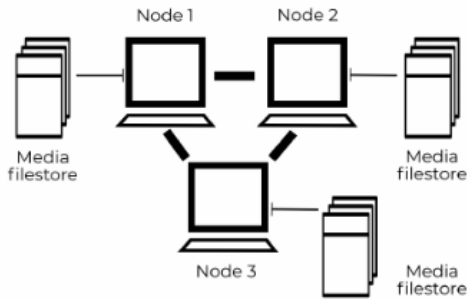
<sup>1</sup> Corresponding Author



[그림 1] JPEG-blockchain 트랜잭션 데이터 예시

블록체인의 블록에 올라갈 수 있는 데이터의 크기에 제약이 있기 때문에, 원본 이미지 파일의 경우 블록체인의 블록에 직접 포함시키기에는 어려움이 따른다. 이를 해결하기 위해 JPEG-blockchain framework에서는 원본 이미지 파일의 경우 별도의 저장소에 파일을 저장하고, 저장된 저장소의 위치정보 역시 블록 트랜잭션 데이터에 포함시키도록 하고 있다.

[그림 2]는 JPEG-blockchain framework의 전체 구성 예시를 보여준다. 각 노드는 블록체인에 등록된 블록을 의미하며, 각 블록의 트랜잭션 데이터에는 파일이 저장된 장소의 위치를 비롯하여, 이미지 파일과 관련된 모든 정보들이 담겨있다. 이를 통해 블록체인을 통한 검증은 물론 원본 이미지 파일로의 접근 역시 가능하다.



[그림 2] JPEG-blockchain 네트워크 구성 예시

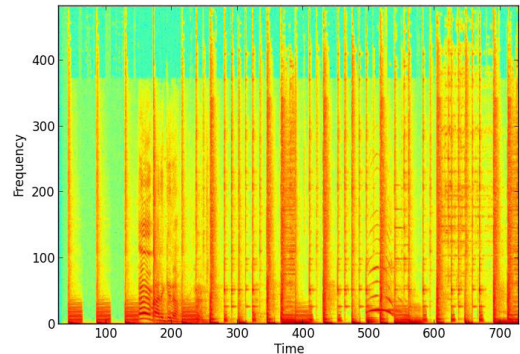
## 2.2 dejavu project

dejavu는 python으로 개발된 오픈소스 프로젝트로써, 입력된 음원에 대해 일련의 처리 과정을 거친 후 각 음원만의 특징을 지닌 audio signature를 추출하도록 한다. 또한, 추출된 각 audio signature들의 비교를 통해 서로 동일한 음원인지의 여부를 판별 가능하다[6].

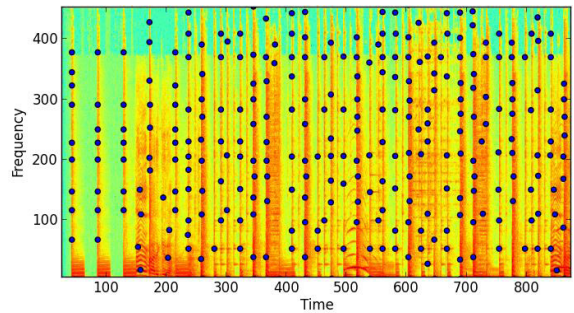
dejavu에서 입력된 음원은 FFT(Fast Fourier Transform)를 통해 파형의 형태를 지닌 spectrogram으로 변환된다. [그림 3]은 FFT를 변환된 음원 파일의 spectrogram 추출 예시를 보여준다. 이후, 변환된 spectrogram에서 각 파형의 peak(최고점)를 검출하여(시간, 주파수)의 쌍으로 나타낸다. [그림 4]는 spectrogram에서 추출한 peak들을 도식적으로 나타낸 결과이다.

이렇게 계산된 peak값들을 나열 후, hash함수를 적용하면 해당 음원의 audio signature를 추출할 수 있다. dejavu에서는 이렇게 얻은 hash값들에 binary과정을 한 번 더 진행하여

최종적으로 이전 hash값에 비해 크기가 감소된 audio signature를 추출한다.



[그림 3] 생성된 spectrogram의 예시



[그림 4] spectrogram에서 추출한 peak(최고점)들의 예시

## 3. 블록체인을 통한 audio signature의 검증

### 3.1 블록체인 활용 방안

블록체인의 블록은 헤더(Header)와 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 hash연산은 단방향 연산만을 수행하기 때문에 암호화 결과의 역산을 통해 이전 블록의 데이터를 복호화하는 것이 어렵도록 설계되어 있다. 또한, 블록체인의 모든 참여자(노드)들은 모두 같은 블록 데이터를 공유하게 되어있기 때문에 데이터의 무결성 보장이 가능하며, 일부 특정 노드나 블록체인 관리자에 의해 무단으로 데이터의 위·변조가 불가능하다.

이러한 블록체인의 특징을 활용하여, 음원의 특징을 추출한 audio signature를 블록체인의 블록에 포함시킨다면 추후 생성될 블록들과의 비교를 통해 해당 음원의 저작권에 대한 검증이 가능하다. 하지만, 현재 대부분의 블록체인은 한 번에 생성 가능한 블록 크기에 제한을 두고 있다. 비트코인의 경우는 1MB로 블록 크기를 제한하고 있다. 이더리움 역시 평균적으로 20KB에서 30KB 정도 크기의 블록이 생성되고 있으며, 최대 1MB까지도 그 크기를 제한하고 있다.

이에, 추출한 audio signature 데이터가 블록체인의 블록 생성 제한 크기를 초과하지 않는지에 대한 검증이 필요하다.

또한, 블록체인과 audio signature 를 통해 저작권에 대하여 검증이 완료되었다 하더라도 추후 원본 파일에 대한 접근이나 비교를 위한 요구 등의 요청이 있을 수 있으므로, 이를 해결하기 위한 추가적인 방안이 요구된다.

### 3.2 Audio signature 추출 결과

먼저, audio signature 를 직접 추출하여 블록체인의 블록에 포함시킬 수 있는 가능성에 대해 파악하고자 한다. audio signature 의 추출 대상으로는 mp3 확장자의 10 개 음원 파일을 선정하였으며, [표 1]에서 각 음원 파일의 재생 시간과 크기를 보여준다. 음원 파일 확장자의 경우, 가장 대중적으로 사용되는 3 개의 확장자(wav, flac, mp3) 중 가장 사용 빈도가 높고, 비교적 음원파일의 크기가 작은 mp3 를 선택하여 테스트를 진행하였다.

음원 파일 번호	재생 시간(초)	크기(MB)	확장자
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

[표 1] 음원 파일의 재생 시간, 파일 크기

선정한 mp3 음원 파일에서 추출한 audio signature 의 크기는 아래 [표 2]의 결과와 같다.

음원 파일 번호	audio signature 크기(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] 추출된 audio signature 의 크기

[표 2]의 데이터를 분석한 결과, 3 번 음원의 audio signature 크기가 6.4MB 로 가장 작았고, 1 번 음원의 audio signature 크기가 9.5MB 로 가장 크게 나타났다. 가장 작은 크기인 3 번 audio signature 조차 블록체인의 생성 가능한 최대 크기인 1MB 를 초과한다.

### 3.3 P2SH(Pay to Script Hash)

비트코인 상의 거래는 트랜잭션에 작성된 스크립트(script) 의 실행을 통해 이루어진다[7]. 스크립트는 잠금 스크립트(Locking script) 와 해제 스크립트(Unlocking script) 로 구분할 수 있다. 잠금 스크립트는 거래를 위해 충족되어야 하는 조건들이 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 public key 를 활용하기 때문에, 거래 실행을 위해서는 private key 를 활용한 해제 스크립트를 제시하여 검증과정을 거쳐야 한다. 하지만, 이러한 방법은 거래에 참여한 대상자가 여럿일 경우, 각 참여자의 public key 를 모두 포함시켜 잠금 스크립트를 작성해야하기 때문에, 그 크기가 커진다는 단점이 있다.

이를 해결하기 위해 P2SH 는 각 참여자의 public key 를 모아 하나의 redeem script 를 생성하고 해시 과정을 거친 후, 거래의 잠금 스크립트 작성에 활용한다. [그림 5]에서는 n 개의 public key 를 사용하여 작성한 redeem script 와 redeem script 의 해시를 활용한 잠금 스크립트 및 해제 스크립트의 작성 예시를 보여준다. 해시 과정을 거쳐 작성된 redeem script 는 20bytes 의 크기로 고정되어 있기 때문에, 거래 참여자의 public key 를 모두 나열하는 기존의 방법에 비해 훨씬 효율적인 공간의 활용이 가능하다.

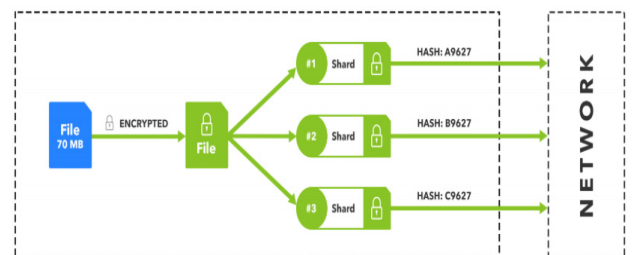
```

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 5] redeem scrip 와 잠금, 해제 스크립트

### 3.4 IPFS(InterPlanetary File System)

IPFS 는 Torrent 로 대표되는 P2P 기반의 분산파일저장 방법으로써, 하나의 파일을 여러 개의 조각으로 나누어 관리하도록 하는 방법이다[8]. IPFS 에서는 먼저 원본데이터 파일의 위·변조가 불가능하도록 일련의 암호화 과정을 거친다. 이후 암호화된 파일은 보다 작은 크기의 여러 개의 샤드(Shard) 로 분할하고, IPFS 에 연결된 여러 노드들에 분산되어 저장된다.



[그림 6] IPFS 샤드 분할 및 DHT 적용 예제

여러 노드에 분산 저장된 데이터들은 DHT(Distributed Hash Table) 라는 구조를 통해 관리된다. 분할된 노드들은 각각

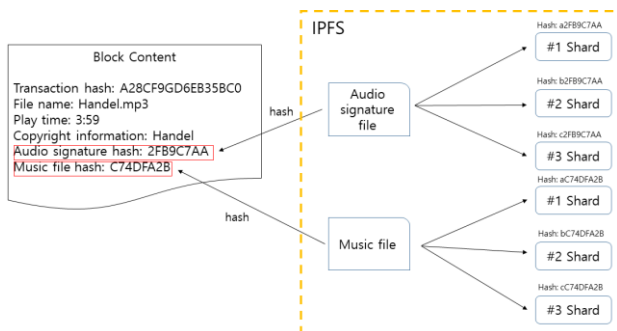
key, value 쌍의 구조를 지니며, 각 노드를 구별할 수 있는 고유한 해시 값을 key 값으로 가진다. value 값에는 해당 노드가 저장된 위치나 자신과 관련이 있는 노드의 정보가 담겨있다.

[그림 6]의 예시에서 70MB 크기의 파일을 IPFS 를 사용하여 3 개의 노드로 분할하였다. 분할된 노드들은 DHT 를 통해 관리되기 때문에 각각 key, value 의 값을 갖는다. 각 노드들은 원본 파일의 해시 값(9627) 에 특정 문자나 숫자를 추가하여(A9627, B9627, C9627) key 값으로 사용한다. 이는 분할된 각 노드들이 9627 의 해시 값을 갖는 원본파일로부터 분할되었다는 것을 의미한다. 분할된 각 노드들은 value 값으로 자신이 저장된 저장소의 위치를 갖고 있기 때문에 원본 파일로의 통합이나 관리가 가능하다.

### 3.5 제안하는 방법

P2SH 에서 해시 함수를 적용하여 redeem script 의 크기를 20bytes 의 고정 크기로 축소시킨 방법을 추출한 audio signature 와 원본 음원 파일에 적용한다. 이렇게 생성된 audio signature 와 음원 파일의 20bytes 해시 값을 블록 트랜잭션 데이터에 추가하여 블록체인에 포함시킨다.

audio signature 파일과 음원 파일의 경우, IPFS 를 활용하여 별도의 노드로 분할하여 관리한다. IPFS 의 노드들은 DHT 구조를 갖고 있기 때문에 추후 audio signature, 혹은 원본 음원 파일에 대한 비교 요구에 응할 수 있다.



[그림 7] 블록체인을 활용한 audio signature 및 음원파일 검증 방법

[그림 7]은 본 논문에서 제안한 방법의 활용 예시를 보여준다. 추출한 audio signature 와 원본 음원 파일에 해시함수를 적용하여 각각 20bytes 크기의 해시 값(2FB9C7AA, C74DFA2B) 을 추출한다. 이렇게 얻은 해시 값은 블록 트랜잭션 데이터에 추가되어 블록체인에 포함시킨다. audio signature 파일과 원본 음원 파일은 IPFS 를 통해 여러 노드로 분할하여 관리한다. 이 때, 블록 트랜잭션 데이터에 포함시킨 각각의 해시 값(2FB9C7AA, C74DFA2B) 에 특정 문자나 숫자를 포함시켜 분할된 각 노드의 key 값으로 활용한다. [그림 7]의 예에서 audio signature 노드의 경우 각각 a2FB9C7AA, b2FB9C7AA, c2FB9C7AA 의 해시 값을 갖고, 음원 파일의 노드의 경우 aC74DFA2B, bC74DFA2B, cC74DFA2B 의 해시 값을 key 로 갖는다. 이를 통해 추후 audio signature 파일이나 원본 음원 파일에 대한 접근이 가능하다.

### 4. 결론 및 향후 연구 과제

최근 비트코인에서는 segwit 이라는 방법을 통해 4MB 까지 블록의 크기를 확장하려는 시도가 진행되고 있으며, 이더리움도 생성 가능한 블록의 크기를 늘리려는 노력이 진행 중이다. 하지만, 비트코인과 segwit 을 활용하여 4MB 의 블록이 생성 가능하더라도 본 논문에서의 결과로 얻은 가장 작은 audio signature 의 데이터조차 당기에 한계가 있었다.

이에, 1MB 정도의 블록 크기에 audio signature 를 포함시킬 수 있는 방안으로 P2SH 를 적용하는 가능성을 살펴보았다. 그 결과, audio signature 의 크기를 20 바이트로 축소시켜 블록체인 블록에 포함시키기에 제약이 없었다. 또한, IPFS 를 적용하면 audio signature 의 해시 값을 통해 원본 파일의 저장 및 접근에 대한 관리가 가능하다는 결론을 얻었다.

다만, 본 논문에서는 제안한 두 가지 방법에 대하여 주로 블록의 크기(Scalability) 에 중점을 두고 연구를 진행하였으며, 소요 시간, 비용 등 효율성의 측면에서는 고려하지 않았다. 이에, 사후 연구로 실제 시스템을 구현하여 구체적인 조건에 대한 실험이 요구된다.

### 감사의 글

본 논문은 2019 년 정부(산업통상자원부)의 재원으로 한국산업기술평가관리원의 지원을 받아 수행된 연구임(1415162348, 미디어사울인터넷 거래 및 컴팩트 데이터 표현을 위한 표준 기술 개발).

### 참고 문헌

[1] Youtube 광고 서비스, [https://www.youtube.com/intl/ko/ads/?&subid=kr-ko-ha- yt-bk-c-pit!o3~CjwKCAjw0N3nBRBvEiwAHMwvNrnMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc\\_Ad98wAPoh5iTBoCBokQAvD\\_BwE~%7badgroup%7d~kwd-463486203081~1727016377~337034874168&gclid=CjwKCAjw0N3nBRBvEiwAHMwvNrnMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc\\_Ad98wAPoh5iTBoCBokQAvD\\_BwE&gclsrc=aw.ds](https://www.youtube.com/intl/ko/ads/?&subid=kr-ko-ha- yt-bk-c-pit!o3~CjwKCAjw0N3nBRBvEiwAHMwvNrnMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc_Ad98wAPoh5iTBoCBokQAvD_BwE~%7badgroup%7d~kwd-463486203081~1727016377~337034874168&gclid=CjwKCAjw0N3nBRBvEiwAHMwvNrnMfFqjLUOGS-OMsm8jSxcjPkAlx9Mon7z3BRJc_Ad98wAPoh5iTBoCBokQAvD_BwE&gclsrc=aw.ds), (accessed May. 1, 2019).

[2] 2018 상반기 업종분석 리포트, <https://www.slideshare.net/MezzoMedia/2018-106564325>, (accessed May. 1, 2019).

[3] 트위터 음악 저작권 가이드, <https://www.twitcr h.tv/p/ko-kr/legal/community-guidelines/music/>, (accessed, May. 1, 2019).

[4] Youtube 음악 저작권 가이드, <https://creatoracademy.youtube.com/page/lesson/arti st-copyright?hl=ko>, (accessed May. 1, 2019).

[5] 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.

[6] Dejavu project,  
<https://github.com/worldveil/dejavu> , (accessed May. 5, 2019).

[7] Bitcoin transaction guide,  
[https://bitcoin.org/en/transactions – guide#introduction](https://bitcoin.org/en/transactions-guide#introduction), (accessed May. 5, 2019).

[8] IPFS Documentation, <https://docs.ipfs.io/>,  
(accessed May. 1, 2019).