디지털 콘텐츠 자기주권 신원 관리를 위한 DID 연구

백영태O, 민연아*
OO김포대학교 멀티미디어과,
*한양사이버대학교 응용소프트웨어공학과
e-mail: hannae@kimpo.ac.krO, yah0612@hycu.ac.kr*

A study on DID self-sovereign identity for digital content management

Baek, YeongTaeO, Min Youn A*
ODept. of Multimedia, Kimpo University,
*Dept. of Applied Software Engineering, hanyang cyber University

● 요 약 ●

본 논문에서는 디지털 콘텐츠의 유통과정의 복잡함과 창작자에 대한 권리를 보장하기 위하여 블록체인 기반 플랫폼을 통하여 투명하고 무결성이 보장된 자기권한 관리가 가능하도록 DID(Decentralized Identity)의 적용을 연구하였다. DID의 효율적 적용을 위하여 DID문서와 Verifiable Credential과 presentation의 관리상 특징을 고려하고 DID를 통한 인증과정에서 발생하는 다양한 메타데이터에 대하여 차별화된 암호화 기법 적용이 가능하도록 하였다. 본 논문의 연구를 통하여 디지털 콘텐츠에 대한 자기권한 관리가 보다 간단해지고 권리인증 과정 시 안정된 성능 제공이 가능할 것으로 사료된다.

키워드: 디지털 콘텐츠(Digital Content). DID(Decentralized IDentity), 블록체인(Block Chain)

I. Introduction

스마트 디바이스와 네트워크의 발전에 힘입어 디지털 콘텐츠 수요가 모바일 중심으로 증가하고 있으며 창작자에 대한 디지털 권리 관리에 대한 관심이 높아지고 있다[1]. 디지털 권리관리란 저작권자가 자신이 제작한 자료에 대한 사용권을 제어 및 제한하는데 사용되는 모든 기술을 지칭한다[2].

최근 증가하는 디지털 콘텐츠에 대하여 디지털 권리에 대한 투명한 관리의 필요성과 디지털 콘텐츠 창작자에 대한 권익을 보장하기 위하여 블록체인 기반 DID(DID, Decentralized IDentity)의 기술 적용이 필요하다.

II. Preliminaries

1. Related works

스마트 시대에 따라 다양한 창작자에 의한 디지털콘텐츠가 다량으로 게시되고 있다. 이에 따라 디지털 콘텐츠의 저작권의 투명한 인증 및 이력관리를 통한 창작자 보호에 대한 관심이 높아지고 있다.

Table 1. Infringement of copyrighted works by content[3]

No	contens	Infringement scale
1	Movie	772 billion Won
2	Music	609 billion Won
3	Game	518 billion Won
4	Publishing	312 billion Won
5	Broadcast	176 billion Won

2015년 보고된 조사에 의하면 2013년의 디지털 콘텐츠 불법복제물에 의한 시장침해 비율은 81.6%이며 유통의 피해액은 2조3천억원에 달한다[3].

블록체인은 분산네트워크상의 노드들 간 분산원장을 관리하는 탈중앙화 지향 시스템으로 디지털 콘텐츠의 권한관리에 필요한 투명한 이력관리 및 인증과정에 대한 관리가 가능하다[4][5].

최근 빠르고 투명한 인증이 가능한 블록체인 기반 신원인증(DID)에 대한 관심이 높아지고 있다.

DID는 기존 개인정보를 보관하던 서비스 중개기관이 개인정보를 관리하지 않고 분산네트워크를 통하여 신원증명이 가능한 차세대 개인인증 기술이다[5][6].

DID는 개인정보 및 각종 인증에 대한 내용을 자신이 직접 관리하거나, 발급기관별 공개키의 공유를 통하여 신뢰를 기반으로 인증 및

관리를 한다[5].

DID 활용 사례로 2020년 기준 경상남도의 'DID기반 디지털 공공서비스 플랫폼 구추 사업' 및 병무청의 '블록체인 간편인증 서비스' 및 금융권의 인증서 발급 등도 DID 기반의 블록체인 기반 신원인증사업을 들 수 있다[5][6][7].

기존의 중개기관을 통한 인증 시에는 전자서명 진위판별을 중개기관 중심으로 처리하였다. 하지만 DID의 경우 분산된 네트워크에 연결된 기관들이 공유한 공개키를 통하여 개인정보에 대한 진위판별을 기관 스스로 처리할 수 있다. 이 과정에서 합의알고리즘을 통하여 인증과정의 무결성을 보증할 수 있다.

III. The Proposed Scheme

본 논문에서는 디지털 콘텐츠의 자기주권관리를 위한 방법으로 DID의 활용가능성을 연구하였으며 상세 방법으로 디지털 저작권리의 특징을 감안하여 자기주권관리ID 및 인증과정에 대한 메타데이터의 암호화 방법을 연구하였다.

Verifiable Credential을 통하여 관리되는 개인정보에는 발급자 정보 및 자격정보, 발급자 서명 등 매우 중요한 증명정보가 포함되기 때문에 암호화된 형태나 월렛을 통한 관리 등이 이루어진다. Table.2은 Verifiable Credential의 sample 코드이다.

Table 2. Verifiable Credential Sample

```
Verifiable Credential
{
  "@context": "https://w3id.org/future-method/v1",
  "id": "did:example:01234..#keys-1.",

  "publicKey": [{
    "id": "did:example::01234..#keys-1",
    "type": "RsaVerificationKey2020",
    "controller": "did:example::01234..",
    "publicKeyPem": "----about public key-----₩r₩n"
  }, {
    "id": "did:example::01234..#keys-2",
    "type": "Ieee2410VerificationKey2018",
    "controller": "did:example:01234..",
    "publicKeyPem": "----about public key-----₩r₩n"
  }],
```

본 논문에서는 Verifiable Credential에 대한 메타데이터 중 해시함수에 대한 암호화 처리 및 신뢰 노드에의 공유를 통하여 자기권한관리가 보다 간단해지고 권리인증 과정 시 안정된 성능 제공이 가능하다.

IV. Conclusions

본 논문에서 제안한 자기주권 ID관리를 위한 연구방법으로 DID문서관리의 이원화 및 Verifiable Credential 및 Verifiable Presentation의 메타데이터에 대한 암호처리 및 관리방법을 제안하였다. 해당 방법에 대하여 DID문서관리 및 인증과정이 간단해지고 보다 안정된 성능으로 블록체인기반 기술 활용이 가능하다.

REFERENCES

[1] RS Global, "Digital Content Market Outlook and Technology Development Strategy (5G Commercialized in 2019)", 2019.07

[2] https://ko.wikipedia.org/wiki/%EB%94%94%EC%A7%80%ED%84%B8_%EA%B6%8C%EB%A6%AC_%EA%B4%80%EB%A6%AC

[3] G.J.Ryu, "ICO Main factor to promote convergence of digital content industry and blockchain technology", Journal of the Korea Contents Association, 2019

[4] https://medium.com/iotrustlab/did-decentralized-id-%EB%8A%94-%EC%96%B4%EB%96%BB%EA%B2%8C-%EB%8F%99%EC%9E%91%ED%95%A0%EA%B9%8C-857ca824ea0

[5] https://www.mk.co.kr/news/it/view/2020/05/543989/

[6] Korea Information Technology Agency, “Disclosure of digital ID authentication service using blockchain,” D.gov, 2017.11.

[7] Song Min-jung, “Identifying the identity of the digital age and linking blockchain technology,”2017.12 from http://www.hellot.net/new_hellot/magazine/magazine_read.html?code=202&idx=38221&public_date=2017-12"