

지혜콘텐츠 유통에 적합한 스마트계약 기반 저작권 보호 모델

윤성현*

백석대학교 ICT학부 교수

The Smart Contract based Copyright Protection Model for Wisdom Contents Distribution

Sunghyun Yun*

Professor, Division of ICT, Baekseok University

요약 지혜콘텐츠는 일반인에 의해서 만들어지며 생활에 필요한 유용한 팁들로 구성된다. 기존의 저작권 보호 시스템은 주로 전문 저작자 또는 기업을 대상으로 하기 때문에 일반인들이 사용하기에는 그 절차가 까다롭고 비용이 많이 소요된다. 블록체인 기반 시스템은 제 3자의 도움 없이 구성원들의 자발적 기여로 블록에 저장된 트랜잭션을 검증할 수 있다. 따라서, 지혜콘텐츠 저작자의 저작권 보호를 위해서는 블록체인 기반의 저작권 보호 모델이 적합하다. 본 논문에서는 블록체인 네트워크에서 실행되는 스마트계약 기반의 저작권 보호 모델을 제안한다. 제안한 모델은 스마트계약 발행, 콘텐츠 구매 그리고 수익 분배 단계로 구성된다. 판매자와 저작자 간의 계약 합의를 위하여 디지털 서명 기법이 적용된다. 스마트계약은 저작자 정보, 콘텐츠 정보, 그리고 지분 비율을 상태로 저장한다. 지혜콘텐츠 구매 시 구매 대금은 스마트계약으로 전송되며 계약에 명시된 지분 비율에 따라서 저작자와 판매자 주소로 재분배된다. 제안한 모델은 일반인 저작자들이 카페, 블로그, 유튜브 등의 지혜콘텐츠를 등록 및 관리하는데 적합하다.

주제어 : 블록체인, 스마트계약, 지혜콘텐츠, 수익 분배, 저작권 보호

Abstract Wisdom contents is made by an ordinary person and contains life tips helpful in general. As the existing copyright management systems are designed for the corporate or professional authors, it's not easy to use and requires high cost for the ordinary person to get the copyright. Blockchain based system can notarize the block of transactions without help of trustful third party such as existing copyright protection center. Thus, blockchain based copyright protection model is needed to protect the ordinary author's copyright. In this study, we propose the smart contract based copyright protection model which run on the blockchain network. The proposed model consists of smart contract creation, contents purchase and profit sharing stages. The digital signature scheme is used to get the contract agreed by the seller and the author. The smart contract stores the author information, contents information and the percentage of the share as states. If the contents is sold, the sales tokens are redistributed to the author and the seller according to the share. The proposed model can be applied to the ordinary person's copyright registration and management for Wisdom contents distributed in cafe, blog, YouTube, etc.

Key Words : Blockchain, Smart Contract, Wisdom Contents, Profit Sharing, Copyright Protection

1. 연구 배경

스마트계약은 블록체인 네트워크에서 실행되는 컴퓨터 프로그램으로 트랜잭션에 저장되어 배포된다. 스마트 계약은 컴퓨터 프로그램이기 때문에 다목적으로 응용될 수 있으며 이더리움 블록체인에서 처음 그 개념이 소개되고 적용되었다[1,2]. 이더리움 네트워크에 접속된 노드들은 EVM(Ethereum Virtual Machine) 모듈만 있으면 블록체인에 저장된 스마트계약을 실행할 수 있다. 자바 바이트코드를 JVM(Java Virtual Machine)에서 실행하는 것과 비슷한 원리이다. 스마트계약은 이더리움을 비롯한 많은 블록체인에서 각각의 목적에 따라서 사용되는데 [3], 본 논문에서 제안하는 스마트계약은 이더리움 블록체인을 기반으로 한다.

블록체인은 기존의 데이터베이스와 마찬가지로 정형화된 구조의 데이터를 저장한다. 기존의 서버 기반의 데이터베이스 시스템은 데이터 무결성을 보장받으려면 서버를 전적으로 신뢰해야 하는데, 블록체인은 구성원들의 자발적 기여로 블록체인에 저장된 데이터의 무결성을 보장할 수 있다. 만약 서버를 신뢰할 수 없다면, 서버에 의한 데이터베이스 조작이 가능하다. 블록체인에 참여한 노드들 중에서 채굴자들은 합의 알고리즘에 따라서 블록을 결정하고 이를 블록체인에 저장하는 역할을 수행한다. 업데이트된 블록체인은 채굴자 및 구성원들이 동일한 복사본을 저장하기 때문에 블록체인에 저장된 데이터를 조작하는 것은 계산상 불가능하다. 더불어, 블록체인에 참여한 모든 노드가 동시에 정지하지 않는 한 블록체인 서비스는 멈추지 않기 때문에 가용성이 매우 높다[3, 4].

블록체인 네트워크에서 실행되는 DApp(Distributed App)의 일종인 스마트계약은 컴퓨터 프로그램이기 때문에 다목적으로 블록체인을 활용할 수 있게 해준다. 스마트계약은 다른 스마트계약의 함수를 호출할 수 있고, 웹 등의 프론트엔드 프로그램은 여러 개의 스마트계약 프로그램들을 연동할 수 있다[5].

지혜콘텐츠는 생활에 도움이 되는 일반인들의 아이디어와 경험으로 구성되며 유튜브, 카페, 블로그 등과 같은 인터넷 커뮤니티에서 유통된다[6, 7]. 기존의 저작권 보호 시스템은 콘텐츠 개발 전문 기업과 전문 저작자를 대상으로 한다. 한국저작권정보원과 같은 정부기관의 감독 하에 저작권 관리가 이루어진다. 일반인들이 사용하기에는 비용이 많이 들고 등록 절차가 복잡하기 때문에 대부분의 지혜콘텐츠는 저작권 등록 없이 인터넷에 직접 배포된다[8, 14, 15].

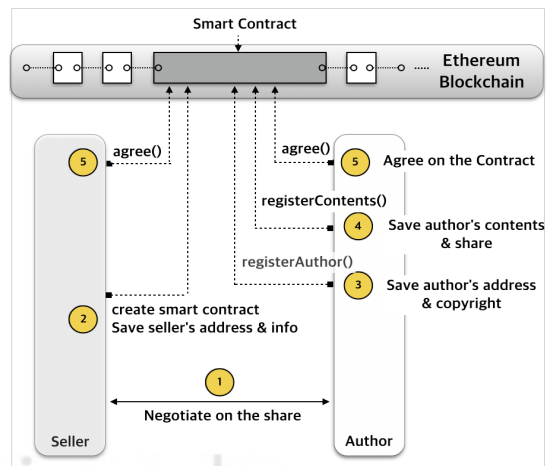
인터넷과 스마트폰의 보급으로 지혜콘텐츠에 대한 수요는 계속 확산되어 가고 있으며 이를 활용한 새로운 비즈니스 모델이 폭 넓게 보급되고 있는 추세이다[9, 10]. 하지만 저작권 보호 기반이 취약한 지혜콘텐츠는 항상 불법 복제 및 배포의 위험성이 높기 때문에, 원저작자의 저작 의욕을 감소시키고 관련 콘텐츠의 보급에 걸림돌이 될 수 있다[11, 12, 13]. 따라서 일반인도 손쉽게 저작물을 등록하고 그 권리를 보호받을 수 있는 새로운 유형의 저작권 보호 모델의 개발이 필요하다.

블록체인 기술은 커뮤니티 구성원들의 자발적 참여로 서로 부정할 수 없는 증거를 만들어낼 수 있다. 저작권보호원과 같은 신뢰할 수 있는 제 3의 기관이 필요 없기 때문에 지혜콘텐츠를 위한 저작권 보호 기반으로 최적이다.

본 논문에서는 블록체인으로 지혜콘텐츠 저작권을 관리할 수 있는 스마트계약 모델을 제안한다. 제안한 모델은 스마트계약 생성, 지혜콘텐츠 구매 및 수익 분배 단계를 포함한다. 저작자 정보, 콘텐츠 정보, 판매 대금에 대한 지분 비율은 스마트계약의 상태로 저장한다. 저작자 등록, 콘텐츠 등록, 구매, 수익 분배 프로세스는 프론트엔드에서 사용할 수 있도록 스마트계약의 함수로 설계한다.

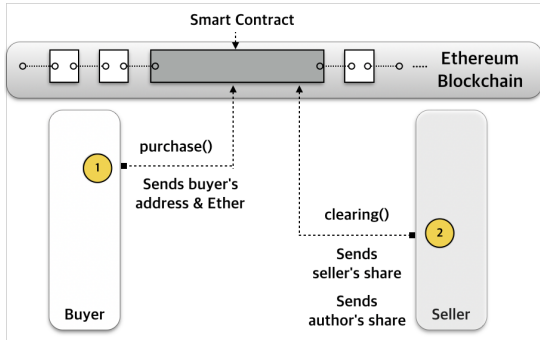
블록체인에 등록된 콘텐츠의 지분 비율과 이에 따른 수익 분배는 변조할 수 없는 스마트계약 함수에 의해서 실행된다. 실행 결과는 새로운 트랜잭션에 포함되어 블록체인에 저장되기 때문에 지혜콘텐츠 저작자와 판매자는 공정하고 투명한 거래를 보장받을 수 있다.

2. 제안한 모델



[Fig. 1] Copyright Registration & Share Agreement

그림 1과 그림 2는 스마트계약 기반의 저작권 보호 및 수익 분배 모델을 보여준다. 제한한 모델은 저작자 등록, 판매자 등록, 콘텐츠 등록, 콘텐츠 구매, 지분에 따른 수익 분배 단계로 구성된다. 계약 생성을 위해서 판매자와 저작자는 사전에 지분 비율에 동의해야 한다. 스마트계약은 판매자에 의하여 생성되며 동일한 콘텐츠이어도 판매자에 따라서 지분 비율은 변할 수 있다.



[Fig. 2] Contents Purchase & Profit Sharing

가정 1. 스마트계약의 상태로 저장되는 저작자, 판매자, 콘텐츠, 구매 내역, 정산 내역에 대한 데이터 구조는 다음과 같이 정의한다.

- 저작자 정보를 저장하기 위한 구조체는 저작자의 이더리움 주소 EA(External Address), 소속, 이름 등의 개인 정보로 구성된다.

```
struct Author {
    address aAddr;
    // 저작자 소속, 기관 등
    // 본인을 식별할 수 있는 정보로 구성
}
```

- 판매자 정보를 저장하기 위한 구조체는 판매자의 EA, 쇼핑몰 URL, 상호명 등의 정보로 구성된다.

```
struct Seller {
    address sAddr;
    bytes32 sUrl; // 쇼핑몰 URL
    // 기타 판매자 정보로 구성(명칭 등)
}
```

- 지혜콘텐츠 정보를 저장하기 위한 구조체는 지혜콘텐츠 해쉬값, 저작자 구조체 Author, 판매자 구조체 Seller, 저작자와 판매자의 지분 비율로 구성된다. 지분의 단위는 %이며 저작자의 지분은 share이고 판매자의 지분은 100-share가 된다.

```
struct Contents {
    bytes32 chash; // 지혜콘텐츠 해쉬값
    Author owner; // 콘텐츠 저작자
    Seller seller; // 콘텐츠 판매자
    uint share; // 저작자 지분 (%)
}
```

- 구매 내역을 저장하기 위한 구조체는 지혜콘텐츠 구조체 Contents, 구매자의 EA, 구매자의 송금액으로 구성된다. 송금액은 구매자가 이더 단위의 콘텐츠 구매 대금을 스마트계약으로 전송한 값이다.

```
struct Purchase {
    Contents contents; // 구매 콘텐츠
    address pAddr; // 구매자 주소
    uint amount; // 구매 대금(단위: ETH)
}
```

- 정산 내역을 저장하기 위한 구조체는 구매 내역 구조체 Purchase, 저작자의 EA, 저작자에게 송금한 이더, 판매자의 EA, 판매자에게 송금한 이더로 구성된다.

```
struct ProfitShare {
    Purchase contents; // 구매 정보
    address pAddr; // 저작자 주소
    uint pAmount; // 송금액(단위: ETH)
    address sAddr; // 판매자 주소
    uint sAmount; // 송금액(단위: ETH)
}
```

가정 2. 스마트계약에서 계약 합의, 저작자 등록, 판매자 등록, 콘텐츠 등록, 구매, 정산을 위한 함수는 다음과 같이 정의한다.

- agree()
 - 저작자 및 판매자에 의해서 호출된다. 저작자 및 판매자는 스마트계약에 대해서 동의하면 이 함수를 호출하여 각자의 서명을 스마트계약으로 전송한다. agree 함수는 verify 함수를 호출하여 저작자 및 판매자의 서명을 검증하고 이 값들을 상태로 저장한다. 저장된 서명은 업데이트 할 수 없도록 설정한다.
- verify()
 - 저작자 및 판매자의 서명을 검증한다.
- registerAuthor()
 - 저작자에 의해서 호출되며 저작자 정보를 스마트계약으로 전송한다. registerAuthor 함수는 저작자 정보를 상태로 저장한다.
- registerContents()
 - 저작자에 의해서 호출되며 지혜콘텐츠 정보를 스마트계약으로 전송한다. registerContents 함수는 콘

텐츠 정보를 상태로 저장한다. 지혜콘텐츠는 저작자가 생성한 콘텐츠 해쉬값으로 식별된다.

- purchase()

구매자에 의해서 호출된다. 구매자가 쇼핑몰에서 지혜콘텐츠를 구매하면 구매 대금을 스마트계약으로 전송한다. purchase 함수는 전송된 구매 대금을 확인하고 구매 내역을 상태로 저장한다. clearing 함수를 호출하여 정산을 한다.
- clearing()

purchase 함수에 의해서 자동으로 호출된다. 상태로 저장된 지분 비율에 따라서 구매 대금을 저작자와 판매자에게 재분배한다.

가정 3. 스마트계약은 판매자에 의해서 생성되고 이더리움 블록체인에 등록된다. 판매자가 스마트계약을 생성하면 생성자 함수가 호출되어 판매자 정보가 등록된다.

가정 4. 스마트계약에 저장되는 판매자의 서명, 저작자의 서명, 지분 비율은 스마트계약이 소멸될 때 까지 수정할 수 없다.

2.1 스마트계약 생성 및 발행

- 단계 1: 판매자와 저작자는 콘텐츠 판매 가격과 지분 비율을 협의한다.
- 단계 2: 판매자는 스마트계약을 생성한다. 생성자 함수가 호출되어 판매자 정보를 스마트계약의 상태로 저장한다.
- 단계 3: 스마트계약이 포함된 트랜잭션은 채굴자에 의해서 블록에 포함된다.
- 단계 4: 블록에 포함된 스마트계약 트랜잭션은 합의 알고리즘에 의하여 블록체인에 등록된다.

2.2 저작자 및 저작물 등록

- 단계 1: 저작자는 스마트계약의 registerAuthor 함수를 호출하여 저작자 주소, 이름, 소속 등의 정보를 스마트계약으로 전송한다.
- 단계 2: 스마트계약은 저작자 정보를 상태로 저장한다.
- 단계 3: 저작자는 스마트계약의 registerContents 함수를 호출하여 저작자 주소, 판매자 주소, 지분 비율을 스마트계약으로 전송한다.
- 단계 4: 스마트계약은 콘텐츠 정보를 상태로 저장한다.

2.3 계약 합의

- 단계 1: 저작자는 스마트계약에 저장된 저작자 정보, 콘텐츠 정보, 판매자 정보, 지분 비율을 확인한 후에 agree 함수를 호출하여 저작자의 서명을 스마트계약으로 전송한다.
- 단계 2: 판매자는 스마트계약에 저장된 저작자 정보, 콘텐츠 정보, 판매자 정보, 지분 비율을 확인한 후에 agree 함수를 호출하여 판매자의 서명을 스마트계약으로 전송한다.
- 단계 3: agree 함수는 verify 함수를 호출하여 저작자와 판매자의 서명이 올바른지 검증한다. 검증에 성공하면 단계 4를 진행하고, 그렇지 않으면 agree 함수로 생성된 트랜잭션을 롤백한다.
- 단계 4: agree 함수는 저작자 서명과 판매자 서명 상태를 저장한다.
- 단계 5: 모든 구성원들은 스마트계약의 verify 함수를 호출하여 계약이 유효한 지 확인할 수 있다.

2.4 콘텐츠 구매

- 단계 1: 구매자는 purchase 함수를 호출하여 콘텐츠 구매 대금을 스마트계약으로 전송한다.
- 단계 2: purchase 함수는 구매자가 보낸 이더가 판매 대금과 맞는지 검증한다. 검증에 성공하면 단계 3을 진행하고, 그렇지 않으며 purchase 함수로 생성된 트랜잭션을 롤백한다.
- 단계 3: purchase 함수는 구매 내역을 상태로 저장한다.
- 단계 4: purchase 함수는 clearing 함수를 호출한다.

2.5 수익분배

- 단계 1: clearing 함수는 지분 비율에 맞게 콘텐츠 판매 대금을 저작자와 판매자에게 재분배한다.
- 단계 2: clearing 함수는 정산 내역을 상태로 저장한다.

3. 안전성 분석

제안한 스마트계약 모델에서 판매자와 저작자가 계약 내용과 수익 분배에 대해서 부인할 수 없음을 분석한다.

정리 1. 판매자와 저작자는 스마트계약 내용에 대해서 부인할 수 없다.

(증명) 판매자와 저작자는 블록체인에 등록된 스마트 계약을 조회하여 사전에 합의한 계약과 맞는지 확인한다. 사전 합의된 계약과 맞으면 판매자와 저작자는 agree 함수를 호출하여 각각의 디지털 서명을 스마트계약으로 전송한다. agree 함수는 서명을 검증하고 올바른 서명이면 스마트계약의 상태로 저장한다. 함수 호출로 생성되는 스마트계약 트랜잭션은 채굴자들에 의해서 이더리움 블록체인에 등록된다. 이더리움 블록체인의 특성상 블록체인에 등록된 트랜잭션은 변조할 수 없다. 판매자의 서명과 저작자의 서명은 블록체인에 등록되고 이 상태 변수 값은 가정 4에 의해서 업데이트 될 수 없다. 모든 구성원은 디지털 서명 검증을 위해서 verify 함수를 호출하여 판매자 및 저작자의 서명을 검증할 수 있다. 따라서 서명 생성 및 검증에 사용된 디지털 서명이 안전하다고 가정하면 판매자와 저작자는 상호 합의한 스마트계약에 대해서 부인할 수 없다. Q.E.D.

정리 2. 판매자와 저작자는 스마트계약에 의해서 판매 대금이 공정하게 분배되었음을 부인할 수 없다.

(증명) 판매자와 저작자에 의해서 사전 합의된 지분 비율은 스마트계약의 상태로 저장된다. 정리 1과 마찬가지로 지분 비율은 블록체인에 등록되고 가정 4에 의해서 수정할 수 없다. 쇼핑몰에서 지혜콘텐츠가 판매되면 구매자는 스마트계약의 purchase 함수를 호출하여 구매 대금을 스마트계약으로 전송한다. purchase 함수는 clearing 함수를 호출하여 판매자와 저작자에게 지분에 따라서 판매 대금을 재분배하고 거래 내역과 정산 내역을 상태로 저장한다. purchase 함수에 의해서 거래 내역과 정산 내역이 포함된 트랜잭션이 발행되어 블록체인에 등록된다. 따라서 판매자와 저작자는 판매 대금 재분배가 공정하게 이루어졌음을 부인할 수 없다. Q.E.D.

4. 결론

본 논문에서는 지혜콘텐츠를 만드는 일반인 저작자에게 적합한 스마트계약 기반의 저작권 보호 모델을 제안하였다. 제안한 스마트계약 기반 모델은 저작자 등록, 콘텐츠 등록, 판매자 등록, 콘텐츠 구매 그리고 수익 분배 단계로 구성된다. 스마트계약은 판매자에 의해서 발행되고 동일한 콘텐츠이어도 판매자가 다르다면 지분 비율을 달리하여 새로운 계약을 생성할 수 있다. 콘텐츠 구매 및

수익 분배를 위한 함수는 저작자와 판매자가 스마트계약에 합의하여 서명했을 경우에만 호출할 수 있다. 디지털 서명의 특성 상 저작자와 판매자는 합의한 스마트계약에 대해서 상호 부인할 수 없다. 스마트계약의 상태는 갱신될 때 마다 블록체인에 등록되기 때문에 제 3자의 도움 없이 그 내용의 무결성을 보장할 수 있다. 따라서 제안한 모델은 일반인들이 저작하는 지혜콘텐츠를 위한 저작권 보호 모델로 적합하다.

REFERENCES

- [1] R.Modi, Solidity Programming Essentials, Packet Publishing, 2018.
- [2] Ethereum Foundation, <https://ethereum.org/>, 2019.
- [3] Melanie Swan, Blockchain, O'Reilly, 2015.
- [4] A.M.Antonopoulos, Mastering Bitcoin 2nd Edition, O'Reilly, 2017.
- [5] T.Tagomori, Blockchain Programming for the Engineer, Hanbit Media, 2018.
- [6] H.S.Lim, Development of distribution and diffusion service technology through individual and Collective Intelligence to digital contents, ICT R&D program of MSIP/IITP 1st Year Annual Report, 2014.
- [7] J.H.Han and O.J.Cho, "Platform business Eco-model evolution: case study on KakaoTalk in Korea," Journal of Open Innovation, DOI:10.1186/s40852-015-0006-8, 2015.
- [8] Korea Copyright Protection Agency, <https://www.kcopa.or.kr>, 2019.
- [9] D.Hinchcliffe, "The app store: The new 'must-have' digital business model," <http://www.zdnet.com/article/the-app-store-the-new-must-have-digital-business-model>, 2010.
- [10] Business Model Breakdown - Quirky.com, <http://www.lumosforbusiness.com/blog/722/28-06-2010/%20Business+Model+Breakdown+%20Quirky.com>, 2010.
- [11] W.Zeng, H.Yu, and C.Y.Lin, Multimedia Security Technologies for Digital Right Management, Elsevier, 2006.
- [12] A.Piva, F.Bartolini, and M.Barni, "Managing copyright in open networks," IEEE Internet Computing, pp.18-26, 2002.
- [13] R.Bill, T.Bill, and M.Stephen, Digital Right Management: Business and Technology, M&T Books, 2002.
- [14] Korea Copyright Commission <https://www.copyright.or.kr>, 2019.
- [15] Copyright Registration, https://www.mcst.go.kr/kor/s_policy/copyright/knowledge, 2019.

윤 성 현(Yun Sunghyun)

[중신회원]



- 1997년 2월 : 고려대학교 일반대학원 컴퓨터학과 (이학박사)
- 1998년 3월 ~ 2002년 2월 : LG 전자 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 ICT학부 부교수

<관심분야>

블록체인, 사물인터넷, DRM, 정보보호