블록체인을 활용한 특별관리임산물 품질관리 시스템의 설계

유성현, 이재호, 정지원, 원유재*
충남대학교 컴퓨터공학과
{yoursaint, no3313, poju8944, yjwon}@cnu.ac.kr
*Corresponding author

Design of Quality Management System for Special Forest Product using Blockchain

Sunghyun Yu, Jaeho Lee, Jiwon Jeong, Yoojae Won*
Dept. of Computer Science and Engineering, Chung-Nam National University

요 약

특별관리임산물의 관리·감독을 위하여 법률을 바탕으로 품질관리제도를 마련하고 있으며, 현재 문서를 통해 관리하고 제도적인 신뢰에 의존하는 방식에 머물러 있다. 이는 많은 비용을 발생시키며, 제도를 악용하는 사기 사례가 발생하고 있다. 본 연구에서는 문제점을 해결하기 위해 블록체인을 이용한 특별관리임산물 품질관리 시스템을 제안한다. 해당 시스템은 품질 관리를 위한 문서를 법률에 따른 양식에 따라 전자문서로 생성하고, 문서 정보를 분산장부에 저장하여 누구나 확인 할 수 있도록 한다. 전자 문서들은 기관의 데이터베이스에 보관하여 확인 할 수 있도록 하며, 분산장부의 문서 정보 등록 이력을 통해 품질관리 이력을 추적하고 검증할 수 있도록 한다.

1. 서론

특별관리임산물은 산양삼의 법적 명칭이며 산양삼은 인삼의 구분중 하나로 우리가 보통 인삼이라고 칭하는 가삼(家蔘)과는 재배방법이 다르다. 산양삼은 산지에서 파종 또는 이식하여 농약을 사용하지 않고 최대한 산삼, 야생삼과 가깝게 키우는 삼을 일컫는다. 가삼과 품종의 차이가 크지 않기 때문에 전문가가 아닌 일반 소비자는 산양삼과 인삼을 구별하기 어렵다. 따라서 「산지관리법」과 「임업 및 산촌진흥 촉진에 관한 법률」로 생산과정을 관리하고 있으며 법률을 바탕으로한 품질관리 프로세스를 마련해 제도적인 신뢰를 바탕으로 품질을 관리하고 있다.

품질관리 프로세스는 재배지, 종자, 종묘 확보부터 유통판매단계에 이르기까지 생산의 전 과정에 대하여 관리를 수행한다.[1] 하지만 현재 4차 산업혁명 시대라는 표현이 무색하게 「임업 및 산촌 진흥촉진에 관한 법률 시행규칙」과 그의 별지 서식을 이용한 지정된 문서를 통해 모든 과정을 관리한다. 심지어 지정된 문서 중 생산과정기록부의 경우 특별관리임산물 재배자가 수기로 작성하는데, 3년을 주기로 전문기관에 제출되며 이마저도 제출과 함께 실시하는 현장 확인이 기록 검증의 전부이다.

정리하자면, 프로세스 진행을 위해서 많은 문서가 작성되고 첨부됨에도 불구하고 기술적 신뢰가 아닌 제도적 신뢰를 바탕으로 한 검증 방법에 의존하고 있어 행정 처리에 많은 비용이 소모되고 있다. 또한 이러한 검증 방법 속에서 소비자가 판매되고 있는 산양삼을 확인할 수 있는 방법은 제도적으로 마련된 품질검사 합격증이 유일하다. 산양삼은 90%가 소비자 직거래[2]이기 때문에 이를 악용한 인삼의 산양삼 둔갑 사례는 소비자의 금전적 피해를 발생시키고 전체 산양삼 농가에 대한 신뢰도를 하락 시키고 있다. 따라서 문제 해결을 위해 기술적 신뢰를 바탕으로 한 품질관리 시스템의 구축이 필요하다[3].

본 논문에서는 블록체인을 이용한 특별관리임산물 품질관리 시스템을 제안한다. 해당 시스템은 품질관리를 위한 문서를 법률에 따른 양식에 따라 전자문서로 생성하고, 문서 정보를 분산장부에 저장하여 누구나 품질 관리 이력을 확인 할 수 있도록 한다. 전자 문서들은 기관의 데이터베이스에 보관하여 확인 할 수 있도록 하며, 분산장부에 저장된 문서의 이력을 통해 문서검증을 수행할 수 있도록 한다.

2. 관련연구

1) 기존 특별관리임산물 품질관리 시스템

현재 특별관리임산물의 품질관리를 위한 시스템은 한국임업진흥원의 산양삼 재배이력 조회[4] 및 함양산양삼생산이력제[5] 등이 있다. 산양삼 재배이력 조회의 경우 품질검사 합격증 진본 검증을 수행하며 이력을 확인 할 수 없기 때문에 프로세스별 확인 일자와 수확 시 사진을 열람 할 수 있다. 함양산양삼 생산이력제의 경우 전국 최초로 산양삼 생산이력을 휴대폰을 이용하여 기록하는 제도다. 하지만 생산사진과 사진 등록일 정도를 확인 할 수 있기 때문에 기록의 검증을 수행하기는 어려우며, 해당 지자체 이외의 산양삼은 기록 확인이 불가하다.

2) 블록체인

ⅰ) 블록체인

블록체인에 기록된 데이터는 블록 단위로 관리되며 블록들은 자신보다 앞서 생성된 블록의 해시 값을 참조하고 있다. 이를 P2P로 연결된 분산 네트워크의 참여자가 서로 나눠 갖게 되는데 과반수이상의 참여자가 나눠가지고 있는 체인을 유지한다. 이 때문에 기록된 데이터에 대한 위변조가 불가능에 가깝다. 따라서 유지중인 블록체인의 무결성 및 신뢰성을 보장할 수 있다. 전통적인 데이터베이스보다 성능이 떨어지고 성능을 위해 블록의 크기가 1MB정도로 제한되어 크기가 큰 데이터나 파일을 업로드 하는데에는 적합하지 않다[6].

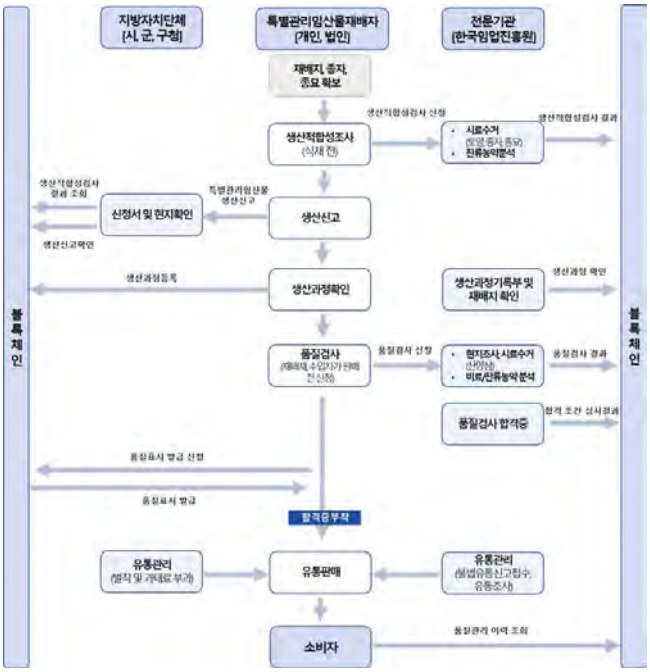
ⅱ) 트랜잭션과 스마트 컨트랙트

트랜잭션은 외부로부터 블록체인 네트워크에 데이터를 전송하는 방법이다. 이때 블록체인 플랫폼에 따라 트랜잭션의 양식, 트랜잭션의 내용에 행동을 정의한 코드를 블록체인 네트워크에 등록하고 지정된 양식의 트랜잭션을 보내 특정한 행동을 수행하도록 할 수 있는데, 이를 스마트 컨트랙트라 한다. 이를 이용하면 블록체인에 원하는 양식으로 데이터를 기록할 수 있다[7]. 하지만 스마트 컨트랙트 시스템은 데이터가 블록체인 안에 존재하지 않거나 블록체인에 입력되는 과정에서 위변조가 발생한다면 신뢰하기 어렵다는 오라클 문제를 가지고 있다[8].

본 연구는 기술적 신뢰를 확보하기 위해 블록체인을 사용하여 시스템을 구축하며, 스마트 컨트랙트를 사용하여 생성된 전자문서의 정보를 블록체인에 기록한다. 또한 블록체인의 기록을 이용하여 전자문서를 검증하고 관리 이력을 추적할 수 있도록 한다. 이를 통해 기술적인 신뢰를 바탕으로 하는 특별관리임산물 품질관리 시스템을 구축하고자 한다.

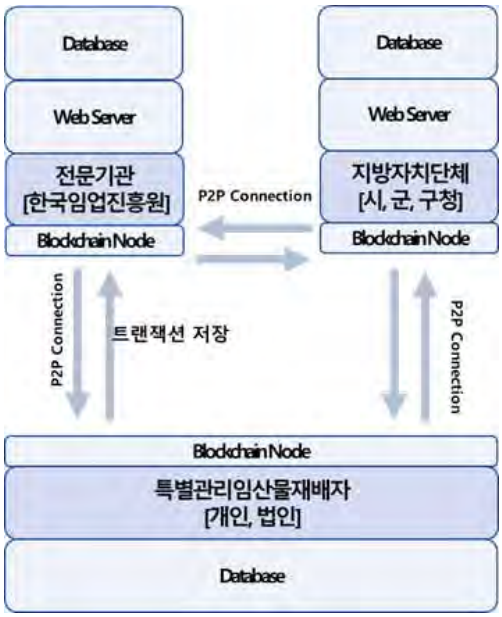
3. 블록체인 활용 특별관리임산물 품질관리

본 논문은 기존 품질관리 프로세스를 바탕으로 구성되며 법적서식을 만족하는 전자문서를 생성하고 문서의 정보를 블록체인에 기록한다. 블록체인에 기록된 전자문서의 정보는 이해관계자간문서 참조 시 참조된 전자 문서의 검증수단으로 이용되며 그 이력은 품질관리 이력추적을 위해 사용된다.



(그림 1) 시스템 구성도

1) 블록체인 네트워크 설계



(그림 2) 시스템의 블록체인 네트워크

시스템 구성 이해관계자들은 각각 블록체인 노드를 구축하고 상호 P2P연결되며 각자의 Database를 가

지도록 설계하였다. 이해관계자별 생산하는 문서는 본인의 Database에 저장되며 상호 참조가 가능하다.

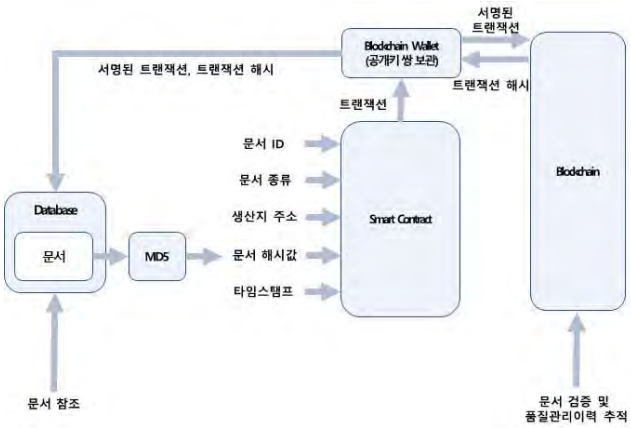
2) 문서 정보 블록체인 기록 스마트 컨트랙트 설계

```
pragma solidity >=0.4.21 <0.7.0;

contract SanyangsamQCDocument {
    string documentId;
    string documentType;
    string address;
    string hashvalue;
    string timestamp;

    event AddQCDocument(string _documentId, string _documentType, string
_address, string _hashvalue, string _timestamp);

    function addQCDocument(string _documentId, string _documentType, string
_address, string _hashvalue, string _timestamp) public {
        documentId = _documentId;
        document_type = _document_type;
        address = _address;
        hashvalue = _hashvalue;
        timestamp = _timestamp;

        emit AddQCDocument(address, document_type, timestamp, hashvalue);
    }
}
```

(그림 3) 문서 정보 기록 스마트 컨트랙트

문서의 정보 중 문서를 검증하고 이력을 추적할 수 있는 정보를 선정하여 해당 정보를 기록할 수 있도록 보편적인 스마트 컨트랙트 언어인 솔리디티(v.0.6.12)로 설계 하였다[9]. 기록되는 정보는 문서 ID(혹은 문서이름), 문서의 종류(「임업 및 산촌 진흥 촉진에 관한 법률 시행규칙」에 정의), 생산지 주소, 전자문서의 해시값, 전자문서의 타임스탬프이다.

3) 시스템 동작 설계



(그림 4) 시스템 동작 설계

각자의 Database에 저장된 전자 문서는 MD5 해시 함수를 이용하여 문서 해시값으로 변환된다. 이후 문서 정보와 문서의 해시값을 이용하여 스마트 컨트랙트 트랜잭션을 작성한다. 트랜잭션은 등록자의 블록체인 지갑의 비밀키로 서명되어 블록체인 네트워크에 전송되며 블록체인은 해당 데이터를 기록한다. 해당 동작을 통해 문서 검증 및 품질관리이력을 추적 할 수 있도록 설계하였다.

스마트 컨트랙트 트랜잭션은 이더리움[7]에서 그림 5과같이 전송할 수 있으며 블록체인은 기록후 트랜잭션 해시를 전송자에게 반환한다.

```
> contract = eth.contract(contractAbiDefinition).at("스마트 컨트랙트 주소")
[abi information]
> Contract.addQCDocument("문서 ID", "문서 종류", "생산지 주소", "문서 해시값", "타임스탬프",{from:등록자지갑계정,gas:소모가스량})
"트랜잭션 해시"
```

(그림 5) 트랜잭션 전송 방법

4) 오라클 문제 예방

블록체인 네트워크에 전송되는 서명된 트랜잭션과 전송 이후 블록체인으로 부터 응답받는 트랜잭션 해시는 등록자의 데이터베이스에 기록하고 서명된 트랜잭션을 디코드 하여 실제 전송된 트랜잭션이 올바른지 검증한다. 또한 트랜잭션 해시를 이용해 기록된 내용을 조회하여 올바르게 저장되었는지 확인하여 오라클 문제를 예방한다. 오라클 문제가 발생했다면 해당 스마트 컨트랙트의 타임스탬프 값을 갱신하여 올바른 서명된 트랜잭션을 다시 전송한다.

4. 실험

1) 실험 환경

Hyperledger Besu(Java based Ethereum)를 docker(v19.03.11)[10]의 인스턴스로 작성하여 컨테이너로 네트워크를 구축한다. nodejs(v10.19.0)[11]로 서버를 구축하고 DB는 실험에서 사용하지 않고 일반 파일 시스템을 이용하였다. 트랜잭션 전송자의 블록체인 지갑은 Metamask(v8.0.8)[12]를 사용한다.

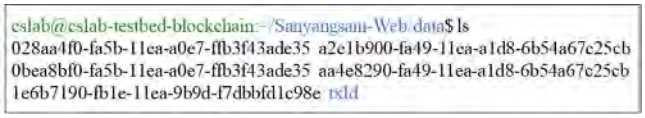
2) 실험 과정 및 결과

3절 각항의 설계와 같이 시스템을 구축하였고 동작이 원활하게 이루어지는지에 대해 실험을 진행하였다. 블록체인 네트워크 구축이후 스마트 컨트랙트를 네트워크에 등록했으며 시스템을 이용하여 문서 등록과 검증을 수행하였다.

(그림 6) 문서정보 블록체인 등록

문서 등록시에 생산지 주소, 문서 종류와 문서 업로드를 수행하면 트랜잭션을 생성하고 로컬 블록체

인 지갑을 통해 서명된 트랜잭션을 블록체인 네트워크에 전송하며 기관의 서버(데이터베이스)에 문서와 서명된 트랜잭션(Raw Tx)을 전송하는 것을 확인 할 수 있었다.



(그림 7) 서명된 트랜잭션과 해시 서버 저장

검증의 경우 블록체인에 기록된 전자 문서와 동일한 문서일 때 정상적으로 검증되었으며 변조되거나 다른 정보를 제공할 경우 검증이 수행되지 않았다.

(그림 8) 문서 검증 성공

Raw Tx는 기관의 데이터베이스에 저장되어 있는 서명된 트랜잭션이며, File Hash Check는 검증 대상 문서의 해시값, Raw Tx Input은 Raw Tx의 내용중 등록된 문서의 hash값, Tx Hash는 트랜잭션 해시, 마지막으로 BlockChain Network Input은 Tx Hash를 이용해 블록체인 네트워크에서 응답받은 트랜잭션의 내용 중 등록된 문서의 해시값 만을 표시한 것이다. 이때 File Hash Check와 Raw Tx Input, BlockChain Network Input이 같아야 검증이 수행되며 그림은 값이 모두 같기 때문에 검증이 완료된 것을 확인 할 수 있었다.

(그림 9) 문서 검증 실패

해당 실험은 생산지 주소, 문서 종류, 타임스탬프 정보는 정상적으로 기입하고 검증 대상 파일을 위조된 파일을 삽입했을 때의 화면이다. 검증 대상 파일만 위조되었기 때문에 Raw Tx Input과 Blockchain Network Input은 같지만 File Hash Check가 다르기 때문에 검증에 실패하는 것을 확인 할 수 있었다.

5. 결론 및 향후 연구

본 논문에서는 블록체인 네트워크를 구축하고 스마트 컨트랙트로 전자 문서로 작성된 품질관리문서에 대하여 문서의 정보를 블록체인에 저장하여 문서를 검증하고 이력을 추적할 수 있도록 하여 블록체인을 이용한 특별관리임산물 품질관리 시스템을 제안한다. 실험을 통해 이해관계자별로 관리하는 품질관리문서를 P2P로 연결된 블록체인 네트워크에서 등록하고 검증할 수 있다는 가능성을 보였다. 향후 연구를 통해 IoT기기 및 스마트폰을 이용한 생산과정기록에 대한 추가적인 검증방법을 마련하여 완성도를 높일 예정이다.

[Acknowledgement]

본 연구는 산림청(한국임업진흥원) 산림과학기술연구개발사업(2020184C10-2022-AA02)의 지원에 의하여 이루어진 것입니다.

참고문헌

[1] 전권석, et al. 산양삼 표준재배지침 개정판. 국립산림과학원, 2018

[2] 한국임업진흥원, 산양삼 생산·유통실태조사, 2018

[3] 기사 “산양삼 불법 유통·판매 5년여간 800건 넘어…단속인원은 2명”, 뉴시스, 2018년 10월 15일 등록, 2020년9월27일 접속, https://www.newsis.com/view/?id=NISX20181015_0000443117

[4] “산양삼 정보 다드림”, 한국임업진흥원, 2020년9월27일 접속, https://sam.kofpi.or.kr/

[5] “산양삼생산이력제”, 함양산양삼생산이력제, 2020년9월27일 접속, http://www.hygn.go.kr/san3.web

[6] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[7] Vitalik Buterin, A next-generation smart contract and decentralized application platform

[8] BERRYHILL, Ryan; VENERIS, Andreas. ASTRAEA: A decentralized blockchain oracle. IEEE Blockchain Technical Briefs, 2019.

[9] “Solidity – Solidity 0.6.12 documentation”, Solidity, 2020년9월27일 접속, https://solidity.readthedocs.io/en/v0.6.12/index.html

[10]Merkel, Dirk. "Docker: lightweight linux containers for consistent development and deployment." Linux journal 2014.239 (2014): 2.

[11] “About | Node.js”, nodejs, https://nodejs.org/ko/about

[12] ”Metamask Docs”, MetaMask, https://docs.metamask.io/guide/