

거래자 중심의 블록체인 기반 선하증권 연구

이주영*, 김현아*, 성채민*, 김정민**

*서울여자대학교 정보보호학과

**KT(Korea Telecom)

dudwn03090@gmail.com, vikim4911@gmail.com, tjdc0als01@gmail.com, cocowin@naver.com

A study on the trader-centered blockchain-based bill of lading

Ju-Young Lee*, Hyun-A Kim*, Chae-Min Sung*, Joung-Min Kim**

*Dept. of Information Security, Seoul Women's University

**KT(Korea Telecom)

요 약

블록체인은 다수의 노드 네트워크 내에서 거래내역을 분산 저장함으로써 투명성을 확보하는 기술이다. 최근에는 금전적 가치를 지닌 선하증권(Bill of Lading, B/L 서류)에 블록체인을 적용하여 무결성을 확보하고 거래 과정을 간소화 하기위한 연구가 진행되고 있다. 본 논문에서는 거래자 중심의 블록체인 기반의 선하증권 시스템을 제안한다. 수출자는 발행 받은 선하증권을 AI(Artificial intelligence)기반의 OCR(Optical character recognition)기능을 통해 블록체인에 등록하고, 각국 은행에서 열람하여 신용장거래를 진행한다. 수입자는 선하증권 정보를 담은 QR(Quick Response code)코드로 자기증명을 하여 물품을 인도 받게 된다. 이는 수출자 측에서는 선적서류를 우편으로 보낼 시간과 비용을 단축하고, 서류의 무결성을 입증할 수 있다는 점에서 큰 효과를 얻을 수 있다. 수입자 측에서는 서류가 등록됨과 동시에 확인할 수 있고, 해당 거래를 신뢰할 수 있다는 이점을 갖는다. 마지막으로 은행 측에서는 선적서류에 대해 보안성을 갖출 수 있고 검증이 더 신속하게 이루어질 수 있다.

1. 서론

블록체인 기반의 선하증권 시스템에 대한 연구는 활발하게 진행되고 있다[1]. 기존 종이 서류가 갖는 문제점 중 많은 부분을 블록체인이 해결하기 때문이다. 그 중 하나는 금전적인 가치를 지니는 중요 문서임에도 불구하고 우편 송부가 되기 때문에 훼손 및 분실로부터 자유롭지 않다는 것이었다. 또한 서류 위·변조 여부를 확인하기 어려워 사기 거래가 빈번하게 일어난다. 하지만, 블록체인 기반의 선하증권 시스템은 PDF 등의 전자문서의 형식으로 공유되어, 문서의 훼손 및 분실의 위험을 낮출 수 있다. 블록체인은 트랜잭션이라는 거래내역을 블록이라는 장부에 저장하여 여러 노드가 분산 저장하기 때문에 위조, 변조가 거의 불가능하다. 게다가 스마트계약은 특정 조건이 만족 되어야 실행이 되기 때문에 계약불이행 등의 사기행각을 예방할 수 있다는 점에서 공정한 거래 환경을 조성하는데 기여할 수 있다.

더 나아가 본 연구에서는 AI 기반의 OCR 기능을 통한 선적서류 등록 과정 간소화 및 QR 코드를 통한 수

하인 자기증명 과정을 통해 물품 인도 자동화를 가능하도록 설계하였다.

2. 관련 연구

2.1 블록체인 기반의 선하증권 시장 동향

세계 최대 선사 머스크와 IBM 이 협력하여 구축한 TradeLens 가 대표적인 선사 중심의 블록체인 기반 전자원장 플랫폼이다. 수송현황에 대한 모든 추적정보를 안정적으로 통합되어 제공한다는 점이 특징이다. Hyperledger Fabric 기반으로 구현했으며, 암호화 ID 를 통해 네트워크 피어 구성원을 참여시킬 수 있다. 반면 삼성 SDS 의 Cello Trust 는 물류 통합 서비스 플랫폼으로 고객 맞춤형 된 정보를 제공한다. 최적 경로에 따른 물류비 절감, 유통 이력 관리 등이 대표적인 서비스이다. 삼성 자체개발 블록체인 Nexledger 로 프라이빗 네트워크와 퍼블릭 네트워크의 특성을 모두 가지고 있다.

대표적인 선사인 MSC 도 블록체인 기반의 e-B/L 을 본격 도입하였고, 중국 대규모 공급업체인 알리바바도 국제항만공동체시스템협회(IPCSA)에서 진행하는 블록체인 선하증권 개발 계획에 공동 참여하였다.

2.2 블록체인과 스마트컨트랙트

블록체인이란 대규모 노드 네트워크에서 여러 개의 트랜잭션(거래내역)을 블록 장부로 만들어 노드들이 분산 저장함으로써 거래의 무결성을 보장할 수 있는 기술이다.

스마트컨트랙트란 사전에 코드를 통해 계약의 조건과 이행을 명시하고, 특정 조건이 만족할 때 해당 계약이 실행되는 스크립트이다. 이는 중개인의 역할을 수행함으로써 거래자들 간의 p2p (Peer to Peer)거래를 실현할 수 있다.

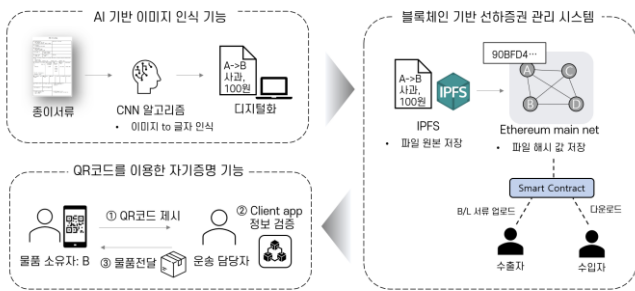
2.3 CNN 알고리즘

여러 연구에서 딥러닝 알고리즘 중 CNN(Convolutional Neural Network)이 OCR 기능에서 좋은 성능을 보인다고 알려져 있다[2].

따라서 본 연구에서는 CNN 알고리즘으로 다양한 선하증권 양식을 사용하여 글자 특징을 추출 및 학습한다. 서로 다른 양식의 선하증권 서류에서 글자 데이터만 추출하는 OCR 기능을 구현하도록 한다.

3. 거래자 중심의 블록체인 기반 선하증권

3.1 플랫폼 구성도



<그림 1> 플랫폼 구성도

3.1.1. AI 기반의 OCR 기능

선하증권 양식이 통일되지 않았기 때문에 서로 다른 이미지에서는 정확한 글자를 추출하는 것이 중요하다. 따라서 많은 딥러닝 알고리즘 중, 이미지 학습 및 판단에 효과적인 CNN 알고리즘을 적용함으로써 유연적인 글자 인식 기능을 할 것을 기대하였다. 이렇게 추출된 문자열은 블록체인에 저장된다.

3.1.2 Ethereum 블록체인 기반의 분산저장 기능

블록체인에 저장되는 파일의 크기가 한정적이기 때문에, 추출된 서류정보는 IPFS(Inter Planetary File System)라는 분산형 파일 시스템에 저장된다. IPFS는 분산 해시 테이블로 파일 관리를 하기 때문에, 저장된 파일은 해시 값으로 반환된다. IPFS 시스템은 암호화되지 않으므로 모든 노드에게 공개됨을 고려하여 업로드, 다운로드 할 시에는 비대칭키 암호화 방식을 사용해야 한다.

반환된 해시 값은 선적서류의 지문(fingerprint) 역할로, 블록체인에 저장된다. 이때 해운 물류의 특성상 시시각각 거래의 파기, 생성, 변경 등이 발생한다는 점을 고려해 거래의 유연성 및 확장성을 포용할 수 있는 Ethereum 플랫폼으로 선정하였다.

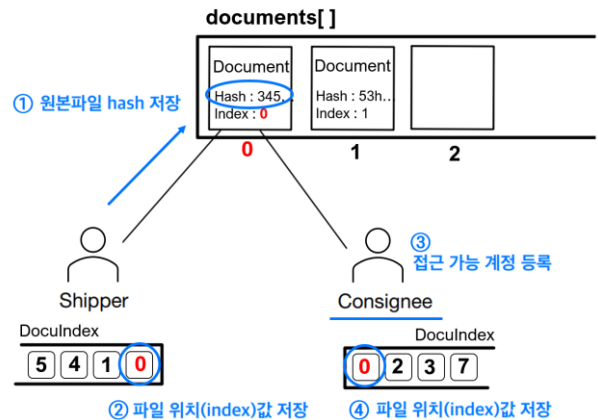
3.1.3 자기증명 QR 시스템

물품인도를 받기 위해 수입인은 선하증권을 제시하여 물품과 교환 해야한다. 블록체인과 연동된 디앱(DApp, Decentralized Application)에서는 해당 계정 소유의 선하증권 해시를 QR 코드 형태로 보여줄 수 있고, 이를 통해 물품을 수령 받을 수 있다.

해당 거래자가 실제 거래자인지 확인과정인 검증시에는 QR 리더기를 통해 수입인의 QR 코드를 읽으면 선하증권의 해시 값과 블록체인의 주소가 나오고, 해당 주소의 원본 해시 값을 얻어 일치 여부를 확인한다. 일치한다면, 실제 거래 참여자라는 의미이다.

3.2 블록체인 동작 및 구현 방법

3.2.1 계정과 서류 연동 원리



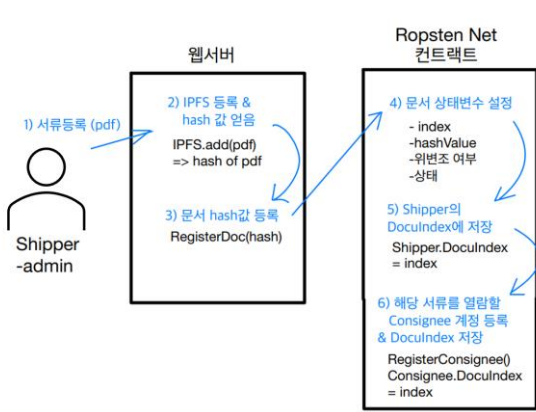
<그림 2> 노드 계정과 선하증권 연동 방법
수출인(Shipper)이 발행받은 서류의 해시값을 블록체인에 저장한다. 해시값이 저장된 주소(index = 0)를 수출인의 상태변수인 DocuIndex에 저장한다. 해당 서류에 접근가능한 수입인(Consignee)을 등록한 후, 해당 계정의 상태변수 DocuIndex에 동일한 주소값을 등록한다. DocuIndex 상태변수는 계정이 소유한 문서의 위치를 저장하는 변수이다.

3.2.2 사용자 등록, 서류 및 접근 가능 계정 등록



<그림 3> 사용자 등록

수출인은 디앱(DApp)을 이용하고자 계정을 생성한다. RegisterShipper() 컨트랙트 함수가 호출되고, 인자로 수출인의 계정주소를 넘긴다.

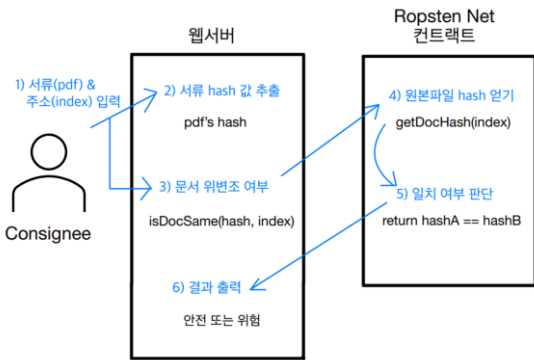


<그림 4> 서류 등록 및 접근 가능 계정 설정

등록된 수출인은 서류를 업로드 할 수 있는데, 원본은 IPFS 에 업로드한 뒤 파일의 해시값을 블록체인에 등록을 한다. 서류 등록을 위한 RegisterDoc() 함수가 인자로 해시값을 넘겨주며 호출된다. 수출인이 해당 서류와 연결되기 위해 수출인의 상태변수 DocuIndex 에 서류의 index(위치정보)를 저장한다. 이제 수출인은 서류 위치정보를 이용해 접근할 수 있게 되었다.

수출인은 해당 서류를 열람할 수 있는 수입인을 등록할 수 있다. 수입인의 계정을 등록한 뒤, 동일한 방식으로 수입인의 DocuIndex 상태변수에 파일의 위치정보를 저장한다. 이제 수입인은 문서에 접근할 수 있다.

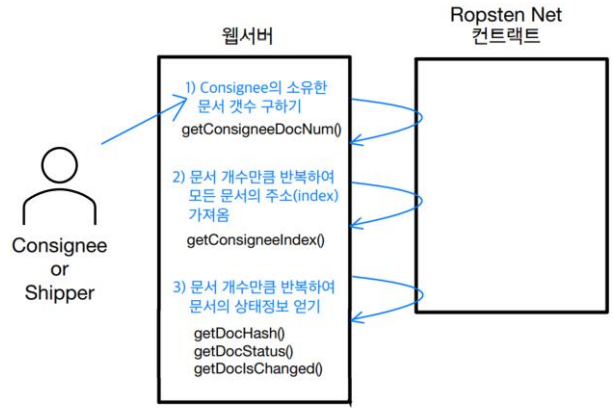
3.2.3 서류 위·변조 비교 기능



<그림 5> 서류 위·변조 비교 기능

수입인(Consignee)은 소유한 서류가 실제 금전적인 가치를 유지하고 있는가를 확인할 때 사용할 수 있는 기능이다. 확인하고 싶은 서류를 pdf 로 스캔하여 업로드한다. 추출된 해시 값과 DocuIndex 에 있던 파일 위치(index)를 파라미터로 isDocSame() 함수를 호출한다. 해당 index 로 접근하여 원본 해시 값을 불러오고, 현재 해시 값과 동일한지 여부를 확인한다.

3.2.4 서류 리스트 출력 기능



<그림 6> 서류 리스트 출력 기능

자신의 계정과 연동된 문서 정보를 불러오는 기능이다. solidity 에서는 구조체를 사용할 수 없어 해당 상태변수를 반복문으로 불러와야한다. 먼저 소유한 문서 개수를 얻어서, 그 수만큼 반복하여 문서의 주소(index)를 가져온다. 그러면 문서의 개수만큼 다시 반복하여 문서의 정보(Hash, Status, IsChanged)를 불러온다.

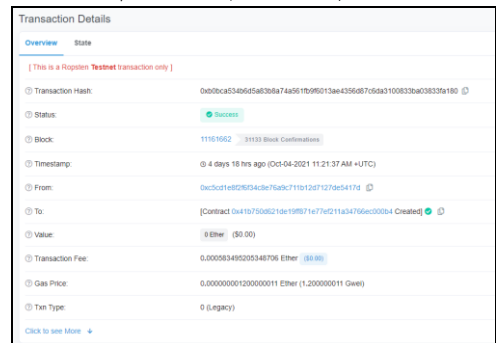
3.2.4 스마트컨트랙트 구현 및 배포

```

1 pragma solidity ^0.5.16;
2
3 contract DocumentTransfer {
4     struct Shipper {
5         uint[] DocuIndex;
6         bool isRegistered;
7     }
8
9     struct Consignee {
10        uint[] DocuIndex;
11        bool isRegistered;
12    }
13
14    struct Document {
15        uint index;
16        uint hashValue;
17        bool isChanged;
18        uint status;
19    }
20
21    modifier onlyRegisteredShipper() {
22        require(shipper[msg.sender].isRegistered,
23            "the caller of this function must be a registered Consignee");
24    }
25
26    modifier onlyRegisteredConsignee() {
27        require(consignee[msg.sender].isRegistered,
28            "the caller of this function must be a registered Consignee");
29    }
30
31
32
33    mapping(address => Shipper) public shippers;
34    mapping(address => Consignee) public consignees;
35    Document[] public documents;
36
37    constructor() public {}
38
39    function registerShipper(address _shipperAddress)
40        public
41        onlyRegisteredConsignee()
42        returns (Shipper) {
43        require(!shipper[_shipperAddress].isRegistered, "the shipper is already registered");
44        shipper[_shipperAddress].isRegistered = true;
45    }
46
47    function registerConsignee(address _consigneeAddress, uint _index)
48        public
49        onlyRegisteredShipper()
50        returns (Consignee) {
51        require(!consignee[_consigneeAddress].isRegistered(),
52            "consignee[_consigneeAddress].DocuIndex = _index");
53        consignee[_consigneeAddress].DocuIndex = _index;
54        consignee[_consigneeAddress].isRegistered = true;
55    }
56
57    function registerDoc(uint _hashValue, address _consigneeAddress) public onlyRegisteredShipper {
58
59    }
60
61 }

```

<그림 7> 스마트컨트랙트 코드



<그림 8> Ropsten 네트워크에 배포된 컨트랙트 모습 solidity 언어를 사용하여 위 기능들을 구현한 모습이다. 이 컨트랙트는 실제 Ropsten 테스트 네트워크에서 배포 완료하였다.

4. 결론 및 향후 연구

블록체인을 기반으로 한 거래 시스템은 상호간의 신뢰성을 높일 뿐만 아니라, 기존의 신용장 서류 검증 절차 과정과 전송 비용 및 시간을 축약하는데 큰 역할을 할 수 있을 것으로 기대한다.

본 논문에서는 거래자 중심의 블록체인 선하증권을 제안하였다. AI 기반의 OCR 기능으로 서류 등록의 과정을 간편화 하고, QR 코드를 통한 자기증명 기능으로 물품 인도 과정을 축소 및 인력 낭비 감소의 효과를 기대할 수 있다.

더 나아가 추후 연구에서는 노드 미참여자와의 서류 교환 및 노드 연동 방안에 대한 연구를 진행하여 실무에서 블록체인이 범용적으로 사용되고, 해안 물류 분야에 보안성을 강화하는데 기여할 수 있기를 기대한다.

Acknowledgement

본 논문은 해양수산부 실무형 해상물류 일자리 지원사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다.

참고문헌

- [1] Hee-sung Bae, The Applications of Blockchain Technology on Electronic Bill of Lading, KOREA INTERNATIONAL COMMERCE REVIEW, 2019
- [2] Naragudem Sarika, Nageswararao Sirisala, Muni Sekhar Velpuru, CNN based Optical Character Recognition and Applications, IEEE, 2021
- [3] 김종권, 유광현, 출입통관에서의 블록체인 기술 활용 증대 가능성에 관한 연구, The Journal of Korea Research Society for Customs, 2020
- [4] 최석범, 블록체인 선하증권의 상용화에 관한 연구, 2019
- [5] Mihaela Gabriela Belu, Application of Blockchain in International Trade: An Overview, The Romanian Economic Journal, 2019
- [6] Mathis Steichen, Beltran Fiz, Robert Norvill, Wazen Shbair, Radu State, Blockchain-Based, Decentralized Access Control for IPFS, IEEE, 2018
- [7] Shubham Desai¹, Rahul Shelke, Onkar Deshmukh, Harish Choudhary, Prof. Santosh S. Sambare, Blockchain based secure data storage and access control system using IPFS, Journal of Critical Reviews, 2020
- [8] N.Nizamuddina, K.Salaha, M.Ajmal Azadb, J.Arshadc, M.H.Rehmand, Decentralized document version control using ethereum blockchain and IPFS, ScienceDirect, 2019
- [9] Jin Sun, Xiaomin Yao, Shangping Wang, Ying Wu, Blockchain-based Secure Storage and Access Scheme For Electronic Medical Records in IPFS, IEEE, 2020
- [10] 정순형, 블록체인 기반 스마트 주식 거래 시스템의 설계 및 구현, 석사학위 논문, 2016
- [11] 이은영, 문정현, 한채림, 이일구, 블록체인 네트워크 보안 위협 탐지 기술 동향 분석, 2021
- [12] 양성훈, 진회용, 김상균, 거래 비용 절감을 위한 블록체인 기반 재능거래 플랫폼, 방송공학회논문지, 2020
- [13] 박하영, 전민준, 이수현, 블록체인 기반 웹툰 플랫폼 BlockToon, 한국컴퓨터정보학회, 2019
- [14] 한상우, 배민수, 황경호, 동형암호를 사용한 블록체인 기반 전자투표 시스템 개발, 한국통신학회, 2019
- [15] 최환석, 박민영, 송유빈, 이우섭, 블록체인 기반의 신뢰적 거래 플랫폼 개발, 한국디지털콘텐츠학회, 2021
- [16] 성기정, 정채린, 조은아, 이종호, 김희영, 김영우, 이경현, 블록체인 기반 교내 전자투표 시스템, 한국 정보보호학회, 2018
- [17] 최낙훈, 김희열, 메타마스크와 연동한 블록체인 기반 사용자 인증모델, 한국인터넷정보학회, 2019