KIPS Trans. Softw. and Data Eng.
Vol.11, No.7 pp.283~290
ISSN: 2287-5905 (Print), ISSN: 2734-0503 (Online)

https://doi.org/10.3745/KTSDE.2022.11.7.283

A Study on the Blockchain-Based Bill of Lading System to Improve Usability

Ju-young Lee† · Hyun-a Kim† · Chae-min Sung† · Joung-min Kim†† · Sungwook Kim†††

ABSTRACT

Blockchain is a technology that secures integrity and transparency by distributing and storing transaction details within multiple node networks. Recently, research is being conducted to secure integrity by applying blockchain to Bill of Lading (B/L documents) of monetary value. In this paper, we study a blockchain-based bill of lading system to improve usability. The shippers register the issued bill of lading on the blockchain, and banks in each country read it to conduct L/C transactions. The consignees receive the goods after completing certification with a quick response code (QR) containing the bill of lading information. Through this, shippers enjoy merits in that they can shorten the time and cost of sending shipping documents by mail and prove the integrity of the documents. The consignees have the advantage of being able to check the documents at the same time as they are registered and trust the transaction. Finally, on the bank side, the security of shipping documents is ensured and verification can be done quickly.

Keywords : Blockchain, Bill of Lading, Smart Contract, DApp

사용성 개선을 위한 블록체인 기반 선하증권 거래 시스템 연구

이 주 영† · 김 현 아† · 성 채 민† · 김 정 민†† · 김 성 욱†††

요 약

블록체인 기술은 거래를 투명하게 관리함으로써 중앙통제 없이 신뢰 가능한 P2P 거래를 가능하게 한다. 최근에는 금전적 가치를 지닌 선하증권(Bill of Lading, B/L서류)의 무결성을 확보하기 위해 블록체인을 적용한 연구가 진행되고 있다. 본 논문에서는 사용성 개선을 위한 블록체인 기반의 선하증권 시스템을 제안한다. 수출자는 선사로부터 발급 받은 선하증권을 블록체인에 저장하고, 은행에서 이를 조회하여 신용장 거래를 수행한다. 수입자는 선하증권 서류의 지문이 담긴 QR코드(Quick Response code)로 신원증명을 완료한 뒤 화물을 인도 받게 된다. 수출자는 우편으로 보낼 시간과 비용을 절약하고, 물품의 보안을 강화할 수 있다는 점에서 큰 효과를 거둘 수 있다. 수입자의 경우 선적 서류가 블록체인 네트워크에 등록되자마자 서류를 열람할 수 있고, 신뢰를 바탕으로 거래를 수행할 수 있다는 이점을 갖는다. 뿐만 아니라 은행에서는 선적서류에 대한 검증을 더욱 신속하게 수행할 수 있다.

키워드 : 블록체인, 선하증권, 스마트컨트랙트, 디앱

1. 서 론

최근에 블록체인 기반의 선하증권(Bill of lading, B/L) 시스템이 여러 연구를 통해 활발하게 제안되고 있다[1-3]. 선하증권 거래 시스템이 블록체인에 주목하는 이유는 종이 서류의 많은 한계점을 해소할 수 있기 때문이다. 우편 송부의 큰 문제점 중 하나는 선하증권이 금전적인 가치를 지니는 중요한 문서임에도 불구하고 훼손과 분실이 발생할 수 있다는 것이다. 또한 서류가 진본인지 확인하기 어렵다는 점에서 위변조 등 사기 범죄의 가능성이 열려있다.

블록체인 기술은 선하증권 시스템의 이러한 문제점을 해결하는데 매우 유용하다. 우선 시스템에서 선하증권을 PDF와 같은 전자형태의 문서로 공유함으로써 문서의 훼손 및 분실 가능성을 현저히 낮출 수 있다. 또한 블록체인은 다수의 트랜잭션을 블록에 저장하여 여러 노드가 나눠서 보유하기 때문에 위변조가 거의 불가능하다. 게다가 공정한 무역 거래 환경을 조성하는데 기여할 수 있는데, 이는 스마트계약이 특정 조

※ 이 논문은 서울여자대학교 학술연구비의 지원에 의한 것임(2022-0142).
※ 이 논문은 2021년 한국정보처리학회 ACK 2021에서 "거래자 중심의 블록체인 기반 선하증권 연구"의 제목으로 발표된 논문을 확장한 것임.
† 비 회 원 : 서울여자대학교 정보보호학과 학사과정
†† 비 회 원 : KT 강북/강원 법인고객본부 AI TF 차장
††† 정 회 원 : 서울여자대학교 정보보호학과 조교수
Manuscript Received : January 4, 2022
First Revision : March 9, 2022
Accepted : March 11, 2022
* Corresponding Author : Sungwook Kim(kim.sungwook@swu.ac.kr)

건을 만족시켜야 실행이 되고 계약불이행 등의 사기행각을 예방하는 기능을 제공하기 때문이다.

하지만 이러한 블록체인 기반 시스템에도 사용성 측면에서 한계점이 존재한다. 첫 번째, 기업이 새로운 시스템으로 전환하기 위해서는 많은 비용을 치러야 한다는 것이다. 구체적으로, 블록체인 기반 시스템을 적용하기 위해서는 기존 종이 서류에서 디지털 문서를 사용하는 체제로 전환이 필요한데, 이는 현업에서 큰 부담으로 작용한다. 두 번째, 여전히 화물을 인도받기 위한 과정이 복잡하다. 디지털 문서임에도 불구하고, 수입인은 선사에게 선하증권을 제시하여 발급받은 화물인도지시서(Delivery Order, D/O)를 본선 또는 터미널에 있는 운송인에게 제시하여야 물품을 수령할 수 있다. 즉, 선하증권 그 자체로 물품의 소유권을 입증할 수 있음에도 불구하고 화주가 직접 선사를 찾아가야 하는 복잡한 과정이 있다.

본 연구에서는 위에 언급한 한계점에 대응하기 위해 사용성이 증대된 블록체인 기반 선하증권 시스템을 제안한다. 제안 시스템은 탈중앙화된 분산 거래 환경을 제공하기 위해 이더리움 네트워크를 기반으로 설계되었으며 사용성 증대를 위해 다음과 같은 기능을 제공한다. 첫 번째, 기존 종이 서류 기반 시스템도 포괄할 수 있도록 종이 서류의 디지털화를 자동적으로 수행한다. 이를 위해 AI(Artificial Intelligence)기반 OCR(Optical Character Recogniti-on)을 활용한다. 두 번째, 화물 인도 과정 간편화를 위해 QR코드(Quick Response Code) 기능을 도입하였다. 이를 통해 수입인은 물품 소유자의 고유한 값을 제시할 수 있고, 물품 인도 자동화가 달성된다. 마지막으로, 분산 파일 시스템 IPFS(InterPlanetary File System)를 통해 거래 속도를 개선한다.

2. 관련 연구

2.1 시장 동향

TradeLens는 대표적인 선사 중심의 전자원장 플랫폼으로 머스크와 IBM이 협력하여 설계하였다[4]. TradeLens는 수송 현황에 대한 트래킹 정보를 모아 안정적으로 통합 제공한다는 점이 특징이다. Hyperledger Fabric 기반으로 구성됐으며, 암호 ID로 네트워크 피어 구성원을 참여시킬 수 있다. 반면 물류 통합 서비스 플랫폼으로는 삼성의 Cello Trust로 고객 맞춤형 정보를 제공한다[5]. 최적의 경로를 따라 물류비 절감, 유통 이력 관리 등이 대표적인 기능이다. 삼성이 자체적으로 개발한 블록체인 Nexledger 위에서 운용되며, 프라이빗과 퍼블릭 네트워크의 특성을 모두 가지고 있다. MSC도 블록체인 기반의 e-B/L을 본격적으로 도입하였고[6], 중국 대규모 공급업체인 알리바바도 국제항만공동체시스템협회(IPCSA)가 주도한 블록체인 선하증권 개발 계획에 공동 참여하였다[7].

	Tradelens	Cello Trust	CargoX	Ours
Structure				
Framework	○ Data sharing and cooperation .	○ Optimal route, distribution history management.	○ Blockchain document transfer system	○ Blockchain document transfer system
Network	○ Hyperledger fabric	○ Samsung's self-developed blockchain accelerator, Nexledger	○ Ethereum, IPFS	○ Ethereum, IPFS
Difference	○ Hyperledger fabric ○ Global Shipping Business Network	○ Nexledger ○ Hyperledger fabric	○ Ethereum,IPFS ○ Stability of ownership transfer of B/L	○ Ethereum,IPFS ○ compatibility of paper-system ○ Automation of identification

Fig. 1. Comparison between Platforms

본 연구의 시스템은 중앙 기관이 없는 분산 거래 환경을 제공하기 위해 Tradelens, CelloTrust와 다르게 이더리움 네트워크에 기반하고 있다. CargoX의 경우도 동일한 이더리움 네트워크에 기반하고 있는데 본 연구의 시스템은 사용성을 개선하기 위해 기존 종이 서류 체제와의 호환성, 그리고 신원 증명의 자동화 기능을 추가적으로 고려한다. Fig. 1은 본 연구가 제안하는 시스템과 기존 시스템을 비교, 분석한 표이다.

2.2 블록체인과 스마트컨트랙트

블록체인은 수많은 노드로 구성된 P2P(Peer-to-Peer) 네트워크가 트랜잭션이 기록된 장부를 공유하고 분산 저장함으로써 거래의 유효성 및 무결성을 보장하는 기술이다. 스마트 컨트랙트는 계약의 중개인 역할을 수행하는데 계약 전 코드에 조건과 이행을 명시하고, 조건이 충족되었을 때 계약 내용을 실행한다. 따라서 기존 중개인을 대체하여 P2P 거래를 상호신뢰를 보장하면서 수행한다.

2.3 CNN과 OCR

CNN(Convolutional Neural Network)은 인공신경망 모델로 이미지 데이터를 처리하는데 활용되며, OCR 서비스에서도 높은 활용성을 가진다[8]. 따라서 본 연구에서는 CNN 알고리즘을 OCR에 적용함으로써 서로 다른 선하증권 양식에서의 글자 특징을 추출하여 학습하고, 이를 통해 적절한 문자 영역을 추출하여 디지털화할 수 있도록 설계하였다.

3. 블록체인 기반 선하증권

3.1 시스템 개요

Fig. 2는 본 연구에서 제안하는 블록체인 기반 선하증권 거래 시스템의 구조를 보여준다. 제안 시스템은 아래 3가지 기능을 제공하도록 설계되었다.

1) AI 기반의 OCR 기능

선하증권 양식이 서로 다르기 때문에 규격화되지 않은 이

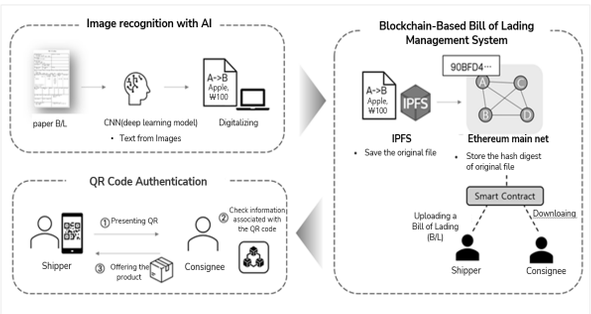

Fig. 2. Platform Architecture

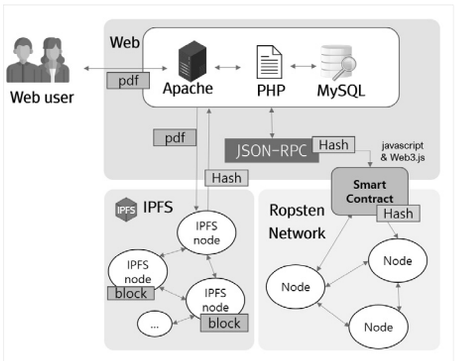

Fig. 3. Framework

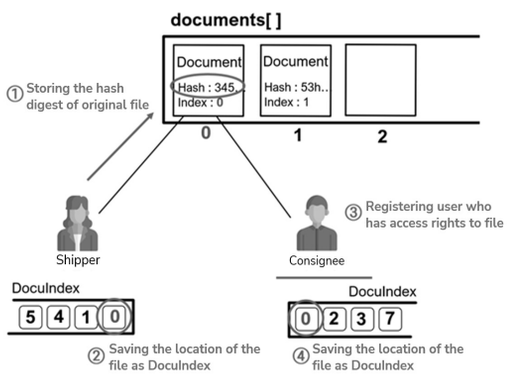

Fig. 4. Linkage of Node Account and Bill of Lading

미지에서 의도에 맞는 문자열을 추출하는 것이 필요이다. 따라서 이미지 학습과 예측에 특화한 CNN 모델을 활용하여 효과적으로 문자열 추출하고 인식하도록 하였다. OCR로 추출된 문자열(계약 내용)은 블록체인 네트워크에 기록된다.

2) IPFS 및 Ethereum을 활용한 데이터 분산 저장 기능

블록체인에 저장 가능한 데이터의 사이즈에 한계가 있기 때문에, 추출된 계약 데이터는 IPFS(Inter Planetary File System)라는 분산 파일 관리 시스템에 저장된다. IPFS는 분산 해시 테이블로 파일을 관리하기 때문에, 파일이 저장되면 저장 파일 정보가 해시값으로 반환된다. 다만 IPFS는 데이터 암호화 기능을 제공하지 않고 불특정 노드가 저장 데이터에 접근하는 것을 허용하기 때문에 데이터 업로드 및 다운로드 시 비대칭 키 암호화를 사용할 필요가 있다.

반환된 해시값은 저장 선하증권을 유일하게 가리키는 지문(fingerprint) 데이터이며 블록체인에 저장된다. 또한 본 시스템은 블록체인 플랫폼으로 Ethereum을 사용한다. 그 이유는 무역 거래 특성상 거래 생성, 거래 파기, 그리고 거래 변경 등의 이벤트가 지속적이고 빈번하게 발생하는데 Ethereum이 거래 확장성 및 유연성을 제공하고 있기 때문이다.

3) 신원증명 QR코드 시스템

화물을 인도받기 위해 수입인(Consignee)은 선하증권을 제시하여 물품과 교환해야 한다. 블록체인과 연동된 디앱(DApp, Decentralized Application)은 해당 수입인 계정의 선하증권 해시값을 QR코드로 제시함으로써 소유권을 증명하는 기능을 제공하고, 이를 이용해 물품을 수령한다. 구체적으로, 해당 주소의 원본 해시값을 가져와서 일치 여부를 확인하고, 일치한다면 실제 거래 참여자임을 증명하는 원리이다.

3.2 시스템 설계

1) 프레임워크

Fig. 3은 본 연구에서 블록체인 기반의 선하증권 시스템을 구현하기 위한 프레임워크를 보여준다. 프레임워크는 크게 웹 서버, 분산파일시스템, 그리고 이더리움 네트워크로 구성된다. 웹 서버는 Apache, PHP, MySQL으로 구성되고, 사용자들에게 웹 서비스를 제공한다. Off-chain으로는 IPFS, On-chain으로는 Ropsten network를 사용한다. IPFS는 분산 파일시스템으로 가스비 문제로 이더리움에 파일의 원본을 저장하기 어렵기 때문에 도입되었다. Ropsten network는 이더리움 main 네트워크에 배포하기 전 테스트를 위해 사용되는 네트워크이다.

2) 계정과 서류 연동

수출인(Shipper)이 발행받은 서류를 블록체인에 등록한다. 즉, 해시값이 저장된 주소(index=0)를 수출인 구조체의 변수인 DocuIndex에 입력한다. 해당 서류에 접근할 수 있는 수입인 계정을 등록하고, 해당 계정의 변수 DocuIndex에 해당 서류의 주소값을 저장한다. DocuIndex 상태변수는 계정과 연관된 서류의 위치를 저장하는 변수이다. Fig. 4는 이러한 과정을 보여준다.

3) 사용자 등록, 서류 및 접근 가능 계정 등록

수출인은 디앱(DApp)을 이용하고자 계정을 생성한다. Fig. 5와 같이 RegisterShipper() 컨트랙트 함수가 호출되고, 인자로 수출인의 계정주소를 넘긴다.

등록된 수출인은 서류를 업로드 할 수 있다. 구체적으로

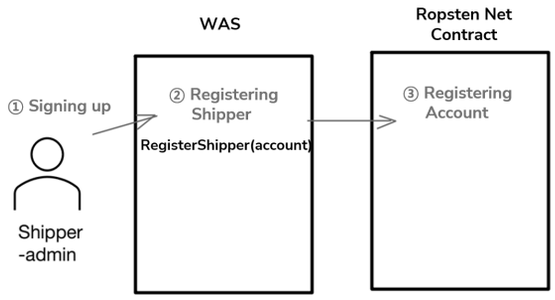

Fig. 5. Shipper Registration

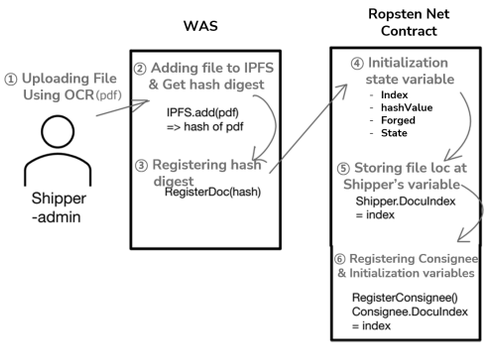

Fig. 6. Document Registration and Account Set-up

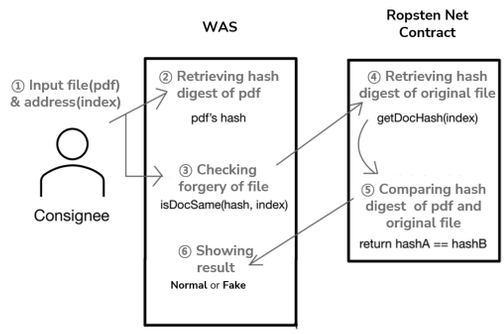

Fig. 7. Detection of Document Forgery

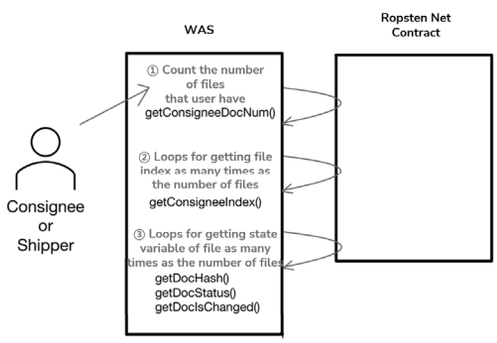

Fig. 8. Management of Linked Documents

OCR기능으로 기존 종이 서류에서 거래 정보를 추출한 뒤 IPFS.add() 함수를 통해 원본은 IPFS에 업로드 한다. 그리고 RegisterDoc() 함수가 위 과정에서 반환된 파일 해시값을 입력으로 받아 이를 블록체인에 저장한다. 또한 RegisterDoc() 함수는 수출인과 서류를 연결하기 위해 수출인의 상태변수 DocuIndex에 파일 위치값(index)을 블록체인에 저장하는 기능도 수행한다. 수출인은 계약 관계인인 수입인을 등록하고 서류를 연결함으로써 파일을 공유할 수 있다. 수입인 계정을 등록한 뒤 동일한 방법으로 수입인의 상태변수 DocuIndex에 파일의 위치값을 저장한다. 이로부터 수입인은 서류의 위치 정보를 통해 문서에 접근할 수 있게 된다. Fig. 6은 이상의 기능을 수행하는 과정을 보여준다.

4) 서류 위변조 비교 기능

선하증권은 물품의 소유권을 주장할 수 있는 서류이다. 서류 위변조 비교 기능을 통해 수입인이 열람한 선하증권이 실제 가치(물품 소유권)가 있는지를 아래의 과정에 따라 확인할 수 있다. 즉, 확인 대상 선하증권을 pdf로 저장하여 업로드한다. 그로부터 계산된 해시값과 파일 위치(index)를 인자로 isDocSame() 함수를 호출한다. 해당 index로 접근하여 해시값을 가져오고, 현재 해시값과 일치하는지 여부를 확인한다. Fig. 7은 서류 위변조 비교 작업 흐름도를 보여준다.

5) 서류 리스트 출력 기능

서류 리스트 출력 기능은 자신과 연관된 서류 정보를 가져오는 기능이다. solidity는 구조체를 지원하지 않기 때문에 상태변수를 반복하여 불러와야 한다. 먼저 관련 서류의 개수 정보를 얻고, 그 개수대로 반복하여 서류의 주소(index)를 가져온다. 그리고 서류 개수만큼 반복하여 문서의 정보(Hash, Status, IsChanged)를 불러온다. Fig. 8은 이상과 같이 연동된 문서를 불러오는 작업 흐름도를 보여준다.

4. 시스템 구현

4장에서는 3장에서 설계한 시스템을 구현한 결과를 소개한다. 코드는 GitHub에서 확인할 수 있다[9]. 본 연구에서는 Ubuntu 20.04.3 LTS, 메타마스크 10.3.0, IPFS 0.9.1, Truffle 5.4.13, Solidity 0.5.16, Ganache 6.12.2 버전을 사용하였다. 이더리움은 신뢰할 수 있는 중앙기관 없이 거래할 수 있다는 점과, 디파이(Decentralized Finance, 분산형 금융)의 경우 탈중앙 시스템을 기반으로 결제, 투자, 대출 등을 제공한다는 점에서 활용도가 점차 높아졌다[10]. 게다가 이더리움의 거래 속도는 2.0으로 업그레이드되면서 무거운 연산량을 개선함으로써 1만 4000TPS(Transaction per Second)에 달할 것으로 예측된다[11]. 이는 하이퍼레져 패브릭(Hyperledger Fabric)의 3-4000TPS만큼이나 빠른 속도이다. 이러한 이유로 최근 높은 활용도와 충분한 거래 속도를 가진 이더리움에 대해 큰 수요가 발생했고, 본 논문에서도 이더리움 프레임워크를 사용하여 개발하였다.

Fig. 9. Webpage for Shipper

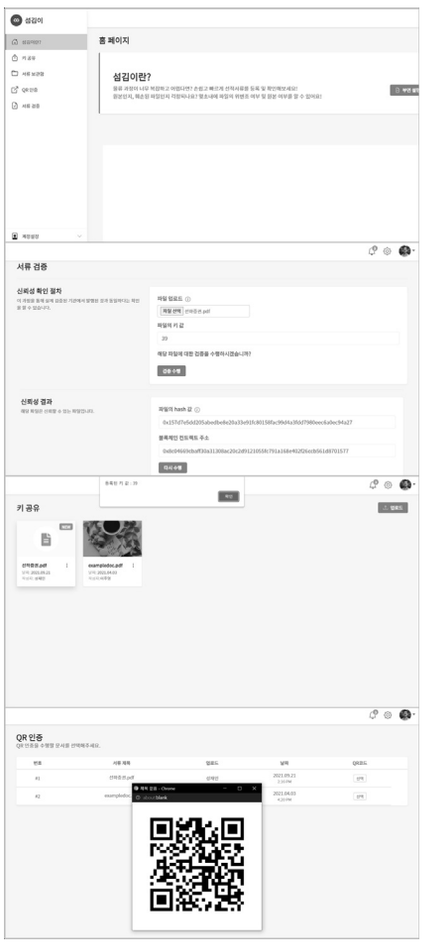

Fig. 10. Webpage for Consignee

4.1 웹페이지 화면

스프링 기반으로 제작한 웹페이지로, 수출인 페이지와 수입인 페이지로 나뉜다.

1) 수출인 페이지

Fig. 9와 같이 수출인 페이지는 서류 공유, 서류 보관함, 키 공유, QR코드 검증 페이지로 구성된다. 서류 공유에서는 OCR을 통해 추출된 서류 정보의 원본은 IPFS에, 원본의 해시값은 블록체인에 저장된다. 이는 거래 중인 수입인과 등록된 서류를 함께 공유하게 되는 기능이다. 수입인의 계정 구조체의 변수에 서류의 위치를 저장함으로써 가능하게 된다. 서류 보관함에서는 공유한 파일을 볼 수 있고, 해당 선하증권을 다운받을 수 있다. 키 공유에서는 수입인에게 필요한 파일의 위치 값을 공유하는 페이지이다. QR코드 검증에서는 수입인이 제시한 서류의 해시값이 실제 선하증권이 맞는지를 검증하는 페이지이다.

2) 수입인 페이지

Fig. 10과 같이 수입인 페이지는 서류 검증, 서류 보관함, 키 공유, QR코드 인증 페이지로 구성된다. 서류 보관함에서는 수출자가 수입인을 대상으로 공유한 파일을 열람할 수 있다. 그 파일이 실제 선하증권이 맞는지 확인하기 위해서는 서류 검증 페이지를 사용해야 한다. 블록체인에 저장된 서류의 해시값과 사용자가 입력한 서류의 해시값이 일치하는지 여부를 판단해 출력한다. QR코드 인증 페이지는 소유한 선하증권 해시값으로 QR코드를 생성하게 되는 원리로, 신속하게 물품을 인도받을 수 있게 된다.

4.2 웹페이지 동작

Web3.js는 웹페이지에서 저수준 JSON-RPC API를 감싸서 자바스크립트로 만든 고급 API이다[12]. Web3.js를 통해 블록체인 네트워크와 상호작용할 수 있다. 웹페이지에서 배포된 컨트랙트를 호출하기 위해서 해당 컨트랙트의 ABI (Application Binary Interface)와 컨트랙트 주소를 함께 사용했다. 웹 오브젝트에 적절한 자바스크립트 함수를 할당하고, 해당 자바스크립트 함수는 특정 컨트랙트 함수를 호출하도록 한다. 컨트랙트 함수는 구조체의 상태변수를 읽거나 쓰는 원리로 동작한다. 예를 들어 _registerDoc() 자바스크립트 함수는 사용자에게 입력받은 consigneeAddress(수입

```
function _registerDoc() {
    $("#DocRegistrationMessage").html('');
    consigneeAddress = $("#setting-input2").val();
    shipperAddress = $("#signup-ID").val();
    var _hash = HashValue;
    DocumentTransfer.at(contractAddress).deployed()
    .then(instance => instance.isRegisteredShipper(shipperAddress))
    .then(isRegisteredShipper => {
        if (isRegisteredShipper)
        {
            instance.registerDoc(_hash, consigneeAddress);
            $("#DocRegistrationMessage").html("Registration successed.");
        }
        else
        {
            $("#DocRegistrationMessage").html("The shipper is unknown.");
        }
    })

function _isDocSame() {
    $("#DocCompareMessage").html('');
    var _index = $("#setting-input2").val();
    var _hash = HashValue;
    DocumentTransfer.deployed()
    .then(instance => instance.isDocSame(_hash, _index))
    .then(isDocSame => {
        if (isDocSame)
        {
            setDocisChanged(_index, 0);
            $("#DocCompareMessage").html('This file matches the original. You
        }
        else
        {
            setDocisChanged(_index, 1);
            $("#DocCompareMessage").html('This file is inconsistent with the
        }
    })
}
```

Fig. 11. Webpage Implementation with Javascript

```
struct Shipper {
    uint [] DocuIndex;
    bool isRegistered;
}

struct Consignee {
    uint [] DocuIndex;
    bool isRegistered;
}

struct Document {
    uint index;
    bytes hashValue;
    bool isChanged;
    uint status;
}

modifier onlyRegisteredShipper() {
    require(shippers[msg.sender].isRegistered,
        "the caller of this function must be a registered Consignee");
    _;
}

modifier onlyRegisteredConsignee() {
    require(consignees[msg.sender].isRegistered,
        "the caller of this function must be a registered Consignee");
    _;
}

mapping(address => Shipper) public shippers;
mapping(address => Consignee) public consignees;
Document [] public documents;

constructor() public { }
```

Fig. 12. Structure of Smart Contract

인 계정)과 _hash(파일 해시값)을 인자로 컨트랙트 함수인 registerDoc()함수를 호출한다. Fig. 11은 이상의 웹페이지 동작을 수행하는 자바스크립트이다.

4.3 스마트컨트랙트

스마트컨트랙트는 solidity언어로 0.5.16버전에서 작성되었다. 수입인과 수출인 그리고 서류 구조체를 생성하였다. 수입인과 수출인은 각각 소유한 서류 위치를 담은 변수, 그리고 계정 등록 여부를 확인하는 변수가 있다. 서류 구조체에서는 해당 선하증권의 위치, 해시값, 위변조 여부 그리고 상태를 담는 변수를 가진다. 수입인과 수출인의 계정과 구조체를 묶기위해 mapping을 사용했다. 또한 여러 선하증권을 통합 관

```
function registerShipper(address _shipperAddress)
    public {
    require(!shippers[ _shipperAddress].isRegistered, "the shipper is a
    shippers[ _shipperAddress].isRegistered = true;
}

function registerConsignee(address _consigneeAddress, uint _index)
    public onlyRegisteredShipper {
    if (consignees[ _consigneeAddress].isRegistered){
        consignees[ _consigneeAddress].DocuIndex.push(_index);
    } else {
        consignees[ _consigneeAddress].DocuIndex.push(_index);
        consignees[ _consigneeAddress].isRegistered = true;
    }

}

function registerDoc( bytes memory _hashValue, address _consigneeAddres
    uint _index =
    documents.push(Document({
        index : 0,
        hashValue: _hashValue,
        isChanged: false,
        status : 1
        }));
    documents[_index].index = _index-1;
    shippers[msg.sender].DocuIndex.push(_index -1);
    registerConsignee(_consigneeAddress, _index-1);
}

function getDocHash(uint _index) public
    returns (bytes memory) {
    documents[_index].status = 2;
    return documents[_index].hashValue;
}
```

Fig. 13. Functions of Smart Contract

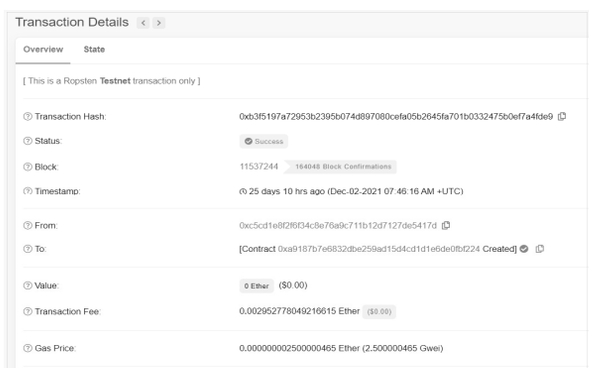

Fig. 14. Deployed Contract

리할 documents 리스트를 구성하였다. Fig. 12는 구현한 스마트컨트랙트 구조를 보여준다.

Fig. 13과 같이 컨트랙트 내의 구조체의 변수를 읽거나 쓰기 위해 함수를 사용한다. 예를 들어 registerDoc()함수는 자신의 계정과 수입인 계정의 DocuIndex(소유한 문서 리스트)에 등록된 파일의 해시값을 입력한다. 이 과정을 통해 특정 계정이 소유한 파일의 위치를 알 수 있고, 해시값을 가져올 수 있다. IPFS에서 해시값을 입력하여 최종적으로 파일의 원본을 다운받을 수 있다.

Fig. 14와 같이 구현한 컨트랙트는 실제 Ropsten 테스트 네트워크에서 배포 완료하였다. 배포된 컨트랙트는 Ether Scan에서 확인할 수 있다[13].

5. 결론 및 향후 연구

본 논문에서는 블록체인 선하증권 시스템을 설계 및 구현하였다. 블록체인을 사용한 선하증권 거래 시스템은 거래자

간의 신뢰성과 편의성을 높이고, 기존의 신용장 관련 문서 검증 프로세스 과정과 비용, 그리고 시간을 줄이는 기능을 제공한다. 제안 시스템은 더 나아가 AI 기반의 OCR 기능으로 서류 등록의 과정을 간편화하고, QR코드를 통한 물품 인도 과정을 간결화한다는 장점을 가지고 있다. 현재 사용자 웹페이지 개발과 스마트컨트랙트 배포를 완료하였다. 향후 OCR기능과 QR코드의 기능 구현과 웹 서버와 컨트랙트 간 연동 기능 개발을 진행할 예정이다.

References

[1] H. S. Bae, "The applications of blockchain technology on electronic bill of lading," *Korea International Commerce Review*, Vol.34, No.2, pp.121-139, 2019.

[2] M. L. Shope, "The bill of lading on the blockchain: An analysis of its compatibility with international rules on commercial transactions," *Minnesota Journal of Law, Science & Technology*, Vol.22, No.1, pp.167-170, 2021.

[3] J. H. Yang, "Applicability of blockchain based bill of lading under the rotterdam rules and UNCITRAL model law on electronic transferable records," *Journal of Korea Trade*, Vol.23, No.6, pp.120-124, 2019.

[4] T. Jensen, S. Henningsson, and J. Hedman, "Delivery business value with blockchain technology: The long journey of tradelens," *MIS Quarterly Executive*, Vol.18, No.4, pp.18-21, 2019.

[5] M. C. Im, Automating imports and exports, predicting and optimizing logistics…SI Big 3, Digital Logistics Betting [Intenet], https://www.ajunews.com/view/20220117085045762#PL2poliIsueId=ISUE_000000000000989&menuNo=200046&pageIndex=1.

[6] Steven Kim, MSC introduces blockchain-based e-B/L [Internet], https://www.cargonews.co.kr/news/articleView.html?idxno=47309.

[7] I. S. Chung, Alibaba Launches Antchain-based Trade Finance Platform Trusple [Internet], https://www.coindeskkorea.com/news/articleView.html?idxno=71723.

[8] N. Sarika, N. Sirisala, M. S. Velpuru, "CNN based optical character recognition and applications," *2021 6th International Conference on Inventive Computation Technologies*, pp.23-27, 2021.

[9] Designing and Developing Blockchain-based Bill of Lading SysTem [Internet], https://github.com/ZZerow/SWUperpower.

[10] William Foxley, Amazon Managed Blockchain at Last Supports Ethereum, Ending a Two-Year Tease [Internet], https://www.coindesk.com/tech/2021/03/02/amazon-managed-blockchain-at-last-supports-ethereum-ending-a-two-year-tease/.

[11] N. J. Baeck, The reason why DeFi's core ETHERUM continues to rise beyond FinTech [Internet], https:// trendw.kr/2021-01056859.t1m.

[12] R. Infante, "Building Ethereum Dapps," MANNING, Hanbit Media (2020), pp.361, 2020.

[13] Etherscan, Transaction Details [Internet], https://ropsten.etherscan.io/tx/0xb3f5197a72953b2395b074d897080cefa05b2645fa701b0332475b0ef7a4fde9.

[14] J. J. Kim, and K. H. Yu, "A study of the possibility for increasing the use of blockchain technology for import and export customs clearance," *The Journal of Korea Research Society for Customs*, Vol.21, No.4, pp.51-69, 2020.

[15] S. B. Choi, "A study on the commercialization of blockchain bill of lading," *Korea Logistics Review*, Vol.29, No.1, pp.97-110, 2019.

[16] M. G. Belu, "Application of blockchain in international trade: An overview," *The Romanian Economic Journal*, Vol.22, No.71, pp.2-16, 2019.

[17] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for IPFS," In *Proceedings of the IEEE Ithings-Greencom-Cpscom-Smartdata 2018*, pp.1499-1506, 2018.

[18] S. Desai, R. Shelke, O. Deshmukh, H. Choudhary, and S. S. Sambare, "Blockchain based secure data storage and access control system using IPFS," *IEEE Access*, pp.59389-59401, 2020.

[19] N. Nizamuddina, K. Salaha, M. A. Azad, J. Arshadc, and M. H. Rehmand, "Decentralized document version control using ethereum blockchain and IPFS," *Science Direct*, Vol.76, pp.183-197, 2019.

[20] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, pp.2411-2502, 2020.

[21] S. H. Jeong, "A design and implementatation of blockchain based smart stock trading system," Masters thesis, Soongsil University, 2016.

[22] S. h. Yang, H. Y. Jin, and S. K. Kim, "Implementation of a blockchain-based talent trading platform to reduce transaction costs," *The Korean Institute of Broadcast and Media Engineers*, Vol.25, No.6, pp.922-934, 2020.

[23] H. Y. Park, M. J. Jeon, and S. H. Lee, "BlockToon: Webtoon platform based on blockchain," *Korea Society of Computer Information*, Vol.27, No.2, pp.41-44, 2019.

[24] S. W. Han, M. S. Bae, and G. H. Hwang, "Development of electronic voting system based on blockchain using homomorphic encryption," *The Korean Institute of Communications and Information Sciences*, Vol.44, No.1, pp.171-174, 2019.

[25] C. H. Suk, M. Y. Park, Y. B. Song, and W. S. Rhee, "Development of a blockchain based trusted trading platform," *Korea Digital Contents Society*, Vol.22, No.8, pp.1153-1163, 2021.
[26] K. J. Sung, C. R. Jeong, E. N. Cho, J. H. Lee, H. Y. Kim, Y. W. Kim, and K. H. Rhee, "An intramural electronic voting system based on blockchain," *Korea Institute of Information Security & Cryptology*, Vol.28, No.4, pp.779-787, 2018.
[27] N. H. Choi, and H. Y. Kim, "A blockchain-based user authentication model using metamask," *Korea Society For Internet Information*, Vol.20, No.6, pp.119-127, 2019.

이 주 영
https://orcid.org/0000-0002-0962-1896
e-mail : jn322@swu.ac.kr
2018년 ~ 현 재 서울여자대학교 정보보호학과 학사과정
관심분야 : Blockchain & Penetration testing

김 현 아
https://orcid.org/0000-0001-9195-9329
e-mail : vikim1210@swu.ac.kr
2019년 ~ 현 재 서울여자대학교 정보보호학과 학사과정
관심분야 : Front-end Develop

성 채 민
https://orcid.org/0000-0003-1077-4627
e-mail : cmalice@swu.ac.kr
2019년 ~ 현 재 서울여자대학교 정보보호학과 학사과정
관심분야 : Front/Back-end Develop & Blockchain

김 정 민
https://orcid.org/0000-0001-8627-865X
e-mail : cocowin@naver.com
1994년 고려대학교 정보공학과(학사)
2003년 고려대학교 응용전자공학(석사)
1996년 ~ 2013년 KT 기술거래, 신사업기획
2013년 ~ 2020년 KT 기술 조사, 경영기획 BDO
2021년 ~ 현 재 KT 강북/강원 법인고객본부 AI TF 차장
관심분야 : AI & Service Robot & Technology Trading

김 성 욱
https://orcid.org/0000-0003-4789-3347
e-mail : kim.sungwook@swu.ac.kr
2005년 서울대학교 수학과(학사)
2012년 서울대학교 수학과(석・박사)
2014년 ~ 2020년 삼성전자 Samsung Research 연구원
2020년 ~ 현 재 서울여자대학교 정보보호학과 조교수
관심분야 : Cryptography & Privacy Protection & Blockchain