The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 3, pp.97-103, Jun. 30, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.3.97
JIIBC 2019-3-13

블록체인 기반의 계약관리 플랫폼 연구

A Study on Contract Management Platform Based on Blockchain

김성환*, 김영곤**

Sunghwan Kim*, Younggon Kim**

요 약 ICT 기술의 발달에 따라서 계약관리 과정을 어플리케이션 기반으로 통합하여 관리하는 방식의 전자계약 시스템이 널리 보급되어 있으며, 최근에는 블록체인 기술을 활용한 개선방법들이 연구되고 있다. 그러나 계약관리 시스템에는 처리성능, 보안 취약성, 데이터 오 입력, 서비스 접근성 문제를 가지고 있다. 본 논문에서는 블록체인, 스마트 컨트렉트, Rest API의 구성을 가지는 블록체인 기반 계약관리 플랫폼을 제안하였다. 제안되는 플랫폼에는 기존의 합의인증 알고리즘의 처리 성능과 보안 취약성 문제를 해결한 RPBFT 알고리즘과 참여자의 데이터 오 입력 방지와 투명성을 강화하기 위한 알고리즘을 프로세스를 함께 제시하였다. 본 논문에서 제안한 블록체인 기반 계약관리 플랫폼은 개선된 처리 성능과 보안성, 신뢰성, 투명성을 가진 사용환경을 제공하고, 구축에 대한 부담 없이 API를 통해 사용이 가능하므로 비용 절감 측면과 기술의 확산 측면에서도 효과를 기대할 수 있다.

Abstract Electronic contract systems are widely used to integrate and manage the contract management process based on the development of ICT technology. Recently, improvement methods using block chain technology are being studied. However, contract management systems have processing performance, security vulnerabilities, data entry, and service accessibility issues. In this paper, we propose a block - chain based contract management platform with block chain, smart contract, and Rest API. The suggested platform includes the RPBFT algorithm which solves the processing performance and security vulnerability of the existing consensus authentication algorithm, and the algorithm to prevent data entry and enhance transparency of participants. The block-chain-based contract management platform proposed in this paper provides a use environment with improved processing performance, security, reliability, and transparency, and can be used through API without burdening construction. Therefore, The effect can be expected.

Key Words : Blockchain, Ledger, Management, RPBFT, Smart Contract, Random node, Validation

*김성환, 한국산업기술대학교 컴퓨터공학과 linne@kpu.ac.kr
접수일자 2019년 5월 9일, 수정완료 2019년 5월 30일
게재확정일자 2019년 6월 7일

Received: 9 May, 2019 / Revised: 30 May, 2019 / Accepted: 7 June, 2019
*Corresponding Author: ykkim@kpu.ac.kr
Department of Computer Engineering, Korea Polytechnic University, Korea

Ⅰ. 서 론

ICT 기술의 발달에 따라서 종래에 인쇄물 형태로 출력한 문서를 기반으로 관리되었던 제안, 참여, 이행, 검증, 지급단계에 이르는 계약관리 과정의 산출물들을 전자적 형태로 저장하고 계약의 진행 단계별 프로세스를 정의하여 어플리케이션 기반으로 통합하여 관리하는 방식의 전자계약 시스템이 대중화되어 가고 있다.

전자계약 시스템은 계약의 모든 과정을 전자적 형태로 저장하고 협업할 수 있기 때문에 불필요한 과정을 최소화 하여 업무 효율성을 향상시킬 수 있다[1].

그러나, 중앙화 시스템의 특성상 재해에 대한 취약성이 있으며, 계약의 위변조 등의 침해요인이 증가하는 문제점과 시스템 사용자들 간의 데이터 공유가 원활하지 않아 투명성이 저하되는 문제점이 있다. 또한 데이터의 입력 실수로 인해 원본의 데이터 오류가 발생할 수 있으며, 개발 및 운영에 대한 기술적, 비용적 부담으로 인해 서비스 접근성이 떨어지는 문제점이 있어, 기술 확산에 어려움이 있다[2].

본 논문에서는 기존 블록체인 기반 계약관리 시스템의 문제점을 해결하기 위해 블록체인과 스마트 컨트렉트, REST API의 구성된 블록체인 기반 계약관리 플랫폼을 제안하였다.

제안된 플랫폼은 기존의 합의 인증 알고리즘이 가지고 있는 처리 성능과 보안 취약성 문제점을 개선하여 고안한 RPBFT(Random Practical Byzantine Fault Tolerance) 합의인증 알고리즘을 적용하였고, 계약 제안단계부터 계약이 종료 단계까지 단계별로 효과적으로 프로세스를 수행할 수 있도록 스마트 컨트렉트를 활용하여 구현하는 방법을 고안한 알고리즘과 프로세스를 적용하였다.

Ⅱ. 관련 연구

1. 블록체인

블록체인은 일종의 분산된 디지털 장부라고 할 수 있다. 이 장부는 위변조할 수 없는 암호학적 기술로 만들어지며 거래(Transaction) 과정과, 발생한 거래를 모아 시간이 매우 오래 걸리는 특정 조건의 해시 값을 갖게 하는 난수(Nonce) 찾기 문제로 거래 내용의 위변조를 방지할 수 있는 작업증명(Proof of Work) 단계 등으로 만들어지며, 블록체인 인증 프로세스는 그림1과 같다.

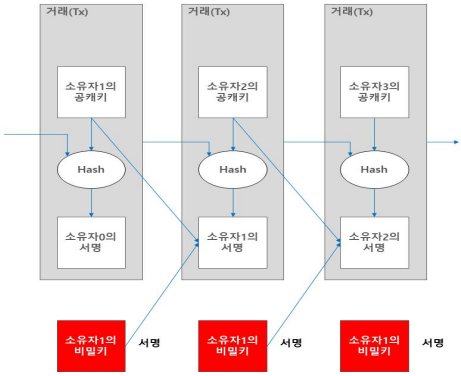

그림 1.블록체인 인증 프로세스
Fig. 1.Blockchain authentication process

분산장부 시스템을 통한 투명한 거래로 보안, 감독, 규제 비용 절감 가능 하며 P2P 네트워크 방식을 기반으로 참여자간 직접 거래가 이루어지기 때문에 중개기관 수수료가 발생하지 않는 장점이 있다[3].

블록체인은 탈 중앙화 구조이기 때문에 다수 참여자의 인프라를 공유하여 사용할 수 있어 대규모의 IT 장비와 인력으로 구성된 인프라를 요구하지 않는 장점을 가지고 있으나, 분산성과 익명성을 보장하는 시스템의 구조상 직접적인 통제가 필요한 시스템에 적용하기 어려운 문제가 있다.[4]

분산 원장 기술은 거래와 관련된 모든 데이터가 참여자들에게 공개하는 특성을 가지고 있어 정보 공개를 원하지 않거나 법 제도상 공개되지 않아야 하는 정보를 가지고 있는 환경에는 적용할 수 없는 문제가 있다. 이러한 문제점을 해결하기 위해 제한된 참여자를 위한 프라이빗 블록체인 기술들을 활용하여 적용하기 위한 대안이 연구되고 있다.[5].

2.스마트 컨트렉트(Smart Contract)

스마트 컨트렉트는 블록체인 플랫폼에 구현되어 있는 소프트웨어로 사전에 부여한 조건의 만족 유무에 따라 계약이 자동으로 이행되도록 보장하는 기능을 한다. 그러므로 스마트 컨트렉트는 인간의 개입 없이 스스로 이행하게 되므로 신뢰성을 보장할 수 있으며, 계약 참여자들 간의 신뢰를 시스템적으로 해결하기 위해 지정된 조건 범위에서 자동으로 이행되는 구조를 가지고 있다.

스마트 컨트렉트는 알고리즘 반복적으로 수행하는 과정을 가지므로, 지정된 조건에서는 효율적으로 처리 성능과 신뢰성을 가지는 장점이 있다. 스마트 컨트렉트의 활용분야는 비정형 데이터 처리를 통해 복잡한 의사 결정

이 요구되는 부분에 자동화를 목적으로 적용이 가능한 장점이 있다. 그러나 현재까지 스마트 컨트렉트는 블록체인 마다 활용방법에 차이가 있으며, 실제 성능 저하 현상과 보안 안정성에 대한 단점을 가지고 있어 개선이 필요하다[6],[7],[8].

3. 기존의 계약관리 시스템

종래의 계약관리 시스템은 전자계약 방식의 도입을 위해 서버, 사설인증서, 전자계약 시스템, Client 프로그램 등의 구성을 가지고 있다.

기존의 계약관리 시스템과 같은 구성의 시스템은 중앙관리의 특성상 4가지의 문제점을 가지고 있다.

첫째, 시스템 운영 주체가 쉽게 내용을 조작할 수 있다. 둘째, 투명하게 시스템이 공개되지 않아 신뢰성이 떨어진다. 셋째, 시스템의 장애 발생 시 서비스가 중단될 수 있다. 넷째, 법인 인증서, 사설인증서, 개인인증서 등의 다양한 인증서를 사용하기 때문에 관리가 어렵다.

확인된 문제점들을 개선하기 위해 블록체인 기술을 적용하여 개선한 시스템이 연구되고 있다. 개선된 블록체인 기반 계약관리 시스템은 기존 시스템의 문제점을 개선하였으나, 처리성능 문제와, 보안 취약성, 입력 단계에서의 오류, 시스템에 참여하기 위해 노드로 참여해야 하는 서비스 접근성 문제점이 있다[9].

본 논문에서는 기존의 블록체인 기반 계약관리시스템이 가지는 문제점을 개선하기 위한 블록체인 기반 계약관리 플랫폼을 제안하였다.

Ⅲ. 본문

1.계약관리 플랫폼 아키텍처

기존의 블록체인을 기반으로 만들어진 계약관리 시스템을 사용하기 위해서는 노드를 구성하여 참여해야 하는 문제점을 해결하기 위하여 본 논문에서는 블록체인 플랫폼, 스마트 컨트렉트, 클라이언트용 API로 구성되는 아키텍쳐를 제안하였다. 제안되는 계약관리 플랫폼은 문제점을 해결하기 위해 종래의 방식과 같이 노드를 구성하여 참여도 가능하고, 노드를 구성하지 못할 경우에는 계약관리 플랫폼에서 제공하는 REST API를 이용하여 참여할 수 있도록 하였다.

제안되는 블록체인 기반 계약관리 플랫폼의 아키텍처는 그림2와 같다.

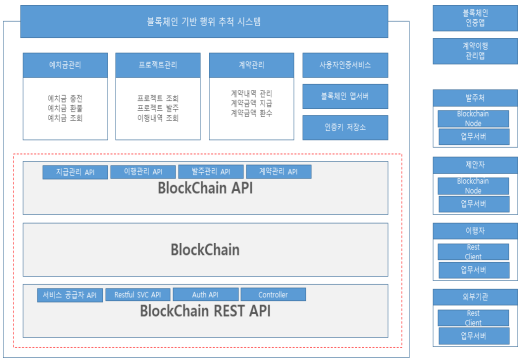

그림 2.블록체인 기반 계약관리 시스템 아키텍처
Fig. 2. Block Chain Based Contract Management System Architecture

2. RPBFT(Random Practical Byzantine Fault Tolerance)알고리즘

본 논문에서는 기존의 PBFT(Practical Byzantine Fault Tolerance)의 알고리즘의 처리 성능과 악의적 노드에 의한 취약성 문제점을 개선하기 위하여 RPBFT 합의인증 알고리즘을 고안하였고 그 동작하는 프로세스는 5단계로 구성된다.

1)최초 클라이언트에서 트랜젝션이 발생하여 합의를 요청하는 과정을 가진다.

2)Primary Node를 Random array를 이용하여 등록된 노드 중에서 무작위로 선정한다.

3)Pre-Prepare 과정을 통해 Primary Node가 요청에 대한 시퀀스 번호를 부여하고 다른 노드에 합의 요구를 위해 멀티캐스트 한다.

4)Prepare 과정을 통해 각 노드가 검증을 수행하고 그 결과를 자신 이외의 노드에 멀티캐스트 한다.

5)Commit 단계에서 각 노드가 Commit 메시지를 멀티캐스트 하며, 이후 4/5 이상의 다른 노드에서 같은 Commit 메시지를 보내오면 Commit 완료 상태로 기록한다.

본 논문에서 제안되는 노드 무작위 선정 알고리즘의 처리절차는 크게 2단계로 구성된다.

첫째, Primary Node가 악의적일 수 있는 가능성을 최소한으로 낮추기 위해 무작위로 노드를 선정하는 과정을 제한하였다. 선정 방법은 random array를 이용하여 난수를 발생하여 무작위로 Primary Node를 선정하는 과정을 가지며, Primary Node의 무작위 선정을 위한 알고리즘은 그림 3과 같다.

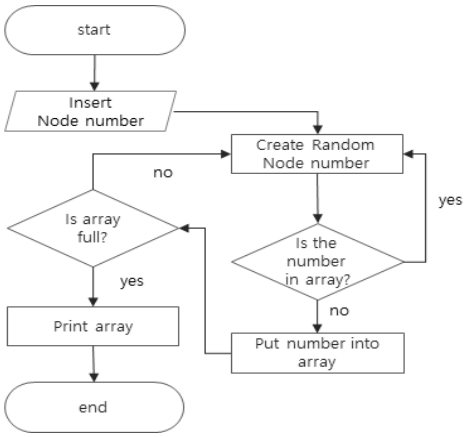

그림 3.노드 무작위 선정 알고리즘
Fig. 3. Node Random Recommendation Algorithm

둘째, 종래의 N = 3f + 1 구조의 성능 저하를 해결하기 위해서 (N − f) − f개의 메시지가 악의적 노드에서 보낸 f개의 메시지보다 많아야 하는 조건을 충족하면서, 최대 수용 f 값을 낮추어 시스템의 부하를 낮출 수 있도록 N = 5f + 1의 악의적 노드 허용 값을 가지는 알고리즘을 제안하였다.

제안된 방법은 Public 블록체인 환경에서는 보안성이 저하되는 문제점이 발생할 수 있으나, 사용자 식별을 전제로 운영되는 Private 환경에서는 계약과정에서의 노드 간의 합의 과정을 간소화하여, 처리 성능을 강화하는 것이 한정된 자원에서 효율성을 제공할 수 있다. 본 논문에서 제안한 계약관리 시스템 합의인증 알고리즘은 그림4와 같다.

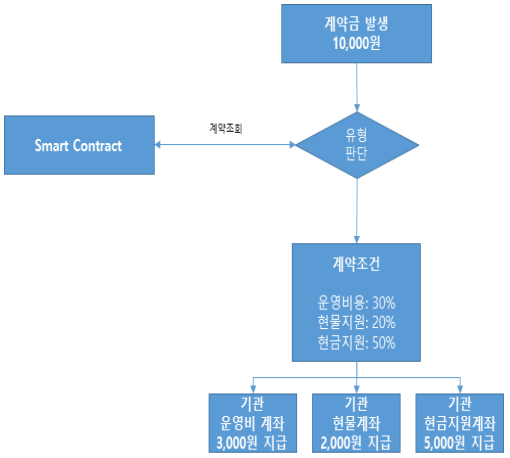

그림 4.계약관리 시스템 합의인증 알고리즘
Fig. 4. Contract management system agreement algorithm

3. 블록체인 기반 계약관리 시스템의 프로세스

본 논문에서 제안되는 블록체인 기반 계약관리 시스템의 인증 프로세스는 발주단계와 제안자 연계단계, 계약관리 단계, 이행관리 단계로 구성되어 있으며, 최초 사용자 인증을 통해 자격을 가지고 있는 사용자인지 확인하는 절차 이후 각 단계마다 부인방지를 위해 전자서명 검증 모듈을 이용하였다.

검증 작업을 통해 신뢰성을 확보하도록 하며, 계약 단계별로 확인되는 자격증명 모듈은 전자서명 이전 단계에서 부정한 접속을 방지하고, 참여자의 신원을 확인하는 용도로 이용된다. 블록체인 기반 계약관리 시스템 인증 프로세스는 그림5와 같다.

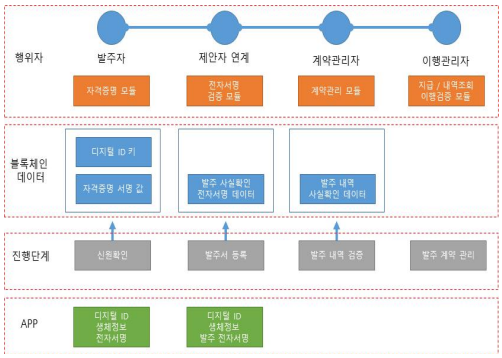

그림 5.블록체인 기반 계약관리 시스템 인증 프로세스
Fig. 5. Block Chain Based Contract Management System Certification Process

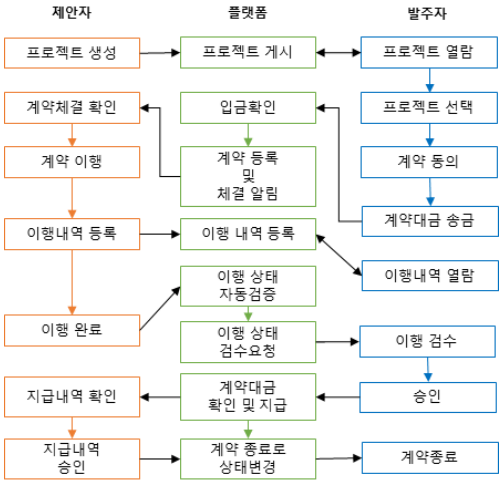

그림 6. 블록체인 기반 계약관리 시스템 프로세스
Fig. 6. Block Chain Based Contract Management System Process

계약 단계별로 구성되는 모든 프로세스를 종합하면 프로젝트의 등록 단계에서 계약이 생성되는 과정과 제안자와 이행자가 프로젝트를 이행하는 단계에서의 지급 및 이행을 검증하는 절차와 함께 최종적으로 계약 완료단계까지 수행한다. 블록체인 기반 계약관리 시스템의 프로세스는 그림6과 같다.

가. 프로젝트 생성단계

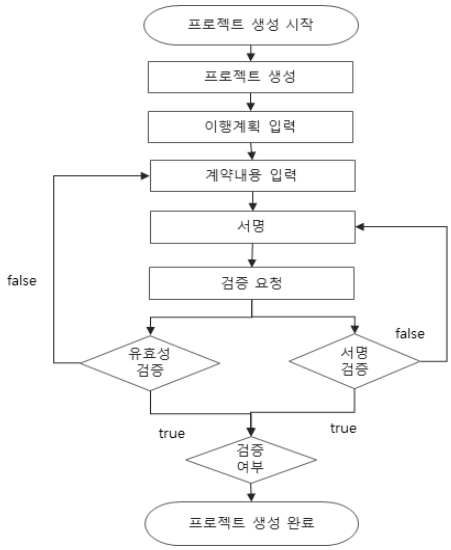

그림 7.프로젝트 생성 알고리즘
Fig. 7.Project creation algorithm

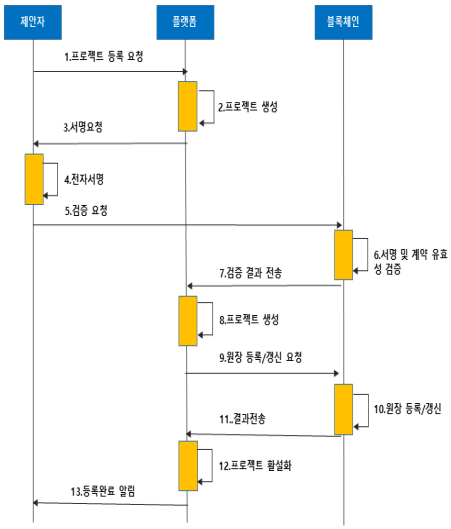

그림 8. 프로젝트 생성 시퀀스 다이어그램
Fig. 8. Project creation sequence diagram

프로젝트 생성단계에서는 프로젝트의 소개 및 이행계획을 입력한 후 계약 내용을 입력하여 계약 등록을 요청하고, 전자서명 절차를 통해 계약의 유효성과 서명의 검증 과정에서 검증 결과가 정상일 경우에 생성되는 과정을 가진다. 프로젝트 생성 알고리즘은 그림7과 같고, 프로젝트 생성 시퀀스 다이어그램은 그림8과 같다.

나. 계약체결 단계

계약 체결단계에서는 발주자가 프로젝트 내용을 열람한 후 원하는 거래를 선택한 후 계약 발주금액을 입력하고 발주 요청 단계에서 계약의 부인 방지를 위해 전자서명 절차를 수행한 후 서명의 유효성 검증 결과가 유효한 경우에 최종적으로 계약이 체결되는 단계를 가진다. 계약 체결 단계 알고리즘은 그림 9와 같고 계약체결단계 시퀀스 다이어그램은 그림 10과 같다.

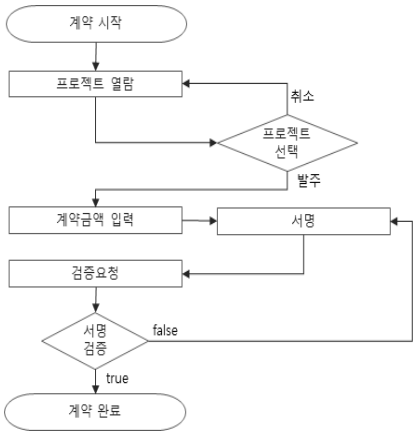

그림 9. 계약체결 단계 알고리즘
Fig. 9. Contract concluding phase algorithm

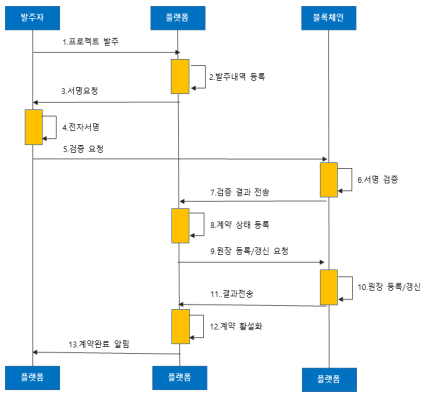

그림 10.계약체결단계 시퀀스 다이어그램
Fig. 10. Contract phase sequence diagram

다. 계약이행 단계

계약 이행단계에서는 입력되는 데이터의 유형을 분류하는 절차를 가진다. 신규 계약인 경우 원장 생성을 하고 이행 과정으로 분류될 경우 스마트 컨트렉트로 유효성 검증을 하여 계약에서 지정한 범위를 벗어난 오 입력을 방지하는 절차를 가지며, 이행 내역을 등록하는 자의 부인 방지를 위한 인증과정을 가진다. 유효성 검증 절차에서의 검증 실패의 경우 부정 입력 및 오 입력으로 분류하여 계약 데이터 등록을 하지 않고 종료하여 데이터 무결성을 보장할 수 있다. 계약 이행단계 알고리즘은 그림 11과 같다.

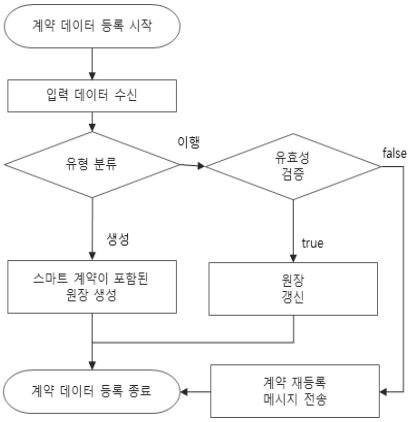

그림 11.계약 이행단계 알고리즘
Fig. 11. Contract fulfillment phase algorithm

라. 계약 조회단계

계약 조회단계에서 계약자는 시스템에 로그인을 완료한 상태에서 계약조회 요청이 가능하다.

계약조회 요청 단계에서는 사용자 클라이언트를 이용하여 부정한 용도로 계약을 조회하여 계약정보가 유출되는 것을 방지하기 위한 절차를 가진다.

시스템에서 생성되는 Seed Word 기반의 난수표 값을 Challenge and Response 방식으로 정상적인 값을 사용자가 입력하여 응답하는 방식의 인증절차를 가진다.

사용자의 계약이행 목록을 조회하기 위해 계약번호를 입력하거나 계약명을 입력하여 조회하는 과정을 가지며, 조건 검증 시 일치하는 항목을 열람을 할 수 있다. 열람 이력이 기록되면서 계약조회 과정은 종료된다. 본 논문에서 제안한 계약조회 알고리즘은 그림 12와 같다.

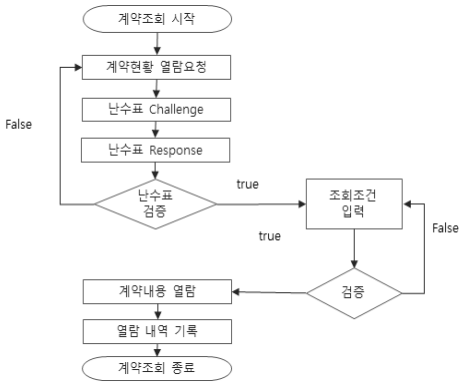

그림 12.계약 조회 알고리즘
Fig. 12. Contract inquiry phase algorithm

Ⅳ. 결론

본 논문에서는 기존의 중앙화 구조의 계약관리 시스템에 나타나는 성능저하, 보안 취약성, 데이터 입력 오류, 초기 비용 부담으로 인한 서비스 접근성 문제를 해결하기 위해 기존의 계약관리 시스템이 가지는 클라이언트 서버 구조에 블록체인, 스마트 컨트렉트, Rest API를 결합하여 계약관리 시스템 아키텍처 플랫폼을 제안하였다.

제안된 블록체인 기반 계약관리 플랫폼은 기존의 계약관리 시스템의 문제를 해결하기 위해 3가지 방법을 제안하였다.

첫째, 악의적 노드에 의한 보안 취약성 문제를 해결하기 위해 Random array 기술을 활용하여 Primary Node를 무작위로 선정하는 절차를 추가하여 악의적 노드가 발생할 가능성을 최소화 할 수 있는 방법을 제안하였다.

둘째, 성능저하 문제를 개선하기 위해 합의를 위한 조건인 (N − f) − f개의 메시지가 악의적 노드에서 보낸 f개의 메시지 보다 많아야 하는 조건을 충족하면서, 시스템의 부하를 감소시키기 위해 시스템의 악의적 노드의 최대 허용 수를 낮추어 N=5f+1의 Fault를 보장하도록 개선한 RPBFT 알고리즘을 제안하였다.

셋째, 스마트 컨트렉트를 통해 계약에서 지정한 범위를 벗어난 데이터 입력을 방지하기 위한 유효성 검증절차를 가지며, 사용자 인증과 별도로 프로젝트 생성, 체결, 이행의 각 단계별로 부인 방지와 계약 유효성 검증을 위한 전자서명 검증 절차로 신뢰성을 확보하였다. 계약 이

행 단계에서 스마트 컨트렉트로 계약 조건 충족 여부를 확인하는 절차로 계약을 이행하는 이행 단계의 신뢰성을 확보하였다. 계약 조회 단계에서는 시스템에서 생성되는 Seed Word 기반의 난수표 값을 Challenge and Response 방식으로 응답 값을 사용자가 입력하는 값을 검증하는 절차로 보안을 강화하여 데이터 유출을 최소화하는 알고리즘과 프로세스에 대해 제안하였다.

본 논문에서 제안되는 블록체인 기반 계약관리 플랫폼은 각 단계별로 데이터 유효성 검사와 검증 절차를 통해 신뢰성과 보안성을 확보하고, 계약 참여자들에게 투명하게 공유되어 투명성을 확보하여 신뢰성 있고 투명한 계약관리 환경을 제공할 것이며, 구축 및 개발에 대한 부담없이 플랫폼 서비스를 사용할 수 있어 비용 절감 측면과 기술의 확산 측면에서도 효과를 기대할 수 있다.

향후 블록체인 기반 계약관리 플랫폼의 아키텍처와 알고리즘을 기반으로 하여 모든 기부 단계가 참여자 모두에게 공개되며, 이력 추적이 가능한 스마트 기부관리 플랫폼을 구현하고자 한다.

References

[1] Jae-Nam Kim, Jong-Ryeol Park, "Study on the Electronic Contract", Journal of The Korea Society of Computer and Information, Vol. 19, No. 6, pp.129-138, June 2014.
DOI: http://dx.doi.org/10.9708/jksci.2014.19.6.129

[2] Seok-beom Choi, Jae-woo Jeong, Tae-hwan Kim, In-kyung Kim, "A Study on the Electronic Contract Service and Cases", The Journal of internet electronic commerce research, Vol. 7, No. 2, pp.171-195, July 2007.
DOI: http://dx.doi.org/10.9708/jksci.2014.19.6.129

[3] Jae-pil Ryu, Hyun-Joon Shin "Blockchain Technologies and Applications", Journal of Information Technology and Architecture, vol.15, no.3, pp. 357-364, Sep, 2018.
DOI: http://dx.doi.org/10.15616/BSL.2018.24.3.196

[4] Satoshi Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System", Oct, 2008.
DOI: 10.17487/RFC7662

[5] Soon-duck Yoo , Ki-heung Kim, "A Study on Improvement for Service Proliferation Based on Blockchain", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 18, No. 1, pp.185-194, Feb, 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.1.185

[6] Chul-Jin Kim, "A Static and Dynamic Design Technique of Smart Contract based on Block Chain", Journal of the Korea Academia-Industrial, Vol. 19, No. 6 pp. 110-119, March, 2018.
DOI: https://doi.org/10.5762/KAIS.2018.19.6.110

[7] Je-ho Song, Sang-Hyeok Kim, Sungyong Park, "Experiment and Analysis of Ethereum Smart Contract Performance Decline", KIISE Transactions on Computing Practices, Vol. 24, No. 7, pp. 381-384, July, 2018.
DOI:https://doi.org/10.5626/KTCP.2018.24.7.381

[8] Ji-Sun Park, Taek-Young Youn, Hye-Bin Kim, Kyung-Hyune Rhee, Sang-Uk Shin, "Smart Contract-Based Review System for an IoT Data Marketplace", Sensors Vol.18 No.10, pp. 3577, Oct, 2018.
DOI: http://dx.doi.org/10.3390/s18103577

[9] Kyoung-Nam Lee, Gyea-hyung Jeon, "A Study on Improvement of Used-goods Market Platform Using Blockchain", Journal of Digital Convergence Vol. 16. No. 9, pp. 133-145, July, 2018.
DOI: https://doi.org/10.14400/JDC.2018.16.9.133

저 자 소 개

김 성 환(정회원)

•2009년 2월 : 열린사이버대학교 정보통신공학과(공학사)
•2017년 8월 : 한국산업기술대학교 소프트웨어융합공학과(공학석사)
•2017년 9월 ~ 현재 : 한국산업기술대학교 컴퓨터공학과 박사과정
•관심분야 : 소프트웨어공학, 정보통신시스템, 분산형 원장기술

김 영 곤(정회원)

•1983년 2월 : 경북대학교 전자공학과(공학사)
•1985년 2월 : 연세대학교 본대학원 전자공학과(공학석사)
•2000년 2월 : 한국과학기술원 전산학과(공학박사)
•1985년 ~ 2007년 : KT 수석연구원
•2007년 ~ 현재 : 한국산업기술대학교 컴퓨터공학과 교수
•관심분야 : 소프트웨어공학, 정보통신시스템, 객체지향 분석 및 설계