

블록체인 기반 탈중앙화 신원증명 환경에서의 계약 플랫폼

조정화*¹, 유수빈*², 유수민*³, 손애선*⁴*

Contract Platform in a Blockchain-based Decentralized Identity Environment

Jung-Hwa Jo*¹, Soo-Bin Yoo*², Su-Min Yoo*³, and Ae-Seon Son*⁴*

본 연구는 문화체육관광부 및 한국저작권위원회의 2019년도 저작권연구개발사업의 연구결과로 수행되었음.
(2019-SC-9500)

요 약

최근, 통신 기술의 발전과 개인 디바이스의 보급에 따라 전자 계약 기술이 금융, 보험, 부동산, 근로 계약 등 다양한 산업 분야에 적용되고 있다. 전자 계약 플랫폼에 대한 관심이 커짐에 따라 시장규모는 지속해서 성장하고 있고 기존의 전자 계약 플랫폼을 개선하기 위해 중앙 정부와 기업에서 많은 투자를 하고 있다. 그러나 계약 시스템은 여전히 중앙 집중구조에서 운영되어 악의적인 사용자에 의해 계약서가 위·변조가 되고 온라인으로 주고받는 계약서는 권리의 유효성을 검증하지 못하는 문제를 가지고 있다. 본 논문에서 제안하는 플랫폼은 블록체인(Blockchain)을 기반으로 보안성, 투명성을 강화하고 탈중앙화 신원증명(DID, Decentralized Identity) 환경에서의 계약을 체결하여 사용자의 자격 및 신원을 검증하고, 계약서를 직접 관리하여 악의적인 사용자에게 의해 계약서 위·변조를 방지할 수 있는 플랫폼을 제안하고자 한다.

Abstract

Recently, with the development of communication technology and the spread of personal devices, transfer contract technology is being applied to various industrial fields such as finance, insurance, real estate, and labor contracts. As interest in the electronic contract platform grows, the market size continues to grow and the central government and enterprises are investing heavily to improve the existing electronic contract platform. However, the contract system is still operated in a centralized structure, and the contracts are forged or altered by malicious users, and the contracts exchanged online have a problem that the validity of the rights cannot be verified. The platform proposed in this paper reinforces security and transparency based on Blockchain, and concludes a contract in a decentralized identity (DID) environment to verify the user's qualifications and identity, and We would like to propose a platform that can prevent forgery or falsification of contracts by malicious users by directly managing them.

Keywords

blockchain, decentralized identity, online contract platform, smart contract, information security

* 경주스마트미디어센터 연구원 (*²교신저자) · Received: Nov. 24, 2020, Revised: Dec. 24, 2020, Accepted: Dec. 27, 2020

- ORCID¹: <https://orcid.org/0000-0002-1144-7153>

- ORCID²: <https://orcid.org/0000-0001-8095-7862>

- ORCID³: <https://orcid.org/0000-0001-5643-1422>

- ORCID⁴: <https://orcid.org/0000-0001-5153-2929>

· Corresponding Author: Soo-Bin Yoo

Strategic Planning Dept. Gyeongju Smart Media Center, 587-18

Gyeonggam-ro, Gyeongju, 38118, Korea

Tel.: +82-54-781-2943, Email: yoosobin@silgam.or.kr

I. 서론

통신 기술의 발전과 개인 디바이스의 보급에 따라 전자 계약 플랫폼이 금융, 보험, 부동산, 근로 계약 등 다양한 분야로 확장되고 있다. 전자 계약 플랫폼은 계약의 공고, 참여, 이행, 검증, 정산단계에 이르는 과정을 온라인에서 전자 문서 형태로 저장하기 때문에 불필요한 과정을 최소화하여 계약 업무의 효율성을 증가시킬 수 있다.

그러나 중앙 집중구조로 이루어진 전자 계약 플랫폼은 계약서의 위·변조 가능성, 보안의 취약성 등 다양한 문제점과 계약 당사자가 계약서를 e-mail, 메신저로 주고받아 계약을 체결하는 과정에서 개인의 신원 및 자격, 권리 유무를 검증하지 못하고 진행하고 있다.

본 논문에서 제안하는 플랫폼은 기존의 계약 플랫폼의 문제점을 해결하기 위해 블록체인(Blockchain) 기반 탈중앙화 신원증명 환경에서 계약을 위한 플랫폼을 제안한다. 제안하는 플랫폼은 블록체인 2세대 모델인 이더리움(Ethereum)을 기반으로 구현하였다. 이더리움은 비트코인과 다르게 블록 내부에 스마트 컨트랙트를 저장하여 모든 노드에 합의를 통해 공유된다. 본 논문에서 신원 증명서(Verifiable credential)를 스마트 컨트랙트에 저장하여 모든 참여자에게 투명하게 공유하며, 탈중앙화 신원증명(DID, Decentralized Identity)으로 사용자(Holder)가 계약서를 직접 관리할 수 있도록 구현했다.

II. 관련 연구

2.1 블록체인

블록체인은 데이터를 중앙서버에 보관하고 관리하는 방식이 아닌 참여자가 데이터를 공유하고 관리하는 분산원장으로 정의할 수 있다.

블록체인을 통한 투명한 거래로 보안에 대한 비용이 절감되며, P2P 네트워크 방식을 기반으로 참여자 간에 직접 거래가 이루어져서 중개 수수료가 발생하지 않는다[1].

블록체인의 구조는 가장 작은 단위인 트랜잭션(Transaction)과 트랜잭션들의 집합인 블록(Block), 블

록들이 연결되어 구성된 블록체인 구조로 구성되어 있다. 블록체인에서 트랜잭션은 참여자간의 거래 내역을 의미하며, 각 트랜잭션에 디지털 서명을 통해 거래에 대한 위·변조가 없음을 확인한다.

블록은 특정 시간 동안 모인 다수의 트랜잭션 집합으로 신규로 생성된 블록은 네트워크 내의 모든 참여자, 즉 노드에 전송되고 블록에 대한 검증을 통해서 블록은 각 노드가 가지고 있는 최근 블록에 연결된다, 연결된 블록은 수정이 불가능하여 영구히 저장된다. 이런 과정을 거쳐 블록체인이 형성된다.

제안하는 논문에 기반을 두고 있는 블록체인 네트워크는 2세대 블록체인, 이더리움이다. 이더리움은 블록체인 기술을 기반으로 스마트 컨트랙트 기능을 구현하기 위한 분산 컴퓨팅 플랫폼이자 운영체제로, 2015년 비탈릭 부테린이 개발한 2세대 블록체인이다[2].

이더리움은 비트코인과 달리, 스크립트 언어의 제한을 풀고 튜링 완전언어를 제공함으로써 스마트 컨트랙트를 이용한 모든 형태의 개발이 가능하도록 EVM 실행환경을 지원한다[3]. 제안하는 논문의 플랫폼은 블록체인 영역(Verifiable data registry)에 저장 공간으로 구현한다.

2.2 DID

DID는 사용자가 직접 자신의 데이터를 스스로 생성하고 관리하는 구조이다. DID의 표준을 제시하고 있는 단체 중 하나인 W3C에서는 Verifiable Credential Model의 신원 정보 검증 방식을 통해 DID 모델을 설명한다.

검증이란 사용자의 서명을 통해 신원 데이터의 진위검증이 가능하며, 그 진위 검증한 내용은 사용자가 임의로 변경 불가능하다. 서명은 사용자의 신원 정보를 설명하는 구조화된 정보이다. 또한, 해당 검증모델의 참여자로 인증하려는 사용자는 자신의 정보를 관리하는 주체이다. 사용자에 대한 검증 가능한 정보를 제공하는 신원정보 발행자(Issuer)는 사용자 신원 및 신원정보를 증명한다. 사용자의 신원 또는 상태에 대한 인증이 필요한 서비스 제공자(Verifier)는 블록체인에 저장된 신원증명 내역을 통해 사용자의 신원을 확인한다[4]-[6].

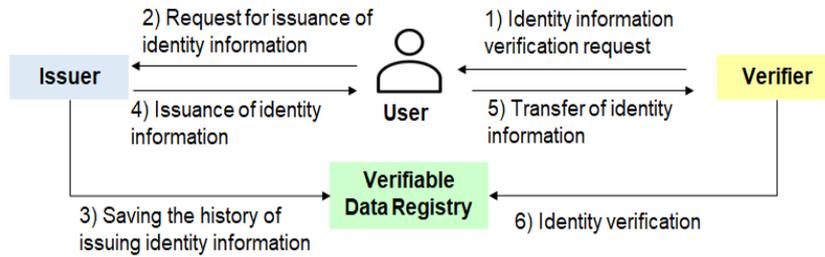


그림 1. 탈중앙화 신원증명 검증 과정

Fig. 1. DID verification process

DID는 개인의 검증 가능한 신원 정보(Verifiable credentials)를 분산 네트워크에 저장해 놓기 때문에 별도 중앙 서버 없이도 개인정보를 관리할 수 있다.

2.3 전자계약(Electronic Contract) 플랫폼 사례

전자 계약 플랫폼이 성장하면서 위·변조 문제, 보안 문제를 개선하는 계약 플랫폼이 등장하고 있다. 기존의 블록체인 기반 계약 관리 플랫폼 연구에는 RPBFT(Random Practical Byzantine Fault Tolerance) 합의인증 알고리즘을 사용하여 참여자가 트랜잭션을 발생하여 합의를 요청하는 과정에서 Primary Node를 Random array를 이용하여 등록된 노드를 무작위로 선정한다. 이후 Primary Node가 멀티캐스터를 통해 다른 노드와 합의를 이루는 검증 방법을 기반으로 플랫폼을 구성하였다[7]. 노드를 랜덤으로 선정하여 합의를 이루는 과정에서 많은 시간이 소요되며, 등록된 노드는 모두 공개되어 있어 예측 불가능성을 만족시킬 수 없으며, 다른 노드에 의해 조작 가능성이 존재하기 때문에 여전히 위·변조의 가능성이 제기되고 있다.

공정거래를 목표로 구현된 Ujo는 블록체인을 기반으로 하여 공정하고 효율적인 분산형 음악 플랫폼을 제공하고 있다. 사용자의 신원을 독자적으로 증명하고, 콘텐츠 및 거래 내역에 대하여 수정할 수 없도록 블록에 저장하여 정산되도록 하고 있다[8]. 그러나 Ujo는 전자지갑의 한 종류인 메타마스크로 사용자의 신원증명과 거래내역을 관리하고 있어 메타마스크의 시드정보를 분실했을 경우 사용자의 거래 이력이 손실될 위험이 존재한다.

최근 블록체인이 성장하면서 INSTSIGN, Chain SIGN[9],[10]등 기존의 전자계약 시스템에 블록체인 기술을 활용한 전자계약 플랫폼이 등장하고 있다.

이러한 플랫폼은 블록체인이 가지고 있는 장점인 분산 저장된 상태에서 다수의 노드의 합의 알고리즘의 통해 위·변조를 막고 기존의 번거로웠던 계약 절차를 자동화하여, 계약 업무에 소요되는 시간과 비용을 절약하여 업무 효율성을 높일 수 있다. 하지만 이러한 플랫폼도 서명 단계에서 공용인증서를 사용하고 있어 인증수단이 분실되거나 해킹 당하였을 경우 지면 계약서 못지않은 위험을 가지고 있다.

본 논문에서는 기존의 전자 계약 플랫폼의 문제점을 개선하기 위해 블록체인 기반 탈중앙화 신원 증명환경에서의 계약 플랫폼을 제안한다.

III. 본 문

3.1 계약 플랫폼 구성도

서론 2.3의 전자계약 플랫폼 사례에 나온 위·변조의 가능성, 신원증명 및 거래내역을 전자 지갑으로 관리하면서 발생할 수 있는 신원정보 분실, 악의적인 해커에게 쉽게 정보가 유출된다는 문제점을 해결하기 위해 본 논문에서 블록체인 기반 탈중앙화 신원증명 환경에서 계약 플랫폼을 제안한다.

그림 2와 같이 제안하는 블록체인 기반 탈중앙화 신원증명 환경에서의 계약 플랫폼은 크게 Ethereum environment, Web environment, Authentication means, Database 등으로 구성된다. Ethereum environment은 프로젝트, 계약, 신원 증명서를 저장한다.

환경 구성은 Geth 1.9.2에 노드3개로 구성하였으며 운영환경은 Amazon EC2, Ubuntu 20.01.1 LTS이며 네트워크 대역폭은 10 Gbps로 운영한다. 사용자들의 체결한 스마트 계약은 Solidiy0.4.24로 구현하였다. 블록체인 환경에서 거래 정보의 유효성 검증, 합의, 거래 정보를 송신 및 수신할 수 있는 P2P 네

트위크, 블록체인 각 노드의 주기적인 상태를 확인한다. Web environment은 Node.js 12.18.3, React-native-cli 2.0.1로 웹 환경을 구현하였으며, 사용자가 프로젝트를 생성하여 계약을 체결한다. Authentication means은 사용자의 인증 수단 모바일 앱이나 전자 지갑중 하나인 Metamask 8.1.5로 사용자의 개인정보

관리, 계약, 정산 신원 증명서를 관리한다. 데이터베이스는 NoSql인 Cloud Firestore 2.0.1로 구축하였으며 프로젝트, 계약 체결 내역 정보, 신원 증명서 발급 내역 등을 저장한다.

제안하는 플랫폼의 서비스 시나리오는 그림 3에서 설명한다.

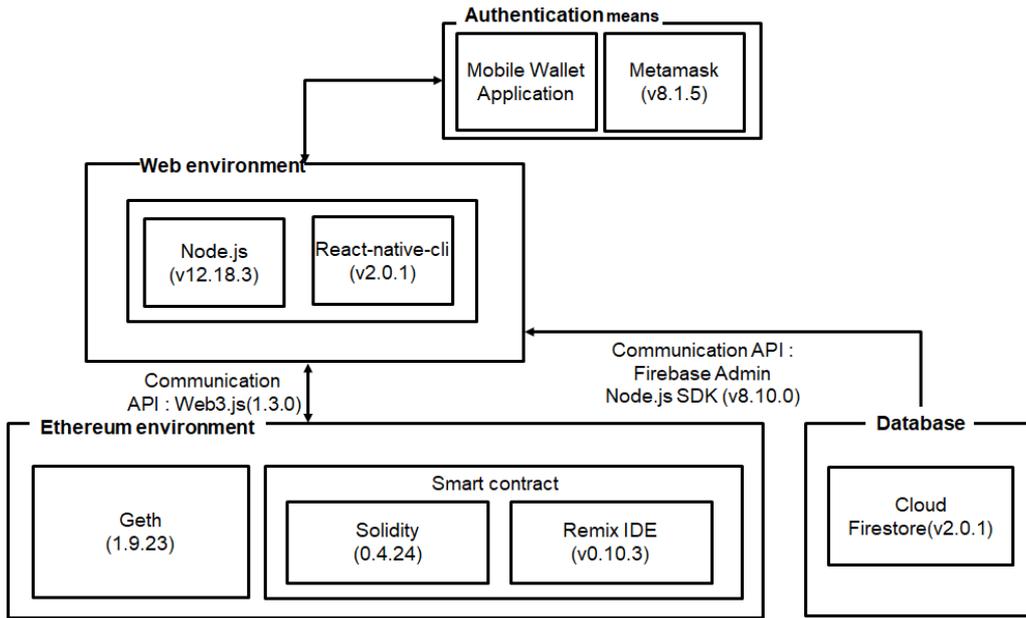


그림 2. 계약 플랫폼 환경 구성도
Fig. 2. Contract platform environment diagram

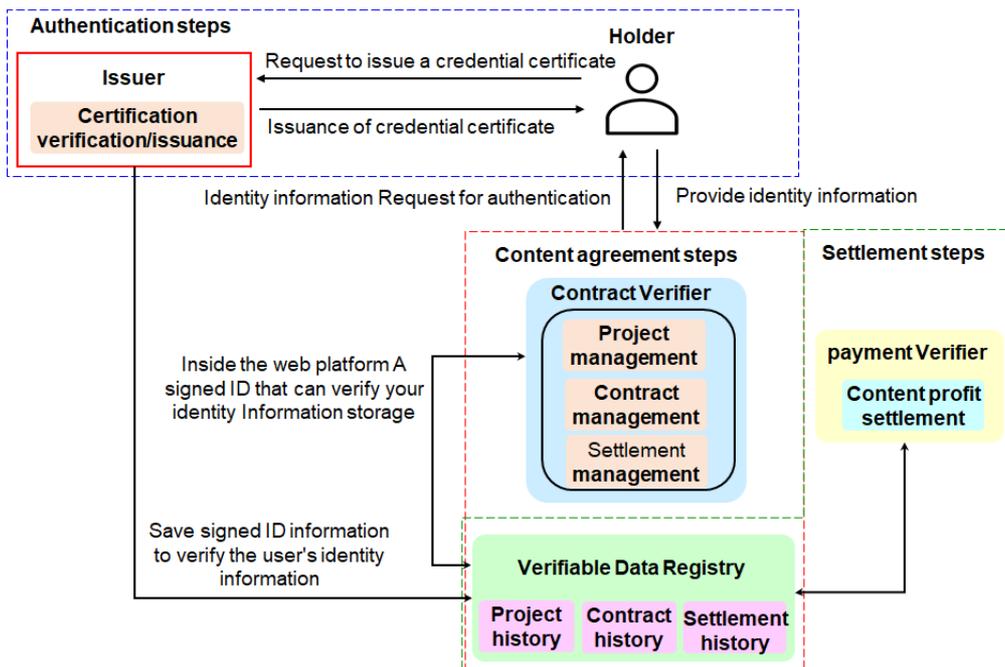


그림 3. 플랫폼 서비스 구조도
Fig. 3. Platform service structure diagram

사용자는 신원 증명서를 서비스 제공자에게 제공하여 신원 검증을 받고 계약 플랫폼을 이용한다. 사용자는 자신의 신원 정보 중에서 계약에 필요한 정보만 신원 증명서로 직접 관리하기 때문에 개인 정보 유출에 대한 위험이 적다.

플랫폼은 크게 인증단계, 서비스 영역으로 나눈다. 사용자는 신원정보 발행자에게 신원인증을 받으면 서비스를 사용할 수 있다

사용자는 계약체결을 위해 프로젝트를 생성한다. 생성된 프로젝트는 블록체인에 저장되며, 사용자의 요구와 일치하는 프로젝트를 조회하면 저장된 프로젝트를 스마트컨트랙트로 호출하여 계약을 체결할 수 있다. 계약은 1:1 또는 1:N 계약이 체결될 수 있다. 체결된 계약은 스마트 컨트랙트를 이용하여 블록에 저장된다. 계약이 이행되면 사용자는 신원정보 발행자에게 신원증명서를 확인하여 자동으로 수익을 정산할 수 있다[11].

제안하는 논문의 플랫폼은 검증 가능한 신원 증명서를 이더리움에 저장해놓기 때문에 중앙기관·기업 없이도 사용자가 계약서를 관리할 수 있으며, 다수의 사용자가 하나의 프로젝트에 대해 계약을 체결할 수 있다.

3.2 계약 플랫폼의 절차

사용자는 계약을 체결하는 당사자로, 플랫폼에 생성된 프로젝트로 계약을 체결하거나 사용자가 필요한 프로젝트를 직접 생성하여 계약을 체결한다. 서론 2.3 전자계약 사례에 보면 1:1 계약을 체결하여 진행하고 있지만 제안하는 논문에서는 사용자와 다수의 사람이 계약을 체결할 수 있고, 필요한 프로젝트를 생성하여 계약을 체결할 수 있다. 사용자가 프로젝트 생성이나 계약 체결을 위해서는 신원정보 발행자에게 신원 증명서를 발급받아서 진행한다.

신원정보 발행자는 외부 신뢰할 수 있는 공공기관이 아닌 내부 기관이 발행자 역할을 하며 사용자의 신원을 확인하고 신원 증명서를 발급해주고 발급내역은 스마트 컨트랙트를 이용하여 블록에 저장된다.

3.2.1 서비스 시나리오

- ① 사용자는 서비스 제공자에게 서비스 이용과 관련된 검증을 요청받으면 자격발행기관에 신원정보를 기반으로 신원 증명서를 발급받는다.
- ② 사용자는 서비스 제공자의 플랫폼을 이용하기 위해 자격발행기관에서 받은 신원 증명서를 제공한다.
- ③ 서비스 제공자는 사용자가 제공한 신원 증명서를 블록체인 영역에 있는 내용과 일치한지 검증한다.
- ④ 검증이 완료된 사용자는 플랫폼에서 본인 계약에 필요한 정보를 검색 할 수 있다.
- ⑤ 사용자는 본인과 맞는 프로젝트를 열람 또는 생성할 수 있으며 다른 사용자와 계약 요청 및 체결을 할 수 있다.
- ⑥ 사용자는 신원정보 증명서로 계약을 체결한다.
- ⑦ 계약이 이행되면 계약에 사용되었던 신원 정보 증명서로 계약 이행 여부를 확인한다.
- ⑧ 계약관련 산출물은 별도로 관리하며 사용자는 서비스 제공자에게 정산을 요청한다.
- ⑨ 서비스 제공자는 정산 요청을 확인하고 처리한다.

3.2.2 사용자 프로젝트 생성 절차

프로젝트 생성단계에서는 소유자가 발급자에게 신원 증명 증명서를 발급받아서 회원가입 및 로그인을 진행하여 플랫폼 서비스를 이용한다.

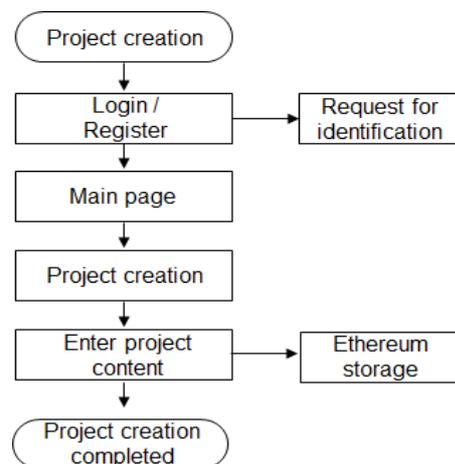


그림 4. 사용자 프로젝트 생성 절차
Fig. 4. Holder contract signing procedure

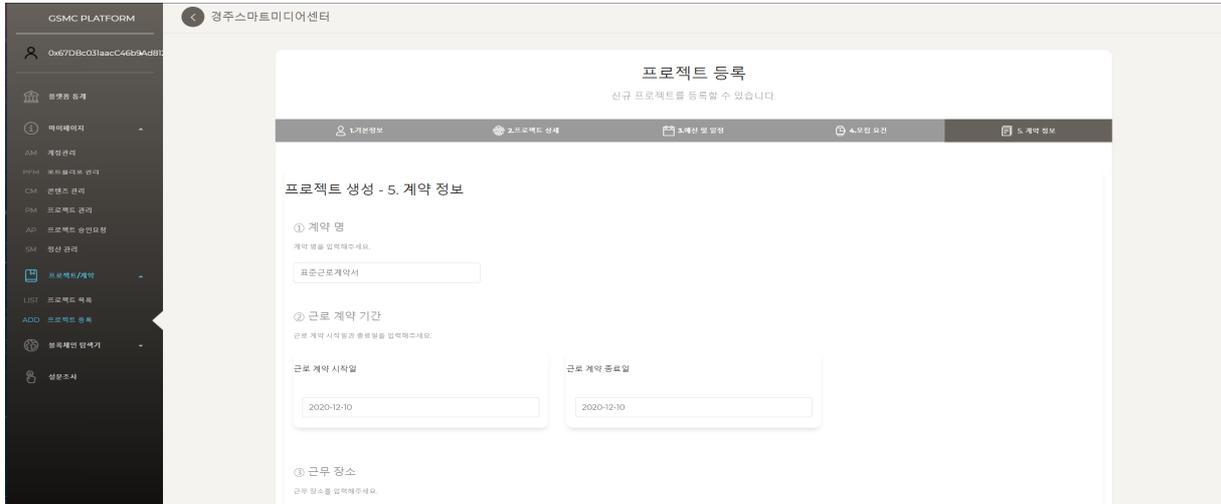


그림 5. 사용자 프로젝트 등록 화면
Fig. 5. Holder project registration screen

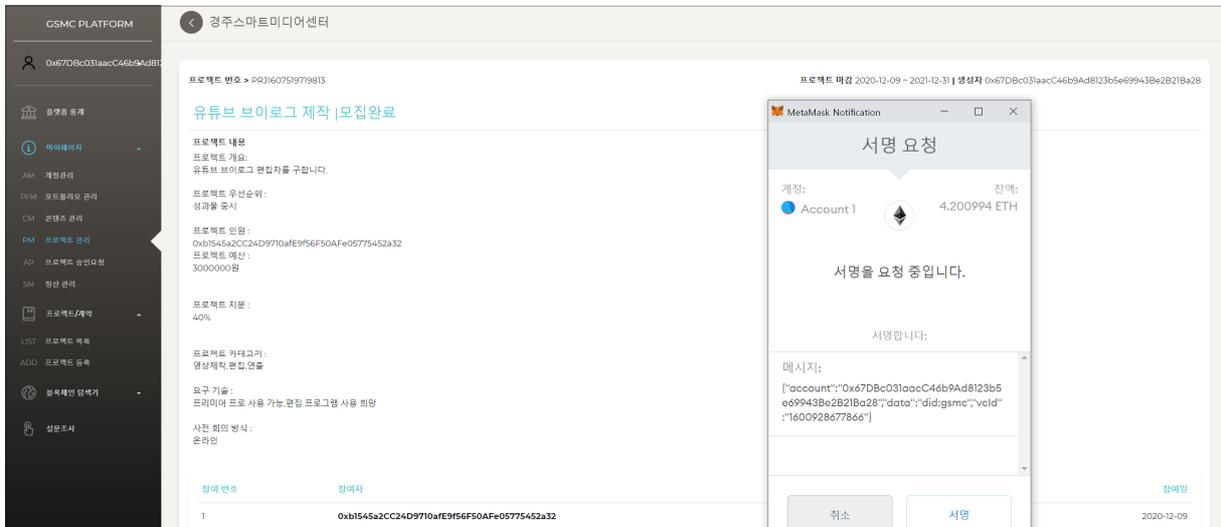


그림 7. 사용자 계약 체결 및 계약 신원 증명서 발급 요청 화면
Fig. 7. Holder contract signing and contract verifiable credential issuance request screen

프로젝트 생성 페이지에서 계약이 필요한 프로젝트 계획 및 예산을 입력하고 프로젝트를 생성한다. 이때 프로젝트 내용은 스마트 컨트랙트로 블록체인 영역에 저장되어 프로젝트의 무결성을 보장한다.

3.2.3 사용자 계약 체결 절차

계약 체결단계에서는 사용자가 프로젝트를 열람한 후 원하는 프로젝트에 참여 요청을 한다. 이때 프로젝트 참여를 희망하는 사용자는 1명일 수 있고 다수의 여러 사람일 수 있다. 프로젝트 생성자는 모집인원을 확인하고 프로젝트를 모집을 마감한다.

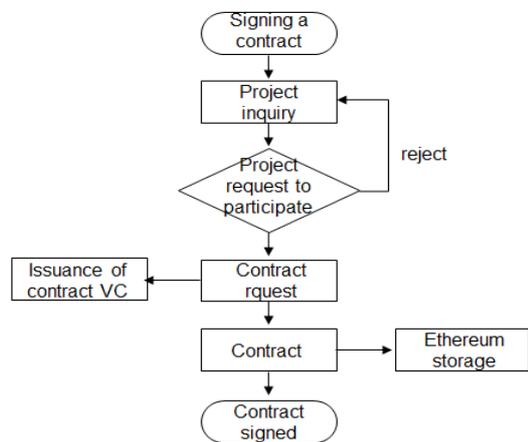


그림 6. 사용자 계약 체결 절차
Fig. 6. Holder contract signing procedure

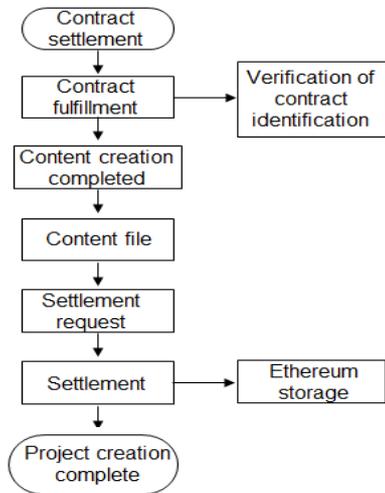


그림 8. 사용자 정산 절차
Fig. 8. Holder settlement process

사용자가 다른 사용자에게 계약을 요청하기 전에 신원정보 발행자에게 계약체결 인증서를 발급받는다. 이후 서로 의견이 일치하면 공정거래위원회에서 지정한 표준계약서 양식에 따라 계약이 체결되며, 계약 내용은 블록체인 영역에 저장된다.

3.2.4 사용자의 정산 절차

정산 단계에서는 사용자 사이에 체결된 계약의 이행이 완료되면 산출되는 결과물, 임금에 대하여 정산을 한다.

계약 당사자 간의 계약이 완료되면 계약 체결 단계에서 발행한 계약체결 인증서로 사용자를 검증하여 완료 여부를 확인한다. 이후 계약이 이행 완료 사용자는 신원정보 발행자에게 정산을 요청하게 된다.

3.2.5 모니터링 시스템

블록체인의 안정성을 확보하기 위하여 그림 10과 같이 블록체인 모니터링을 한다. 계약 체결, 프로젝트 등록, 신원증명서 발급 등 블록에 대한 정보를 확인 할 수 있다.

Block #	Block Hash	Difficulty	Miner	Size	Age	# of Tx's	Gas used
3793	0xc02988...	790.535 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	0.747 kB	8 days 3 hrs ago	2	42,000 m/s
3792	0xc1d771e...	790.921 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	0.747 kB	8 days 3 hrs ago	2	42,000 m/s
3791	0xc9c398b...	794.801 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	1.477 kB	8 days 3 hrs ago	9	189,000 m/s
3790	0xc9c780c...	794.414 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	0.536 kB	8 days 3 hrs ago	0	0 m/s
3789	0xc02110e...	794.027 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	0.536 kB	8 days 3 hrs ago	0	0 m/s
3788	0xc93296c...	793.640 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	0.643 kB	8 days 3 hrs ago	1	21,000 m/s
3787	0xc070571...	794.027 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	0.747 kB	8 days 3 hrs ago	2	42,000 m/s
3786	0xc16788b...	796.355 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	1.269 kB	8 days 3 hrs ago	7	147,000 m/s
3785	0xc0a1a02...	797.911 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	1.165 kB	8 days 3 hrs ago	6	126,000 m/s
3784	0xc0a8b2b...	800.251 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	1.269 kB	8 days 3 hrs ago	7	147,000 m/s
3783	0xc73eb25...	800.641 K	0xecc68f4bbaf25b170c3e43b244f0e2cedd4ddeb6	0.747 kB	8 days 3 hrs ago	2	42,000 m/s

그림 10. 블록체인 모니터링
Fig. 10. Blockchain monitoring

그림 9. 사용자 정산 요청 화면
Fig. 9. Holder settlement request screen

표 1. 기존 전자 계약 vs 제안하는 계약 플랫폼

Table 1. Existing electronic contract vs proposed contract platform

	Existing electronic contract	Proposed contract platform
Convenience	There are many procedures for user authentication before signing a contract	Simplified process by enabling user authentication inside the platform
Security	Contract information loss when the blockchain core is damaged	User identity information and contract management
Differentiation	1:1 contract can be concluded	1:N contract can be concluded
Proof of identity	Public certificate required	User authentication is possible with decentralized identification without public certificate

3.3 평가

제안하는 논문에서 블록체인을 기반 탈중앙화 신원증명 계약 플랫폼은 서론 2.3 전자계약 플랫폼 사례인 NSTSIGN, Chain SIGN는 공용인증서를 통해 계약이 체결되고 있고, 인증수단이 분실되거나 해킹 당했을 경우 지면 계약보다 더 위험한 요소를 가지고 있다. RPFT 합의 알고리즘을 사용한 플랫폼은 노드 자체를 랜덤으로 섭정하여 합의를 이루기 때문에 다른 노드에 의해 조장이 가능하고, 계약에 대한 위변조가 발생할 수 있다. 이러한 단점을 보완하여 신원정보 발행자를 통해 사용자의 신원정보를 확인하고 계약서를 신원증명서로 체결하고 사용자가 직접 신원증명서를 관리하여 신뢰성을 확보한다. 사용자는 신원정보 발행자에게 검증받은 신원인증서는 블록체인 영역에 저장된다.

사용자가 필요에 의해 작성한 프로젝트 정보와 계약서는 블록에 저장되어 모든 사용자에게 공개되어 위변조를 방지한다. 기존 전자계약에서는 1:1 계약을 기반으로 체결되며 제안하는 플랫폼에서는 1:N으로 계약이 이루어져 다자간의 계약이 체결 가능하다. 계약 체결에서 정산까지 기존의 전자계약 프로세스에 비해 간소화되어 시간과 장소에 구애 받지 않고 계약이 체결된다. 계약 완료와 동시에 신속하게 정산이 가능하여 제3자 없이 정산이 가능하여 비용절감이 이루어진다.

IV. 결론 및 향후 과제

전자 계약 플랫폼에 대한 보안, 계약관리에 대한

중요성이 증가하고 있다. 본 논문은 블록체인 기반 탈중앙화 신원증명 환경에서 계약내용, 정산내용 등을 스마트 컨트랙트를 이용하여 블록체인에 기록하는 방식으로 계약내용을 수정하거나 위조하는 것을 방지한다. 탈중앙화 신원증명을 통해 검증된 사용자만 계약을 체결하고 사용자가 신원 증명서를 직접 관리하여 신원정보에 대한 분실 우려를 감소하고, 계약 당사간의 신뢰를 확보할 수 있다.

추후 계약이 체결되고 당사자 간의 업무를 진행하는 과정, 수익 정산에 대한 자동 시험 검증에 대한 구현이 필요하다.

References

- [1] [Promising future technology ② seen as a patent] "Blockchain", <http://www.e-patentnews.com/5486> [accessed: Nov. 17, 2020]
- [2] White Paper. <https://ethereum.org/ko/> [accessed: Nov. 16, 2020]
- [3] Shin Dong-sun, "A Study on Using Blockchain Technology for Airline Business", Inha University Graduate School of Logistics, Feb. 2018.
- [3] Parkyeon, Chonghyun Kim, and Engyu Kim, "Case Study on the Application of Ethereum-Blockchain Technology for Electronic Voting System", Korea Institute of Enterprise Architecture, Vol. 15, No. 2, pp. 201-218, Jun. 2018.
- [4] Decentralized Identifiers (DIDs) v1.0, <https://www.w3.org/TR/did-core/> [accessed: Nov. 17, 2020]
- [5] A Primer for Decentralized Identifiers, <https://w3ccg.github.io/did-primer/> [accessed: Nov. 17, 2020]

- [6] Verifiable Credentials Data Model 1.0, <https://w3c.github.io/vc-data-model/> [accessed: Nov, 16, 2020]
- [7] Kim, Sunghwan and Kim, Younggon, "A Study on Contract Management Platform Based on Blockchain", Korea Citation Index, Vol. 19, No. 3, pp. 97-103, Jun. 2019.
- [8] Ujo Music. <https://ujomusic.com/> [accessed: Nov, 18, 2020]
- [9] Chain SIGN, <http://www.chainsign.co.kr> [accessed: Dec. 14, 2020]
- [10] INSTSIGN, <https://instsign.com> [accessed: Dec. 14, 2020]
- [11] Yoon Dae-geun, "Self-sovereign identity certificate structure analysis", Jpub, pp. 35-53, pp. 76, Jul. 2020.

유 수 민 (Su-Min Yoo)



2019년 2월 : 울산과학대학교
컴퓨터정보학부 소프트웨어
개발전공(공학전문학사)
2019년 6월 ~ 현재 : (재)경주
스마트미디어센터 연구원
관심분야 : 블록체인, 인공지능

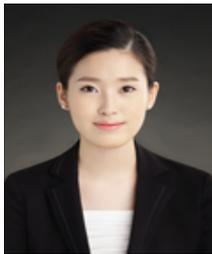
손 애 선 (Ae-Seon Son)



2018년 2월 : 금오공과대학교
컴퓨터공학과(공학사)
2019년 6월 ~ 현재 : (재)경주
스마트미디어센터 연구원
2020년 9월 ~ 현재 : 동국대학교
전자통신공학과(공학석사)
관심분야 : 블록체인, 인공지능

저자소개

조 정 화 (Jung-Hwa Jo)



2015년 2월 : 대구대학교
사회학과(사회학사)
2019년 6월 ~ 현재 : (재)경주
스마트미디어센터 연구원
2020년 9월 ~ 현재 : 동국대학교
전자통신공학과(공학석사)
관심분야 : 블록체인, 인공지능,

데이터통신

유 수 빈 (Soo-Bin Yoo)



2012년 2월 : 동국대학교
정보통신공학과(공학사)
2016년 8월 : 동국대학교
전자통신공학과(공학석사)
2016년 12월 ~ 현재 : (재)경주
스마트미디어센터 주임연구원
2020년 3월 ~ 현재 : 동국대학교

전자통신 공학과(공학박사)

관심분야 : 인공지능, 머신러닝, 데이터통신