

스마트 제조산업의 시험평가서 위변조 방지를 위한 생성형 Smart Contract 설계 및 구현

차중혁¹, 김형진², 이재민³, 김동성^{*}

(주)엔에스랩 기술연구소^{1,2,*}, 국립금오공과대학교 IT융복합공학과^{2,*}

{jh.cha¹, haengg²}@nslab.tech, {ljmpaul², dskim^{*}}@kumoh.ac.kr

Design and Implementation of Generative Smart Contract to Prevent Forgery of Electronic Contract in Smart Manufacturing Industry

Joong-Hyuck Cha¹, Hyeong-Jin Kim², Jae-Min Lee³ and Dong-Seong Kim^{*}

NSLab Co., Ltd. Technology Research Institute^{1,2,*},

Kumoh National Institute of Technology Dept. of IT Convergence Eng.^{3,*}

요약

본 논문은 스마트 제조산업 환경에서 시험평가서의 신뢰성 및 보안성 향상을 위해 생성형 Smart Contract를 제안하고자 한다. 제조산업은 고도화된 기술 및 장비를 도입하기 위해서는 기술 및 장비에 대한 시험평가가 필수적으로 선행되어야 한다. 전통적인 제조산업에서 스마트 제조산업으로 전환됨에 따라 종이 문서 기반의 시험평가서는 보관, 시간 소요, 보안 등의 문제로, 자동 시험평가를 통해 디지털 문서로 보관 및 관리하는 것으로 변화하고 있다. 이러한 전자 시험평가서 발행 환경은 기존 문제들은 해결하였지만, 여전히 내외부로부터 발생하는 위변조에 노출되어 있다. 이에 본 논문에서는 시험평가서 위변조를 방지하기 위해 블록체인 기반의 생성형 Smart Contract 설계 및 구현하고자 한다.

I. 서론

스마트 제조산업은 설계 및 개발, 제조 및 유통 등 생산 과정에서 디지털 자동화 솔루션이 결합된 정보통신기술(ICT)을 적용하여 생산성, 품질, 고객 만족도를 향상하는 지능형 제조산업이다[1, 2]. 이러한 제조혁신은 다양한 기술이 필연적으로 융·결합해야 하며, 고도화된 기술 및 장비 도입이 활발하게 되고 있다. 이러한 기술 및 장비 도입은 성능 검증, 신뢰성 등을 기반으로 추진되며, 일반적으로 시험평가서를 통해 성능 및 신뢰성을 입증하고 있다[3].

전통적인 제조산업에서 시험평가서는 종이 문서 기반으로 발행되고 스캔을 통해 활용하며, 원본은 창고에 특정 기간 보관된다. 이러한 종이 문서 기반 운용은 스캔, 보관 등으로 발생하는 시간과 보관 시 물리적인 훼손 가능성 등의 문제점이 발생한다. 스마트 제조산업에서는 이러한 문제점을 해결하기 위해 시험성능 및 평가를 자동으로 수행하여 PDF 확장자로 평가서를 발행 및 보관하고 있다. 이를 통해 기존 문제점을 해결할 수 있었으나, 여전히 내외부로부터 발생하는 위변조 문제점이 해결되지 못하였다[4].

이에 본 논문에서는 스마트 제조환경에서 시험평가서의 위변조 방지를 위해 블록체인 기반의 생성형 Smart Contract 설계 및 구현하고자 한다. 제안하는 생성형 Smart Contract는 제조환경의 수많은 평가 항목에 동적으로 대응할 수 있게, 사용자가 Smart Contract를 생성할 수 있게 한다. 또한, 블록체인 네트워크는 (주)엔에스랩의 자체 기술인 'PureChain[5]'을 활용하여 구성하였다.

II. 블록체인의 무결성

그림 1은 블록체인의 상세 블록 구조를 보여준다. 블록은 블록 헤시,

블록과 관련된 정보들을 포함하고 있는 헤더(Header), 그리고 거래 데이터를 포함하는 바디(Body)로 나뉜다. 블록 헤시는 헤더 내의 데이터들을 해시화한 데이터이다. 헤더는 일반적으로 6가지의 데이터(이전 해시, 시간, Nonce, Bits, Version, Merkle Root)들을 포함하고 있다. 이전 해시값은 이전 블록의 블록 해시값을 나타내며, 가장 처음 생성된 Genesis Block의 경우에는 0이 입력된다. Time Stamp는 블록이 생성된 시간이고 Nonce는 해시값을 계산하기 위한 임의의 값으로 작업 난이도에 따라 결정이 된다. Bits는 난이도 조절을 위한 수치, 계산 난이도 목표이고, Version은 소프트웨어 버전을 포함한다. Merkle Root는 Merkle Tree 구조의 가장 상위 단계에 생성되는 해시 데이터이며, 블록에 있는 수많은 거래 기록을 모두 해싱하여 Merkle Root 값에 채워짐으로 데이터의 무결성을 확인할 수 있게 된다. 본 논문에서는 이러한 특성을 기반으로 스마트 제조산업에서 시험평가서의 위변조 방지를 하고자 한다.

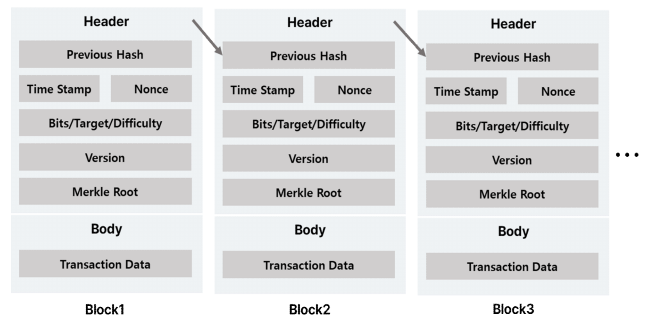


그림 1. 블록체인의 세부 데이터 구조

III. 스마트 제조를 위한 생성형 Smart Contract

스마트 제조환경에서는 다양한 시험 장비에 수많은 시험 항목들을

기준으로 시험평가를 수행하고 있다. 수많은 시험 장비와 시험 항목들에 대해 Smart Contract를 모두 만든다는 것은 불가능에 가깝다. 따라서 현장 실무자들이 시험 항목을 입력하고 해당 항목을 기반으로 Smart Contract가 자동으로 생성이 될 수 있어야 수많은 시험 항목에 동적으로 모두 대응이 가능하다. 따라서 본 논문에서는 Smart Contract에서 Factory 디자인 패턴을 사용하여 생성형 Smart Contract 구조를 설계 및 구현하고자 한다.

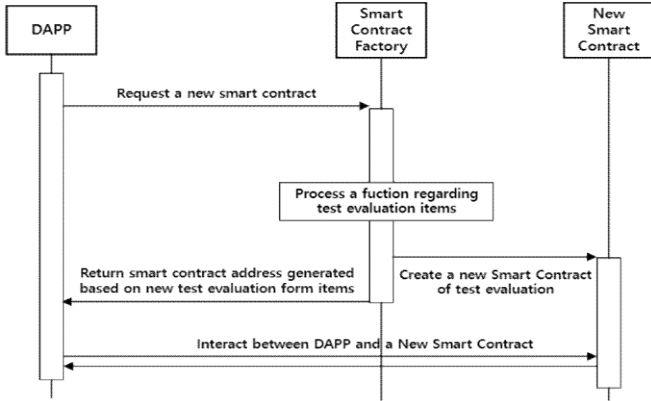


그림 2. 생성형 Smart Contract 시퀀스 다이어그램

생성형 Smart Contract는 그림 2와 같이 Solidity 내에서 DAPP(Distributed APP), Smart Contract Factory, New Smart Contract로 구성된다. 우선, 시험 장비의 관리자가 DAPP의 UI를 사용하여 시험 항목을 입력한다. 입력 완료 시 블록체인 트랜잭션을 통해 Smart Contract Factory에 새로운 Smart Contract 생성 함수가 실행된다. Smart Contract Factory 내에는 Smart Contract Model Class의 동적 배열 인스턴스를 포함하고 있다. 그리고 Smart Contract Model Class 내에는 시험 항목들을 저장할 수 있는 동적 배열을 포함하고 있고, 인스턴스 생성 후 요청된 트랜잭션 데이터를 기반으로 시험 항목을 저장한다. 해당 인스턴스는 Smart Contract Factory 내에 있는 동적 배열 인스턴스에 추가 및 저장된다. 이후 마이닝이 수행되고 새로운 Smart Contract의 주소를 받아, 해당 주소를 기반으로 DAPP과 연결이 되어 해당 시험 항목에 대한 시험평가서를 PDF로 출력할 수 있게 된다.

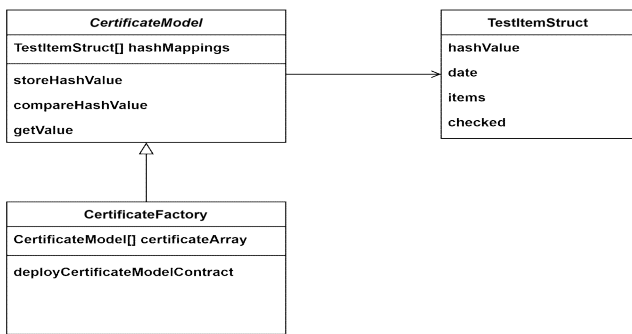


그림 3. 생성형 Smart Contract 클래스 다이어그램

그림 3은 제안하는 시스템의 생성형 Smart Contract의 클래스 다이어그램을 보여준다. 해당 언어는 Solidity로 구축하며 TestItemStruct, CertificateModel, CertificateFactory로 구성된다. TestItemStruct는 해시값, 시험평가서가 발행된 날짜, 테스트 항목, 합격 여부로 구성되고, CertificateModel은 TestItemStruct를 동적 배열로 저장하여 시험평가서가 발행될 때마다 저장한다. 그리고 CertificateModel 내에는 해시값 저장, 해시값 비교, 해시값 가져오기 기능을 포함하고 있다.

이러한 CertificateModel을 CertificateFactory 내에 배열로 저장하고, deployCertificateModelContract를 호출하여 Smart Contract를 동적으로 발행한다.

IV. 구현 결과

그림 4는 시험 항목을 입력받는 UI와 'PureChain[5]' 기반으로 Smart Contract가 배포되고 동작하는 결과를 보여준다.

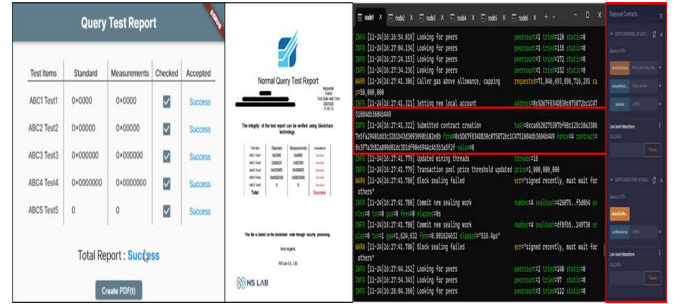


그림 4. 시험평가 입력 UI(좌), Smart Contract 배포 결과(우)

IV. 결론

본 논문에서는 스마트 제조산업에서 운용되는 시험평가서의 위변조 방지를 위한 생성형 Smart Contract 설계 및 구현하였다. 제안하는 생성형 Smart Contract는 ㈜엔에스랩의 'PureChain[5]'을 기반으로 블록체인 네트워크를 구축하고, Factory 디자인 패턴을 활용하여 구현하여 시험 항목에 동적으로 적용 가능하게 하였다. 시험 항목을 입력하는 UI는 크로스 플랫폼을 활용하여 구현하여 다양한 플랫폼을 지원할 수 있게 하였다. 향후에는 새로운 Smart Contract가 발행될 때 발생하는 Gas Fee를 최적화하기 위해 유사한 시험 항목에 대한 최적화 알고리즘 관련 연구를 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2023년도 과학기술정보통신부의 재원을 지원받아 수행된 연구임(1711202170/2023-IT-RD-0083-01).

참고 문헌

- [1] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Efficient Classification of Enciphered SCADA Network Traffic in Smart Factory using Decision Tree Algorithm", IEEE Access Vol.9, pp. 154892-154901, November 13, 2021
- [2] F. B. Islam, J. M. Lee and D. S. Kim, "Smart Factory Floor Safety Monitoring using UWB Sensor", IET Science, Measurement & Technology, Vol. 16, no. 7, pp. 415-425, 2022.
- [3] M. Alsadi, J. Arshad, J. Ali, A. Prince, and S. Shishank, "TruCert: Blockchain-based Trustworthy Product Certification within Autonomous Automotive Supply Chains," Computers and Electrical Engineering, Vol.109, 2023.
- [4] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, et al., "A Blockchain-based Approach for Drug Traceability in Healthcare Supply Chain," IEEE Access, Vol.9, pp.9728-9743, 2021.
- [5] NSLAB, Co., Ltd., Purechain : Blockchain Ecosystem, https://nslab.tech/bbs/board.php?bo_table=publication&wr_id=54, 2023.