

이더리움 블록체인의 성능을 고려한 보상정책을 갖는 이력관리 시스템 개발

홍정민 · 김예진 · 김유정 · 박혜정 · 강은성 · 김형종[†]

Development of Career Management System with Rewarding Policy Considering the Ethereum Blockchain Performance

Jung-Min Hong · Ye-Jin Kim · Yu-Jeong Kim · Hye-Jeong Park · Eun-Seong Kang · Hyung-Jong Kim[†]

ABSTRACT

Private blockchains can apply enhanced security policies that allow only authorized users to participate in the blockchain network. In addition, when used in a career management system where the validity of an individual's career is important, it has the suitable characteristics in terms of information integrity. However, due to the excessive performance requirements of blockchain technology, identifying performance characteristics through simulation can be helpful in stable operation of the system. This paper presents research results that utilized performance evaluation results while constructing a career management system based on the Ethereum blockchain. The service not only serves as a portfolio that records personal career development activities, certification acquisition, and award results, but also provides a community function for career planning to strengthen employment competitiveness. In addition, we present how a compensation policy can be executed to encourage users to participate in career development through community activities. In particular, an appropriate compensation policy was derived by reviewing changes in performance characteristics in accordance with the transaction volume on Geth nodes.

Key words : blockchain services, performance evaluation, Ethereum, Geth node

요약

프라이빗 블록체인은 허가받은 사람만이 블록체인 네트워크에 참여할 수 있는 강화된 보안정책의 적용이 가능하다. 또한, 개인의 이력 사항의 유효성이 중요한 이력관리 시스템에 활용될 경우 정보의 신뢰성 관점에서 우수한 특성을 갖는다. 하지만 블록체인 기술의 과도한 성능요구사항으로 인해 시물레이션을 통한 성능적 특성의 파악은 시스템의 안정적 구현에 도움이 될 수 있다. 본 논문은 이더리움 블록체인 기반의 이력관리 시스템을 구성하면서 성능평가 결과를 활용하는 연구 결과를 제시하였다. 서비스는 개인 경력개발 활동, 자격증 취득 및 수상 결과를 기록하는 포트폴리오의 역할 뿐 아니라, 취업 경쟁력 강화를 위한 진로 설계를 위해 커뮤니티 기능을 제공한다. 또한, 서비스 사용자의 참여 독려로 커뮤니티 기능을 활성화시키고자 어떻게 보상 정책을 적용시킬 수 있는지를 제시한다. 특히, Geth 노드 상에서 거래량에 따라 나타나는 성능 특성의 변화 확인을 통해 적절한 보상 정책을 도출하였다.

주요어 : 블록체인서비스, 성능평가, 이더리움, Geth node

* “본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음” (IITP-2023-2018-0-01799)

본 논문은 2023년 한국정보보호학회의 ‘이더리움 블록체인을 활용한 보상 체계 기반의 이력 통합 관리 시스템’의 확장 버전임.

Received: 22 September 2023, **Revised:** 30 October 2023,
Accepted: 30 October 2023

[†] **Corresponding Author:** Hyung-Jong Kim

E-mail: hkim@swu.ac.kr

Department of Information Security,
Seoul Women's University

1. 서론

취업난이 심화된 현시점, 구직자들은 취업경쟁력을 위해 직무 포트폴리오를 필요로 한다. 직무 포트폴리오(portfolio)란 자신의 특징과 역량 등을 종합적으로 제시할 수 있도록 정리한 자료이다. 이때 구직자들은 전통적인 포트폴리오에서 더 발전된 형태인, e-포트폴리오를 활용한다. e-포트폴리오란 전통적인 포트폴리오에 정보통

신 기술이 접목된 전자적 포트폴리오로서, 기존의 포트폴리오가 내용의 보관, 수정, 운반 등이 어려운 문제점을 보완하기 위해 활용된다(Shon, 2011). 구직자, 입시생 등 현대 사회를 살아가고 있는 대부분의 사람들은 본인의 경험을 정리하고, 강점을 표현할 반영구적 수단이 절실히 필요한 상황이다.

개인은 자신의 포트폴리오 기록, 진로 계획을 위한 활동 검색을 위해 각기 다른 서비스를 사용하고 있다. 본 연구에서는 개인의 활동 내역, 자격증 취득 및 수상 결과물을 위변조 없이 신뢰성 있게 기록할 수 있고 동시에 진로 설계에 참고할 수 있는 정보 공유 기능과 참여 독려를 위한 보상을 함께 제공하는 통합 관리 포트폴리오, 커뮤니티, 보상체제 기능을 제공하는 이더리움 블록체인 기반의 이력관리 웹 시스템을 설계하고 개발한다.

포트폴리오는 사용자의 활동 내역 데이터를 통합 관리 및 저장하는 기능을 한다. 사용자의 활동 데이터에는 참여 프로젝트, 현장실습, 공모전 수상, 자격증 취득 등이 기록된다. 커뮤니티는 공통 관심분야를 가진 사람들이 모여 정보를 공유하는 정보 공유의 장 역할을 한다. 사용자들은 자신이 참여한 활동에 대한 후기를 공유하고, 질문할 수 있다. 마지막으로 포인트 제도를 통해 활동 후기 정보 공유에 따른 보상을 제공한다. 사용자는 활동 후기 작성을 통한 포인트 보상을, 본 시스템은 질 높은 활동 후기 확보를 통한 플랫폼 경쟁력을 얻을 수 있을 것이다. 포인트 시스템은 제한된 노드만이 참여할 수 있는 프라이빗 블록체인 기술과 솔리디티 언어를 사용하는 스마트 컨트랙트를 기반으로 한다(Wood, 2014; Bartoletti and Pompianu, 2017).

본 연구에서는 즉각적인 보상을 바라는 개인과 블록체인 성능의 균형을 맞추고자 포인트 비율에 따른 트랜잭션 발생 기준을 변경해가며 성능을 측정하여 가장 효율적인 포인트 기준을 정한다. 성능평가는 자바스크립트(JavaScript)로 작성된 시뮬레이터에서 보상 기준이 되는 좋아요, 대댓글과 환급 함수에 따라 트랜잭션을 발생시켜 함수 시작부터 모든 트랜잭션이 완료된 후 함수가 완료되는 시점까지의 시간을 측정하는 방식으로 진행한다.

2. 기존 연구

블록체인을 이용한 다양한 서비스의 구성에 대하여 여러 응용 프로그램 형태로 제시된 구현 사례가 존재한다. 블록체인을 활용한 개인 경력 관리 및 유통 시스템 설

계 연구는 채용 시 개인의 경력을 위조하여 취업하는 경우가 발생하는 문제점을 해결하기 위해 개인 경력 정보를 블록체인으로 관리하고, 검증해줄 수 있는 시스템을 제안하였다(Bae and Shin, 2020).

Decentralized Identifier와 허가형 블록체인을 활용한 개인정보 주권화 및 이력추적 시스템 설계 연구는 개인정보 활용 서비스의 증가에 따라 개인정보의 오남용 발생에 대한 우려를 해소하고자 허가형 블록체인과 DID를 활용하여 개인정보를 보호하고 개인정보의 이력을 추적할 수 있는 시스템을 설계하였다(Kim et al., 2022).

프라이빗 블록체인 및 스마트 컨트랙트 기반 고성능도 클라우드센싱 보상 메커니즘 연구는 해당 연구 성능평가 및 타 시스템 비교를 통해 클라우드센싱 보상 시스템의 실현 가능성을 보이고자 했다. 클라우드센싱 시스템에 프라이빗 블록체인을 도입함으로써 서버가 제공한 보상과 사용자가 제공한 데이터를 불가변적으로 기록하며, 스마트 컨트랙트를 통해 센싱 데이터에 대한 평가를 자동화하고 그 과정을 사용자에게 공개하여 서버와 사용자 간의 신뢰도를 구축하는 방법을 제시한다(Yun and Kim, 2018).

DEVS-based Experimental Framework for Blockchain Services에서는 이더리움 블록체인 기반의 서비스 환경을 구성하고 이의 성능을 평가하기 위한 평가 프레임워크의 디자인을 제시하고 있다. 해당 연구를 통해 블록체인 기반의 서비스 환경의 성능분석이 어떤 형태로 진행되어야 하는지를 파악할 수 있다(Kim and Kim, 2021).

신뢰성 있는 경력 증명을 위한 블록체인 기반 디지털 배지 프레임워크 설계 연구는 구직자의 경력 검증 절차를 최소화하고자 프라이빗 블록체인 네트워크 기반의 프레임워크를 설계하여 트랜잭션에 경력 정보를 저장하여 무결성과 신뢰성을 보장받는다. 이에 디지털 배지를 활용하여 저장된 경력을 기존 채용 과정에서 사용할 수 있는 프레임워크를 제안하였다(Jeong and Jung, 2022).

블록체인을 활용하면 개인의 활동 이력에 대해 신뢰성을 보장할 수 있다. 본 연구에서는 통합적인 이력관리 기능을 제공하기 위해 블록체인을 활용해 위변조 불가한 활동 기록 및 검증에 더해 활동 후기 공유를 통해 진로 설계에 도움을 받을 수 있는 커뮤니티 및 보상 또한 제공하고자 한다. 또한, 자바스크립트 기반의 성능평가 시뮬레이터를 구동시킬 시나리오를 작성하고 한 기능을 수행하는 데에 발생하는 트랜잭션이 완료된 후까지의 시간 측정을 통해 블록체인 기반의 보상체제의 성능을 평가하여 성능을 최적화하고자 했다.

3. 블록체인 기반 이력관리 서비스 설계

3.1 이력관리 시스템 모델

이더리움 블록체인을 활용한 이력관리 웹 시스템은 대회 및 활동 주최 측과의 인증을 통해 참여 및 수상 내용의 진위를 증빙한다. 주최 측은 참여자 및 수상자 명단을 시스템에 제공하며, 본 서비스는 이를 통해 인증을 요청한 사용자와 일치하는지 확인한 후 참여 및 수상 인증을 발급할 수 있다. 나아가 사용자는 웹 커뮤니티를 통해 유사한 관심 분야를 가진 사람들의 활동 후기를 열람하거나 참고 자료로 활용할 수 있다. 활동 참여 및 수상에 대한 인증 데이터는 서비스 DB에 기록되어 추후 활동을 통합 관리하는 데에 사용할 수 있으며 시스템에서의 활동에 따른 포인트 기록 데이터는 이더리움 블록체인을 활용한 스마트 컨트랙트를 통해 관리된다.

3.2 웹서비스

웹 서비스에 필요한 데이터는 각각의 특성에 맞게 블록체인과 외부 저장소에 따로 저장되도록 분류하였다. 블록체인에는 커뮤니티 활동에 따른 포인트 및 포인트 지급 내역이 저장된다. 외부 저장소에는 변동성이 높은 사용자의 개인정보와 참여 활동 기록, 커뮤니티 내 활동 기록 및 웹 서비스 사용에 따른 부가자료가 저장된다.

Table 1. Data Classification System

	External Storage	Block Chain
Data	Personal Information	Point and Point Payment histories according to Community Activities
	Activity Participation Records	
	History of Activities in Community	
	Additional Data according to Service Use	

활동을 등록할 때 서비스의 흐름은 Fig. 1과 같다.

- ① 기존에 대회 및 활동 주최 측에게서 받은 정보를 기반으로 인증 가능한 활동 목록을 사용자에게 제공한다.
- ② 사용자가 등록하고자 하는 활동이 인증 가능한 활동 목록에 있을 경우, 명단에 사용자 정보가 있는지 인증 절차를 거쳐 기록을 DB에 저장한다.
- ③ 사용자가 목록에 없는 활동을 등록하고자 할 경우, 추가적인 인증 절차 없이 기록만 DB에 저장한다.

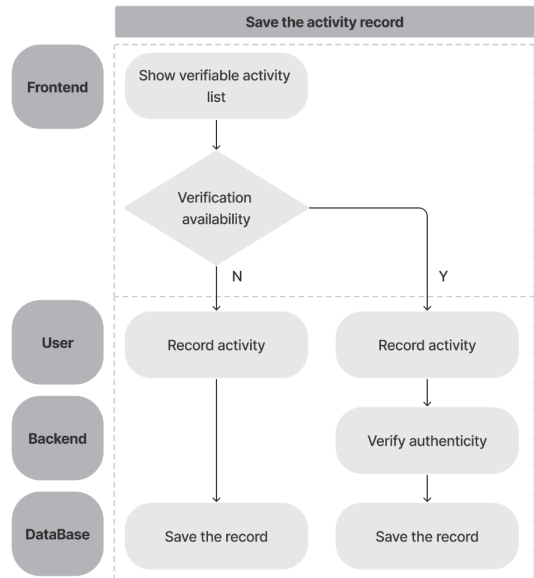


Fig. 1. Activity Registration Flowchart

서비스 사용자들은 커뮤니티 기능을 통해 공통 관심 분야를 가진 사람들의 활동 후기를 열람하고 댓글을 통해 소통하며 취업 활동을 위한 참고 자료로 활용할 수 있다. 포인트 지급 시스템은 커뮤니티에서의 사용자의 활동 정도를 척도로 하며 활동 정도는 사용자의 게시글이 좋아요를 받은 개수, 사용자가 타 사용자의 게시글에 대댓글을 남긴 횟수를 의미한다. 사용자가 지급받은 포인트는 서비스 내의 마이페이지에서 확인이 가능하며, 마이페이지에서 포인트가 갱신되는 빈도는 SmartContract 성능평가를 통해 검증된 효율적인 주기를 따른다. 세부 내용은 3.3절에서 다루기로 한다.

3.3 블록체인 네트워크

이더리움 블록체인을 활용한 이력관리 웹 시스템의 포인트 산정 시스템은 스마트 컨트랙트에 명시된 조건에 따라 수행되며 커뮤니티 내 사용자의 활동 정도를 척도로 한다. 스마트 컨트랙트의 개발은 Remix IDE(Antonopoulos and Wood, 2018)를 사용하였으며 Geth Private Network를 사용해 배포된다. 스마트 컨트랙트가 동작하는 흐름은 Fig. 2와 같다.

- ① 사용자가 후기를 등록하면 DB에 글과 작성된 글에 달린 좋아요 개수, 대댓글 개수가 기록된다.
- ② 사용자의 좋아요, 대댓글 개수가 서비스 활동에 따라 스마트 컨트랙트의 조건을 달성할 시, 사용자는

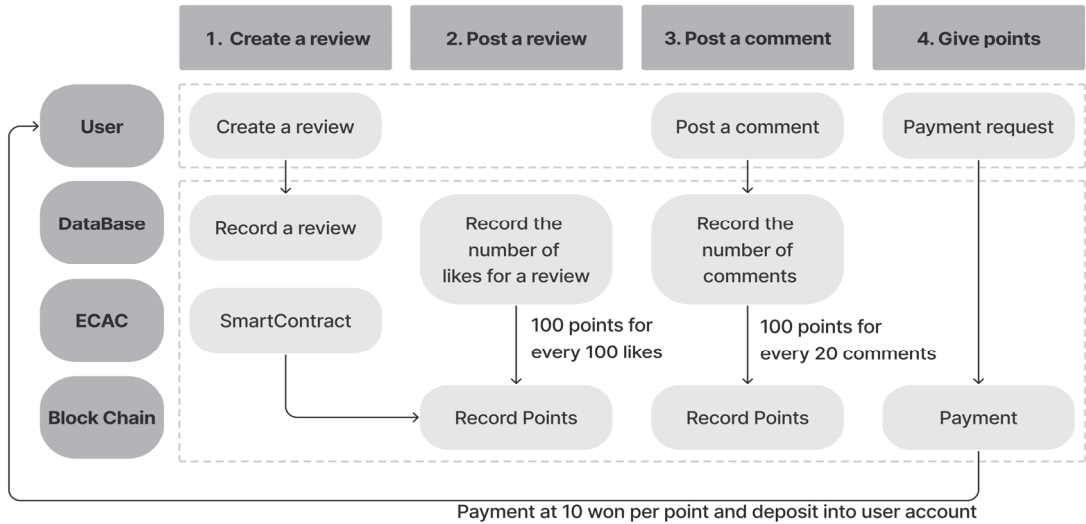


Fig. 2. Smart Contract Flowchart for Point Payment System

스마트 컨트랙트를 통해 자동으로 포인트를 지급 받는다.

- ③ 일정 수준 이상의 포인트가 누적될 시 포인트 현금화 요청이 가능하며 사용자 요청이 발생할 시 운영 시스템에 명시된 환율에 따라 사용자 계좌로 현금이 지급된다.
- ④ 모든 포인트 지급 및 정산 내역은 무결성 보장을 위해 블록체인 블록에 저장된다.

블록체인 네트워크 및 통신 구조는 Fig. 3과 같다.

- ① 블록체인 블록 블록체인 프로세스 실행을 위한 서버로, 서버 내에는 스마트 컨트랙트 프로세스 및 블록 채굴(Mining) 프로세스, 올바른 블록 생성을 위한 상호검증 로직 생성을 담당하는 합의 알고리즘(Consensus), 암호화폐처리 프로세스 및 가상머신(EVM)으로 구성된다(Moon et al., 2020).
- ② 대외기관 대외기관 측에서 주관한 대회 및 자격증에 참여한 활동자의 정보가 담긴 DB이며, 활동자명, 활동자의 전화번호와 소속, 그리고 활동자가 참여한 활동명으로 구성된다. 해당 정보들은 규격화된 DB에 저장되어 본 서비스의 운영시스템으로 전달된다.
- ③ 운영시스템 사용자의 활동 자격 및 인증 기록, 포인트 지급 관련 거래 조건 처리, 웹 서비스 모니터링 및 집계를 위한 관제 시스템으로 서버 내에는 블록체인 노드가 설치되어 있다. 이는 블록체인

Node API를 통해 WAS(Web Application Server)와 연동된다.

- ④ WEB 서버/WAS DBMS(Data Base Management System)와 연동하여 데이터를 관리하고, 블록체인과 연동하여 스마트 컨트랙트 로직을 처리한다. 사용자 인터페이스를 위한 웹서비스를 제공하며 Node.js 중심의 프레임워크를 사용해 구현 및 운영한다.

최근 인터넷상의 개인정보 보호가 중요한 사회, 경제적 이슈로 부각됨에 따라 기업 내부의 정보시스템에 산재해 있는 개인정보의 보호와 체계적인 관리의 필요성도 대두되고 있다. 본 연구에서는 Education Certification And Community(이하 ‘ECAC’라 한다) 프라이빗 블록체인 기반 웹 플랫폼 내의 사용자들의 개인정보를 보호한다.

사용자 개인정보를 AES 알고리즘을 활용해 암호화하여 별도의 DB에 저장한다. 블록에는 암호화된 개인정보에 해시 알고리즘을 적용하여 도출된 해시값만을 올리는 방법을 고안하였다. 해당 암호화 모델은 사용자 개인정보의 해시값만 블록에 올려 중요한 정보는 식별할 수 없도록 한다. 해당 개인정보가 필요한 때에 DB에 있는 암호화된 개인정보를 복호화하고, 그것을 다시 해시하여 블록에 올라가 있던 해시값과 비교 검증 작업을 수행한다.

다음은 본 연구 내 사용된 개인정보 암호화 및 저장 기술에 대한 흐름을 자세히 기술한 것이다.

- ① Client에서 암호화할 사용자의 개인정보와 사용자

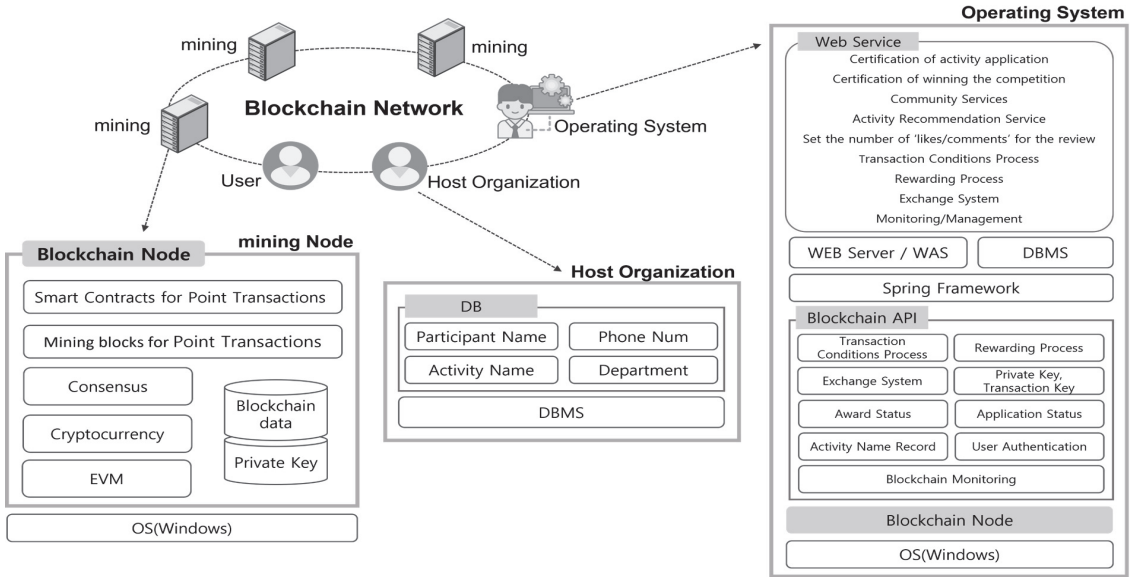


Fig. 3. Blockchain network and communication process

인증서를 별도로 구축한 서버에 보내어 암호화 및 저장 요청을 한다.

- ② 사용자 인증에 성공하면 요청받은 개인정보를 AES 알고리즘으로 암호화하여, DB 서버에 저장한다. 이때, 암호화에 사용한 x값을 복호화 시 사용하기 위해 DB에 같이 저장한다. key 값은 하드웨어 정보로 암호화하여 별도의 공간에 안전하게 보관하도록 하였다.
- ③ 저장이 완료되면 개인정보 암호문을 해시하고, DB로부터 반환받은 해당 Index와 해시된 개인정보 원문을 Client에 반환해준다. 위의 암호화하는 과정과 해시 하는 과정은 PKI 보안 모듈의 기능을 사용한다. 이를 통해 사용자의 개인정보는 보호하고, 서비스 제공자인 ECAC는 별도의 DB를 통해 사용자의 개인정보를 효과적으로 관리할 수 있다.

4. 이더리움 블록체인 성능평가

본 연구에서는 이더리움 블록체인의 성능을 트랜잭션 발행 포인트의 기준점을 변화시켜가며 측정할 시간에 따라 평가하였다. 좋아요 함수와 대댓글 함수 실행에 따라 지급되는 포인트의 비율을 조정하면서 트랜잭션 코드를 수정하였다. 이를 통해 1포인트부터 200포인트까지 다양한 시나리오에서의 성능을 평가하였고, 최종적으로 성능 저하 및 최적 기준점을 식별하고자 하였다.

4.1 이더리움 블록체인 성능평가 방법

성능평가 항목은 블록체인의 속도를 결정하는 대표적인 요소인 Transaction per Second, 블록 생성 시간, 블록 생성 확정 시간으로 구성한다. TPS는 과도한 트랜잭션이 발생했을 때 초 당 몇 개의 처리 속도를 보이는 지를 구할 수 있다. 블록 생성 시간이란 블록이 생성되는데 걸리는 시간으로 네트워크의 Latency에 해당한다. 블록 생성 확정 시간은 거래 내역이 최신 블록에 저장되어 있음을 보증해주는 시간을 의미한다. 본 연구에서는 다음 세 가지 방법으로 TPS를 측정하여 성능을 평가하고자 한다.

- ① Apache JMeter를 사용하여 TPS 측정
- ② 메인넷과 가장 유사한 테스트넷인 Ropsten을 사용하여 TPS 측정
- ③ Hyperledger Caliper를 이용하여 TPS 측정

연산이 발생하는 부분은 사용자의 커뮤니티 활성도를 계산하여 포인트를 지급하는 스마트 컨트랙트이다. 따라서 종속변수는 활성도 연산 코드의 위치로 하여 다음과 같이 구분한다.

- ① 사용자 활성도에 따라 포인트를 지급하는 연산 코드를 블록체인 스마트 컨트랙트 내에 구현한 경우
- ② 연산의 잦은 반복으로 인한 자원 낭비와 성능 하락 방지를 위해 사용자 활성도에 따라 포인트를 지급하는 연산 코드를 Web 환경에서 계산하여 계산된 포인트 개수를 블록체인에서 받아오는 경우

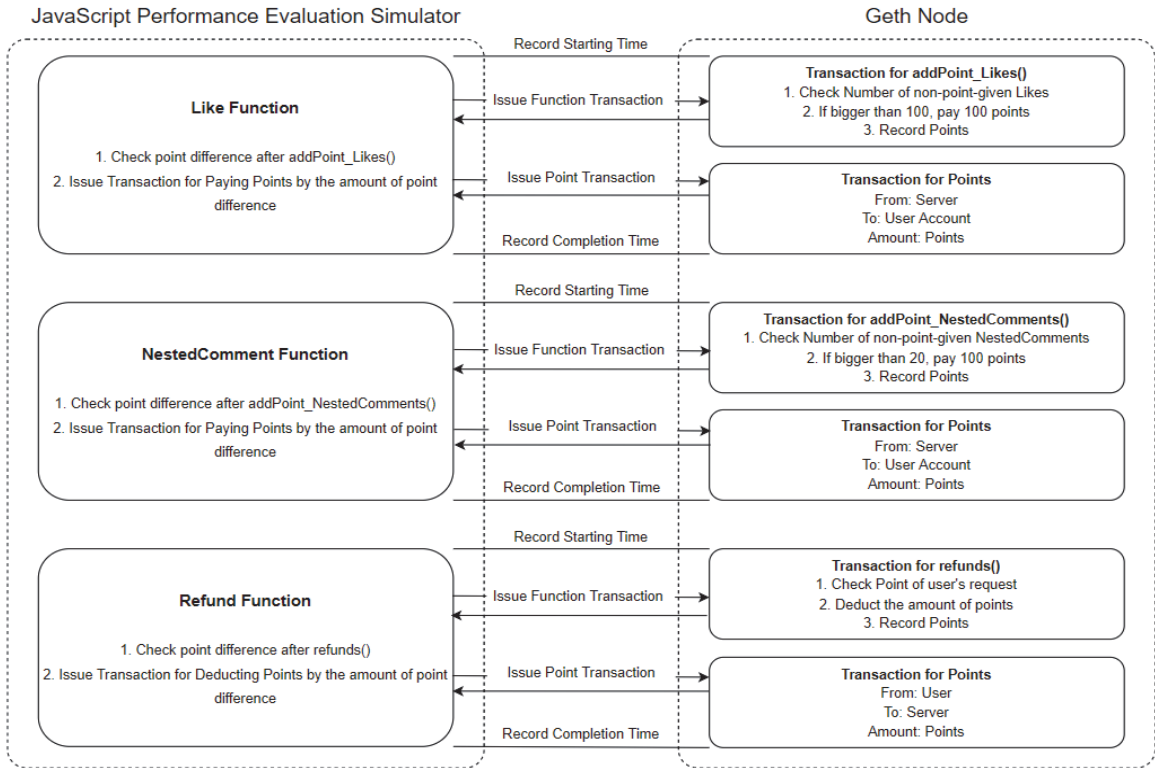


Fig. 4. Performance Evaluation Simulating Process

4.2 성능평가 시나리오 및 결과 분석

성능평가가 진행되는 시나리오는 Fig. 4와 같다.

- ① 사용자의 게시글이 좋아요를 받으면 포인트가 미 지급된 좋아요 개수에 따라 포인트를 지급하는 좋아요 함수를 실행하는 트랜잭션을 발생시킨다. 이후, 변화한 포인트 비율에 맞게 이더를 지급하는 트랜잭션을 발생시킨다.
- ② 사용자가 답변을 위해 대댓글을 남기면 포인트가 미 지급된 대댓글 개수에 따라 포인트를 지급하는 대댓글 함수를 실행하는 트랜잭션을 발생시킨다. 이후, 변화한 포인트 비율에 맞게 이더를 지급하는 트랜잭션을 발생시킨다.
- ③ 사용자가 포인트의 현금화를 요청하면 해당 양만큼 포인트를 차감하는 환급 함수를 실행하는 트랜잭션을 발생시킨다. 이후, 변화한 포인트 비율에 맞게 이더도 차감하는 트랜잭션을 발생시킨다.

각 시나리오에서의 성능평가 결과를 토대로 분석한 내용은 Table. 2와 Fig. 5와 같다.

Table. 2. “Points Payment Transaction” Execution Time for Likes and Comments Function ver.1

Points per Transaction	Like Function	Comment Function	Total Execution Time
1p	840s	1320s	2160s
5p	240s	300s	540s
10p	180s	240s	420s
20p	60s	120s	180s
50p	32s	53s	85s
100p	14s	18s	32s
150p	8s	45s	53s
200p	3s	44s	47s

성능평가 실행 결과에서 150p, 200p의 경우, 포인트를 모았다가 트랜잭션을 지급하므로 좋아요 포인트 지급 때는 트랜잭션이 발생하지 않고, 대댓글 포인트 지급 때는 트랜잭션이 발생한다. 이에 따라 좋아요 포인트 지급 시간은 줄었으나, 대댓글 포인트 지급 시간은 오히려 증가했음을 확인할 수 있다.



Fig. 5. "Points Payment Transaction" Execution Time for Likes and Comments Function ver.2

4.3 성능 최적화 분석

성능 최적화를 위해 각 시나리오에서의 총 수행시간을 계산하였다. 결과적으로 100포인트당 트랜잭션을 지급할 경우가 전체 실행시간 측면(Total Execution Time)에서 가장 우수한 성능을 나타냈다. 이는 좋아요 함수와 대댓글 함수의 수행시간을 고려할 때 가장 효율적인 포인트 기준임을 시사한다.

5. 블록체인 기반 이력관리 시스템 구현

본 장에서는 본 논문에서 구현한 이력관리 시스템의 실 운영 방식을 사용자 인터페이스를 통해서 제시하고자 한다.

사용자가 참여한 대외활동 및 대회 기록을 등록하는 활동 등록 페이지와 등록된 활동에 한하여 후기를 작성하게 되는 페이지는 각각 Fig. 6과 Fig. 7과 같다.

활동 등록

이름

전화번호

활동명 ▼

주최 기관

등록하기

등록하고자 하는 활동이 없나요? [추가 활동 등록](#)

Fig. 6. Register Activity

Review

제목

작성자

내용

TAG

저장 삭제

Fig. 7. Register Activity-Review

서비스 사용자가 공통 관심 분야를 가진 사람들의 활동 후기를 열람하고 댓글을 통해 소통하며 취업 활동을 위한 참고 자료로 활용할 수 있는 커뮤니티 기능은 Fig. 8과 같다.

트랙 집중 교육이 시작되고 처음에는 디지털 포렌식이 아닌 보안 컨설팅에 가게 되어서 두려움이 가득했습니다.

그러나 수업이 진행 될수록 디지털 포렌식보다 보안 컨설팅이 더 재미있다고 느꼈고,

디지털 포렌식보다 적성에 잘 맞는 분야를 찾을 수 있어서 좋은 경험이었다고 같습니다.

궁금한 점을 댓글로 남겨주세요!

yujeong

케이실드주니어와 BOB 교육 중 어떤 프로그램을 추천하시나요?

jeongmin

정보보안에 대한 기초부터 배우고 싶으실 경우 케이실드주니어 교육을 추천하고, 연구를 경험하고 싶으실 경우 BOB를 추천합니다

yujeong

답변 감사합니다

Fig. 8. Community Activity

서비스 사용자는 자신이 참여한 활동 및 기록을 조회할 수 있으며, 커뮤니티 활동도에 따른 누적 포인트를 확인 및 환급받을 수 있는 마이페이지는 Fig. 9와 같다.

회원 정보

MEMBER

SWU

가입 일자: 1월
등록한 활동: 5개
작성한 리뷰: 2개
포인트: 100Points

▶ 스코어링 보기
▶ 회원 정보 수정
▶ 후기 활동 등록

Fig. 9. Mypage Activity

6. 결론

본 논문에서는 간편한 이력관리 및 무결성 보장을 위한 이더리움 블록체인 기반의 이력관리 웹 시스템을 자바스크립트 언어를 기반으로 구축하였다. 또한 솔리디티 언어로 웹 사이트상의 포인트 지급 스마트 컨트랙트를 개발하여 블록체인 Test Network 상의 구동 테스트를 마쳤으며 Truffle을 이용한 Geth Private Network 상의 배포를 수행하였다. 더불어 포인트 비율을 기준으로 한 Geth Private Network 스마트 컨트랙트의 성능평가를 수행하였다. 다양한 시나리오에서의 성능평가를 진행한 결과 100포인트당 트랜잭션을 지급할 경우 최적의 성능을 나타낸다는 결론을 도출하였다. 이러한 결과는 성능 최적화 뿐만 아니라 원활한 서비스 이용을 촉진하며, 더 나아가 사용자들의 활동에 대한 신속한 보상 요구를 어느 정도 해소할 수 있을 것이다.

본 시스템의 활용으로 기업은 위변조 검증 절차를 통해 지원자의 검증된 이력을 열람하고, 사용자는 웹 사이트를 활동·수상 이력에 대한 순위 관리 및 각종 활동에 대한 양질의 정보를 제공받을 수 있을 것으로 기대한다.

References

Antonopoulos, A. M., & Wood, G. (2018). *Mastering Ethereum: Unlocking the Power of Smart Contracts and Decentralized Applications*. O'Reilly Media.

Bae, S.H., Shin, Y.T. (2020) "Design of Personal Career Records Management and Distribution using Block Chain", *Journal of Korea Institute of Information, Electronics, and Communication Technology*, 13 (3), 235-242.

Bartoletti, Massimo & Pompianu, Livio. (2017). *An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns*. *Lecture Notes in Computer Science*. 10.1007/978-3-319-70278-0_31.

Jeong, S.W., Jung, H.J., (2022). "Design of Blockchain based Digital Badge Framework for Reliable Career Verification", *Journal of Korean Institute of Information*, 20(9), 147-153.

Kim, J.H., Hong, W.K., Woo, J.S, (2022). *Personal Data Sovereignty and Tracking System using Decentralized Identifier and Permissioned Blockchain*. *KNOM Review*, 25(1), 16-27.

Kim, T.Y., Kim, H.J., "DEVS-based Experimental Framework for Blockchain Services," *Simulation Modelling Practice and Theory*, 108(1), April of 2021, (SCI)

Moon, Y.B, Heo, T.W., Lee, C.H., Doh, Y.M., (2020), *Blockchain Based Energy Trading Technology for the Community*, *Electronics and Telecommunications Research Institute*, 35(6).

Shon, J.G. (2011), *A Study on e-Portfolio Standardization*, *Journal of Lifelong Learning Society*, 7(2), 137-156.

Wood, G., (2014) *Ethereum: A Secure Decentralized Generalised Transaction Ledger*. *Ethereum Project Yellow Paper*, 151, 1-32.

Yun, J.H., Kim, M.H., (2018). *Private Blockchain and Smart Contract Based High Trustiness Crowdsensing Incentive Mechanism*. *Journal of The Korea Institute of Information Security and Cryptology*, 28(4), 999-1007.



홍 정 민 (ORCID : <https://orcid.org/0009-0009-1122-7108> / everlasting090@swu.ac.kr)

2020~ 현재 서울여자대학교 정보보호학과 학사과정

관심분야 : 백엔드, AWS, 블록체인 성능평가



김 예 진 (ORCID : <https://orcid.org/0009-0009-9884-3316> / bijou__ye@swu.ac.kr)

2020~ 현재 서울여자대학교 정보보호학과 학사과정

관심분야 : 개인정보보호, 백엔드



김 유 정 (ORCID : <https://orcid.org/0009-0001-4314-1247> / yujeong@swu.ac.kr)

2019~ 현재 서울여자대학교 정보보호학과 학사과정

관심분야 : 정보보안, AWS, 안드로이드



박 혜 정 (ORCID : <https://orcid.org/0009-0005-7045-132X> / wjd0611@swu.ac.kr)

2020~ 현재 서울여자대학교 정보보호학과 학사과정

관심분야 : 백엔드, 인공지능



강 은 성 (ORCID : <https://orcid.org/0009-0008-5963-1786> / ekang@swu.ac.kr)

1982 서울대학교 전자계산기공학과 공학사

2017 연세대학교 정보시스템학석사

2003~2008 안랩 연구소장

2008~2013 SK커뮤니케이션즈 CSO

2014~2017 CISO Lab 대표

2017~2019 블록체인오에스 CISO

2023~현재 서울여자대학교 정보보호학과 조교수

관심분야 : 개인정보보호, 위협관리, 공급망보안



김 형 중 (ORCID : <https://orcid.org/0000-0002-0608-5397> / hkim@swu.ac.kr)

1996 성균관대학교 정보공학과 공학사

1998 성균관대학교 정보공학과 공학석사

2001 성균관대학교 전기전자 및 컴퓨터공학과 공학박사

2001~2007 한국정보보호진흥원 수석연구원

2004~2006 미국 Carnegie Mellon University, CyLab 국제공동연구원

2013~2014 미국 Carnegie Mellon University, ECE, Visiting Professor

2007~현재 서울여자대학교 정보보호학과 정교수

관심분야 : 개인정보보호, 블록체인 서비스 성능평가, 클라우드 서비스 보안 모델