JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 23, No. 11: 1462~1470, Nov. 2019

블록체인 기반 공개 논문 심사 시스템

권용빈[1] · 장경배[1] · 최승주[1] · 서화정[2*]

Open Peer Review System based on Blockchain

Yong-been Kwon[1] · Kyoung-bae Jang[1] · Seung-ju Choi[1] · Hwa-jeong Seo[2*]

[1]Graduate Student, Department of IT Engineering, Hansung University, Seoul, 02876 Korea
[2*]Assistant Professor, Department of IT Engineering, Hansung University, Seoul, 02876 Korea

요 약

연구자는 연구 결과를 논문의 형태로 작성하여 학회에 투고하고 투고된 논문은 심사자의 면밀한 심사를 받은 뒤 학계에 공개되어 학문의 발전에 쓰인다. 이렇듯 심사 과정에 의해 연구 결과가 학계에 알려질지 결정되기 때문에 적절한 심사 시스템에 대해 많은 논의가 이루어지고 있다. 본 논문에서는 현재 심사 시스템에서 발생하고 있는 문제점들을 살펴보고 이에 대한 해결책으로 블록체인 기반 공개 논문 심사 시스템을 제안한다. 제안하는 시스템은 기존의 시스템과 다르게 개방적인 심사 구조를 가지며 투명성을 통해 공정하고 깊이 있는 평가를 보장한다. 동시에 블록체인을 사용함으로써 발생할 수 있는 프라이버시, 용량 문제에 대한 해결책을 제공한다. 최종적으로 제안하는 심사 시스템을 구현하여 결과를 보인다.

ABSTRACT

The researcher writes the result of the research in the form of paper. The submitted papers gets careful peer review by the reviewers and used for the development of academic studies after it gets published. There has been numerous debate about the review system, as the review process determines whether the results will be known to academia. In this paper, we investigate the problems in the present review system and propose a open peer review system based on blockchain. The proposed system has an open peer review structure unlike the existing one and ensures fair and in-depth evaluation through transparency. The system also provides a solution to the privacy and capacity problems that may arise from the use of blockchain. Lastly, we implement the proposed peer review system and show the results.

키워드 : 블록체인, 논문 심사, 스마트 컨트랙트, 공개 심사

Keywords : Blockchain, Peer review, Smart contract, Open review

Received 6 July 2019, **Revised** 26 July 2019, **Accepted** 25 August 2019

*** Corresponding Author** Hwa-jeong Seo(hwajeong84@hansung.ac.kr, Tel:+82-2-760-8033)
Assistant Professor, Department of IT Engineering, Hansung University, Seoul, 02876 Korea

Open Access http://doi.org/10.6109/jkiice.2019.23.11.1462 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

연구자는 지식을 탐구하는 집단이다. 학회는 연구자들 간의 지식 공유가 일어나는 기관이며 이를 통해 탐구 활동은 가속화된다. 지식의 공유는 논문이라는 매개물 통해 이루어진다. 논문은 연구자들의 탐구 결과를 논리정연하게 작성한 글이다. 이렇듯 연구 활동이 논문을 매개하여 공유되기 때문에 연구자 평가는 주로 논문으로 이루어지게 된다.

연구자들은 자신의 연구 결과를 잘 정리하여 학회에 투고하게 된다. 투고된 논문은 적절한 심사를 거쳐 학술지에 게재되고 이를 통해 지식이 공유되고 축적된다. 만약 심사 단계에서 논문으로서의 가치를 인정받지 못한다면 지식은 공유되지 않으며 축적되지도 못하기 때문에 공정한 심사가 중요하다. 심사는 동일한 혹은 유사한 분야의 동료 연구자에 의해 시행되는데 해당 분야에 대한 전문성이 있어야 적절한 심사가 가능하기 때문이다. 많은 연구자들이 이러한 심사 과정이 필요하다고 인지하고 있지만 동시에 심사 과정에 많은 문제점이 있다고 말하고 있다. 실제로 심사 과정에서는 연구 윤리와 관련된 문제, 심사자 선정에 관한 문제 등 다양한 문제들이 발생해 왔으며 이를 해결하기 위한 다양한 연구가 활발하게 진행 중이다[1].

현재의 심사 시스템에서의 심사 위원단은 보통 3명으로 이루어진다. 적은 수의 심사 위원단에 의한 심사는 심사자의 주관이 크게 작용하기 때문에 적절한 심사라고 보기 어렵다. 또한 저자들이 심사자를 알 수 없는 경우가 많은데 이 경우 심사자의 익명성이 보장되는 장점이 있지만 심사자의 주관적 개입이 극대화될 수 있으며 이에 따른 출신 국가, 성별 등 다양한 편견에 따른 차별이 존재한다[2-3]. 무엇보다도 전 심사 과정이 비공개로 진행되기 때문에 심사 과정에 문제들이 발생하더라도 쉽게 발견하기 어렵다는 치명적인 단점이 존재한다. 또한 표절이나 이중 게재와 같은 연구 윤리에 어긋나는 행동들을 심사 과정에서 방지하기 위해서는 학회 간의 소통이 중요하다고 알려져 있지만[4] 현재의 폐쇄적인 심사 구조에서는 이러한 소통을 어렵게 한다.

이러한 문제들을 해결하기 위해 공개 심사 방식이 제안되었다[5]. 공개 심사는 다수의 심사자가 공개된 장소에서 심사하는 개방적인 구조되는 형태로 객관성, 투명성이 확보된다. 하지만 이에 따른 문제도 제기되고 있다[6]. 가장 큰 문제점은 익명성이 보장되지 않기 때문에 적합한 심사자를 구하기 어렵다는 점이다. 예를 들어, 후배 연구자들이 선배 연구자들의 심사를 어려워하는 경우이며 이는 연구자간 네트워크가 촘촘할수록 더 심화되기 때문에 활성화된 학문 분야일수록 심사자를 찾는 것이 더 어렵게 된다.

본 논문에서는 공개 시스템의 장점을 유지하면서 단점을 해결하는 새로운 형태의 공개 심사 시스템을 제안한다. 심사 과정의 투명성과 무결성을 위해 블록체인 기술을 이용했으며 심사자, 저자의 익명성과 논문이 게재불가 판정을 받을 경우 아이디어 보호를 보장하기 위해 스마트 컨트랙트를 이용한다. 2장에서는 해당 연구와 관련한 연구들을 살펴보고 3장에서는 제안하는 심사 시스템을 기능을 중점으로 설명한다. 4장에서는 이에 대한 구현을 보이고 5장에서 결론을 내린다.

Ⅱ. 배 경

본 절에서는 비공개 심사에서 발생하는 문제점들을 살펴보고 이를 해결하기 연구되고 있는 다양한 공개 심사 형태를 살펴본다. 다음으로 블록체인과 스마트 컨트랙트의 개념을 알아보고 이를 이용할 수 있는 대표적인 플랫폼 이더리움(Ethereum)을 설명한다.

2.1. 비공개 심사의 문제점

비공개 심사는 편집장이 선택한 소수의 심사자에 의해 비공개로 진행된다. 비공개 심사는 두 가지로 분류되는데 저자가 심사자를 모르는 형태의 부분 비공개 심사 형태와 저자와 심사자가 서로를 모르는 완전 비공개 심사 형태로 분류된다. 부분 비공개 심사 형태는 현재 대부분의 논문 심사에서 이용되는 심사 형태이다. 심사자의 신원이 보호되어 보다 날카로운 심사가 가능하다는 장점이 있지만 노출되는 저자의 신원으로부터 성차별을 비롯한 다양한 차별이 발생하며 경쟁 관계에 있는 저자의 논문 심사를 고의로 지연하는 비윤리적 문제가 발생하기도 한다[4]. 완전 비공개 심사 형태에서는 표면적으로 저자의 익명성이 보장되는 것으로 보이지만 논문을 바탕으로 저자의 추측이 가능하므로 완전히 해결되지 않는다.

분류되는 심사 형태와 무관하게 비공개 심사 형태에

서는 심사 과정이 공개되지 않는데 이로 인해 다양한 문제점들이 발생한다. 먼저 피상적인 심사와 수정이다. 심사자로서 논문을 제대로 심사하지 않고 게재가 판정을 한다거나 저자로서 수정 후 게재 판정을 받았을 경우 피상적인 수정만을 거쳐 다시 제출하는 것을 말한다. 실제 대다수의 연구자들이 빈번하게 목격한 부정 사례로 선정되었으며 학회의 관습이나 분위기가 원인이라고 여겨지고 있다. 다음으로는 이중 게재, 연구 분절, 표절과 같은 연구 윤리와 관련한 문제들이다. 이러한 문제들은 연구자들의 실적에 대한 집착과 실적에 대한 평가가 게재된 논문 수, 게재된 논문의 피인용 수에 따라 결정되는 점을 원인으로 발생한다. 이중 게재란 같은 연구 결과를 또 다른 학회에 게재하는 문제이다. 일종의 자기 표절의 형태로 볼 수 있으며 같은 연구 결과를 여러 학회에 등록하여 마치 많은 연구 활동을 한 것으로 보이도록 하는 형식이다. 연구 분절이란 하나의 연구 결과를 분절하여 여러 곳의 학회에 내는 문제이다. 논문 게재 수, 인용 수를 부풀릴 수 있기 때문에 발생하며 이러한 경우 각각의 논문의 질이 떨어지기 때문에 학문의 발전이 저해된다. 마지막으로 표절은 다른 논문의 연구 결과를 자신의 실적인 것처럼 적는 것을 말한다. 이중 게재, 연구 분절, 표절과 같은 문제들을 다루기 위해서는 학회 간의 긴밀한 협력이 필요하지만 현존하는 시스템에서는 이러한 협력이 용이하지 않다.

앞에서 말한 비공개 심사에서 발생하는 모든 부정들은 심사 과정이 공개되지 않기 때문에 발생하더라도 알기 어렵다는 특징을 갖는다. 다시 말해, 저자가 부당한 차별을 받더라도 이에 대한 증거가 될 자료가 없으며, 저자가 부당한 행위를 저지르더라도 이에 대한 증거를 찾기 어렵다는 점이다. 이를 해결하기 위해 윤리위원회를 설치하는 등 제도적인 장치의 도입하거나 연구 윤리에 대한 교육을 강화하는 등의 해결책에 대한 논의가 되고 있지만 비용적인 문제가 들며 결국 연구자의 윤리 의식에 의존해야 한다는 점에서 한계가 있다.

2.2. 공개 심사

공개 심사 형태는 논문 심사에 투명성을 제공하기 위해서 제의되었다. 이를 실천하기 위한 많은 연구가 진행중에 있고 아직 체계가 정립되지는 않은 심사 형태이다. 좁은 의미에서는 저자와 심사위원의 정보를 공개하는 심사 형태를 의미하며 넓게는 공개된 네트워크에서 저자와 다수의 심사자가 서로 상호작용하며 논문을 검증하는 심사 형태를 말한다. 이러한 형태의 심사를 도입하면 비공개 심사에서 발생했던 많은 문제를 해결할 수 있게 된다. 먼저 심사를 볼 수 있는 절대 다수 이용자가 감시자의 역할을 하게 되어 저자에 대한 비윤리적 차별과 같은 저자에 대한 편견, 동일 분야 연구자에 대한 견제로서의 고의 심사 지연과 같은 행위가 방지된다. 다수의 심사자가 참여할 수 있기 때문에 일부 심사자가 가진 편견, 이해관계에 따른 부당한 심사 혹은 심사자의 역량 부족에 따른 부족한 심사의 영향력이 분산된다. 오히려 심사자들 사이의 상호작용이 활성화되므로 더 깊은 심사가 가능해진다. 또한 신분이 드러나기 때문에 피상적인 심사, 피상적인 수정과 앞서 말한 연구 윤리와 관련한 문제들 또한 방지된다. 공개적인 구조이므로 학회 간의 협력이 용이하며 긴밀한 협력을 요구했던 문제들 역시 적절한 조치를 취할 수 있게 된다. 이처럼 공개 심사 형태는 비공개 심사의 많은 문제점들을 해결하는 것으로 보인다. 그러나 이러한 공개 심사 방식 또한 제약 사항이 존재한다. 첫 번째는 학회를 중심으로 시스템이 구축된다면 이용자가 시스템을 신뢰할 수 있는가의 문제이고 두 번째는 비공개 심사에서 익명성으로 보장되었던 심사자의 신원이 밝혀짐에 따라 심사자에 대한 저자의 보복이 두려워 심사를 꺼리는 현상이 발생한다는 것이다. 세 번째 제약 사항은 논문 심사를 위해 논문이 공개된 네트워크에 공개된다는 점이다. 다시 말해 가치 있는 연구 결과를 포함하는 논문이 모종의 이유로 게재불가 판정을 받을 경우 저자의 아이디어, 연구 결과가 표절될 수 있다는 점이다. 표절에 대한 추적도 불특정 다수에게 공개되는 특성 때문에 사실상 불가능해지며 원저작권자로서의 권리를 입증하기도 어려워진다.

본 논문에서는 논문 심사에 블록체인과 스마트 컨트랙트를 적용하여 심사에 신뢰할 수 있는 투명성을 제공한다. 익명성을 보장하여 심사 권한을 보장하면서도 부당한 심사는 감시를 통해 저지한다. 저자의 논문에 대한 저작권을 보호하며 원저작권자로서의 권리를 입증할 장치를 제공한다.

2.3. 블록체인과 스마트 컨트랙트

블록체인은 네트워크에서 발생하는 모든 행위를 트랜잭션이라는 형태로 기록한다. 이러한 트랜잭션의 묶음을 블록이라 한다. 네트워크에 존재하는 블록들은 모

두 해시라는 알고리즘을 통해 연결되어 있다. 이전 블록의 해시 결과는 다음 블록에 포함이 되며, 다음 블록은 이러한 정보를 포함해서 본 블록의 해시 값을 생성한다. 이로 인해 이전 블록에 기록된 데이터에 변조가 있게 되면 그 블록에 대한 해시 결과가 다음 블록에 기록되어 있는 해시 결과와는 완전히 다른 형태를 취하게 된다. 이는 연쇄적으로 네트워크의 모든 블록의 정보에 영향을 미치게 되된다. 따라서 이미 발생했던 트랜잭션을 변조하기 위해서는 해당 트랜잭션을 포함했던 블록을 포함하여 그 이후에 네트워크에 존재하는 모든 블록의 해시 값을 변조해야한다. 이러한 블록에 대한 정보는 네트워크에 참여한 모든 노드들이 복제하여 갖고 있기 때문에 블록을 변조하더라도 다수에 의해 블록이 변조되었다는 사실이 밝혀지게 된다. 이를 통해 블록체인은 네트워크의 무결성을 보장한다. 또한 모든 블록이 다수의 참여자에게 복제되어 이용되므로 네트워크에서 발생되는 행위들에 대한 투명성 또한 보장되며 이러한 장점을 이용해 다양한 서비스들이 개발되고 있다[7]. 최근에는 블록체인에 대한 연구로서 트랜잭션을 선택적으로 기록하거나 트랜잭션을 발생한 대상을 익명화 해주는 연구들도 활발하게 시도되고 있다[8].

스마트 컨트랙트란 블록체인 네트워크 위에서 특정한 조건을 만족할 시 코드를 실행하는 기술이다. 블록체인의 발전된 형태로 일컬어지며 화폐의 거래를 넘어 등록한 연산들을 자동으로 처리하며, 데이터 또한 교환을 할 수 있다는 특징을 활용해 다양한 형태의 서비스들이 개발되었다.

본 논문에서는 블록체인의 무결성과 투명성이란 특징을 바탕으로 스마트 컨트랙트를 활용하여 기존 논문 심사 과정에서 발생했던 문제들을 해결하고자 한다.

2.4. 이더리움

이더리움은 스마트 컨트랙트를 대표하는 블록체인 플랫폼이다. 솔리디티(solidity)라는 프로그래밍 언어를 사용하여 스마트 컨트랙트를 구현하며 이를 이용해 다양한 분산형 어플리케이션(DApp, Decentralized Application)을 구현할 수 있다. 현재 이더리움을 이용한 많은 서비스들이 제공되고 있으며 기술과 관련한 많은 연구들도 진행되고 있다[9].

2.5. 블록체인이 가진 법적 과제

블록체인은 초기에 가상 화폐로서 주목 받았다. 이에 따라 실물이 없는 화폐, 자금 세탁 등의 이슈로 법적인 연구가 진행되어왔다. 또한 현재는 개인정보보호 강화의 세계적인 추세와 블록체인이 적용되는 분야가 매우 다양해짐에 따라 프라이버시에 대한 연구가 많이 진행되고 있다. 만약 다루는 데이터가 저작권과 관련한 문제를 가질 경우, 이러한 데이터가 복제되어 다수의 노드에 복사된다는 점이 문제가 된다. 마지막으로 컨트랙트에 대한 설계에 대한 문제가 배포 뒤 발견된다면, 그 전까지의 계약에 대한 효력은 어떻게 될 것인가를 생각해 보아야 한다. 이러한 블록체인의 기술적인 특성 아래 발생할 수 있는 문제들을 해결하기 위해 많은 연구들이 진행되고 있다. 서비스에 블록체인을 적용하기 위해서 이들을 충분히 고려해야 한다.

Ⅲ. 제안하는 시스템

3.1. 심사 과정의 공개 데이터화

기존의 시스템에서는 심사에 대한 내용을 공개된 네트워크에 저장하지 않으며 심사에 따른 수정 및 보완 기록도 저장하지 않는다. 특히 수정 후 게재 판단을 받을 경우 논문이 제대로 심사되고 보완 되었는지 알기 어렵다. 예시가 되는 사례는 피상적인 심사 또는 그러한 수정이 발생하는 경우이다. 저자가 학계에서 가지는 영향력이 크거나 학회의 분위기 상 게재 불가 판정을 내리기 어려운 것이다. 이러한 경우 저자와 심사자는 분쟁이 발생하지 않지만 결과적으로 논문의 질이 떨어질 수 있다. 따라서 본 논문에서는 심사 전 과정을 데이터화 하여 저장하는 것을 제안한다. 이를 통해 적절한 심사가 이루어졌는지 심사에 따른 적절한 보완 및 수정이 이루어졌는지 그리고 부당한 심사 또는 피상적인 심사가 발생하진 않았는지에 판단할 수 있는 근거를 마련한다. 다시 말해, 심사자는 저자의 명성이나 학회의 분위기와 상관없이 공정하고 면밀한 심사를 해야 한다. 심사 과정에서 발생 했던 모든 데이터에 대한 내용은 블록체인 네트워크에 기록이 되며 이에 심사를 진행한 과정의 근거가 된다. 이때 저장하는 데이터는 아래 그림 1과 같다.

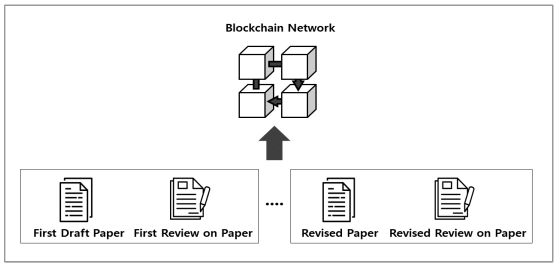

Fig. 1 Data to be written to the Blockchain

먼저 블록체인 스마트 컨트랙트에 최초 논문과 심사자들의 심사평을 저장한다. 최초 논문과 심사평을 비교함으로써 적절한 심사가 이루어졌는지 알 수 있다. 만약 수정 후 게재 판단을 받을 경우 추가적으로 수정된 논문을 함께 저장하여 적절한 수정이 이루어졌는지 알 수 있게 한다. 마지막으로 수정 후 재심사 판단을 받는 경우 수정된 논문과 수정된 논문에 대한 심사평을 추가로 저장하여 논문 심사에 대한 검증이 가능하도록 한다. 이렇게 심사 전 과정을 공개 데이터화하여 저장하게 된다.

3.2. 데이터 저장소

블록체인 특성상 블록체인에 저장되는 데이터들은 네트워크에 참여한 사용자들이 데이터를 각자 지정한 공간에 복사하여 갖게 된다. 그런데 이러한 데이터는 블록이 계속해서 생성됨에 따라 늘어나게 된다. 이는 게재되는 논문의 수가 매년 증가하고 있다는 사실과 더불어 [10] 블록체인 네트워크의 데이터 부하를 지수적으로 증가시키는 이유가 된다. 이러한 문제들을 다루기 위해 논문과 심사평을 블록체인 네트워크에 직접 저장하지 않고 저장된 주소만을 저장하는 구조를 생각해 볼 수 있다. 그런데 이러한 저장 방식을 택하는 경우, 주소내의 데이터가 변경이 되었을 시 심사 평가에 대한 무결성을 제공할 수 없게 된다. 이를 해결하기 위해 블록체인 네트워크에는 주소와 함께 주소에 저장된 논문 등의 데이터의 해시 결과를 함께 저장하게 된다. 따라서 심사 과정이 심사 이후에 조작된다면 해시 결과가 변경되게 되고 이 값은 무결성이 보장되는 블록체인 네트워크에 저장된 해시 결과와 다른 값을 갖게 된다. 이를 통해 심사 이후의 조작을 방지하면서 블록체인 네트워크 부하를 최소화할 수 있다. 데이터 저장소는 학회에서 관리하도록 한다. 따라서 데이터 무결성 보장에 대한 책임은 학회에 있게 된다.

3.3. 주소 암호화

논문은 심사를 거쳐 게재불가 판정을 받을 수 있다. 그런데 공개된 네트워크에서 심사를 거친 뒤 게재불가 판정을 받는다면 저자의 연구 결과는 표절의 위험에 처할 수 있다. 특히 블록체인의 데이터는 다수의 사용자에게 복제되고 생성된 블록들이 해시로 연결된 구조를 띠고 있어 중간 블록이 변조될 수 없는데, 이는 블록체인에 올라간 데이터는 삭제가 사실상 불가능하다는 것을 의미한다. 제안하는 시스템에서는 네트워크 위에서 논문을 투고하고 심사가 이루어지기 때문에 논문이 블록체인과 연결된 저장소에 등록되게 된다. 이러한 구조에서는 게재불가 판정을 받더라도 저장소에는 논문과 심사평이 남아있게 된다. 이러한 문제점을 해결하기 위해 저장소 주소를 암호화하여 블록에 저장하는 기법을 이용하며 도식화하면 그림 2와 같다.

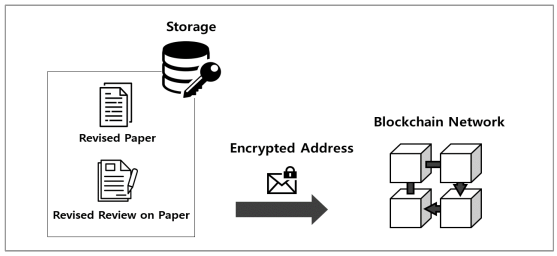

Fig. 2 Writing an encode the storage address on Blockchain Network

저자, 심사자는 주소에 접근할 수 있어야 하므로 복호화 키가 제공된다. 따라서 심사 중에 논문에 접근할 권한을 가지는 개체는 저자와 심사자가 된다. 심사에 직접적으로 참여하지 않는 다른 네트워크 참여자들의 경우 논문이 심사 중인 사실만 알 수 있다. 하지만 일반 네트워크 참여자들도 주소에 접근할 수 있어야 심사 과정에 투명성을 부여할 수 있고 심사 과정에 대한 감시가 가능할 것이다. 제안하는 시스템에서는 저자의 논문을 보호하면서도 투명성을 제공하기 위해 다음과 같은 방법을 제시한다. 먼저 심사 결과로 게재가 판단이 나올 경우에만 복호화 키를 공개함으로써 모든 네트워크 참여자들이 저장소에 접근할 수 있게 한다. 논문 게재가 이루어진 뒤에는 아이디어를 보호할 이유가 없기 때문이다. 적절한 심사 및 심사에 따른 논문 수정이 이루어졌는지 검증하는 시점은 논문 게재 이후가 된다. 네트워크 참여자들은 게재 이후 공개된 심사 과정을 평가하여 그 타당성

을 검증하게 된다. 만약 심사 결과가 게재불가로 나온다면 복호화 키는 공개되지 않고 주소는 암호화된 채로 블록에 남게 된다. 따라서 심사가 종료된 이후에도 네트워크 참여자들은 저장소에 접근할 수 없으며 논문 내용은 보호된다. 이 때, 저자는 복호화 키를 공개할 권한을 갖는다. 복호화 키를 공개할 경우 저자의 논문과 논문에 대한 심사평이 모든 네트워크 참여자에게 노출되며, 참여자들은 부당한 심사가 있었는지 검증할 수 있게 된다. 만약 부당한 심사 과정을 숨기기 위해 데이터 저장소에 대한 조작이 발생한다 하더라도 그 해시가 네트워크에 올라와 있기 때문에 조작을 감지할 수 있다. 이러한 방법으로 연구 결과를 보호하는 한편 부당한 심사에 대한 검증 방법을 마련할 수 있다.

3.4. 적절한 심사자 찾기

본 절에서는 공개 심사에서 적절한 심사자를 찾기 어려웠던 문제를 해결하는 방법을 다룬다. 공개 심사에서는 심사자의 신원이 드러나기 때문에 직접적인 이해관계가 있는 관계에서의 보복이 두려워 제대로 된 평가를 할 수 없다는 문제가 있었다. 제안하는 시스템에서는 심사 과정이 드러나기 때문에 제대로 된 평가를 해야겠지만 그럼에도 이해관계가 있다면 심사를 꺼려 심사자를 찾는 것이 어려워질 수 있다. 블록체인에서 익명화를 제공하는 많은 기법들이 연구되고 있다[8]. 제안하는 시스템에서는 심사자들 중 한 명만을 서명자로 둠으로써 각 심사자를 보호할 수 있다. 이를 링 시그니쳐 기법이라고 한다. 이 경우 심사자와 심사 결과의 일대일 매핑이 불가능하므로 익명성이 보호된다. 하지만, 잘못된 심사에 대해 심사자 개개인에 대한 책임 역시 물을 수 없게 된다. 또 다른 방법으로는 믹싱 방법이 있다. 입력과 출력을 뒤섞는 방법이다. 이 경우 컨트랙트만이 매핑에 대한 정보를 가지고 있게 하여 공개된 네트워크에서는 누가 어떤 심사 결과를 내렸는지 알 수 없지만 부당한 심사에 대한 각각의 피드백들은 컨트랙트를 경유하여 심사자들에게 전해질 수 있도록 할 수 있다. 또한 영지식 증명을 활용할 수 있다. 영지식 증명 중에서도 Zk-SNARKs 기법을 이용하여 익명성을 보장할 수 있다. 각 심사자들은 동형암호로 암호화된 심사 결과를 보내고 컨트랙트는 이를 검증하여 결과만을 등록할 수 있다. 이 경우에는 컨트랙트와 심사자 사이에 어떤 식으로 심사 결과를 검증할 것인지 사전 협의가 필요할 것이다. 위와 같은 방법들을 통해 심사자의 익명성을 보호하여 심사자가 신원 공개의 부담을 가지지 않고 공정한 평가를 하도록 할 수 있다. 또한 블록체인은 공개된 네트워크임을 고려하여 제안하는 시스템에서는 기존과 다른 방식으로 심사자를 선정한다. 기존의 심사자는 편집자 재량 혹은 저자의 제안으로 선정되었다. 이러한 방식은 심사자의 역량이나 심사에 대한 신뢰를 보장할 수 없다. 본 논문에서 제안하는 시스템은 블록체인이라는 공개되는 네트워크를 이용하므로 네트워크의 모든 참여자가 심사를 지원할 수 있다. 심사자로서의 자격에 대한 검증은 아래와 같이 진행한다. 네트워크에 참여하는 사람들은 특정 분야에 게재된 논문 수, 인용 수와 같이 기존의 연구자 평가에 널리 사용되어온 지표와 더불어 참여한 심사에 대한 평가를 더한 연구자 점수라는 새로운 평가 지표를 갖는다. 이는 심사 데이터가 남기 때문에 가능해진다. 이 연구자 점수에 기준하여 심사자의 자격을 검증하게 된다. 이를 통해 공개된 네트워크에서도 심사자의 신원을 보호하면서도 점수를 통해 검증된 심사자를 선정할 수 있게 된다. 연구자 점수는 자신의 심사가 좋은 평가를 받을수록 올라가므로 심사의 질과 심사 참여에 대한 동기를 제공할 것으로 예상된다. 이는 기존 시스템에 비해 적절한 심사자를 찾기 용이해 진다는 것을 의미한다.

3.5. 저자의 익명성 보호

기존의 시스템의 경우 저자의 성별, 국적, 이해관계에 따른 차별이 발생하였다. 제안하는 시스템인 블록체인 네트워크에서는 주소를 이용하므로 기본적으로는 저자에 대한 정보를 알 수 없다. 하지만 논문이 공개되었을 시 이 주소를 논문과 매핑하면 실세계의 저자와 주소의 연결을 만들 수 있다. 정확하게 말한다면 저자가 트랜잭션을 통해 만들어 낸 저장소 주소와의 연결을 통해 이러한 연결을 만들 수 있다. 여기에 링 시그니쳐 기법을 사용한다면 다수가 모여 다수의 주소를 생성해 내고 그 주소를 나눠 갖는 방법으로 익명성을 보장할 수 있다. 먼저 논문 심사 시 저장소를 생성해 낸 주소를 찾기 어렵기 때문이다. 논문이 게재가 된 이후 저자가 공개되더라도 논문을 통해 저자의 주소를 찾는 것은 어렵다. 하지만 이러한 기법을 이용하더라도 연구 내용이나 문체 등을 통해 저자를 유추할 수 있을 것이다. 이러한 경우 주소의 추적과 무관하게 차별이 발생할 수 있다. 하지만 제안하는 시스템에서는 다수의 심사자가 참여

하므로 이러한 주관에 의한 평가가 최소화 될 것이고 논문 심사가 끝난 뒤에도 다수의 네트워크 참여자에 의해 해당하는 심사가 부정될 것이다.

3.6. 법률적 장치

기존의 심사 시스템에서는 발생하는 부정에 대한 증거 자료를 확보하기 어려웠다. 하지만 블록체인에서는 네트워크 내부에서 시행한 행위들이 검증되므로 이를 증거로서 이용할 수 있다. 예를 들어, 심사와 관련된 부정 발생 시, 저장소에 저장된 심사 내용을 첨부할 수 있으며 이에 대한 무결성은 블록체인 네트워크에 올라온 해시를 통해 보장된다. 또한 기존의 저자 차별과 같은 윤리적인 문제 또한 네트워크 참여자에 의해 감시되게 된다. 발생하는 프라이버시의 경우 상술한 심사자, 저자의 익명성을 보호하는 장치들로써 해결될 수 있다. 저작권을 가지는 논문의 성격 상 복제되어 저장되는 것은 저작물의 가치를 떨어뜨릴 수 있어 문제가 된다. 하지만, 제안하는 시스템에서는 주소만을 네트워크에 저장하기 때문에 저작물인 논문은 한 곳에만 저장되므로 이에 대한 문제를 다룰 수 있다. 저장소에 대한 관리 책임은 각 학회에 있으며 학회는 논문집 출간, 학회 간 협력 등을 위해 저장소를 관리하는 이점을 가진다. 그렇지만 원본에 대한 훼손, 조작 등은 불가능한데 이는 논문과 심사의 해시값을 블록체인 네트워크가 가지고 있기 때문이다. 마지막으로, 컨트랙트 결함이 중간에 발생할 시 지금까지 게재된 논문의 처리 방법이다. 이 경우, 다수의 심사자에 의해 심사되고 다수의 네트워크 참여자에 의해 그 심사가 인정받아왔다면 게재된 논문을 인정할 수 있을 것이다. 다수의 합의 행위가 이미 이루어졌다고 보이기 때문이다.

Ⅳ. 구 현

제안하는 시스템은 웹과 이더리움 네트워크를 연동하여 구현하였다. 이더리움의 스마트 컨트랙트는 솔리디티 언어를 이용하여 작성하였으며 웹페이지와의 연동을 위해 web3 인터페이스를 사용하였다.

4.1. 스마트 컨트랙트

본 절에서는 위에서 제시한 논문 심사 평가 시스템을 솔리디티 언어를 사용해 표 1과 같이 구현한다.

Table. 1 Implementation of open peer review system using Ethereum smart contract

```
pragma solidity ^0.5.2
contract PaperEvaluation{
  address owner;
  address [] public evaluator;
  uint [] public evaluatorScore;
  address submitter;

  uint private key;
  string private storageAddress;
  mapping(uint => string) public storageDateHash;

  bool [] private  voteEval;
  bool makeItPublic;

  constructor(address [] memory eval, uint [] memory
evalScore, address submitterAddr, uint restoreKey) public {
    owner = msg.sender;
    submitter = submitterAddr;
    key = restoreKey;
    evaluator = eval;
    evaluatorScore = evalScore;
    //boolean has default value of false
  }
```

컨트랙트에 포함되는 정보로는 스마트 컨트랙트 배포자 주소, 심사원들의 주소, 심사원들의 연구자 점수, 논문 제출자 주소, 복호화 키, 논문 및 심사평이 저장되어 있는 저장소의 주소, 심사원들의 논문 게재 여부 투표 결과, 게재 여부가 있다. 앞서 말한 각종 정보들은 스마트 컨트랙트가 배포될 시 생성자에 포함이 되어 블록체인에 기록이 된다. 저장되는 정보들 중에서 저장소의 주소는 암호화되어 기록이 될 것이며 이를 복호화 할 수 있는 키의 값은 기본적으로 공개되지 않는 변수로 선언이 되어 논문이 게재되거나 저자의 동의가 있기 전까지는 공개되지 않는다.

해당 스마트 컨트랙트에서 공개가 되는 내용은 할당된 논문을 평가하기 위해 참여한 심사위원들의 주소 값과 인원수, 저자의 주소, 해당 논문의 게재 여부 그리고 저장소에 대한 무결성을 보장하기 위한 해시 값이 될 것이다. 저장소에 대한 해시 값은 논문이 수정이 되었을 때 해당 날짜와 함께 변화된 해시 값을 업데이트해 저장한다. 코드와 시연 영상은 [11,12]에서 확인할 수 있다.

Ⅴ. 결 론

본 논문에서는 기존의 폐쇄적인 논문 심사 시스템에서 발생할 수 있는 문제점을 알아보고 이를 해결할 시스템을 제안하였다. 현존하는 문제점에 대한 해결책으로 공개 심사 제도가 제안되었지만 이러한 제도 또한 한계점을 가짐을 확인하였다. 이를 해결하기 위해 투명하면서도 공개 심사 제도의 한계점을 해결할 수 있는 블록체인 기반 공개 논문 시스템을 제안하였다. 제안한 시스템에서는 기존에는 저장되어 다루지 않았던 심사 과정을 데이터화를 제안함으로써 심사를 검증할 근간을 만들었다. 또한 블록체인에 데이터를 올림으로써 심사 데이터에 대한 무결성과 투명성을 확보하는 방법을 제시하였다. 이 때 블록체인의 용량 문제를 해결하기 위해 데이터 저장소를 따로 사용하는 방법을 제시하였으며 또한 무결성을 보장하기 위해 해시 결과를 저장하는 방식을 택하였다. 또한 본 논문에서 제안하는 시스템에서는 블록에 저장되는 내용은 삭제가 불가능하며 다수의 참여자에게 복제되기 때문에 게재불가 판정을 받더라도 연구 결과를 숨길 수 없게 된다. 이를 위해 주소를 암호화하여 저장하고 이를 필요에 따라 분배함으로써 연구 결과를 표절로부터 안전하게 지킴과 동시에 투명한 논문 검증이 가능하게 하였다. 마지막으로 적절한 심사자를 찾기 위해 기존에 존재하는 익명화 기법을 도입함으로써 신원을 보호하였다. 공개된 네트워크에서 누구나 심사위원을 지원할 수 있게 하여 다수의 심사자를 확보할 수 있었고 심사자격에 대한 검증으로 기존에 널리 사용되던 연구자 평가 지표인 논문 게재 수, 논문 인용 수에 제안하는 시스템에서 참여한 심사에 대한 평가를 더한 연구자 점수를 이용하였고 이를 통해 심사 참여에 대한 동기와 양질의 심사 평가를 기대할 수 있게 구성하였다. 제안하는 시스템에서는 심사 시스템에서 발생할 수 있는 법률적 문제를 기술적으로 다룰 수 있을 것으로 기대되며 다양한 익명성 보장 기법을 활용하여 개인정보 보호를 완성할 수 있을 것이다.

ACKNOWLEDGEMENT

This research was partly supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2014-1-00743) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation) and this research was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1 C1B5075742).

References

[1] C. Ferguson, A. Marcus, and I. Oransky. “The peer-review scam,” *Nature,* vol. 515, no. 7528, pp. 480-482, Nov. 2014.

[2] M. Helmer, M. Schottdorf, A. Neef, and D. Battaglia, “Research: Gender bias in scholarly peer review,” *Elife*, vol. 6, pp. e21718, Mar. 2017.

[3] C. J. Lee, C. R. Sugimoto, G. Zhang, and B. Cronin, “Bias in peer review,” *Jounal of the American Society for Information Science and Technology*, vol. 64, no. 1 , pp. 2-17, Jan. 2013.

[4] R. Smith, “Peer review: A flawed process at the heart of science and journals,” *Journal of the Royal Society of Medicine*, vol. 99, no. 4, pp. 178-182, Apr. 2006.

[5] S. V. Rooyen, F. Godlee, S. Evans, N. Black, and R. Smith, “Effect of open peer review on quality of reviews and on reviewers’ recommendations: a randomised trial,” *BMJ*, vol. 318, pp. 23-27, Jan. 1999.

[6] Nature. Perspective: The pros and cons of open peer review [Internet]. Available: http://blogs.nature.com/peer-to-peer/2006/06/perspective_the_pros_and_cons.html.

[7] Y. Guo, and C. Liang, “Blockchain application and outlook in the banking industry,” *Financial Innovation*, vol. 2(1), pp. 24-36, Dec. 2016.

[8] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in *Proceeding of IEEE Symposium on Security and Privacy (SP)*, pp. 839-858, May. 2016.

[9] S. Tikhomirov, “Ethereum: state of knowledge and research

perspectives," *Springer Nature 2018*, vol. 10723, pp. 206-221, Feb. 2018.
[10] Ministry of Science and ICT, Status of Science and Technology Papers(NSI) [Internet]. Available: http://index.go.kr/potal/stts/idxMain/selectPoSttsIdxMainPrint.do?idx_cd=1334&board_cd=INDX_001.
[11] Github. CCTV implementation code [Internet]. Available: https://github.com/DragonBeen/OpenPeerReview.
[12] Youtube. Demonstration CCTV cooperation authentication model using Ethereum platform[Internet]. Available: https://youtu.be/2YbanK0j1Zk

권용빈(Yong-been Kwon)

2018년 2월: 한성대학교 정보시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, 암호구현

장경배(Kyoung-bae Jang)

2019년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2019년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, 양자암호

최승주 (Seung-ju Choi)

2019년 2월: 한성대학교 영어영문학과 학사
2019년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야 : 블록체인, IoT

서화정(Hwa-jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야 : 정보보호, 암호화 구현, IoT