Journal of The Korea Society of Computer and Information
Vol. 24 No. 5, pp. 73-80, May 2019
www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.05.073

A Study on the PSP-Platform for the Atomicity of Distributed Ledger

Eun-Hee Lee*, Yong-Ik Yoon*

Abstract

In Korea, a budget of tens of trillion won is put into the national R & D project every year. Thanks to these efforts, Korea's ICT industry is gaining global attention. However, there are still a lot of problems that are lacking in terms of the cycle of managing national ICT R&D projects. In particular, the issue of sharing is very insufficient throughout the cycle of the national ICT R&D. In this paper, In this paper, We propose a platfom that can be shared throughout the cycle of managing blockchain-based national ICT R&D projects. This platform we call the Perfect Sharing Project Platform (PSPP). We describe that PSPP can achieve excellent research results through information sharing of project process[1-2]. To support the perfect sharing, this platform uses a new notion of consensus algorithm, called POA (Proof of Atomicity). This platform is suitable for sharing information.

▸Keyword: Distributed system, PSP-Platform, sharing project information, sharing duplication project information, distributed ledger, consensus.

I. Introduction

우리나라는 매년 수십조 원의 예산을 국가 연구개발과제에 투자하고 있다. 이는 정보통신기술의 원천기술 확보뿐만 아니라 글로벌 시장에서 기술의 우위를 선점하기 위해서 지속적인 투자를 하고 있다[3-6]. 지속적인 ICT 기술과 산업발전에 힘입어 한국의 ICT 산업은 세계적인 주목을 받고 있다. 하지만 한국의 ICT R&D과제는 여러 부처 및 기관에서 수행하고 있어서 연구과제의 기획-평가-과제 관리-성과 관리 부분에서의 공유가 어려운 상황이다. 국가 ICT R&D과제의 공유 문제점을 해결하기 위해서 우리는 블록체인 기술 기반으로 공유플랫폼을 제안한다. 2016년 세계경제포럼(WEF)에 따르면 2025년까지 블록체인 기술이 세계 GDP의 10%를 차지할 것으로 예상한다[3-6].유엔미래보고서 2050과 세계 IT시장조사기구는 10대 유망 기술에 블록체인 기술이 계속 포함되고 있다. 블록체인 시장은 현재 4배 수준으로 2021년까지 연평균 83% 성장할 것으로 전망된다[7-9]. 블록체인 기술은 비트코인 등 금융서비스에 초점을 맞췄지만 점차 다양한 서비스로 확대되고 있다. 본 논문에서는, 국가 R&D과제 관리에 블록체인 기술을 적용하여 국가 R&D과제 결과물의 불충분한 공유, 일부 중복된 과제 기획 및 연구결과물의 제출 등에 관한 문제를 해결하고자 한다. 국가 R&D과제 정보 공유로, 우리는 더 나은 국가 R&D과제를 제안할 수 있을 뿐만 아니라 연구 결과물의 중복도 방지 할 수 있다. 본 연구는 데이터 개방성, 보안성, 안정성, 효율성의 특성을 바탕으로 국가 R&D 과제의 정보공유에 블록체인 기술을 활용하는 것을 목표로 한다. 우리는 PSPP (Perfect Sharing Project Platform)라는 플랫폼을 제안한다. 국가 R&D과제의 완벽한 공유를 지원하기 위해, PSP-플랫폼은 블록체인 기술의 중요한 요소인 합의알고리즘을 제안한다. 본 논문에서 제안하는 합의알고리즘은 원자성증명(POA)방법이라고 불리며, 새로운 개념의 합의 알고리즘을 사용한다. 원자성증명(POA)알고리즘은 분산시스템인 점을 감안 할 때 각 노드에 동일한 정보를

• First Author: Eun-Hee Lee, Corresponding Author: Yong-Ik Yoon
*Eun-Hee Lee (eunhee@iitp.kr), School of IT Engineering, Sookmyung Women's University
*Yong-Ik Yoon (yiyoon@sm.ac.kr), School of IT Engineering, Sookmyung Women's University
• Received: 2019. 04. 19, Revised: 2019. 05. 20, Accepted: 2019. 05. 20.
• This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(2018R1D1A1B07047112).

저장할 수 있어야 하는데 일부 노드에서는 블록을 동일하게 복제하지 못하거나 불필요한 블록이 복제되는 결함이 있을 수 있다. 이러한 문제를 해결하기 위해 원자성 증명(POA)알고리즘에서는 모든 참여자가 블록 생성에 찬성하는 블록만 블록 생성이 가능하다.

본 논문의 2장에서는 블록체인 관련 연구 동향 및 합의 알고리즘에 대한 전반적인 내용을 간략하게 소개하고, 3장에서 우리가 제안하는 플랫폼에 대한 특징을 소개한다. 또한 우리가 제안하는 합의알고리즘에 대한 소개와 기존 합의알고리즘과 장단점을 비교한다. 4장에서 우리는 제안한 합의알고리즘과 기존 합의알고리즘에 대한 성능 분석과 추후 연구방향에 대한 결론을 내린다.

II. RELATED WORKS

1. Blockchain Technology Trllends

블록체인(Blockchain)은 '블록(block)'과 '체인(chain)'을 결합해 만든 단어이다. 블록은 데이터를 나타내며 블록체인은 검증된 데이터의 연결이다. 블록체인은 이전블록까지의 정보를 가지는 체인이다[10-12]. 블록체인은 서비스 유형에 따라 다양한 정보를 가지고 있다. 즉 블록체인 기술은 중앙 관리 없이 P2P 네트워크를 통해 거래 기록 및 관리 권한을 분산시켜 데이터를 기록 및 관리한다. 블록체인 기술은 특정 기간 동안 생성된 모든 거래 정보를 기록하는 블록을 만들어 모든 회원에게 전송하고, 회원에 의해 검증되면 기존 블록체인에 연결함으로써 블록체인을 구성한다. 이 과정에서 모든 노드는 거래 정보를 기록하는 동일한 분산 원장을 가지고 있으며, 블록체인은 참가자 합의에 의해 동일하게 업데이트된다. 합의에 참여하는 모든 참가자가 데이터의 적합성을 판단하고 이에 동의해야 한다. 이 과정은 각 노드들이 분산된 원장을 공유하고 이를 관리하기 위해 합의알고리즘을 사용한다. 대표적인 합의알고리즘은 POW(Proof of Work)이며, 최근에는 POW의 단점을 보완한 합의알고리즘인 POS(Proof of Stake), DPOS(Delegated Proof of Stake)와 PBFT (Practical Byzantine Fault Tolerance)가 대표적인 합의알고리즘으로 사용되고 있다. 합의알고리즘은 블록체인 기술의 매우 중요한 요소 중의 하나이므로 본 논문에서는 다양한 방법의 합의알고리즘에 대해 연구한다.

1.1 POW(Proof of Work)

POW(Proof of Work)은 나카모토 사토시의 논문에서 처음 도입되었으며, 주로 비트코인과 같은 암호화폐에서 사용되고 있는 합의알고리즘이다[13]. Public 블록체인에서 널리 이용되므로 에너지 소비 측면에서 많은 손실이 우려된다[14]. 블록을 생성하기 위해서는 채굴(mining)이라는 과정을 걸쳐야 하는데, 이는 특정 값(Nonce)을 찾기 위한 과정이다. 네트워크의 노드는 다음 블록을 생성하기 위해 블록 A 또는 블록 B를 선택해야한다. 비트코인에서는 블록(B)의 해시 값을 다음과 같이 정의한다.

$$Hash(B) \leq M/D \qquad (1)$$

수식(1)에서, D는 난이도가 되며, [1,M]의 범위에 속한다. M은 D의 최대 값(2^{256}-1)이며, 조건을 만족시키는 블록 B의 해시 값을 반복적으로 수행하여 해시 값을 얻는다. 성공적으로 해시 값을 얻은 참여자(Miner)는 전제 블록체인 노드에 얻은 값을 알리고 블록체인의 마지막 블록에 블록체인을 연결하여 새로운 블록체인을 완성한다. 블록체인기술의 장점 중 하나가 위변조를 방지 할 수 있다는 점이다. 블록체인에서 위조를 시도하려면 위의 과정을 반복 수행해야하기 때문에 위조를 방지 할 수 있다. 즉 위조를 시행하고 있는 중에도 블록은 계속 생성되고 생성된 블록은 계속 블록체인으로 연결이 가능하므로 위변조가 사실상 불가능한 기술이다.

1.2 POS(Proof of Stake)

POS(Proof of Stake)는 POW의 단점을 보완하여 제안된 합의알고리즘이다. POW 방법은 정보 독점 및 거래 누락과 같은 문제의 독점력이 50% 이상인 참여자에 의해 유발 될 수 있다. 이러한 문제점을 보완하기 위해서 블록을 생성하는 참가자의 지분과 생성된 시간을 통해 새로운 블록(정보)의 생성에 영향을 주는 POS방법이 제안되었다. POS(Proof of Stake) 방법은 다음과 같이 정의한다[15].

$$Hash(hash(Bprev),A,t) \leq bal(A)M/D \qquad (2)$$

수식(2)에서, Bprev는 이전 블록, A는 주소, t는 타임 스탬프 그리고 bal(A)는 현재 소유 된 지분이다. D는 난이도이고 M은 D의 최대 값이다. 블록 B의 해시 값은 A가 소유한 지분과 난이도에 영향을 받는다. POS 방법은 블록 생성 주기를 단축할 수 있다. 따라서 소유한 지분이 많은 참여자 일수록 블록 생성이 쉬워진다. 그러나 참여자의 지분 금액이 클수록 블록 생성이 쉬워짐에 따라 초기 지분을 배분할 때 공정성 문제가 발생 할 수 있다.

1.3 DPOS(Delegated Proof of Stake)

DPOS(Delegated Proof of Stake)방식은 POS방식의 단점인 지분의 불공정 배분 방식을 보완하기 위해 특정인원에게만 블록을 생성하고 증명 할 수 있도록 권한을 위임하는 것이다[16]. POS방식의 경우 일정 지분을 소유한 모든 노드에게 블록 생성 및 증명 권한이 주어지므로 많은 시간이 소요된다. 하지만 DPOS방식의 경우, 투표결과에 따라 블록을 생성하고 증명하는 노드를 결정하므로 비교적 적은 노드로 인해 합의 시간 및 비용을 줄일 수 있다. 그리고 투표한 노드는 직접 블록을 생성하는 대신 자신의 지분을 선출된 대표자에게 위임 할 수 있으며, 위임 받은 노드들은 선출한 노드 대신 블록을 생성/증명

할 수 있다. DPOS알고리즘의 블록 생성/검증자 수는 해당 체인의 합의 규칙에 따라 달라 질 수 있다.

예를 들어, N개의 블록 생성자들이 있을 때 DPOS 블록체인은 다음과 같은 순서로 진행된다.

1. N개의 블록 생산자들이 블록 생산자 후보군에서 선출되어야 하며 선출되는 대표자 노드는 아래 식 (3)을 만족하여야 한다. 식(3)에서 $n(VoterA)$는 노드 A를 대표자로 선출한 사용자 수, $n(Voterall)$은 투표에 참여한 사용자의 수를 의미한다[5].

$$n(VoterA) > \frac{n(Voter\,all)}{2} \qquad (3)$$

2. I번째 블록 생성/검증 대표자가 I번째 블록을 서명(I=N이 될 때 까지), 이때 블록생산자의 (2/3+ 1)이상이 투표하면 블록이 확정되어 생성된다.

만약 선출된 대표자가 악의적으로 블록을 생성하면 다음번 투표에서는 해당 블록 생성자에게 투표하지 않게 되므로 자연스럽게 블록 생성자에서 배제 할 수 있다. 그리고 블록생산자 수가 제한되어 있기 때문에 DPOS는 POW와 POS보다 큰 규모의 트랜잭션을 처리 할 수 있다는 장점이 있다. 하지만 대표노드만 블록생성에 참여하기 때문에 진정한 탈중앙화 시스템인지 여부는 논란이 되고 있다. 또한 블록의 수가 적더라도 대표노드로 뽑힐 수 있는 점과 보안에 취한하다는 단점이 있다.

1.4 PBFT(Practical Byzantine Fault Tolerance)

PBFT는 악의적인 노드가 존재하여도 성공적으로 합의 할 수 있는 알고리즘이다. PBFT는 속도 및 보안성은 매우 뛰어나지만, 확장성이 매우 떨어지는 단점이 있다. 비잔틴 장애를 허용하는 합의알고리즘 중 처음으로 높은 수행능력을 보여준 알고리즘으로, 대표자 선정 및 투표(메시지 교환) 과정으로 합의가 이루어진다[17]. PBFT는 투표를 기반으로 하는 합의알고리즘의 기초로 많이 활용된다. 인터넷, 블록체인과 같은 네트워크는 보통 비동기식 네트워크를 사용한다. 비동기식 네트워크의 경우 노드간 합의가 이루어졌다면 어떤 노드에 접근하든 그 값은 동일해야 하다는 의미의 Safety와 블록체인에서 블록의 합의에 문제가 없다면 네트워크 내에서 분명 합의가 이루어진다는 의미의 Liveness를 모두 완벽히 만족하는 합의알고리즘을 설계하는 것이 불가능하다[17]. 비동기 네트워크에서는 어떤 한 노드에서 문제가 발생했을 경우 그 노드에서 합의가 됐는데 단순히 응답에 오랜 시간이 걸리는 건지, 아니면 합의 과정에서 충돌이 발생해서 응답하지 않는 건지 알 수 없기 때문이다. 비동기 네트워크에서 배신자 노드가 f개 있을 때, 총 노드 개수가 3f+ 1개 이상이면 해당 네트워크에서 이루어지는 합의는 신뢰 할 수 있다는 것을 수학적으로 증명한 알고리즘이다[3]. 합의를 이루어 블록이 블록체인에 생성되었다면, 어느 노드에서 블록체인의 특정 블록을 검색하면 동일한 결과를 얻을 수 있다. 하지만 네트워크 합의 요건을 충족하지 못한 request는 생성되지 못하기 때문에 Liveness가 다소 부족하다. PBFT는 전체 노드 중 66%를 초과한 노드가 정직하다면 합의 할 수 있다. 그와 반대로, 전체 노드 중 66%를 초과한 노드가 거짓말을 하는 경우에도 합의가 이루어지므로, 이에 대한 보완이 필요하다.

2. National R&D Project management Process

우수한 국가 R&D 과제를 발굴하기 위해 기술 동향 분석 및 미래 ICT기술 개발에 대한 계획을 수립해야한다. ICT 기술 분석을 위해 필요한 기술 키워드를 도출하여 기획을 위한 기술을 분류한다. 기술 키워드 도출을 통해 필요한 기술에 대한 수요를 분석한다. 그리고 도출된 기술에 관심 있는 사람들을 위해 기술수요조사를 실시한다. 기술수요조사는 전담기관 홈페이지 및 관련 부처의 홈페이지를 통해 30일 이상 실시한다[15-17]. 이 시기에 관심 있는 기술에 대해 수요를 제기 할 수 있으며, 제기한 수요기술은 전문가들에 의해 과제로 기획 할 수 있다. 이 시기에 기획위원회(과제 기획 전문가 그룹)는 기술 수요조사서 및 기술 분석 보고서를 검토하여 필요한 기술에 대해 기획을 실시한다. 기획위원회는 제출된 기술수요조사서를 기반으로 RFP(Requset for Proposal)를 작성한다. 기획위원회는 당해 연도 예산을 고려하여 *기획될 과제의 수를 기획한다.* 이때 기획위원회는 기획될 과제보다 3배 이상 많이 RFP를 작성한다. 기획위원회에서 작성된 RFP는 전문가 그룹의 검토를 통해 실제로 기획될 과제 수의 1.5배만이 실제 기획과제로 선정된다. 기획 단계 전반에 걸쳐 공유 절차는 이루어지지 않고 있다. 단지 기획과정에 참여하는 전문가만이 기획 과정을 공유한다. 기획과정에서 공유가 전혀 이루어지지 않기 때문에 중복 기획, 우수하지 않은 기술의 기획 등 문제점이 발생 할 수 있다. 우리는 지금부터 평가-관리-성과에 대한 프로세스를 기술한다. 기획된 과제에 대해 전담기관 및 관련 부처 홈페이지 등을 통해 과제에 관심 있는 사람들을 대상으로 30일 이상 공고를 실시한다. 이 과제에 관심이 있는 연구자들은 RFP를 작성하여 전담 기관에 제출해야 한다. 전담기관은 제출된 RFP를 접수하고, 최고의 과제를 선정하기 위한 평가를 실시한다. 이 평가를 우리는 선정평가라고 한다. 선정평가에서 선정된 과제는 국가연구개발사업으로서 관리한다. 국가 R&D 과제는 평가 이력, 과제 정보 변경, 진행 상황 점검 등의 프로세스를 통해 관리한다. 이 과정에서 생성된 정보는 과제관리의 정보로 사용된다. 연구 과제의 결과물로서, 논문, 특허, 기술 이전 수, 상용화 수, 사업화 매출액 등을 주로 관리한다. 이러한 결과는 연구 성과로서 등록, 검증 및 관리한다. 공유 문제는 R&D과제의 전주기 프로세스 동안 문제로서 제기됐지만 이에 대한 대안은 제대로 없는 실정이다.

III. The Proposed Platform

1. PSP(Perfect Sharing Project) Platform

본 논문에서 제안하는 플랫폼인 PSP(Perfect Sharing Project) 플랫폼은 국가 ICT R&D 과제 프로세스, 즉 기획-평가-과제 관리-연구성과 관리에 대한 과제 정보로서 공유를 보장하기 위해 제안한다. 일반적으로 블록체인기술은 거래 위변조를 원칙적으로 막을 수 있는 기술이다. 또한 블록 생성 및 검증에 대한 국가 ICT R&D 과제의 과정도 제공한다. 그러나 과제 관련 정보를 제공하는 단계에서는 사용자마다 차별화 할 수 있는 권한을 부여한다. 사용자는 주어진 권한을 통해 원하는 정보를 얻는다. 아래 그림 1에서 보듯이 사용자는 PSP-플랫폼을 통해서 과제 정보를 얻을 수 있다[1].

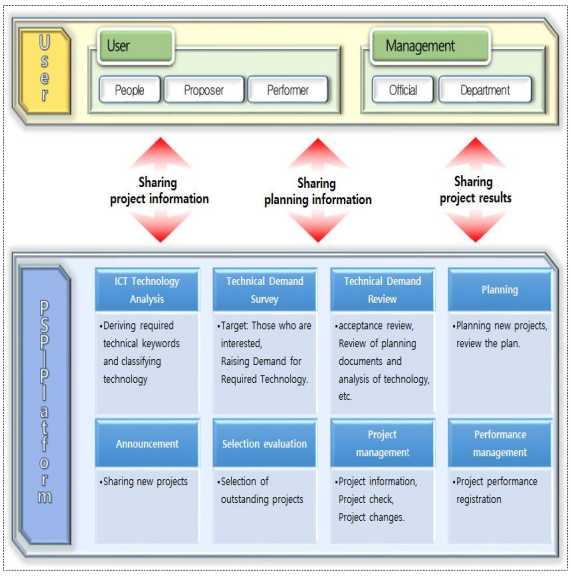

Fig. 1. Proposed PSP-Platform

사용자는 크게 사용자와 관리자 두 단계로 나뉜다. 사용자는 크게 3단계로 분류되는데 이는 일반사용자, 과제 제안자 및 과제 수행자로 분류한다. 일반사용자들은 PSP-플랫폼의 과제정보 요약서를 간단히 읽을 수 있다. 제안자는 과제 정보 대부분을 읽을 수 있고 검토 할 수 있다. 만약 제안자에 의해 과제 및 연구 결과물의 중복성이 의심 될 때에 제안자가 블록 생성을 제안 할 수 있다. 그리고 제안자는 PSP-플랫폼의 과제 정보에 근거해, 새로운 과제를 제안할 수 있다. 즉 제안자는 과거에 수행한 적이 있는 과제정보를 확인 할 수 있으므로 중복으로 과제를 제안하는 문제점을 방지 할 수 있다. 수행자는 과제 정보와 관련된 읽기 및 쓰기를 할 수 있지만 거의 모든 과제 정보에 대해서 읽기만 가능하다. 수행자는 블록을 생성 할 수 있다. 수행자는 과제에 대한 책임을 가지고 있다. 우리는 블록체인 기반의 PSP-플랫폼을 통해 국가 연구개발 과제에 관한 정보를 사용자에게 공유할 수 있다. 관리자는 과제 진행 정보를 공유하기 위해 과제정보를 PSP-플랫폼에 등록한다. 표1은 국가 ICT R&D 과제의 전주기 프로세스를 8단계로 설명한다[18].

Table 1. ICT R&D Process

Process	Subject and content
ICT Technology Analysis	o department : As a stage of planning, Keywords for required technologies and classifications of technologies.
Technical Demand Survey	o The department is based on derived keywords. Conducting a survey on the demand for technology needed. o User : Submit a demand survey
Technical Demand Review	o The department reviews and conducts technical analysis of demand survey proposals submitted by experts.
Planning	o The department plans new projects through a group of experts based on the reviewed technical demand survey and analyzed technologies.
Announcement	o The department informs the citizens of the project for more than 30 days
Selection evaluation	o The department selects excellent projects.
Project management	o The department staff manages projects such as basic information on project, checking projects and changing project.
Performance management	o The department perform performance registration and management of projects.

표 2는 사용자별 정보 제공의 범위와 정보 조회의 내용을 기술한다. 각 서비스대상 자별 정보를 열람 할 수 있는 범위와 정보를 입력 할 수 있는 범위가 제시되었다.

Table 2. Service Content

Service subject	Service Content
User	o Only the basic information of the project can be viewed. o However, information can not be input.
Proposer	o From the evaluation stage, information on project management and research achievement management can be inquired. o However, information can not be input.
Performer	o From the evaluation stage, information on project management and research achievement management can be inquired. o Information input evaluation - project management - research achievement stage is possible.
Department	o From the planning stage to the research achievement management stage, information can be inquired. o However, there is no information input authority.
Manager	o From the planning stage to the research achievement management stage, information can be inquired. o Information input evaluation - project management - research achievement stage is possible.

과제 정보 공유를 위해, 표 3에 나타낸 것과 같이 Ledger정보를 구성한다[19-21]. Ledger의 내용은 사용자의 권한에 따라 다르게 구성된다.

Table 3. Contents of Ledger

User	content
Performer	o Enter project change history((Name of project, name of project leader, name of affiliation, affiliation information, project change content) o Enter information when duplicate projects are found(Name of project and plan, name of project leader, name of affiliation, affiliation information, project duplicate content)
Departme nt	o Block creation (Name of project, name of project leader, name of affiliation, block information) o The contents of the project and the duplication of the research result (tName of project, name of project leader, name of affiliation, summary of duplication project)
manager	o Block creation (Name of project, name of project leader, name of affiliation, block information) o The contents of the project and the duplication of the research result (tName of project, name of project leader, name of affiliation, summary of duplication project)

2. PoA(Proof of Atomicity)

블록체인 시스템의 성능에 영향을 미치는 요소 중 하나는 합의알고리즘이다. 합의알고리즘을 통해 새로운 노드가 생성되고 많은 노드가 동일한 정보를 가질 수 있다. 하지만 합의에 공정성을 부여하기 위해 많은 노드가 합의에 참여하게 되면 성능 측면에서 많은 에너지 소비가 발생 할 수 있다. 최근에는 이러한 측면을 보완하기 위해 POS, DPOS 등 다양한 합의알고리즘이 개발되고 있다. 하지만 이러한 알고리즘 중에 완벽한 알고리즘은 없으며 앞에서 설명했듯이 각각의 취약점을 보완하기 위해 본 논문에서는 공정성 문제도 손상하지 않고 과도한 에너지 사용의 문제점을 보완하기 위해서 POA 알고리즘을 제안한다. Satoshi Nakamoto에 의해 제안 된 PoW 합의알고리즘은 새로운 블록을 생성하고자 할 때 블록 검증자의 51%가 동의한다면, 블록을 생성 할 수 있다[22]. 하지만 국가 연구개발 과제의 기획, 평가 및 관리의 전주기 프로세스에서 51%의 참여자만이 찬성하여 과제 정보를 변경하는 것은 잘못된 정보 공유로 큰 피해가 발생 할 수 있는 우려가 있다. 공용 블록체인 방법은 모든 사람에게 정보를 공유하는 측면에서 탈중앙화 측면에서 좋은 방법이다. 그러나 신뢰성 있는 정보의 생성 및 공유 측면에서 공용 블록체인(Public blockchain)과 개인 블록체인(Private blockchain)을 보완해야 한다. 따라서, 우리는 PoA(Proof of atomicity) 알고리즘을 제안한다. PoA 알고리즘은 블록을 생성할 수 있는 많은 관리자가 100% 동의를 해야만 블록을 생성할 수 있다. 생성된 블록은 참여자 모두에게 동일한 정보를 제공 할 수 있다. 예를 들어, 새로운 과제 정보가 악의적 의도에 의해 과제 정보가 변경 혹은 생성되면 국가 R&D 과제의 기획 단계에서부터 중복된 과제 기획으로 과제 생성 단계에서 부터 문제가 발생한다. 이러한 문제가 발생하는 것을 사전에 방지하기 위해 블록을 생성하는 참여자가 100% 동의하고 신뢰할 수 있는 정보를 생성해야한다. 그리고 PoA 알고리즘은 원자성과 일관성을 특징으로 한다. PoA 알고리즘의 원자성 및 일관성 기능은 신뢰성을 높일 수 있다.

- 원자성 : 참여자의 100%가 합의 해야만 블록이 생성된다. 하지만 합의가 중간에 실현되지 못하면 블록은 삭제됨.
- 일관성 : 합의가 성공하면 거래 정보가 업데이트 된다. 이 정보는 어느 노드에서나 동일한 정보를 제공함

PoA 알고리즘의 순서는 그림 2와 같이 실행된다[1].

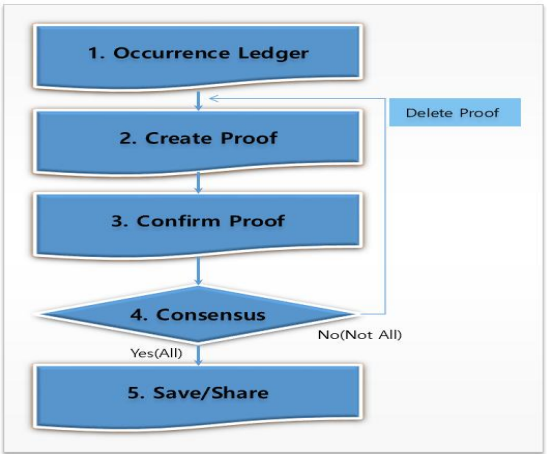

Fig. 2. Proposed PoA(Proof of Atomicity) Algorithm

PoA알고리즘의 상세 알고리즘은 아래와 같다.

1. Proof 요청

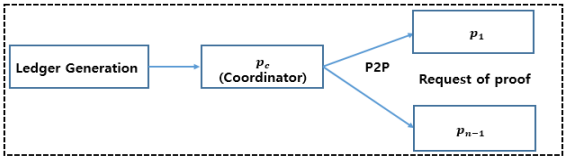

Fig. 3. Proof Request Process

PSP-플랫폼은 과제 관리 전주기에 대한 정보를 공유하고 과제 관리 프로세스를 진행한다. 이 과정에서 R&D과제에 대한 정보를 갱신하거나 과제 및 연구결과물에 대해 중복성이 제기되는 경우가 생긴다. 이럴 경우 PSP-플랫폼에 접근 허락을 받은 사용자는 관련 정보의 업데이트에 대해 Ledger 발생을 요청 할 수 있다. Ledger 발생에 대한 요청이 접수되면 중복성 발생 및 해당 과제의 담당자가 중재자(coordinator) 역할을 한다. 중재자는 Ledger검증의 권한이 있는 참여자로서 전체 N명 중에 한명이다. Ledger의 검증을 위해 Ledger 생성 권한이 있는 관리자들에게 동시에 전송한다.

2. 합의 요청

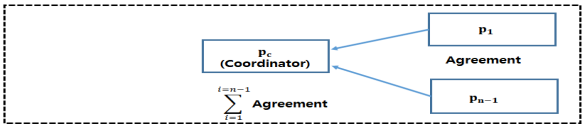

Fig. 4. Consensus Request Process

PSP-플랫폼에 접속한 관리자들은 중재자로부터 받은 Ledger에 대해 합의를 진행한다. 이 과정에서 관리자 전원인 N명이 합의에 참석을 해야 한다. N명이 블록 생성을 검증하게 된다.

3. 합의 과정

3-1. If All

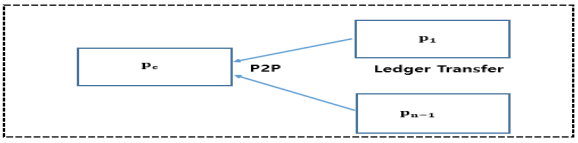

Fig. 5. Consensus Process(If All)

합의에 참석한 관리자 전원이 Ledger발생에 100% 찬성한다면, Ledger는 생성이 가능한 상태로 된다. 이때 Ledger 생성에 합의한 상태로 상태가 변화하며 상태메시지를 중재자와 관리자에게 전송한다. 이는 Ledger의 검증이 가능한 상태가 된다.

3-1-1. Confirm Proof

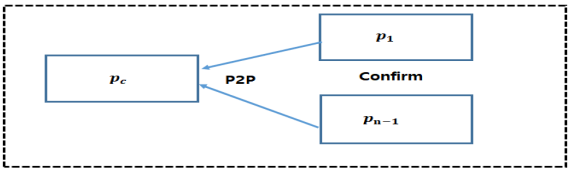

Fig. 6. Confirm Proof Process

Ledger는 생성이 확정된 상태의 Ledger을 참여자 전원이 검증하여 블록으로서 생성 될 준비를 하게 된다. 이 단계에서 Ledger는 블록으로서 검증이 완료된다.

3-2. If !All

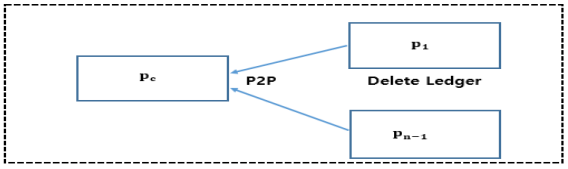

Fig. 7. Consensus Process(If !All)

합의에 참석한 관리자 중 1명이라도 Ledger발생에 찬성 하지 않으면 Ledger 생성에 실패한다. 즉 Ledger는 검증 단계로 전환되지 못하고 삭제된다. 이는 블록생성에 영향을 미치지 못하고 이전상태로 되돌아간다.

4. 블록 생성

합의에 성공한 Ledger는 블록으로서 블록체인에 연결되어 어느 노드에서 검색을 하더라고 동일한 정보가 제공된다. 이는 새로운 블록의 생성과 정보의 업데이트가 성공했음을 의미한다.

Ⅳ. Analysis

블록체인에서 탈중앙성(decentralization), 확장성(scalability), 보안성(security)을 동시에 만족시키는 것은 어렵다. 블록체인의 대표적인 합의알고리즘은 작업증명(POW), 지분증명(POS), 위임지분증명(DPOS) 및 실용적비잔틴합의(PBFT) 방법 등이 있으며 현재 존재하는 합의알고리즘은 트릴레마에 대한 문제를 해결하지 못하고 있다. 이에, 본 논문에서 제안한 합의알고리즘인 POA 알고리즘과 기존의 합의알고리즘인 작업증명(POW), 지분증명(POS), 위임지분증명(DPOS) 및 비잔틴합의(PBFT) 방법을 분석하기 위해서 탈중앙성, 확장성, 보안성 및 성능에 대해서 분석한다. 각 특징에 대해 아래 표1과 같이 분석내용을 정의하였다. 각 특징에 의거하여 합의알고리즘에 대해 분석하였다.

Table 4. Feature Description

Characteristics	Analysis Contents
Decentralization	Number of users participating in block creation
Extensibility	Transaction throughput per unit hour
	The time it takes the transaction to be processed
	Number of users participating in the block chain
Security	Attacking 51% of the data
	Disturbing behavior of malicious nodes
	An attack that creates a double payment by making a fork
	Attacks in which the same user creates multiple accounts and takes control of the system
	Attacks targeted at specific users
	Participants take profits by voting on multiple blocks
	Attacks on users
Performance (efficiency)	common consent to data
	the validity of the agreed results
	Arrive an agreement without a long wait
	Provide correct results for all requests
	Always provide results for all requests
	Agreements are reached in the event of a network failure

작업증명(POW)은 최초의 블록체인 합의 알고리즘으로서 참여자 전원이 자료에 대해 접근권한이 있으므로 탈중앙성이 뛰어나고 블록의 nonce값을 찾는 것이 어려우므로 보안성도

우수한 편이다. 그러나 연산 처리에 필요한 자원 및 에너지 소비 측면이 다소 부족한 편이다. 작업증명(POW)은 주로 Bitcoin, Ethereum 등에서 주로 사용하고 있다.

지분증명(POS) 방법은 작업증명(POW) 방법의 문제점을 극복하기 위한 대안으로 등장했다. 지분증명(POS)은 지분 보유량에 근거하여 블록 생성 및 검증 권한을 부여 한다. 특히 지분증명(POS) 방법 역시 지분을 소유한 참여자 전원이 블록을 생성하고 검증하는 것이 가능하므로 탈중앙성이 뛰어나고 해쉬트리에서 블록의 nonce를 찾는 것이 어려우므로 보안성 역시 높은 편이다. 블록 생성에 지분을 보유한 참여자만 참여가 가능하고 트랜잭션 처리 속도가 다소 부족하여 확장성이 낮다. 지분증명(POS) 방법은 주로 Ethereum Casper, Peercoin 등에 사용되고 있다.

위임지분증명(DPOS) 방법은 블록 생성의 권한을 가진 사람이 위임 받은 일부 사용자이므로 지분증명(POS) 방법의 성능을 개선한 방법이다. 위임지분증명(DPOS)은 투표에 의해 선출된 참여자만 참여하므로 확정성이 뛰어나지만 탈중앙성과 보안성이 부족한 편이다. 그리고 악의가 있는 참여자의 담합 혹은 악의적인 의도에 의해 블록체인의 신뢰성이 저하되는 측면이 있을 수 있다. 이는 블록 생성 및 검증에 참여하는 참여자의 숫자가 적어서 나타는 문제점이다. 위임지분증명(DPOS) 방법은 주로 EOS, Tendermint, Steemit 등에 주로 사용되고 있다.

실용적비잔틴합의(PBFT) 방법은 참여자들간의 정보교환을 통해 합의된 블록을 생성하는 BFT 알고리즘에 메시지 교환 트래픽의 발생 문제를 개선한 방법이다. 실용적비잔틴합의(PBFT) 방법은 비동기식 네트워크에서 사용이 가능하다는 강점을 가지고 있다. 그리고 접근 권한에 따라 블록 생성이 가능하므로 성능면에서도 아주 우수한 방법이다. 하지만 권한이 있는 참여자만이 참여하는 폐쇄된 환경에서 작동하므로 탈중앙성이 낮은 편이다. 또한 이해관계가 있는 소수의 참여자로만 구성되어 있으므로 내부 합의를 통해 모든 데이터를 변조할 수 있어 보안성 측면 또한 취약한 점이 있다. 실용적비잔틴합의(PBFT) 방법은 주로 Hyperledger Fabric, Ripple 등에 사용되었다.

원자성증명(PoA) 방법은 국가 R&D 과제의 공유를 위해 특화된 합의알고리즘이다. 원자성증명(PoA) 방법은 PSP-플랫폼에 있는 관리자들 전원이 블록 생성에 참여 할 수 있다. 블록 생성에 참여하는 관리자들 전원이 합의해야만 블록 생성이 가능하다. 한 명의 관리자라도 블록생성에 합의 하지 않으면 블록 생성은 이루어지지 않는다. 이는 악의적인 의도가 있는 참여자에 의해 잘못된 정보의 생성을 방지하는 좋은 방법이다. PSP-플랫폼은 사용자의 접근과 동시에 사용자 권한을 부여 받으므로 블록 생성을 위한 합의 이전에 사용자에 대한 정보를 파악하게 된다. 그리고 합의를 위해서는 합의에 필요한 정보만 파악하게 되므로 정보에 대한 처리 속도가 빠르다. 그리고 원자성증명(PoA) 방법은 플랫폼에서 권한을 받은 전원이 블록체인 구성에 참석한다. 원자성증명(PoA) 방법은 보안성 측면에서도 우수성을 보인다. 악의적 노드의 교란 행위, 분기(fork)를 만들어 이중지불을 발생시키는 공격, 동일 사용특정 사용자를 겨냥한 공격, 참여자가 여러 블록에 투표하여 이익을 취하는 행위 및 사용자들이 공모하는 공격은 블록 생성 시 100%가 찬성하여야만 블록 생성이 가능하므로 상기 공격에 대해서 해결이 가능하다.

동일 사용자가 다수의 계정을 만들어 시스템을 장악하는 공격은 PSP-플랫폼에 접근과 동시에 사용자를 인증하므로 다수의 계정을 소유하기가 어렵다. 원자성증명(PoA) 방법은 특히 보안성 측면에서 우수하다. 성능의 지표로 삼고 있는 데이터에 대한 공통된 동의, 동의된 결과의 유효성, 모든 요청에 대해 올바른 결과 제공 및 모든 요청에 대해 항상 결과 제공 사항들에 대해서는 블록 생성자들이 모두 동의하는 측면에서 가능하다. 하지만 PSP-플랫폼이 실시간 운용되는 시스템으로 구성되어 있지 않아서 긴 대기 없이 합의에 도달 하는 문제 및 네트워크 오류가 발생해도 합의에 도달하는 부분에 대해서는 100% 신뢰 할 수 없는 실정이다. 앞으로 이러한 부분을 충분히 고려하여 원자성증명(PoA) 방법을 지속적으로 보완 할 예정이다.

표4는 PoW, PoS, DPoS, PBFT와 본 논문에서 제안하는 PoA에 대해 분석한 결과이다. 표5에 의하면, 탈중앙성은 PoW, PoS 및 POA가 높은 편이다. 대표자를 선출하는 방식은 중앙집중 방법의 특징을 반영하고 있어 탈중앙성이 낮은 편이다. 보안성은 악의적 노드 교란 행위, 특정 사용자를 겨냥한 행위, 사용자들이 공모하는 공격 등 합의에 있어서 오류가 발생 할 수 있는 경우에 대해서는 보안성이 취약하다고 정의했다. 따라서 보안성은 PoW, PoS 및 POA가 높은 편이다. 확장성은 단위 시간당 트랜잭션 처리량 빠르고, 블록체인에 참여하는 사용자수가 적은 것 등이 확장성을 측정하는 항목이다. 이러한 요인을 배경으로 확장성은 DPoS 및 PBFT이 높으며 우리가 본 논문에서 제안한 POA가 가장 높다. 동의된 결과의 유효성, 모든 요청에 대해 올바른 결과 제공 및 항상 결과 제공 등에 대해서 측정하는 효율성은DPoS 및 PBFT이 높다.

Table 5. Comparison of the Consensus Algorithm

division	Decentralization	Security	Extensibility	Performance (efficiency)
PoW	high	very high	very low	very low
PoS	high	high	low	low
DPoS	low	low	high	very high
PBFT	low	low	high	very high
POA	high	very high	high	middle

Ⅴ. Conclusions

우리는 블록체인 기술을 기반으로 기획-평가-관리-연구과제 결과물을 공유하기 위해 PSP-플랫폼을 제안했다.

PSPP는 국가 ICT R&D 과제의 전주기에 걸쳐 정보를 공유하는 플랫폼으로서 특히 블록체인 기술의 이슈 사항인 합의 알고리즘을 새로이 제안한 플랫폼이다. 본 논문에서 제안한 원자성증명(POA) 방법은 합의알고리즘의 트릴레마에 대한 문제를 해결하고 합의알고리즘의 탈중앙화, 보안성 및 확장성 측면에서 우수한 성능을 보였다. 앞으로 PSPP에 대한 지속적인 연구를 통하여 과제 관리 플랫폼에 대한 효율성 측면을 보완하여 우수한 과제관리 공유플랫폼으로서 연구하고자 한다.

REFERENCES

[1] Eunhee Lee, Youngik Yoon, “Project Manageement Model based on consistency strategy for Blokcchain Platform”, SERA 2019.

[2] Byeowool kim, Youngik Yoon, “Journalism Model Based on Blockchain with sharing space” Symmetry 11, no 1:19

[3] Karen Fawcett, Jeff Tessler, Claudio Scardovi, Oliver Frischemeier and William Park ”Future of Financial Services in 2030”, Impact of Digitization. 2016.

[4] Don Tapscott and Alex Tapscott, “Blockchain Revolution,” Eulyoo Publishing Co., LTD., 2017.

[5] Hyeon Kwak, “Industrial Trend and Patent Trend of Blockchain Technology,” Korea Knowledge Industry Institute, 2017

[6] Je-young Lee, “Blockchain Technology Trend and Implications,” Science and Technology Policy Institute, 2017

[7] Global Blockchain Technology Market 2017-2021, Technavio, 2017

[8] DLP Piper ”THE BLOCKCHAIN REVOLUTION” Stanford University ,2017.1

[9] Global Blockchain Technology Market 2017-2021, Technavio, 2017

[10] Cellabz“Blcokchain&Beyond” 2015.11

[11] Deloitte “Blcokchain” 2016

[12] Melanie Swan “ Blockchain”, p27-31, 2015

[13] Jakobsson, Markus, and Ari Juels, “Proofs of work and bread pudding protocols.” in Secure Information Network, pp 258-282, septmber, 1999

[14] Choi Jong-seok, Park Jong-kyu, Kim Young-gil, Kim Ho-won, “ A Study on the Conformity of the Application of the Blockchain Agreement Algorithm”. journal of information science, pp 9-16, February. 2018.

[15] “Proof of stake versus Proof of work”, Bitfury Group Whitepaper, 2015.

[16] Daniel Larimer, “Delegated Proof-of-Stake (DPoS)”, Bitshare whitepaper, 2014.Group Whitepaper, 2015.

Authors

Eun-Hee Lee received the B.S and M.S. degrees in Electronic Engineering from Hongik University, Korea, in 2000 and 2002, respectively Eun-Hee Lee is currently a doctoral student at Sookmyung Women's University. She is interested in blockchain technology.

He is a Professor for Dept. of IT Engineering in SookMyung Women’s University, South Korea. He received M.S and Ph.d. degree from Computer Science of KAIST, in 1985 and 1994. He had researched for 15 years (1983~1997) like a member of senior Researcher of ETRI, in Korea. His Research Interests are intelligent service based on Io, Big Data, AI. For future life. he study the intelligent service platforms for the cyber physical system and blockchain system. He is now a Member of ACM, IEEE, KSCI, KIISE, and KIPS.