Journal of Knowledge Information Technology and Systems(JKITS), Vol. 15, No. 1, pp. 11-28, February 2020
https://doi.org/10.34163/jkits.2020.15.1.002

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Survey on Blockchain Technologies Applied to IoT – Focusing on Applied Environment, Consensus Algorithms, and Platforms

Mihui Kim*, Gihun Lee

Department of Computer Science and Engineering, Computer System Institute, Hankyong National University

ABSTRACT

IoT(Internet of Things) and blockchain technologies are at the core of the technologies that form the fourth industrial revolution. In this paper, we examine the researches incorporating blockchain technology for the IoT. It is predicted that the number of IoT devices explode, and the amount of data to be collected and managed would also be significant. Ensuring the security of the device or data generated from the device is a problem to be solved. The blockchain technology is considered as a solution to this problem, because it provides data safety such as decentralization of data management, non-forgery, and traceability. However, it is considered that the inefficiency of the calculation of the consensus algorithm used in existing electronic cryptocurrency management (e.g., Bitcoin) should be improved in order to be applied to the Internet of Things. In this paper, we analyze the characteristics of the blockchain technology applied for the IoT system by classifying recent research into an applied environment (i.e., home, hospital, company and government), consensus algorithm (i.e., Proof of Work, Proof of Stake, and so on), platform (i.e., Ethereum, Hyperledger), and effort for blockchain application. Through the recent research trend analysis, we show the applicability of blockchain technology for constructing the IoT, and suggest future research topics and issues to be resolved.

KEYWORDS: Internet of things, Blockchain technologies, Consensus algorithm, Research trends, Blockchain platforms

ARTICLE INFO: Received 27 November 2019, Revised 18 December 2019, Accepted 7 February 2020.

*Corresponding author is with the Department of Computer Science and Engineering, Hankyong National University 327 ChungAng-Ro, AnSeong-Si, Kyonggi-Do, 17579, KOREA.
E-mail address: mhkim@hknu.ac.kr

1. 서 론

최근 4차 산업혁명이라는 말이 급부상하고 있다. 4차 산업혁명이란 인공지능, 사물인터넷, 빅데이터, 모바일 등 첨단 정보통신기술이 경제·사회 전반에 융합되어 혁신적인 변화가 나타나는 차세대 산업혁명이다. 이러한 기술 중 상호 연계된 센서들이 데이터를 센싱하여 통신 모듈을 통해 전송되어 수집되고 데이터 분석 기술을 통해 인간에게 편리하고 유용한 서비스 제공할 사물인터넷은 그 현실화를 위해 기기 및 데이터의 안전성이 보장되어야 한다. 이를 위해 데이터 관리의 분산화, 위조불가능, 추적가능 등 데이터의 안전성 등을 제공하는 블록체인 기술의 적용 연구가 최근 활발히 진행되고 있다.

본 논문에서는 사물인터넷을 위해 적용된 블록체인 기술 연구에 대해 조사 분석하고자 한다. 특히 적용 환경(가정, 병원, 회사, 정부), 합의 알고리즘(작업증명, 지분증명, 그 외 알고리즘들), 플랫폼(이더리움, 하이퍼레저)으로 분류하여 그 특징을 분석한다. 이러한 분석을 통해 안전한 사물인터넷을 구성하고 관리하기 위해 블록체인의 적용 가능성을 살펴보고, 향후 연구 방향을 제언하고자 한다.

2장에서는 기반 연구로서 블록체인 기술을 소개하고, 사물인터넷과 이를 현실화하기 위해 해결해야할 이슈를 소개한다. 3장에서는 3가지 기준을 가지고 블록체인 기술이 사물인터넷에 적용되기 위한 연구들을 분류하여 그 특징을 분석한다. 4장에서 이러한 분석을 통해 도출한 앞으로의 연구 방향을 제언하고 5장에서 결론을 맺는다.

2. 기반 연구

본 장에서는 기반 연구로서 블록체인 기술에 대해 소개한다. 또한 사물인터넷 특징을 소개하고 사물인터넷의 현실화를 위해 해결해야 할 두 가지 이슈를 소개한다.

2.1 블록체인 기술

블록체인은 Peer-to-Peer(P2P) 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장환경을 제공하며 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술이다. 이 절에서는 블록체인 등장 배경, 블록체인의 사용목적, 블록체인의 작동원리, 블록체인 블록의 구조를 설명한다.

블록체인 기술은 2008년 사토미 나카모토에 의해 처음 제안되었다. 기존의 중앙은행 시스템과 달리 거래 장부의 분산을 통한 완벽한 탈중앙화된 시스템을 제안하였다. 거래 장부의 역할을 하는 블록은 주기적으로 만들어지며 이 블록을 순서대로 연결한 것을 블록체인이라 한다. 모든 사용자(참여자 또는 노드)가 거래 장부를 공유하기 때문에 누구라도 임의로 수정할 수 없는 안전성 덕분에 기존의 중앙은행 시스템을 대신할 수 있는 기술로 고려되고 있다.

블록체인 P2P 분산 네트워크 안에서는 모든 참여자가 거래 정보를 기록하여 저장하고, 각 블록은 참여자들의 검증과 동의를 거쳐 생성된다. 한번 생성된 거래블록은 분산저장 되기 때문에 위조가 불가능하여 중앙에서 관리하는 서버가 없이 안전하게 거래가 가능하게 된다. 따라서 현재 대부분의 시스템 구조인 중앙화를 벗어나 탈중앙화를 하면서 위조불가능과 안전성을 제공하는 것이 블록체인의 사용목적이다.

블록체인은 분산원장기술 (Distributed ledger technology)에 의해 동작한다. 모든 참여자는 자신의 주소를 가지고 있다. A와 B가 거래를 할 경우,

거래 내역을 작성하여 블록체인 네트워크에 전달한다. 네트워크는 모든 노드에게 트랜잭션을 전달한다. 각 노드는 받은 트랜잭션을 대기 목록에 모은다. 대기 중인 트랜잭션은 블록이라는 단위로 묶인 후 블록단위로 처리된다. 트랜잭션을 블록단위로 처리하기 위해서 해시퍼즐을 사용하는데, 이 해시퍼즐은 가능한 조합을 단순 반복하여 답을 찾아내는 문제이다. 이 문제를 가장 먼저 해결한 하나의 노드가 그 블록을 처리하여 기록하게 된다. 이 처리된 블록은 모든 노드에게 다시 전송하고, 모든 노드들은 받은 블록을 검증하게 된다. 이 검증은 해시 퍼즐의 정답이 맞는지와 블록에 기록된 트랜잭션들이 조작되지 않은 기존의 트랜잭션인지 확인한다. 이상이 없으면 블록은 인정을 받고 각 노드는 자신의 블록체인 데이터에 새로 받은 블록을 추가한다.

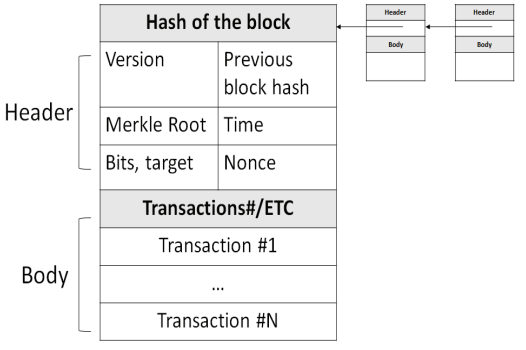

그림 1. 비트코인의 블록 구조
Figure 1. Block Structure of Bitcoin

블록체인 블록의 구조는 어떠한 블록체인을 사용했느냐에 따라 다르다. <그림 1>에서 보이는 것과 같이 비트코인의 블록 구조를 보면 크게 헤더와 바디로 구성된다. 바디는 거래의 내용을 보관하며 헤더는 소프트웨어 버전, 난이도, 이전 블록 해시, 블록 생성 시간, 거래정보 해시, 난스로 구성된다. 블록의 이전블록해시 값은 다음 블록의 난스 값을 찾는데 사용된다.

2.2 사물인터넷과 이슈

사물인터넷이란 센싱, 정보처리, 통신 기능을 통해 인간의 개입 없이 상호 협력하여 지능형 서비스를 제공하는 사물공간연결망을 의미한다. 상호 연계된 센서들이 데이터를 센싱하여 통신 모듈을 통해 전송되어 수집되고 데이터 분석 기술을 통해 인간에게 편리하고 유용한 서비스 제공을 목적으로 하고 있다. 적용분야로는 스마트시티, 헬스케어, 스마트홈, 스마트공장, 에너지분야 등 생활 전반에 퍼져있으며, 사물인터넷 적용은 각 국가의 정부 또는 지자체 주도로 여러 공공분야에 시범사업으로 진행되고 있다. 예를 들어, 미국 시카고주에서는 스마트 시티를 구현하기 위한 사물인터넷 프로젝트 AoT(Array of Things)를 진행하고 있고, 서울시에도 관광 · 안전 IoT 융합실증 프로젝트가 진행되고 있다[3].

사물인터넷의 현실화를 위해 해결해야할 요소로서 엄청난 수의 센서기기들의 관리, 데이터 보안을 꼽을 수 있다. 특히, 스마트시티, 스마트공장 등에는 수많은 센서 기기들로 사물인터넷을 구성할 것이고, 데이터 보안이 철저히 이뤄지지 않는다면 정보 유출뿐만 아니라 인간의 안전 또한 위협받을 수 있는 상황이 가능해진다. 센서기기의 제한된 하드웨어 처리 능력은 기존 보안 메커니즘 적용을 어렵게 한다. 또한 많은 수 기기의 관리라는 측면에서 중앙서버 중심의 보안관리가 적당하지 않다. 이에 분산보안시스템으로서 무결성을 제공해 줄 수 있는 블록체인 기술 적용 연구가 진행되고 있고, 본 논문에서는 어떤 방향의 연구가 진행되고 있는지 분석하고자 한다.

3. 블록체인 활용 연구

본 장에서는 블록체인 기술을 적용한 연구를 3가지의 기준에 따라 분류하여 그 특징을 분석한다. 분류기준은 적용 대상, 합의 알고리즘, 플랫폼이다.

3.1 적용 대상에 따른 분류

표 1. 적용대상에 따른 특징
Table 1. Characteristics by applied targets.

Applied targets	Characteristics
Home	• Management of IoT devices(e.g., doorlock, CCTV camera) in smart home[4] • New education service by crypto currency(PlayCoin) management [5] • Distributed automation for energy sharing between homes on smart grid network[6,7]
Hospital	• Decentralized privacy-preserving healthcare IoT system[8] • Ownership management for medical IoT devices[9]
Company	• Secure fast payment system resisting double-spending problem and hidden transactions problem[10] • Fine-grained transportation/ rent-car Insurance system[11.12] • Decentralized IoT data marketplace for AI learning data[13] • Decentralized loan system based on smart contract[14] • Open and automated customer service system[15]
Government	• Optimized intelligent traffic management system[16-19] • Agri-food supply chain management with traceability [20,21] • Volunteer time bank system for recording the time to serve the elderly as pension system[22] • Education records verification solution[23]

현재 사물인터넷의 다양한 분야 및 환경에 블록체인 기술이 적용되어 연구되고 있다. 본 절에서는 이러한 적용분야 및 환경을 블록체인 기술이 실제로 사용되고 영향을 끼치는 객체로서 보고 가정, 병원, 기업, 정부의 적용대상으로 분류하여 그 특징을 분석한다. 여기에서 4가지의 적용대상은 가정, 병원, 기업, 정부 순서대로 영향을 받는 영역의 크기가 점차 커진다. 블록체인이 분산화 된 네트워크를 형성하므로 적용대상의 크기가 커지고 다른 특징을 가짐에 따라 어떻게 변형되어 적용되는지 특징을 알아본다. 블록체인이 각 적용대상에 적용되며 나타나는 특징을 요약하면 <표 1>과 같다.

병원에 속하는 [8-9]의 연구에서는 정보들의 무결성이 특히 중요하며 철저한 보안이 요구된다. 환자의 수 증가, 부족한 의료진, 점점 심화되는 고령화 사회를 위한 의료시스템 구축 시, 원격으로 의사와 환자를 연결하여 진료를 할 수 있도록 블록체인 네트워크를 형성하는 연구가 진행되고 있다. 이를 통해 의료시스템에서 중요한 개인 의료 정보를 보호하고, 스마트 밴드와 같은 IoT 의료기기로부터 개인 의료 정보를 통신할 때 안전하게 보호할 수 있는 방안에 대하여 연구되고 있다.

기업에 속하는 연구 [10-15]은 주로 탈중앙화한 새로운 형태의 네트워크를 형성하고 스마트 컨트랙트를 이용한 자동화 서비스를 제공하며, 기업 내의 데이터 관리 등의 목적으로 블록체인 적용방안이 연구되고 있다. 그 적용 예로는 보험 시스템, 대출 시스템, 가상 머니 지불 시스템, 직원교육 시스템 등이 있다. 또한 블록체인의 무결성 제공 및 추적가능성 등의 특징을 사용하여 보안 서비스를 제공하고, 더 빠른 기업서비스를 제공하는 것을 목적으로 연구되고 있다. 정부에 속하는 연구 [16-24]는 주로 블록체인의 투명성을 이용한 부정부패 방지, 사회기반시설 관리, 국민 개개인을 P2P 방식으로 연결한 효율적인 관리 시스템 구축, 효율적인

교통시스템 관리, 음식추적 관리, 시민정보 관리, 이민 문제 관리, 연금 관리, 개인 학위 증명 구축 등을 목적으로 연구되고 있다.

가. 가정

가정에 블록체인 기술을 적용한 연구에는 [4-7]가 있다(<그림 2> 참고). [4]에서는 가정에 구성된 보안 및 안전 관리가 중요한 도어락, CCTV 카메라 등으로 구성된 스마트 홈 IoT 장치를 안전하게 관리하고 데이터 무결성을 제공하기 위하여 블록체인 기술을 활용하였다. 기존 블록검증을 위한 연산을 지속적으로 수행해야 하는 PoW(작업 증명)가 아닌 네트워크에 축적된 지분을 통해 블록을 검증하는 PoS(지분 증명), 그 중에서 확장성 부분을 해결하고자 하는 DPoS(위임 지분 증명) 방식으로 스마트 홈 IoT 환경에 적절한 보안용 블록체인 체계를 제안하고 구현하여 그 실현 가능성을 보였다.

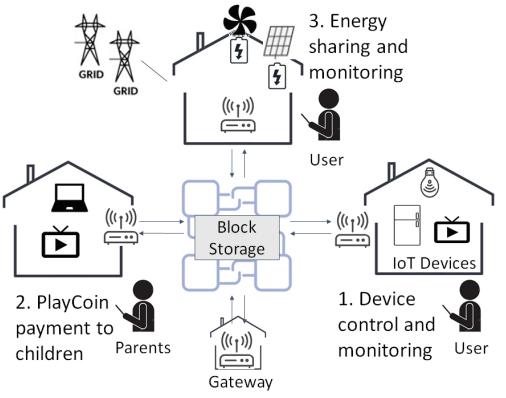

그림 2. 가정에서 블록체인 활용 예 (기기관리, 교육, 에너지관리)
Figure 2. Examples for blockchain application in home (Device management, education, and energy management)

[5]에서는 가정의 가전제품을 노드로 설정하고 블록체인 네트워크로 구성하여 자녀교육에 도움을 줄 수 있는 서비스를 제시하였다. 부모 계정에서는 자녀 계정에 PlayCoin을 부여 할 수 있다. 또한 스마트 컨트랙트를 통하여 미리 입력된 특정 행동(독서, 설거지 등)을 할 경우 자녀는 PlayCoin을 얻을 수 있다. PlayCoin은 집안 내 가전제품을 이용할 수 있는 재화이다. 이를 통하여 자녀들에게 교육적으로 바른 습관을 기르도록 유도할 수 있는 새로운 서비스를 제안하였다. 이는 암호화폐를 가정이라는 환경에 적용하기 위해 블록체인 기술을 가정의 가전 즉 IoT 기기에 적용한 서비스라고 할 수 있다.

연구 [6]에서는 블록체인 네트워크를 통해 이웃간의 효율적인 전력 자원 공유방안, 즉 스마트그리드에 블록체인 기술을 적용한 방안을 제시하였다. 각 가정에는 태양광, 풍력 등으로 부터 전력을 얻고 이를 저장할 수 있는 배터리가 있다. 가정을 지역적으로 묶어 블록체인 네트워크를 형성한다. 스마트 컨트랙트로 미리 정해진 규칙에 따라 각 가정의 전력이 효율적으로 공유되도록 설계하고 구현하였다. 결론적으로 연구[6]는 스마트 그리드 네트워크에서서 필요한 자동화, 분산화 관리를 위해 블록체인 기술을 적용한 것이다. 이와 더불어 블록체인 기술 적용으로 검증가능성(verifiable), 투명성, 무결성, 중복성, 신뢰성을 보장 받을 수 있다.

연구 [7]에서는 [6]와 유사하게 가정의 전력관리를 위해 블록체인 기술을 적용한 방안을 제안하였다. 기존의 전력공급 방식이 3자 의존성이 크기 때문에 탈중앙화된 새로운 전력공급 방식을 제공하기 위해 블록체인 기술을 활용하였다. 스마트 홈의 IoT 장비들을 이용하여 지역적으로 네트워크를 형성하고, 각 스마트 홈에서는 전력 정보를 제공한다. 제안된 블록체인 네트워크는 이 정보를 활용하여 전력을 사고 팔 수 있는 안전한 거래의 기반을 제공한다.

나. 병원

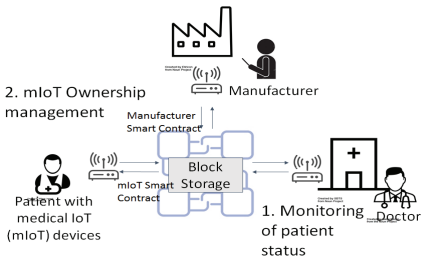

그림 3. 병원에서 블록체인 활용 예 (원격진료, 의료기기 소유자 관리)

Figure 3. Examples for blockchain application in hospital (Remote patient monitoring and mIoT ownership management)

병원에 블록체인 기술을 적용한 연구는 [8,9]가 있다(<그림 3> 참고). [8]에서는 블록체인 네트워크를 통해 원격 진료 시스템을 제안하였다. 증가하는 환자와 부족한 의사의 문제를 해결하기 위한 원격 진료 시스템에는 보안이 무엇보다 중요하다. 기존의 보안모델은 중앙화된 구조 때문에 Single failure(중앙 보안 서버의 장애는 전체 보안서비스 문제와 직결) 문제를 가지고 있고 환자 데이터에 대한 프라이버시 문제가 존재한다. 본 연구에서는 블록체인 기술을 적용하여 IoT 의료기기로부터의 데이터와 트랜잭션 수행에 있어 익명성과 보안성을 제공하 하였다. [9]에서는 증가하는 IoT 의료장비의 신뢰할 수있는 진위, 출처 및 소유권 확인 및 관리를 제공하기 위하여 블록체인 기술을 적용하였다. 민감한 정보를 가지고 있는 IoT 의료장비들은 위조가 가능하다. 따라서 장비가 위조 되었는지 확인하기 위하여 역추적 기능이 필수적이다. 본 연구에서는 블록체인 기술의 특징을 이용한 역추적이 가능한 소유자 관리 시스템을 제안한다.

다. 기업

기업에 블록체인 기술을 적용한 연구들로는 [10-15]이 있다. 최근 사물인터넷과 블록체인 기술이 접목되면서 IoT 기기에서 결제가 이루어지고 블록체인 네트워크에서 이에 대한 검증 및 무결성을 보장해 주는 구조를 선보이고 있다. 그러나 블록체인 기반 암호화 화폐 시스템에서는 더블 스펜딩(double spending, 이중지불) 문제, 즉 이미 사용한 재화를 다른 결제에 이용할 수 있는 문제가 발생할 수 있다. 이러한 더블 스펜딩 문제의 해결책으로서 오프체인(off-chain) 트랜잭션 연구가 진행되었다. 그러나 이 해결책은 메인 네트워크에서 최종 거래 결과만을 저장하기 때문에 많은 거래에 관련된 유용한 정보들이 손실될 수 있다. 이러한 문제를 해결하기 위해 [10]에서는 FastPay라는 지불 방법 Edge-IoT 플랫폼 모델을 제안하였다.

[11]에서는 IoT 데이터 분석과 블록체인 기술을 적용한 쉬운 보험 처리 시스템을 제안한다. 특히 교통 보험 처리에 집중하였다. 다양한 스마트 IoT 장비로부터 GPS정보, 날씨 정보, 속도 정보, 방향 정보, 차량 정보 등을 얻은 후 분석하여 보험 처리를 위한 데이터로 사용한다. 저자는 블록체인의 불변성, 추적 가능성, 투명성이 많은 시간과 비용이 소모되는 보험 처리를 해결하기 위한 좋은 수단이 될 수 있다고 설명하였다. 연구 [11]과 유사하게 [12]에서는 렌트카 보험시스템을 제안하였다. 하지만 렌트카 부분에 초점을 맞추었다. 자동차의 운전 기록 ,주행 특징, 운전자 등의 정보를 수집한다. 데이터들은 무결성을 갖추고 블록체인 네트워크에 기록된다. 보험회사는 보험처리에 드는 시간과 비용을 절약할 수 있다. 또한, 절약된 비용을 이용해 더 좋은 상품을 제공할 수 있다.

[13]에서는 쉽게 데이터를 이용하기 위한 데이터 마켓 형성을 제안한다. 인공지능이 발전함에 따라 인공지능을 학습시키기 위한 데이터가 필수적으로 필요하다. 인공지능의 학습을 위해 필요한 데이터

들을 거래할 수 있는 탈중앙화 된 마켓을 제안하고 있다.

[14]에서는 탈중앙화 된 대출 시스템을 제안하고 있다. 서로에 대한 신뢰 관계가 없이 대출자와 대여자가 스마트 컨트랙트를 통해 대출업무를 처리할 수 있다. 각 체결된 계약들은 블록체인 네트워크의 모든 노드의 장부에 기록된다. 대여자는 손쉽게 위험도를 측정할 수 있으며 스마트 컨트랙트를 통해 계약된 내용이 자동으로 이행된다.

[15]에서는 블록체인 기술을 적용한 자동화된 직원 교육 시스템 제안이다. 직원 교육은 기업에게 반드시 필요한 업무이다. 하지만 직원 교육에는 많은 정보와 비용이 필요하다. 신설 기업들은 직원 교육에 대한 기초정보나 경험이 부족할 수 있다. 이를 위하여 다양한 기업에서 직원 교육정보를 블록체인 네트워크에 제공, 공유하여 다양한 기업에서 이용할 수 있는 시스템이다.

라. 정부

정부에 블록체인 기술을 적용한 연구 논문에는 [16-26]가 있다. [16-19]에서는 블록체인 네트워크를 형성하여 최적화 된 교통 시스템을 제안하였다. 다른 라인에 있는 차들 끼리 블록체인 네트워크를 통하여 누가 끼어들지 결정하는 시스템, 중앙 관리 없이 차 노드끼리 블록체인 네트워크를 형성하여 전체적인 교통흐름 관리 등을 제안하였다.

[20,21]에서는 스마트 농업을 위한 음식 공급 체인 관리 기법을 제안하였다. 제안된 시스템은 블록체인을 이용하여 믿을 수 있고 회계감사가 가능하며 투명한 추적이 가능한 시스템이다. 음식이 생산되어 판매되는 과정이 블록체인 네트워크에 기록되어 추적이 가능하다.

[22]에서는 블록체인 기반 연금 시스템 제안이다. 고령화 시대에 심화되는 연금 문제를 자동적으로 해결하기 위해 스마트 컨트랙트를 이용한 방법을 제안한다. 연금 기관들은 영구히 데이터를 저장할 수 없다는 문제를 가지고 있다. 이를 해결하기 위해 자발적 블록체인 저장 시스템을 구성한다. 데이터 저장에 참여하는 노드들은 코인을 얻을 수 있다. 코인은 다른 서비스(관공서 업무비용 결제, 세금 등)를 위해 사용될 수 있다.

[23]에서는 블록체인을 기술을 이용한 학위증명 시스템을 제안하였다. 각 교육기관은 증가하는 데이터를 관리하는데 문제가 있다. 특히 학위증명을 위한 학위기록 공유에 많은 비용과 시간 낭비를 겪고 있어 이 문제를 해결하기 위해 블록체인 기술과 스마트 컨트랙트를 이용한 자동화된 학위증명 시스템을 제안하였다.

3.2 합의 알고리즘에 따른 분류

다양한 분야에서 블록체인의 응용으로 연구되고 있는 연구 결과물들은 블록체인 합의 알고리즘에 따라 구분 할 수 있다. 합의 알고리즘이란 블록체인에서 새로운 블록을 형성하고 확정하기 위한 노드들끼리 서로 합의하는 과정을 뜻한다. PoW(Proof of Work, 작업증명), PoS(Proof of Stake, 지분증명) 등의 알고리즘이 현재 사용되어 지는 알고리즘의 대부분이다. 기존의 알고리즘의 단점을 보완한 새로운 합의 알고리즘도 계속 제안되는 중이다. 블록체인 네트워크가 작동하기 위해 가장 중요한 부분이며 또한, 합의 알고리즘에 따라 특성이 존재한다. 각 연구의 특성에 부합하는 합의 알고리즘을 선택해야 효율성을 극대화 할 수 있다. <표 2>는 적용된 합의 알고리즘에 따라 연구들의 특징을 요약하였다.

표 2. 적용된 합의 알고리즘에 따른 특징
Table 2. Characteristics by applied consensus algorithms

Algorithm	Characteristics
PoW	• System with security importance and pork temperance(e.g., medical, payment)[7,8,10,17,18,27]
PoS	• Decentralized privacy-preserving healthcare IoT system[8] • Ownership management for medical IoT devices[9]
Others	• Proof-of-Authority[6]: Only validators are allowed to work. In smart grid, participants do not need to have anonymity. • Fast Byzantine fault tolerant[11]: This is faster than PBFT. This is suited for insurance application that have to get a lot of information from IoT devices. • Proof-of-Luck[27]: No need to have computation time, energy. Only Luck is the how to get incentive. This is alternative method for PoW. • Proof-of-Property[28]: New nodes do not have to download whole blockchain. This is good for public blockchain. • Proof-of-Exercise[29]: This is matrix based computation problem. This is alternative method for PoW. • Proof-of-Play[30]: If player exceed optimum level. player is registered for candidate. After that, candidates can get incentive randomly.

가. 작업증명(PoW) 알고리즘

작업증명(PoW) 알고리즘은 블록체인에서 가장 보편적으로 사용 중인 합의 알고리즘으로 컴퓨터 파워를 이용하여 경쟁적으로 해시 연산을 하여 난이도를 만족하는 nonce값을 찾고 이를 검증하는 것으로 합의를 도출하는 방법이다. 단점은 컴퓨터 파워에 따른 부익부 빈익빈 문제, 엄청난 전력 소비 문제가 있다. PoW를 조금 변형한 균형작업증명(ePoW, equilibrium Proof of Work) 알고리즘은 작업증명 방식을 기반으로 하되 채굴에 성공한 노드는 일정 시간 강제로 휴식을 취하여 채굴 기회를 공평하게 나누어 주는 방식의 합의 알고리즘이다.

PoW 알고리즘을 사용한 연구들[7,8,10,17,18, 27]의 공통된 특징은 보안이 중요한 시스템들이다. 보안이 중요한 메디컬 정보 관리 시스템, 포크 상황이 발생하면 안 되는 결제 시스템, 낭비되는 전력보다 보안에 가치를 두는 시스템 등이 PoW 알고리즘을 사용하는 것을 확인할 수 있다.

나. 지분증명(PoS) 알고리즘

지분증명(PoS) 알고리즘은 PoW의 계산력 낭비 문제를 해결하고자 개발되었고, 노드가 보유한 자산에 따라 권한을 분배하여 합의를 도출하고 보상을 분배한다. 작업증명과 다르게 채굴자는 수수료만 가져갈 수 있다. 하지만 두 개의 블록체인이 생성되는 포크 상황에서 두 개 모두에 블록을 생성하는 행위가 가능하다는 문제점이 있다.

PoS를 사용한 연구들[5,8,9,13-16,23,24,27, 32]의 공통된 특징은 PoW의 단점(낭비되는 유지비, 전력 소모량, 전송 속도 등)이 중요한 경우 혹은 스마트 컨트랙트를 사용하기 위한 경우로 분석된다. 스마트 컨트랙트를 제공하는 이더리움 플랫폼 사용을 위한 PoS 알고리즘 선택 또는 스마트 그리드(전력 교환 네트워크)와 같이 채굴은 필요 없고 거래만 이뤄지면 될 경우에 PoS가 채택되는 것을 확인할 수 있다.

위임지분증명(DPoS, Delegated Proof of stake) 알고리즘은 PoS와 비슷하지만 권한을 소수의 대표자에게 위임한다는 차이점이 있다. 지분 보유자들은 지분에 비례한 투표권을 행사하여 자신들을 대신하여 블록 생성과 검증, 네트워크 유지, 합의에 대한 권한을 소수에게 위임한다. 투표에 의해 선출된 소수의 대표자들이 전체를 대신하여 블록을 생

성하여 빠른 합의 속도와 비용이 적게 소요되는 장점이 있으나 소수에 의해 관리가 되는 네트워크가 탈중앙화가 맞는지에 대한 질문이 던져지는 문제점이 있다.

다. 기타 합의 알고리즘

기타 합의 알고리즘으로서 비잔티움 장애 허용(Byzantine fault tolerance) 방식의 알고리즘들이 있다. 예를 들어, PBFT(Practical Byzantine fault tolerance), FBFT(Fast Byzantine fault-tolerant), 텐더민트(Tendermint) 알고리즘이다. 이 방식은 비잔티움 장군 문제의 논리적 딜레마에서 야기되는 실패를 막기 위한 방식으로 일부 노드가 고장 나거나 악의적으로 행동하더라도 계속 동작할 수 있도록 한다.

PBFT 알고리즘은 DPoS 와 같이 대표가 존재하나 3분의 2 이상의 대표자 노드가 합의할 경우 블록이 검증되고 적용된다. BFT를 속도와 실용적인 측면에서 개선한 형태다. 두 단계의 절차를 거쳐 합의를 검증하며 비잔틴 노드의 수가 전체의 33% 이하일 때 합의의 신뢰성을 수학적으로 보장된다[34]. 탈중앙화에서 멀어지나 속도에서 유리하고 보안성을 높인다는 특징이 있다.

FBFT 알고리즘은 빠른 비잔틴장애 허용으로 하이퍼레저 등 컨소시엄형 플랫폼들이 활용하고 있는 기존 PBFT(실용적 비잔틴장애 허용) 알고리즘의 단점을 개선한 형태다. 여러 가지의 정보(날씨, 차량, 속도, GPS위치, 속도, 방향 등)를 수많은 IoT 기기에서 수집하여 처리하는 보험 처리와 같은 서비스에는 각 노드에게 신호를 보내 동의를 구하는 PBFT의 비효율적인 소통 부분을 개선한 FBET 합의 알고리즘이 적합하다[11].

텐더민트(Tendermint) 알고리즘은 Cosmos에서 사용하는 합의 알고리즘으로 PBFT 알고리즘을 공개 및 비공개 블록체인에 맞도록 개량한 합의 알고리즘이다[35]. 텐더민트는 전통적인 합의 알고리즘이 블록체인에 적용된 의미 있는 사례이며 DPoS 개념과 PBFT 개념을 섞어 공개 및 비공개 블록체인에서 사용할 수 있도록 한 합의 알고리즘이다. 기존의 블록체인이 네트워크 공격 노드에 아무런 처벌을 하지 않던 문제인 Nothing of Stake 문제를 해결한다는 장점이 있다. [32]에서 스마트 그리드 네트워크에서 빠르고 안전한 에너지 트랜잭션 처리를 위해 텐터민트 상에 구현한 예를 보이고 있다.

또한, “Proof of”의 이름으로 여러 합의 알고리즘이 고안되었다. 권위증명(PoA, Proof of Authority) 알고리즘은 평판을 기반으로 한 합의 알고리즘으로 특히 사적인(private) 네트워크에 효과적인 해결책이다. 한정된 블록 검증자에 의존하며 블록과 트랜잭션은 시스템의 중개자 역할을 하는 사전 승인된 참여자에 의해 검증되는 알고리즘으로서 스마트 그리드와 같이 참여자(가구)가 증명된 경우 안전한 네트워크를 형성하기에 확정성의 뛰어나다. 스마트 그리드 네트워크에 해당 알고리즘을 적용하였으며[6], 사적인 네트워크에 효과적이며 통화가 필요하지 않다는 특징이 있어 매우 적합하다고 볼 수 있다.

Proof-of-Luck 알고리즘[27]은 TEE 기반으로 구축된다. 해시를 사용하지 않고 랜덤 값을 부착 후 이것이 맞을 경우 블록을 생성할 수 있다. PoW의 해시와 다르게 연산력 낭비가 없어 에너지 낭비를 줄이기 위하여 대신 사용할 수 있는 알고리즘이다.

Proof-of-Property 알고리즘[28]은 이더리움 기반 위에 제안된 절차이다. 최근 생성된 블럭의 상태를 명확하게 하기 위해 트랜잭션에 최근 시스템 상태를 포함시킨다. 이 방법은 참여자가 전체의 블록체인을 다운로드 할 필요가 없이 새로운 트랜잭션에 대한 검증이 가능하기 때문에 새로운 참여자가 많

고 블록체인 네트워크 크기가 계속적으로 커지는 퍼블릭 블록체인에 적합하다.

Proof-of-Exercise 알고리즘[29]은 해시 기반 퍼즐을 매트릭스 기반의 과학적 계산 문제를 해결하는 것으로 대체하는 접근법. 매트릭스는 유용한 실세계 문제를 기반으로 한다. 변경 어려움, 협업 검증 및 참조에 도움이 되는 특징이 있다. PoW의 에너지 낭비가 큰 문제가 될 경우 대체할 수 있다.

Proof-of-Play 알고리즘[30]은 사용자가 직접 게임을 플레이 하는 동안 자동화된 알고리즘이 돌아가며 재화를 얻을 수 있는 알고리즘으로 분산화된 게임 시스템을 구성하기 위하여 제안 되었다. 기존의 낭비문제 없이 게임플레이의 정해진 수준을 넘을 경우 후보로 등록하여 랜덤으로 인센티브를 얻을 수 있다. 이 합의 알고리즘은 적용하려는 분야의 사용목적에 최적화하여 병목현상을 없앨 수 있다.

3.3 블록체인 플랫폼에 따른 분류

표 3. 적용된 블록체인 플랫폼에 따른 특징
Table 3. Characteristics by applied blockchain platforms

Platform	Characteristics
Ethereum	• Automatic operation of smart contract[7,8,10,17,27,30]
Hyperledger	• High performance (e.g., high transaction rate, small network traffic, and low cpu load) on big blockchain for transportation insurance system and smart agriculture

사물인터넷의 다양한 분야에 블록체인 기술이 사용된 연구들을 적용된 블록체인 플랫폼에 따라 구분할 수 있다(<표 3> 참고). 현재 발표된 연구들에서 제안된 시스템을 구현하기 위하여 사용한 플랫폼은 대부분 이더리움이다. 그 이유는 이더리움이 스마트 컨트랙트를 지원하며 스마트 컨트랙트를 이용하여 규칙을 형성하여 자동화된 서비스를 제공하기 때문이다. 블록체인 플랫폼에 따라 다른 특성이 있으며 각 연구 목적에 적합한 플랫폼을 선택하여 적용해야 한다. 현재 이더리움, 하이퍼레저, R3, Ripple 등 다양한 블록체인 플랫폼이 존재하고 있다.

가. 이더리움(Ethereum)

이더리움은 흔히 '2세대 블록체인'이라고 일컫는다. 1세대는 블록체인 기술을 최초로 구현해 보인 비트코인이다. 비트코인은 블록체인 기술을 금융거래 시스템에 접목한 시스템이다. 반면 이더리움은 금융거래에 한정, 특화된 기존 블록체인 시스템을 금융거래 이외의 모든 분야로 확장가능하게 했다. 이더리움에서 가장 중요한 부분은 스마트 컨트랙트이고 이는 합의 프로세스를 자동화한 컴퓨터 프로그램이다. 코드에 적힌 계약 조건이 만족되면 그 즉시 계약이 성사되게끔 한다. 이러한 자동화 처리로 인해 많은 사물인터넷 응용에서 이더리움을 사용하여 블록체인 기술을 구현하였다[5,6,8-10,13,14,22,23,27]

나. 하이퍼레저(Hyperledger)

하이퍼레저는 리눅스 재단에서 주관하는 블록체인 오픈소스이며 여러 산업에 걸쳐 응용 가능한 블록체인 기술을 만드는 것을 목표로 하고 있다[35]. 하이퍼레저는 기업 및 기관을 위한 엔터프라이즈급이라는 특징을 가지고 있으며 현재 가장 실용 가치가 뛰어난 블록체인이라 평가되고 있다. 블록체인의 규모가 커지게 되면 이더리움과 비교하여 하이퍼레저 sawtooth의 성능(지연시간, 네트워크 트래픽, CPU load 등)이 더욱 뛰어나다[20]. 이러한 범위성(scalability) 제공 특성으로 큰 규모의 블록체

인이 필요한 사물인터넷 응용(교통보험 시스템[9], 스마트 농업[18,19])의 프로토타입 구현 시 하이퍼레저를 사용한 것을 알 수 있다.

4. 앞으로의 연구 방향에 대한 제언

본 장에서는 앞서 소개한 사물인터넷에 블록체인 기술 연구에 대한 내용 분석을 바탕으로 앞으로 어떤 주제의 연구가 지속되어야 하는지 그리고 해결해야할 문제들을 제언한다. 궁극적인 블록체인 기술의 목적인 탈중앙화는 현재 시스템의 주된 구성인 중앙화 체계와 정반대의 의미를 가지고 있다. 그러나 수많은 노드로 구성된 사물인터넷 환경에서 모든 노드가 합의 과정에 참여하는 블록체인의 기술이 그대로 적용되는 것은 분명한 한계점이 있다. 따라서 다양한 사물인터넷 응용에 블록체인 기술을 적용하기 위해서는 다양한 노력과 시도가 필요하다. 이에 본 장에서는 다양한 사물인터넷 응용에 블록체인 기술을 적용하기 위해 필요한 블록체인에 관련 연구로서 1) 블록체인 속도 개선, 2) 멀티체인 연구, 3) 블록체인에 대한 공격 대응, 4) 에지컴퓨팅 활용, 5) 합의 알고리즘 변형, 6) 하이브리드 블록체인 7) 표준화 및 타 블록체인 연동, 8) 규제 완화로 정리하여 제언한다.

4.1 블록체인 속도 개선

블록체인에서 속도란 거래처리 속도와 블록 전파 속도가 있다. 초기의 비트코인은 7 TPS(transaction per second)의 처리 속도를 제공하였다. 이후의 블록체인인 이더리움은 20 TPS, 이오스와 하이퍼레저 Fabric은 3000 TPS의 처리 속도를 제공하지만 VISA 카드의 24000 TPS와 비교했을 때 터무니없이 부족하다[37]. 실제 사용되는 중앙시스템의 TPS에 가까워지기 위해 여러 가지 시도가 이뤄지고 있다. 모든 거래정보가 블록에 저장되는 On-Chain 트랜잭션을 벗어나 최종 결과만 메인 체인에 등록하는 Off-Chain 트랜잭션 연구가 진행되고 있다[37]. 단 이 방법은 가상화폐 분야에만 적용이 가능하다는 단점이 있다. 가상화폐가 목적이 아닌 블록체인에서의 속도향상을 위하여 오픈소스 기반 블록체인 계층 위에 새로운 계층을 만들어 트랜잭션 전후처리를 통해 처리속도를 향상시키는 방법이 연구되고 있다[2]. 향후 블록체인 속도 개선에 대한 연구는 계속 진행되어야 할 것이다.

4.2 멀티체인 연구

멀티체인 기술은 기존의 네트워크 구조를 여러 레이어로 구성하고, 각 레이어를 부분적으로 블록체인 기술을 적용하고 각 레이어를 연결하는 방법이다.

기존 연구로서 논문[8]에서는 원격 건강관리 시스템을 위하여 블록체인 기술을 적용하였는데 오버레이 네트워크로 원격 관리 시스템을 구성했다. 오버레이 네트워크(Overlay network)는 물리 네트워크 위에 성립되는 가상의 네트워크이다. 이 네트워크 안의 노드는 가상, 논리 링크로 연결될 수 있고 peer와 peer 간의 연결만 고려한다. [13]에서는 필요한 데이터를 손쉽게 구하기 위한 마켓 형성을 제안하였다. 특히 이 연구에서는 사이드체인 방식이 사용되었다. 사이드체인이란 블록체인 측면에 있는 체인을 연결하는 것으로 기존의 블록체인 기반 플랫폼 서비스를 이용하여 다른 서비스를 제공하는 것을 말한다. 사이드체인을 이용할 경우 현재 다양한 블록체인 플랫폼을 이용할 수 있으며, 참여자가 많아지기 때문에 무결성이 높아진다는 장점이 있다. 그러므로 참여자 수가 현저히 적은 신규 블록체인 플랫폼도 사이드 체인을 이용할 경우 조작방지 위험이 현저히 낮아진다. [23]에서는 학위증

명을 위해 블록체인 기술을 적용 시켰는데 모든 망을 블록체인 네트워크로 형성하겠다는 것이 아니라 각 기관과 개인을 블록체인 네트워크가 연결만 시켜주는 형태로 구성되어 있다.

사물인터넷의 범위성 및 규모성으로 모든 단말 노드가 블록체인의 참여노드로 적용하기에는 무리가 있을 것이다. 사물인터넷 응용의 특징에 따라, 참여노드 수에 따라, 데이터의 종류에 따라 적절한 레이어를 설계하여 멀티체인 기술을 적용하는 연구가 필요할 것이다.

4.3 블록체인에 대한 공격 대응

블록체인을 무력화하는 공격으로는 51%공격이 있다[18]. 51% 공격은 블록체인 네트워크에서 전체 절반을 초과하는 컴퓨팅 자원을 확보하여 원장 기록을 변경하는 공격이다. 이 공격은 모든 노드가 참여하여 합의를 통해 작동하는 블록체인 방식을 노린 방법이다. 51% 공격으로 이중지불, 기존 원장 대체 등의 문제가 발생하며 대상은 주로 소규모 블록체인이다. 왜냐하면 이미 수많은 노드가 참여한 블록체인은 절반 이상 네트워크를 확보하는 것이 불가능에 가깝기 때문에 새로 생긴 블록체인이나 채굴 경쟁이 낮은 소규모를 공격대상으로 잡는다. 블록체인 초기에 해커들로부터 51% 공격을 벗어나 수많은 참여자를 확보하기 위한 방법은 사이드체인이 있다. 기존의 블록체인 기반 플랫폼과 연결하여 51% 공격이 불가능에 가까운 신뢰성을 빌릴 수 있으며 점차 참여자가 많아지기 때문에 충분한 참여자를 확보한 이후에는 스스로 무결성을 가질 수 있다. 그러므로 참여자 수가 현저히 적은 신규 블록체인 플랫폼도 사이드 체인을 이용할 경우 해커들의 51%의 공격 대상으로부터 보호할 수 있다. 블록체인 자체가 공격에 취약하다면 안전한 분산 데이터 관리를 위해 사물인터넷에 블록체인 기술을 적용하는 사례가 줄어들 것이다. 그러므로 블록체인에 대한 다양한 공격에 대한 위협을 분석하고 대응 기법을 연구해야 할 것이다.

4.4 블록체인을 위한 에지컴퓨팅 활용

다양한 블록체인 적용 연구에서 클라우드(cloud) 시스템을 이용하여 블록체인 기술의 적용범위를 확대시키고 다양한 산업 적용하였다[3,7,8,11-13,16,18,21,23,26,31,38]. 이는 처리능력과 저장 공간이 부족한 사물인터넷 단말기기를 위해 블록체인 기술 적용 시, 많은 연구에서 사용한 기반 기술이다. 클라우드 사용으로 지연 발생 시 치명적인 차량 간의 통신이나 지역별로 블록체인을 형성하는 경우와 같이 실시간 통신이 중요한 경우를 제외하고 대부분의 연구에 적용된 것을 확인할 수 있다. 이러한 한계점을 극복하고자 클라우드 분야에서 에지컴퓨팅(edge computing) 연구가 진행되고 있다. 에지컴퓨팅은 중앙 클라우드 서버가 아닌 주변 단말기 주변 노드에서 데이터를 처리하여 기존의 클라우드 컴퓨팅의 데이터 처리 시간을 단축시킬 수 있다. 에지 컴퓨팅은 분산처리 기술을 사용하여 즉시 처리 할 수 있는 데이터는 바로 처리하여 클라우드 기술 이용 시 문제가 되는 속도문제를 해결할 방안으로 기대되고 있다. 에지 컴퓨팅을 통한 자유로운 클라우드의 응용은 블록체인 기술이 적용되는데 큰 도움이 될 것이다.

4.5 합의 알고리즘 변형

합의 알고리즘 변형 연구는 블록체인 기술이 더 많은 분야에서 응용되도록 확대할 수 있다. 기존의 합의 알고리즘의 단점을 보완하기 위한 새로운 합의 알고리즘을 제안하는 다양한 논문[6,11,26-30]들이 존재한다. 기존의 단점을 보완하기 위한 목적도

있지만 자신의 연구 목적과 응용에 적합하게 변경하기 위하여 새로운 알고리즘을 제안하는 경우가 대부분이다. 블록체인 기술이 적용된 연구의 효율성을 더욱 높이기 위해서 새롭게 제안된 알고리즘을 사용하는 것을 볼 수 있다. 기존의 블록체인 기술에서 사용되던 한정적인 합의 알고리즘을 대신하여 새로운 알고리즘을 만드는 것은 불필요한 처리과정을 없애고 적용분야에 최적화하게 한다. 또한 디지털 서명 알고리즘(ECDSA)을 수정하여 병목현상이 발생하는 서명 속 주소를 해독하는 과정을 변형하여 속도를 향상시킬 수도 있다. 이렇게 모든 처리과정에서의 병목현상 발생 지점을 확인하고 지속적인 개선을 시도하여 블록 처리속도의 문제를 개선시킬 수 있을 것이다.

4.6 하이브리드 블록체인 연구

하이브리드 블록체인이란 기존의 퍼블릭 블록체인과 프라이빗 블록체인을 합친 것을 뜻한다. 현재 블록체인 기술의 가장 큰 문제점은 처리속도이다. 블록체인 기술은 모든 노드가 참여하는 탈중앙화가 목표이다. 많은 노드가 합의 과정을 거쳐야 하기 때문에 느린 단점이 있다. 퍼블릭 블록체인은 모든 노드가 참여하기 때문에 느리지만 데이터 투명성이 확실하다. 반면에 프라이빗 블록체인은 빠른 속도와 성능이 우선 시 되기 때문에 참여할 수 있는 노드의 수가 한정적이다. 따라서 이 두 가지를 적절히 조합한다면 블록 전파시간을 줄일 수 있다. 블록체인 안에 멀티 네트워크를 구성하여 참여 노드의 수를 줄일 수 있다. 하이브리드 블록체인, 새로운 합의알고리즘, 비동기식 트랜잭션 처리 방법, 병렬처리 기술, 멀티체인 기술 등 다양한 시도가 복합적으로 적용되어야 현재의 처리속도를 보완할 수 있을 것이다[36,37].

4.7 블록체인 표준화 및 타 블록체인 연동

ISO/TC 307 (Blockchain and distributed ledger technologies)은 2016년 9월 설립된 전 세계에서 가장 활발히 블록체인 기술 및 분산원장 기술 국제표준을 개발하는 국제표준화기구의 기술위원회이다. ISO 기술 산하의 4개의 작업반과 2개의 연구반이 블록체인을 표준 개발을 위하여 설립되었다. 최근 종료된 FG-DLT (ITU-T Focus Group on Application of Distributed Ledger Technology) 회의에서 분산원장 기술 용어 정의가 통과되었다. 블록체인 기술의 국제 표준화 작업은 이제 걸음마 단계라고 할 수 있다. 블록체인의 기본 개념은 이미 오픈소스이기 때문에 특허 출원은 주로 보안, 운용, 활용 등 주변 기술을 중심으로 이뤄지고 있다. 신기술이 사용되어지기 위해서는 표준화가 필수적이다. 표준화는 여러 가지 방면의 시도를 막는다는 우려의 목소리도 있지만, 새로운 기술이 안전하게 확산되기 위해서는 국제 표준화의 성공 여부가 중요하다. 블록체인 국제 표준에 적극 참여하여 우리의 기술로 선점하는 것이 곧 신기술의 대응 속도와 이어지기 때문에 더욱 중요하다.

또한 다양한 블록체인 플랫폼에 구현된 사물인터넷 서비스 간의 상호 연동이 필요할 수 있을 것이다. 블록체인 상호 연동을 위한 기술 및 규격 개발 역시 초기단계이며 ISO/TC 307 및 대학 등에서 관련 논의를 진행하고 있다. 이에 대한 연구 또한 필수적이다.

4.8 블록체인에 관한 규제 완화

현재 많은 나라들이 블록체인을 활용하고 나아가 암호화폐를 공식적인 화폐로 인정한 나라들도 많지만, 우리 정부는 암호화폐를 제외한 블록체인 기술만 육성하겠다고 발표하였다. 블록체인 기술이

다른 기술과 달리 특히 규제에 부딪치는 이유는 블록체인의 특징인 분산성, 불변성, 비가역성 때문이다. 현재 국내 관련 법률 현황에서는 개인정보보호법 및 전자금융거래법에서는 기록의 파기와 정정 및 삭제의 의무를 명시하고 있다. 개인정보보호법 제21조 개인정보의 파기, 개인정보보호법 제36조 개인정보의 정정, 삭제 전자금융거래법 제22조 전자금융거래기록의 생성, 보존 및 파기와 같은 법률조항에서 확인할 수 있다[1]. 블록체인 기술은 어느 정보가 누구의 것인지 알 수 없지만 사실상 역추적을 통해 알아낼 수 있는 방법이 다양하며 익명성이 쉽게 뚫릴 위험이 있다. 또한 수정이나 삭제가 어렵기 때문에 프라이버시 문제, 전자 정보 교정의 어려움 등의 문제에 직면하게 된다. 만약 위치정보가 포함된다면 현재 법률 제 23조 위치정보의 보호 및 이용에서 명시하듯 목적을 달성한 개인위치정보는 즉시 파기되어야 하는데 블록체인 기술상 이것은 불가능하다. 즉 블록체인 기술 자체가 혁신적인 기술이기 때문에 기존의 것을 부수고 새로운 패러다임을 만들어내는 것이 필수적이다. 따라서 새로운 블록체인 기술을 이용한 서비스를 시작하기 전 현재의 규제와 문제가 있는지 확인하고 하나씩 고쳐 나가야 블록체인 기술이 확산될 수 있을 것이다.

5. 결 론

블록체인 기술은 4차 산업혁명의 특징인 초연결 사회에 반드시 필요한 기술이다. 블록체인 기술을 적용한 많은 사물인터넷 기술 및 서비스가 등장하고 있다. 이러한 연구들은 서비스 적용대상, 합의 알고리즘, 블록체인 플랫폼에 따라 다른 관점에서 볼 수 있으며 각각 분명한 특징과 장단점을 가지고 있다. 이러한 분류와 분석을 통해 현재 진행되고 있는 최근 연구의 트렌드를 파악하고, 앞으로 사물인터넷의 다양한 응용에서 블록체인 기술을 적용하고, 그 효율성 및 가능성을 높이기 위해 진행되어야 할 8가지 연구 방향을 제언하였다.

References

[1] Future of Blockchain, KISTEP, 2018.

[2] R. B. Hartley, *Accelerator: achieving 10x blockchain performance on IBM blockchain platform*, IBM Think 2019, Feb. 2019.

[3] X. Liang, S. Shetty, D.Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, *ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability*, In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing IEEE Press, Piscataway, NJ, USA, pp. 468-477, May 2017.

[4] M. Kim, and Y. Kim, *Development of IoT device management system using blockchain DPoS consensus algorithm*, Journal of IKEEE, Vol. 23, No. 2, pp. 508-516, Jun. 2019.

[5] A. L Suchaad, K. Mashiko, and M. H. Z. Abidin, *Blockchain use in home automation for children incentives in parental control*, MLMI 2018 Proceedings of the 2018 International Conference on Machine Learning and MachineIntelligence, pp. 50-53, Sep. 2018.

[6] J. Schlund, L. Ammon, and R. German, *ETHome: Open-source blockchain based energy community controller*, e-Energy '18 Proceedings of the Ninth International

Conference on Future Energy Systems, pp. 319-323, Jun. 2018.

[7] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar, *EnergyChain: enabling energy trading for smart homes using blockchains in smart grid ecosystem*, In Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities, ACM, New York, NY, USA, Article 1, pp. 1-6, Jun. 2018.

[8] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, *A decentralized privacy-preserving healthcare blockchain for IoT*, Sensors, Jan. 2019.

[9] M. Alblooshi, K. Salah, and Y. Alhammadi, *Blockchain-based ownership management for medical IoT devices*, 2018 International Conference on Innovations in Information Technology, pp. 151-156, Nov. 2018.

[10] Z. Hao, R. Ji and Q. Li, *FastPay: a secure fast payment method for edge-IoT platforms using blockchain*, 2018 IEEE/ACM Symposium on Edge Computing, Seattle, WA, pp. 410-415, Oct. 2018.

[11] Z. Li, Z. Xiao, Q. Xu, E. Sotthiwat, R. S. Mong Goh and X. Liang, *Blockchain and IoT data analytics for fine-grained transportation insurance*, 2018 IEEE 24th International Conference on Parallel and Distributed Systems, Singapore, pp. 1022-1027, Dec. 2018.

[12] H. T. Vo, L. Mehedy, M. Mohania, and E. Abebe, *Blockchain-based data management and analytics for micro-insurance applications*, In Proceedings of the 2017 ACM on Conference on Information and Knowledge Management ACM, New York, NY, USA, pp. 2539-2542, Nov. 2017.

[13] K. R. Özyılmaz, M. Doğan, and A. Yurdakul, *IDMoB: IoT data marketplace on blockchain*, 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 11-19, Jun. 2018.

[14] Q. Yang, X. Zeng, Y. Zhang, and W. Hu, *New loan system based on smart contract*, In the 2019 ACM International Symposium, pp. 121-126, Jul. 2019.

[15] W. M. Wang, H. Guo, Z. Li, Y. Shen, and A. V. Barenji, *Towards open and automated customer service: a blockchain-based AutoML framework*, In Proceedings of the 2nd International Conference on Computer Science and Application Engineering) ACM, New York, NY, USA, Article 27, pp. 1-6, Oct. 2018.

[16] Q. Ren, K. L. Man, M. Li, and B. Gao, *Using blockchain to enhance and optimize IoT-based intelligent traffic system*, 2019 International Conference on Platform Technology and Service, Jeju, Korea, pp. 1-4, Jan. 2019.

[17] H. Rathore, A. Samant, M. Jadliwala, and A. Mohamed, *TangleCV: decentralized technique for secure message sharing in connected vehicles*, In ACM pp. 45-48, Mar. 2019.

[18] R. Shrestha, and S. Y. Nam, *Regional*

blockchain for vehicular networks to prevent 51% attacks, in IEEE Access, vol. 7, pp. 95033-95045, Jul. 2019.

[19] R. A. Michelin, A. Dorri, M. Steger, R. C. Lunardi, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, *SpeedyChain: a framework for decoupling data from blockchain for smart cities*, In Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services ACM, New York, NY, USA, pp.145-154, Nov. 2018.

[20] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, *Blockchain-based traceability in Agri-Food supply chain management: A practical implementation*, 2018 IoT Vertical and Topical Summit on Agriculture Tuscany (IOT Tuscany), Tuscany, 2018, pp. 1-4, May. 2018.

[21] J. Lin, Z. Shen, A. Zhang, and Y. Chai, *Blockchain and IoT based food traceability for smart agriculture*, In Proceedings of the 3rd International Conference on Crowd Science and Engineering ACM, New York, NY, USA, Article 3, pp. 1-6, Jul. 2018.

[22] S. Cheng, W. Shi, and H. Zhang, *VOLTimebank: a volunteer system for mutual pension based on blockchain*, In the 2019 International Conference pp. 75-79, Mar. 2019.

[23] M. Han, Z. Li, J. He, D. Wu, Y. Xie, and A. Baba, *A novel blockchain-based education records verification solution*, In Proceedings of the 19th Annual SIG Conference on Information Technology Education ACM, New York, NY, USA, pp. 178-183, Oct. 2018.

[24] C. W. Chiang, E. Betanzos, and S. Savage, *Exploring blockchain for trustful collaborations between immigrants and governments*, In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems ACM, New York, NY, USA, pp. 1-6, Apr. 2018.

[25] A. Alketbi, Q. Nasir and M. A. Talib, *Blockchain for government services-Use cases, security benefits and challenges*, 2018 15th Learning and Technology Conference, Jeddah, 2018, pp. 112-119, May. 2018.

[26] H. Li, K. Gai, Z. Fang, L. Zhu, L. Xu, and P. Jiang, *Blockchain-enabled data provenance in cloud datacenter reengineering*, In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure ACM, New York, NY, USA, pp. 47-55, Jul. 2019.

[27] M. Milutinovic, W. He, H. Wu, and M. Kanwal, *Proof of luck: an efficient blockchain consensus protocol*, In Proceedings of the 1st Woarkshop on System Software for Trusted Execution ACM, New York, NY, USA, Article 2-6 pages, Dec. 2016.

[28] C. Ehmke, F. Wessling, and M. Christoph, *Proof-of-property: a lightweight and scalable blockchain protocol*, In Proceedings of the 1st International

Workshop on Emerging Trends in Software Engineering for Blockchain ACM, New York, NY, USA, pp. 48-51, May. 2018.

[29] A. Shoker, *Brief Announcement: sustainable blockchains through proof of eXercise*, In the 2018 ACM Symposium, pp. 269-271, Jul. 2018.

[30] F. Wu, W. Cai, C.B. Wei, H. Chan, Q. Yan, V. Leung, and H. Yuen, *Proof-of-play: a novel consensus model for blockchain-based peer-to-peer gaming system*, In ACM International Symposium on Blockchain and Secure Critical Infrastructure, pp. 19-28, Jul. 2019.

[31] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, *Mitigating loT device based DDoS attacks using blockchain*, In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems ACM, New York, NY, USA, pp. 71-76, Jun. 2018.

[32] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, G. Sciumè and G. Zizzo, *An energy blockchain, a use case on tendermint*, 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe, Palermo, pp. 1-5, 2018.

[33] XML resources, https://verticalplatform.kr/archives/9984, Oct. 2019.

[34] XML resources, https://PBFT, Practical Byzantine Fault Tolerance, WiKi hashnet, Oct. 2019.

[35] XML resources, http://www.daylifg.com/dstory/tech/detail?idx=561, Oct. 2019.

[36] E. Androulaki, *Hyperledger fabric: A distributed operating system for permissioned blockchains*, in Proc. 13th EuroSyst, p. 30, 2018.

[37] J. Eberhardt, and S. Tai, *ZoKrates-scalable privacy-preserving off-chain computations*, 2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, Halifax, NS, Canada, pp. 1084-1091, 2018.

[38] I. Ahmed, I. AlMallohi, A. Saad, Alotaibi, R. Alghafees, F. Azam, and Z. S. Khan, *Multivariable based checkpoints to mitigate the long range attack in proof-of-stake based blockchains*, In Proceedings of the 3rd International Conference on High Performance Compilation, Computing and Communications ACM, New York, NY, USA, pp. 118-122, Mar. 2019.

블록체인 기술의 사물인터넷 적용에 대한 조사 연구-적용 환경, 합의 알고리즘, 플랫폼 중심으로

김미희[1], 이기훈[2]

[1] *한경대학교 컴퓨터공학과 부교수*

[2] *한경대학교 컴퓨터공학과 학부생*

요 약

최근 4차 산업혁명을 구성할 기술 중 사물인터넷과 블록체인 기술은 그 핵심에 있다. 본 논문에서는 사물인터넷을 위해 블록체인 기술을 접목한 연구들을 살펴본다. 사물인터넷을 구성할 기기 수가 폭증하고, 그 수집 관리될 데이터 양 또한 상당할 것으로 예측하고 있다. 이러한 기기나 기기로부터 생성될 데이터에 대한 안전성 확보는 해결해야할 문제로 대두된다. 이러한 문제의 해결책으로서 데이터 관리의 분산화, 위조 불가능, 추적가능 등 데이터의 안전성 등을 제공하는 블록체인 기술을 꼽고 있다. 그러나 기존 전자화폐 관리(예, 비트코인)에서 사용되는 합의 알고리즘의 계산의 비효율성 등이 사물인터넷에 적용되기 위해 개선해야할 점으로 꼽히고 있으며, 이를 개선한 블록체인 기술이 사물인터넷에 적용되는 연구가 진행되고 있다. 본 논문에서는 이러한 사물인터넷 시스템을 위해 적용된 블록체인 기술 사례를 살펴 보기위해 적용환경(가정, 병원, 기업, 정부), 합의 알고리즘(작업증명, 지분증명), 플랫폼(이더리움, 하이퍼레저) 으로 분류하여 그 특징을 분석한다. 이러한 최근 연구 동향 분석을 통해 사물인터넷 구성을 위한 블록체인 기술의 적용 가능성을 보이고, 앞으로 진행해야 할 연구주제와 해결해야할 사항을 제언한다.

감사의 글

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2018R1A2B6009620).

Mihui Kim received the B.S. and M.S. degrees in Computer Science and Engineering from Ewha Womans University, Korea, in 1997 and 1999, respectively. During 1999-2003, she stayed in Switching & Transmission Technology Lab., Electronics and Telecommunications Research Institute (ETRI) of Korea to develop the MPLS System and the 10Gbps Ethernet System. She also received the Ph.D. degree in Ewha Womans University in 2007. She was a visiting scholar of the department of computer science, North Carolina State University. She is currently an associate professor in the Department of Computer Science and Engineering at Hankyong National University. Her research interests include IoT security, attack defense, and blockchain.

E-mail address: mhkim@hknu.ac.kr

Lee Gihun is a Bachelor student in the Department of Computer Science and Engineering at Hankyong National University. His current research interests include security on mobile crowdsensing and blockchain.

E-mail address: comb0601@gmail.com