한국컴퓨터정보학회 동계학술대회 논문집 제26권 제1호 (2018. 1)

블록체인에 기반한 합의 알고리즘

유승언O, 이병준*, 김경태*, 윤희용*
*성균관대학교 정보통신대학 전자전기컴퓨터공학과
O성균관대학교 소프트웨어대학 소프트웨어학과
e-mail: seyoo90@skku.edu, byungjun@skku.edu, kyungtaekim76@gmail.com, youn7147@skku.edu

Block chain based consensus algorithm

Seung-Eon YooO, Byung-Jun Lee*, Kyung-Tae Kim*, Hee-Young Youn*
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
ODept. of Software, Sungkyunkwan University

● 요 약 ●

현재 우리나라를 비롯해 전 세계적으로 핀테크, 빅데이터, 사물 인터넷, 인공 지능, 공유 경제 등 향후 다가올 미래 세상에서의 주요 기술에 대해 전략적으로 개발 및 산업화를 추진하고 있으며 이러한 흐름을 4차 산업혁명으로 명명하고 있다. 4차 산업혁명의 근간 중에서 분산 데이터베이스의 한 형태로 지속적으로 성장하는 데이터 기록 리스트로써 분산노드의 운영자에 의한 임의 조작이 불가능하도록 고안된 블록체인의 정의와 블록체인에서 사용되는 합의 알고리즘에 대해 설명하였다.

키워드: 블록체인(Blockchain), 합의 알고리즘(Consensus algorithm)

I. Introduction

현재 '비트코인'이라 불리는 가상화폐가 전 세계적으로 열풍이 일고 있다. 2008년 사토시 나가모토라는 사람이 P2P식 전자 결제 시스템을 위한 새로운 프로토콜을 구상했는데 이 전자 결제 시스템에 사용되는 것이 '비트코인'이라 불리는 암호화폐이다. 블록체인은 이 비트코인을 통해 처음 제안한 기술로써 거래 무결성과 거래 내역이 위조되지 않음을 보장한다.[1]

본 논문에서는 분산 데이터베이스의 한 형태로 지속적으로 성장하는 데이터 기록 리스트로써 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안된 블록체인의 정의와 블록체인에서 사용하는 합의 알고리즘에 관해 소개하고자 한다.

II. 블록체인

블록체인은 P2P 네트워크를 통해 이중 지불을 막기 위해 쓰이며 누군가의 보증이 없어도 내용을 신뢰할 수 있게 해주는 기술이다.[2] 대표적인 온라인 가상 화폐인 비트코인에 적용되어있는 블록체인은 '블록(block)'이라고 하는 데이터의 단위를 일정시간마다 생성, '체인(chain)' 사슬처럼 연결하여 데이터를 저장하면 거래기록을 저장한 거래장부가 된다. 이러한 거래장부는 누구나 열람할 수 있게 되어 거래 내역을 투명하게 기록하며 10분에 한 번씩 이 기록을 검증하여 해킹을 막는다.[3]

III. 합의 알고리즘

3.1 POW(Proof of work)

POW는 작업증명으로 불리는 합의 알고리즘으로 컴퓨터의 연산력으로 코인을 얻는 방식이다. 성능이 좋은 컴퓨터, 채굴기를 보유하면 코인을 채굴할 수 있는 속도가 더 빨라지는 방식으로 많은 돈과 많은 전력소비가 필요하다. 과정을 살펴보면, 10분 단위로 발생한 모두 묶어서 하나의 블록으로 생성하여 전체 P2P 네트워크상에 공유한다. 임의의 노드들은 블록n을 검증하기 위한 연산 작업을 수행한다. 6개 이상의 노드가 검증 작업을 완료하면 블록 n을 공식적으로 인정하여 블록체인에 포함시킨다. <그림 1>은 POW 동작 과정을 순서도로 표현한 것이다.

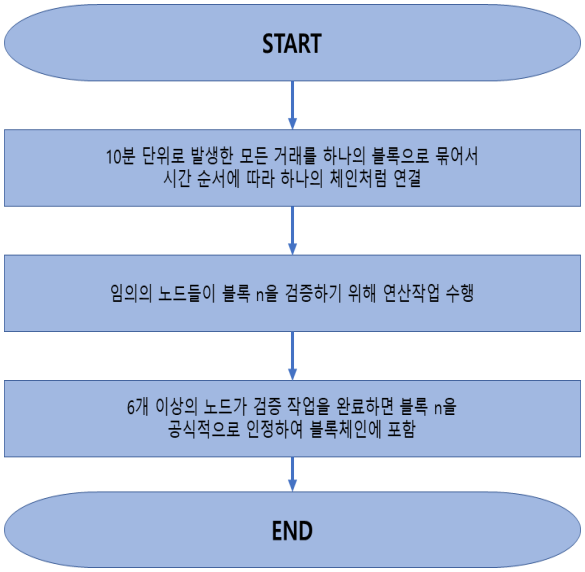

Fig. 1. 비트코인에서 POW의 동작 순서도

3.2 POS(Proof of Stake)

POS는 자산증명으로 불리는 POS의 대안으로 제안된 합의 알고리즘으로 채굴되는 가상화폐를 보유하고 있으면 보유한 지분에 대한 이자로 보상이 지급되는 방식이다. 일반적으로 블록체인을 공격하기 위해서는 공격자가 네트워크의 51% 이상을 점유해야 하는데 POS를 사용하면 총 화폐 중 51% 이상을 점유해야 공격이 가능하므로 해커 입장에서는 POW를 사용할때보다 공격에 많은 비용이 들어가므로 보안성이 높아질 수 있다는 장점이 있다. 많은 수량의 가상화폐를 보유할수록 더 많은 보상이 지급된다.

3.3 POI(Proof of Importance)

POI는 기여도 증명, 중요도 증명으로 불리는 POS의 대안으로 제안된 합의 알고리즘으로 코인지분이 높은 사람들을 보상하는 것은 동일하지만 그 외에 어떤 사람과 거래를 하는지, 얼마나 많은 사람과 거래를 하는지 즉, 네트워크에 기여도가 높은 사람에게 더 많은 수수료를 분배하는 시스템이다.

IV. Conclusions

본 논문은 블록체인과 블록체인에서 사용되는 합의 알고리즘 POW, POS, POI에 대해 설명하였다.

같은 블록체인이라도 사용용도에 따라 가치도 달라지므로 효율적으로 사용가능한 합의 알고리즘을 선택해야 한다. 또한 보안문제가 아직 완벽하지 않기 때문에 보안문제를 보완할 알고리즘 개발이 필요하다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 정보통신·방송연구개발 사업(No.B0717-17-0070, 초연결 IoT 노드의 군집 지능화를 통한 Edge Computing 핵심 기술 연구), SW중심대학지원사업(2015-0-00914), 한국연구재단 기초연구사업 (No.2016R1A6A3A11931385, 실시간 공공안전 서비스를 위한 소프트웨어 정의 무선 센서 네트워크 핵심기술 연구, 2017R1A2B2009095, 실시간 스트림 데이터 처리 및 Multi-connectivity를 지원하는 SDN 기반 WSN 핵심 기술 연구), 삼성전자, BK21PLUS 사업의 일환으로 수행되었음.

REFERENCES

[1] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”. 2008.

[2] Marc Pilkington, “Blockchain Technology: Principles and Applications”, Research Handbook on Digital Transformations, edited by F.Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016.

[3] Andres Guadamuz and Chris Marsden, “Blockchains and Bitcoin: Regulatory responses to cryptocurrencies”, Peer-reviewed journal on the internet, Volume 20, Number 12-7 December 2015