JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 12, pp. 99-104, December 2021
https://doi.org/10.9708/jksci.2021.26.12.099

A Study on Modification of Consensus Algorithm for Blockchain Utilization in Financial Industry

Hong-Gab Im*

*Professor, Dept. of Multimedia, Kimpo University, Gimpo, Korea

[Abstract]

Blockchain technology is a distributed ledger technology that shares the ledger between multiple nodes connected to a distributed network. The data managed through the existing central server is managed through the blockchain, and the transparency, accuracy, and integrity of the transaction data is increased, and the need for data management through the blockchain is increasing. In this paper, recognizing the need for trust-based data sharing between trust-based institutions in the financial industry, this paper describes the process of selecting leader nodes in Raft, a private blockchain consensus algorithm, as a way to increase data management efficiency through blockchain. A modified consensus algorithm is presented. The performance of the modified consensus algorithm and the general Raft consensus algorithm presented in this paper was compared and analyzed based on the transaction processing time, and it was confirmed that the efficiency of the consensus process was increased by applying the proposed consensus algorithm.

▸ **Key words**: Blockchain, financial industry, Consensus algorithm, Raft

[요 약]

블록체인 기술은 분산 네트워크에 연결된 다수의 노드 간 원장을 공유하는 분산 원장기술이다. 기존 중앙 서버를 통하여 관리되던 데이터들이 블록체인을 통하여 관리되며 거래 데이터에 대한 투명성과 정확성 및 무결성이 높아지며 블록체인을 통한 데이터관리의 필요성이 높아지고 있다. 본 논문에서는 금융업에서 신뢰 기반의 기관 간 신뢰 기반의 데이터 공유가 필요하다는 점을 인지하고 블록체인을 통한 데이터관리 효율성 증대를 높이는 방법으로 프라이빗 블록체인 합의 알고리즘인 Raft의 리더 노드 선출과정의 처리 과정을 수정한 합의 알고리즘을 제시하였다. 본 논문에서 제시한 수정 합의 알고리즘과 일반적인 Raft 합의 알고리즘에 대하여 트랜잭션 처리시간을 기준으로 성능을 비교·분석하였으며 제안한 합의 알고리즘 적용을 통하여 합의 과정의 효율성이 높아짐을 확인하였다.

▸ **주제어**: 블록체인, 금융산업, 합의 알고리즘, Raft

• First Author: Hong-Gab Im, Corresponding Author: Hong-Gab Im
*Hong-Gab Im (skydiverpd@kimpo.ac.kr), Dept. of Multimedia, Kimpo University
• Received: 2021. 11. 08, Revised: 2021. 12. 03, Accepted: 2021. 12. 03.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

블록체인 기술 발전과 더불어 금융업계에서 블록체인의 적용사례가 증가하고 있다. 금융업계에서의 블록체인 기술 적용으로는 인증, 해외 송금, 증권거래 등이 있으며 이러한 거래는 대부분 기관과 기관 간의 신뢰 인증 및 합의를 통하여 이루어진다. 금융업에서 기관과 기관 간의 데이터 공유 시 중요한 것은 데이터 공유를 위한 합의 과정의 신뢰성과 안정성이다. 현재 금융업에는 기관 간 합의와 검증을 위하여 프라이빗 블록체인 기반 합의 알고리즘을 사용하고 있으며 향후 금융업에서 폭넓은 활용과 신뢰도 제고를 위해서 현재의 합의 알고리즘에서 안정성을 강화하고 효율성 제고가 필요하다. 본 논문에서는 프라이빗 블록체인의 합의 알고리즘인 Raft((Reliable, Replicated, Redundant and Fault-Tolerant)의 합의 과정 중 리더 노드 수정 과정에 대한 처리 절차를 수정하여 거래 때 안정성과 효율성을 높이고자 한다.

본 논문의 2장에서는 블록체인 기술과 합의 알고리즘에 대하여 설명하고 3장에서는 제안한 알고리즘에 대한 설명 및 성능평가를 한다.

II. Preliminaries

1. Blockchain

블록체인 기술은 분산 네트워크를 통해 관리되는 다양한 거래정보를 효율적으로 관리하기 위한 분산원장 기술(DLT, distributed Ledger Technology)로서 거래정보를 중앙 서버가 아닌 네트워크에 공유되어 관리된다[1].

블록체인 기술은 거래내용에 대한 송금 요청에 대하여 해당 거래정보가 담긴 블록 생성이 진행되며 해당 블록이 네트워크의 모든 참여자에게 공유되어 참여자들이 거래정보 유효성을 상호 검증하고 검증 완료의 경우 블록체인에 연결되는 과정을 가진다[1, 2].

블록체인은 새로 생성된 블록 내 거래정보에 이전 블록의 해시값을 포함하고 있으며 새로 생성된 블록의 정보 역시 그다음 블록에 해시값의 형태로 포함되므로 모든 블록은 체인 구조를 이루며 연결된다[1, 3].

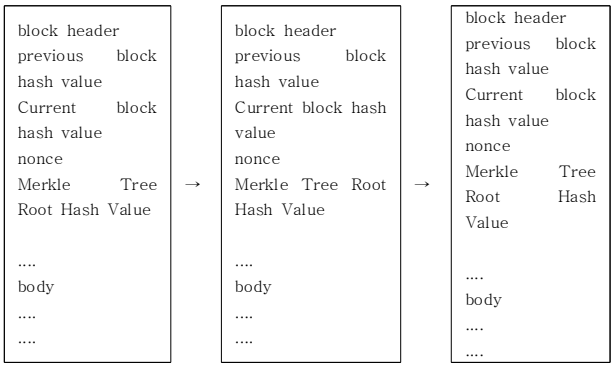

Fig. 1. block data [1, 3]

블록체인은 합의 알고리즘을 통하여 데이터를 검증하고 유효성을 합의하므로 블록체인을 적용하고자 하는 시스템의 합의 알고리즘의 적절한 운영을 통하여 시스템 운영의 효율성을 높이고 보안을 강화할 수 있다.

2. Blockchain application in the financial industry

블록체인 기술을 금융업에 사용할 경우, 다음과 같은 장점을 가질 수 있다.

첫째, 블록체인은 낮은 비용으로 안전한 금융거래시스템을 갖출 수 있다. 블록체인은 거대한 중앙전산망을 갖추지 않고 개별 컴퓨터들이 거래내용에 대한 관리와 합의를 진행하므로 저렴한 비용으로 금융거래를 할 수 있다[4].

둘째, 블록체인을 통한 거래는 거래의 효율성을 보장한다. 전술한 바와 같이 블록체인에 연결된 각 블록은 이전 블록에 대한 정보를 해시값으로 보유하므로 거래내용에 대한 악의적인 수정을 위해서는 네트워크 참여자들의 합의와 모든 블록에 대한 정보수정이 불가피하다. 이는 현실적으로 불가능한 것이므로 이러한 블록체인의 기술적 특징에 의하여 금융에 대한 보안사고 예방을 위하여 블록체인 기술적용의 필요성이 높아진다[5, 6].

셋째, 블록체인 기술 중 스마트 계약 기술에 의하여 다양한 금융상품에 대한 자동 거래실행이 가능하다[7].

국내외 금융업체의 블록체인 도입사례 및 해외 송금과 증권거래 등을 들 수 있다. 먼저 인증 분야에서 별도의 인증기관 없이 공동 인증서를 블록체인으로 공유할 수 있도록 하고 있으며 이를 통하여 금융업체는 인증서 등록의 필요성이 감소하고 이에 따라 수수료 절감 효과가 두드러지고 있다[8, 9].

해외 송금의 경우 블록체인 가입 은행을 통하여 직접 거래함으로써 거래에 대한 처리기관과 수수료 비용의 절감이 가능하다. 증권거래와 보험계약의 경우도 스마트 계약을 통하여 자동거래가 가능하게 되었고 그 외 보험계약 및

대출에서도 블록체인 기술을 통한 활용 가능성이 커지고 있다[10, 11].

금융업뿐 아니라 비금융업에서도 투표, 행정업무, 전력 거래 및 의료정보, 물류 등의 업무에 블록체인 기술을 적용하기 위한 노력이 한창이다[12].

3. Blockchain Consensus Algorithm

블록체인은 거래내용을 기록한 분산 장부이며 각 노드는 자신의 장부를 가지고 있고 각 장부는 합의 알고리즘에 의하여 무결성을 유지한다[1, 13].

블록체인 기술은 네트워크 참여 제한 여부에 따라 퍼블릭 블록체인과 프라이빗 블록체인으로 나뉠 수 있다. 퍼블릭 블록체인은 네트워크 참여를 원하는 누구나 네트워크에 참여하고 블록 생성 및 합의의 기회를 가질 수 있다. 프라이빗 블록체인은 허가된 노드만 네트워크에 참여하고 블록 생성 및 합의의 기회를 가질 수 있다[14].

그림 2는 블록체인의 처리 과정을 도식화하여 정리한 것이다.

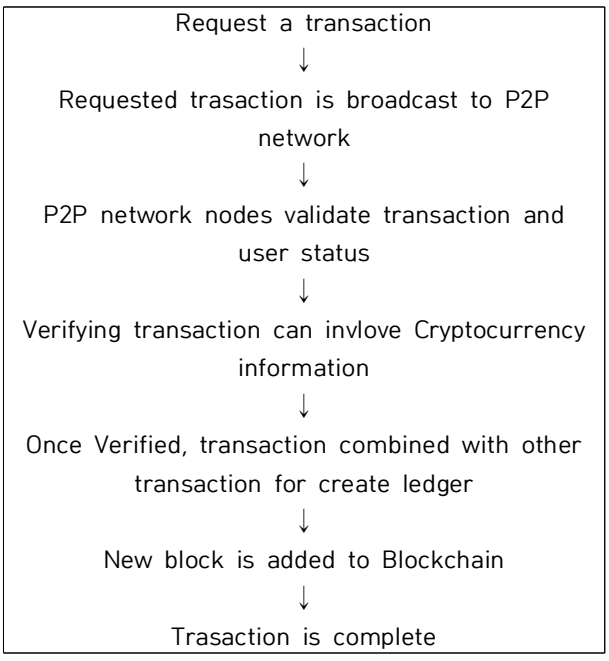

Fig. 2. Blockchain process [1,13]

그림 2와 같이 요청된 트랜잭션은 P2P 네트워크에 공유되며 P2P 네트워크에 있는 노드들은 트랜잭션이라 불리는 해당 거래를 검증하는 과정을 거친다, 검증을 마친 거래내용은 다양한 정보를 가지고 있으며 검증된 거래내용은 블록에 저장된다. 해당 거래내용을 포함하는 블록이 생성되면 블록체인에 추가되며 트랜잭션 공유를 위한 적업이 완료된다. 금융업의 경우 거래를 승인하기 위하여 해당 거래자의 신뢰를 보장하는 소수의 기관 간 합의 과정이 필요하다[13]. 금융업에서 거래를 승인하기 위한 소수의 허가된 기관의 합의 알고리즘 진행을 위하여 PBFT와 Raft 등의 합의 알고리즘이 실행된다.

먼저, 퍼블릭 블록체인의 합의 알고리즘은 작업증명방식(PoW, Proof of Work), PoS(Proof of Stake) 등으로 나눌 수 있으며 프라이빗 블록체인의 합의 알고리즘은 PBFT(Practical Byzantine Fault Tolerance), Raft 등으로 나눌 수 있다[1, 13]. 작업증명방식은 비트코인과 이더리움에서 주로 사용되며 블록 생성을 원하는 노드들이 특정한 논스(Nonce)값을 구하는 수학적 연산 과정을 갖는다. 작업증명방식에 대한 수식은 hash(블록) <= 난이도의 최댓값 / 난이도로 나타낼 수 있으며 블록의 해시값을 옳게 찾기 위하여 빠른 속도와 높은 계산력을 기반으로 지속해서 연산한다[12, 13].

지분증명방식은 작업증명방식의 과도한 계산력 소모를 완화하기 위한 대안으로 제시되었으며 각 노드의 지분이 블록 생성을 위한 권한으로 사용되는 합의 과정을 갖는다[12, 13]

지분증명방식의 수식으로 hash(hash(이전 블록), 계정, 현재 타임 스탬프) <= 계좌의 balance·난이도의 최댓값 / 난이도 롤 나타낼 수 있다. 제시한 수식과 같이 지분증명방식은 계좌의 balance와 난이도에 영향을 받으며 지분을 많이 소유한 노드가 낮은 난도의 연산 하게 됨을 알 수 있다 [12, 13].

지분증명방식은 블록의 생성 주기 단축이 가능하고 과도한 계산력에 대한 낭비를 줄일 수 있으나 블록 생성 지분을 기반으로 해서 지분을 많이 보유한 노드가 블록 생성에 유리하다는 단점을 지닌다[12, 13].

PBFT는 1982년 발표된 비잔틴장군문제 해결을 위한 프로토콜로 제시되었으며 악의적인 노드가 있어도 전체적으로 시스템이 안정적인 동작이 가능하다[12, 13].

Raft에서 네트워크에서 리더 역할을 하는 프라이머리 노드(Primary Node)의 주도하에 순차적으로 명령이 수행되며 만일 프라이머리 노드의 에러 발생 시 빠르게 프라이머리 노드의 재선출 과정을 거친다[12, 13].

그림 2와 같이 전체 노드 N개 중 F개의 노드가 문제가 있을 때 N=3F+1을 만족하면 정상 작동이 보장된다.

따라서 퍼블릭 블록체인의 합의 과정 대비 빠르고 효율적인 거래 진행이 가능하다[13].

Raft는 분산 환경에서 합의를 위하여 투표와 로그의 엔트리 복제과정을 거친다. Raft의 참여 노드들은 투표를 통

하여 과반의 지지를 얻은 리더(leader) 노드를 선출하고 모든 메시지의 수정 내용은 리더 노드를 통해 전달 및 반영하도록 한다[13].

Raft의 노드 상태는 리더(leader), 팔로워(follower), 후보 노드(candidate)의 과정을 가질 수 있다. 리더 노드는 변경내용이 담긴 엔트리(Entry)를 팔로워에게 전송하고, 일정 시간 이내 지속해서 어펜드 엔트리(Append Entry)를 보내 리더 노드의 상태를 다른 노드들이 확인하도록 한다. 만일 리더 노드로부터 어펜드 엔트리를 수신받지 못하면 팔로워들은 자신을 후보 노드 상태로 바꾸고 리더 노드가 될 수 있는 후보로 등록한다. 해당 과정을 통하여 일정한 기간을 두어 리더 노드의 상태 확인 및 재선출과정이 이루어진다. 이 과정에서 리더 노드의 상태 확인 및 재선출을 위한 과정은 다음과 같다 [12, 13].

Raft Node's leader election: performed by leader_election thread
↓
After voting, the node state changes according to the result
↓
Depending on the status, the node's execution process is changed to one of do_leader, do_follower, and do_candidate.
↓
When the election is in progress, the value of Raft Node.state is changed
↓
RaftNode.on_leader, Raft Node e.on_follower, Raft Node.on_candidate are executed at the moment of change

Fig. 3. Raft leader re-election process

그림 3의 과정과 같이 Raft는 리더 노드에 의해 합의와 검증과정이 진행되며 그만큼 리더 노드 역할에 대한 중요성이 부각 된다. 현재 리더 노드 선출과정은 리더 노드 에러 시 기존 노드들을 후보 노드로 선정하는 과정을 거쳐 선정되므로 후보 노드에 대한 신뢰성 검증이 아닌 등록 순서가 선출에 중요한 변수가 될 수 있다, 본 논문에서는 리더 노드 선출 시 신뢰성을 보장하기 위한 변수 처리를 신뢰도 파악을 위한 상태 요건을 추가하였다.

III. The Proposed Scheme

1. Comparative Analysis of Consensus Algorithm and Modified Consensus Algorithm

본 논문에서는 프라이빗 블록체인 합의 알고리즘인 Raft의 리더 노드 선출과정에서 노드들의 상태 변경의 과정을 보다 안전하고 효율적으로 수정하기 위하여 노드의 지분과 활성화 상태를 반영한 노드 재선출 과정을 제안하였으며 후보 노드 선출과정에서 발생하는 연산 비용을 절감하기 위하여 Raft에 존재하던 중복 검사 부분을 완화하고 리더 노드의 검증 권한을 강화하도록 하였다. 이러한 합의 과정을 통하여 리더 노드에 대한 신뢰도를 더욱 높이고 합의 과정에서의 연산 속도의 효율성을 높일 수 있다,

본 논문에서 제안하는 Raft의 수정된 리더 노드 선출과정은 다음과 같다.

leader : Sends the entry containing the change history to the follow

Sending append entries continuously within a certain period of time => Let other nodes check the status of the leader

leader error

If you do not receive an append entry from the leader

Filter candidate node list based on node stake and activation status (existing activity frequency and reliability)

Considerations :

If a specific node has recently progressed to the leader, share update: Stake (γ) = Stake (γ)-α

Average Reliability of a Specific Node: β

Candidate list creation and leader election based on γ and β

Fig. 4. Proposed leader selection process

위의 과정에 대하여 Raft 모듈을 사용하여 python 코드로 작성한 코드 일부는 그림4와 같다. 코드에서 어펜드 엔트리 로그로 거래내용을 전송하고 만일 리더 노드에 오류가 발생하면 팔로워의 지분과 신뢰도에 따라 후보 노드 등록 시 정보가 노출되어 리더 노드 선출에 반영되도록 한다.

```
import os, sys, time
import threading, urllib.request, urllib.error, urllib.parse
from pyRaft import Raft
import threading
#leader call and traversal of reader state
def url_checker(node):
    while not node.shutdown_flag:
        time.sleep(1)
        if node.state != flag:
            continue
        for k, v in node.data.items():
            if not k.startswith('site'):
                continue
...
# Receive a node and make it possible to trade only if you are a leader
def url_check_start(node):
   if not hasattr(node, 'node'):  ...
# Execute re-election algorithm if leader does not work
    node.check_ttl(key)
    if key not in node.data:
        if expected.lower() == 'none':
            node.data[key] = expected
   ...
node = Raft.make_default_node()
...
```

Fig. 5. Proposed leader selection process in Python

2. Performance evaluation and analysis

본 논문에서 제안한 그림 3의 처리 과정과 같이 Raft의 리더 노드 선출과정에서 기존의 Raft 알고리즘과 차별화된 후보 노드 신뢰도를 확인한다. 또한 후보 노드의 지분 상태의 확인을 통하여 노드의 안정성을 확보하고자 한다. 이를 통하여 거래 진행 효율성에서 금융거래의 안정성과 효율성을 높이일 수 있다.

본 논문에서 제안한 합의 과정의 성능을 분석하기 위하여 트랜잭션처리 시간(TPS, Transaction per Seconds)을 측정하였다. 성능측정을 위하여 보트 노드 서버 1대와 채굴 서버 1대의 같은 환경으로 진행하였으며 J Meter 서버를 통하여 성능측정 하였다.

실험에 사용한 컴퓨터 사양으로 intel core i5-10210U CPU @1.60GHz의 프로세서와 8GB의 RAM이 적용되었다.

실험을 위하여 node case는 데이터 공유를 위하여 참여한 노드가 5개 미만인 경우, 6~10개인 경우, 11개 이상인 경우로 나누었으며 해당 데이터에 대한 TPS 실험에 관한 결과 그래프는 다음과 같다. 그래프에서 case 1은 일반적인 Raft 알고리즘이고 case 2는 제안한 알고리즘이다.

본 논문에서 제안한 합의 과정을 통하여 트랜잭션의 처리시간을 측정한 결과는 그림 6과 같다.

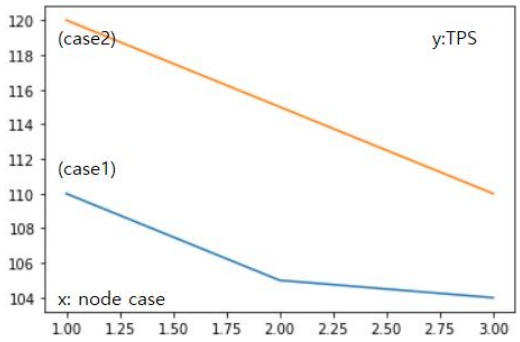

Fig. 6. Performance evaluation result

그림 6의 분석 데이터와 같이 일반적인 Raft 알고리즘 대비 본 논문에서 제안한 알고리즘이 10% 정도 우수한 성능을 보임을 알 수 있다. case 1과 case 2는 10.5% 정도의 성능 향상을 확인할 수 있으며 노드 수가 많은 case 3의 경우 case 1과 case 2 성능 향상이 9% 정도로 다른 경우보다는 조금 저조한 것을 알 수 있다. 노드의 수가 증가하며 검증과정에 대한 연산 비용이 증가한 이유이다.

IV. Conclusions

금융업에서의 블록체인 기술 적용사례가 증가함에 따라 합의 및 검증을 진행하는 기관 간 효율적인 합의 알고리즘 적용의 필요성이 높아지고 있다. 본 논문에서는 프라이빗 블록체인 합의 알고리즘 중 Raft 알고리즘의 리더 노드 선출과정을 수정하여 다양한 기관 간 합의 과정을 효율적으로 할 수 있도록 제안하였으며 트랜잭션 처리시간에 대한 성능평가를 통하여 기존 Raft 알고리즘 대비 10% 정도 성능이 우수함을 증명하였다. 해당 논문의 제한점은 다양한 데이터 공유 및 네트워크에 연결된 노드들의 컴퓨팅 환경에 대한 고려가 부족하다는 것이다. 이러한 제한점을 고려하여 향후 성능평가의 영역을 확대하고 더 안정적인 상황에서 제안한 알고리즘이 적용될 수 있도록 연구할 예정이다.

REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", https://git.dhimmel.com/ bitcoin-whitepaper/, [accessed: Mar. 03, 20201]

[2] Performance Evaluation Items of Blockchain Nodes , http://news.heraldcorp.com/view.php?ud=20190124000136

[3] Buterin Vitalik, "Ethereum white paper", https: //github.com/ethereum/wiki/wiki/%5BKorean%5D-White-Paper. [accessed: Mar. 03, 2021]

[4] Yonatan Sompolinsky and Aviv Zohar, "Secure High-Rate Transaction Processing in Bitcoin", https://fc15.ifcaai/preprocee .dings/paper_30.pdf. Journal of KIIT. Vol. 18, No. 4, pp. 101-107, Apr. 30 2020. pISSN 1598-8619, eISSN 2093-7571 107 [accessed: Mar. 03, 2020]

[5] Dongyan Huang, Xiaoli Ma, and Shengli Zhang "Performance Analysis of the Raft Consensus Algorithm for Private Blockchains", IEEE Transactions on Systems, Man, and Cybernetics: Systems IEEE Trans. Syst. Man Cybern, Syst. Systems, Man, and Cybernetics: Systems, IEEE Transactions, 2020.

[6] Raft.github.io/Raft.pdf [accessed: Mar. 03, 2020]

[7] https://www.geeksforgeeks.org/Raft-consensus-algorithm/ [accessed: Mar. 03, 2021]

[8] Y. A. Park, J. H. Kim, L. K. Kim, and In-kyu, “A Case Study on the Applicationof Ethereum-Blockchain Technology for Electronic Voting System”, Journal of inforamtion technology and architecture,Vol. 15 No. 2 pp. 201-218, 2018.

[9] J. H. Park, “Design of On-Line P2P Financial Transaction Platform Based on Improved PBFT Blockchain”, Hanyang University, 2018.

[10] C. J. Park, and G. M. Park, “Trend Analysis of Application Fields of Blockchain Technology using Patent Data”, The Journal of KINGComputing, Vol. 14, No. 2, pp. 72-81, 2018.

[11] Yixin Li, Zhen Wang, Jia Fan, Yili Luo, Chunhua Deng, and Jianwei Ding, "An Extensible Consensus Algorithm Based on PBFT", 2019 Cyber-Enabled Distributed Computing and Knowledge Discovery International Conference, 2019

[12] M. Castro, and B. Liskov, et al.“Practical byzantine fault Tolerance”, In OSDI, Vol. 99, pp. 173-186, 1999.

[13] Youn-A Min, “The Modification of PBFT Algorithm to Increase Network Operations Efficiency in Private Blockchains”, Applied science, Vol.11, No.14,pp.6313-6320, 2021.

Authors

Hong-Gab Im received the B.S. degree in Visual Design from GwangJu University, Korea, in 1992 and M.S. degrees in Journalism and Mass Communication from Sungkyunkwan University, Korea, in 2010.

He is currently a Professor in the Department of Multimedia at Kimpo University. He is interested in multimedia contents, broadcasting system, IoT platform, and mobile system. Blockchain