JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 23, No. 10, pp. 2067-2074, Oct. 2022

Check for updates

소셜 데이터의 주권과 투명성 및 신뢰성 확보를 위한 소셜 네트워크에서의 블록체인 활용방안 연구

김 선 겸[1*]
[1*]한국건설기술연구원 미래스마트건설연구본부 수석연구원

A Study on the Use of Blockchain in Social Networks for the Sovereignty, Transparency, and Reliability of Social Data

Sun-Kyum Kim[1*]
[1*]Senior Researcher, Korea Institute of Civil Engineering and Building Technology, 283 Goyang-daero, Gyeonggi-do, Korea

[요 약]

최근 소셜 네트워크 서비스는 원 소유자의 데이터가 어떻게 사용되고 있는지 확인하기가 어려워 원 소유자의 이용동의 없이 2차, 3차 가공되어 가공자가 경제적 이득을 취하거나 사용자는 무분별한 정보의 범람으로 인해 사실 관계가 확인되지 않은 정보 구별에 어려움을 겪고 있다. 본 연구에서는 이러한 문제를 해결하기 위하여 블록체인을 소셜 네트워크에 적용하는 방안으로 하이퍼렛저 패브릭(Hyperledger fabric)을 활용하여 소셜 네트워크로부터 분석된 친구 및 주제별 데이터를 수집하고, 주제 기반 커뮤니티 내에서 합의와 검증을 통해 데이터를 블록화함으로써 데이터 주권 확보와 루머/허위정보·가짜뉴스를 필터링 하여 투명성 및 신뢰성 높은 데이터를 제공하는 블록체인 모델을 제시하고 이의 프로토타입의 구현을 서술한다. 하이퍼렛저 패브릭과 IPFS를 활용한 프로토타입을 개발을 함으로써 해당 시스템의 가능성을 확인할 수 있었다.

[Abstract]

Recently, social network services are difficult to check how the original owner's data is being used, so it is processed secondarily or tertiarily without the original owner's consent, so that the processor obtains economic benefits or the user can't confirm the fact due to the indiscriminate overflow of information. It is difficult to distinguish information that is not. In this study, as a way to apply block chain to social networks to solve this problem, Hyperledger fabric is used to collect friends and topical data analyzed from social networks, and consensus and verification within the topic-based community. We present a blockchain model that provides data with high transparency and reliability by securing data sovereignty and filtering rumors/false information/fake news by blocking data, and describes the implementation of its prototype. By developing a prototype using Hyperledger Fabric and IPFS, the potential of the system was confirmed.

색인어 : 블록체인, 하이퍼렛저 패브릭, 소셜 네트워크, 신뢰성, 투명성

Keyword : Blockchain, Hyperledger fabric, Social network, Transparency, Reliability

http://dx.doi.org/10.9728/dcs.2022.23.10.2067

Received 30 August 2022; **Revised** 23 September 2022
Accepted 26 September 2022

***Corresponding Author; Sun-Kyum Kim**

Tel: +82-31-995-0962
E-mail: sunkyumkim@kict.re.kr

Ⅰ. 서 론

블록체인 [1]은 '블록'이라고 하는 데이터들이 체인형태의 분산 데이터 저장 환경으로 연결된 분산원장(distributed ledger) 관리 기술이다. 블록체인은 누구라도 데이터의 위변조가 불가능하고, 거래 내역이 암호화된 블록으로 보관되며, 네트워크에 연결된 모든 참여자가 공동으로 거래 내역을 기록 및 관리하는 탈중앙화의 특징을 가진다. 블록체인은 2016년 세계 경제포럼에서 4차 산업혁명 시대를 이끌어갈 핵심 기술 중 하나로 소개된 블록체인은 비트코인(Bitcoin), 이더리움(Ethereum) 등의 암호화폐로 인해 관심이 더욱더 증대되었다. 주로 신뢰성이 필요한 위·변조 방지와 유통 및 전달 과정, 보안이 필요한 개인 인증 과정, 수익의 재분배가 필요한 분산 상황 등 다양한 분야 및 환경에서 블록체인 서비스 및 연구가 진행되고 있다. 블록체인의 가장 큰 강점으로는 블록체인 네트워크에 연결된 모든 참가자들의 거래내역이 공개되기 때문에 거래의 투명성을 확보할 수 있으며, 노드의 확보가 되지 않으면 조작이 어려우므로 보안문제 또한 해결이 가능하다.

최근 네트워크의 기술적인 발전과 데이터의 저장용량의 증가 등 환경이 빠르게 변화하여 대용량 정보의 처리가 가능해지면서 출처가 모호하고 보호되지 않은 정보들이 매일 같이 생산되고 있다. 특히, 누구나 쉽게 접근할 수 있는 페이스북, 인스타그램, 트위터 등으로 대표되는 소셜 네트워크 서비스는 이런 경향이 더 심화되어 원 소유자의 데이터가 어떻게 사용되고 있는지 확인하기가 어려워 원 소유자의 이용동의 없이 2차, 3차 가공되어 가공자는 경제적 이득을 취하거나 사용자는 무분별한 정보의 범람으로 인해 사실 관계가 확인되지 않은 정보 구별에 어려움을 겪고 있다 [2][3].

이를 극복하고자 블록체인을 활용한 다양한 소셜 네트워크 서비스 [4][5][6][7][8]들이 운영되고 있으나, ID를 만드는 것이 불편하여 접근성이 떨어지며, 불특정인들과 주제에 맞지 않는 커뮤니티의 구성은 데이터의 신뢰성과 투명성을 보장해 주지 않는다.

본 연구에서는 이러한 문제를 해결하기 위하여 블록체인을 소셜 네트워크에 적용하는 방안으로 하이퍼렛저 패브릭(Hyperledger fabric)[9] 을 활용하여 소셜 네트워크로부터 분석된 친구 및 주제별 데이터를 수집하고, 주제 기반 커뮤니티 내에서 합의와 검증을 통해 데이터를 블록화함으로써 데이터 주권 확보와 루머/허위정보·가짜뉴스를 필터링 하여 투명성 및 신뢰성 높은 데이터를 제공하는 블록체인 모델을 제시하고 이의 프로토타입의 구현을 서술한다. 프로토타입은 블록체인을 적용하여 데이터 입력을 하고 이를 정확성 검증을 하며, 원장에 기록할 내용에 대해 합의를 한다.

본 논문의 구성은 다음과 같다. 2장은 블록체인과 관련 연구를 정리한다. 3장의 제안하는 시스템에 대한 설명과 4장에서는 프로토타입 구현 결과를 제시하며, 5장에서 결론으로 마무리 한다.

Ⅱ. 관련 연구

2-1 블록체인

블록체인은 P2P(Peer to Peer) 네트워크, 암호화, 장부, 합의로 구성된 분산 컴퓨팅 기술 기반의 위변조 방지 기술이다. 거래정보는 블록체인 네트워크에 분산되어 있는 수많은 참여자(노드)들에게 공유되며, 이러한 과정 속에서 중개자 없이 탈중앙화(decentralization)의 형태로 공증을 위한 합의 및 승인이 수행되어, 거래자 간의 신뢰 문제를 해결하는 수단이 된다. 그러므로 참여자는 거래 데이터의 타당성 확인, 공개키 기반의 암호화, 합의 및 공증을 통한 단일 블록체인 유지를 통해 데이터를 안전하게 공유할 수 있다.

블록체인의 합의를 위하여 가장 마지막 블록이 블록체인에 연결된 이후에 발생한 모든 거래 데이터를 하나의 블록으로 묶고 새로운 암호화 블록을 생성한다. 새로운 블록의 생성을 위하여 참여자 모두가 해쉬값 계산을 하며, 최초로 계산한 참여자가 새로운 암호화 블록을 생성하며 다른 참여자에게 전송하여 승인을 요청한다. 이와 같은 합의 방식을 작업증명(proof of work)이라고 하며 비트코인에서 이러한 합의 방식을 사용한다. 이외에도 지분 증명(proof of stake) [10], 실용적 비잔틴 포용 방식(practical Byzantine fault-tolerance) [11]등 다양한 방식이 있으며 지속적으로 연구되고 있다.

블록체인은 사용자의 참여방식에 따라 퍼블릭 블록체인과 프라이빗 블록체인으로 나누어 진다. 퍼블릭 블록체인은 모든 참여자가 참여를 하며 참여자 수에 따라 합의에 걸리는 시간이 증가한다. 반면에 프라이빗 블록체인은 참여자를 일부 제한하는 것으로, 합의에 걸리는 시간이 짧기 때문에 거래 데이터 처리 및 관리에 용이하여 비즈니스에 많이 활용된다.

2-2 소셜 네트워크 서비스 블록체인 적용 현황

SteemIT [3]은 누구나 콘텐츠를 만들고 이를 큐레이팅을 한 대가로 암호화폐를 받을 수 있는 서비스이다. Steem, Steem Power(SP), Steem Dolloar(SD) 세가지의 다른 종류의 화폐를 활용하여 운영되는데 Steem은 암호화폐 거래소에서 송금과 거래가 화폐이고, SP는 Steem만 받고 SteemIT을 종료하는 것을 예방하기 위한 영향력이며, SteemIT에서 SD는 콘텐츠 제작자에게 지급하는 스테이블 코인이다.

Lit [4]은 Instagram 및 SnapChat과 같은 소셜 네트워크 서비스 플랫폼에 암호화폐를 통합한 서비스이다. 사용자가 Lit Stories를 통해 스토리를 공유할 수 있고 이에 영향을 고려하여 Mithril 토큰(MITH)을 얻을 수 있다.

HyperSpace [5]는 사용자가 속한 커뮤니티 내에서 콘텐츠를 만들 수 있는 서비스를 제공하는데 사용자는 활동에 대해 보상과 인정을 받는다.

Sapien [6]은 사용자에게 데이터 제한권한을 두어 가짜뉴스를 제어하는 것을 목표로 하는 뉴스 서비스이다. 사용자는

개인 정보를 공유할 수 있는 사람을 결정할 수 있으며, 수신된 뉴스를 관심 분야에 마찍 조정하여 정보를 제어할 수 있다.

SocialX [7]는 모든 데이터(사진, 비디오, 메시지, 게시물 등)가 분산되어 있으며 사용자가 콘텐츠에 대한 피드백을 제공하고 토큰을 보상할 수 있는 서비스이다. 이를 통해 가짜 계정, 가짜 팔로워, 가짜 투표를 추출한다.

FORESTING [8]는 디지털 뱅킹 서비스인 '포레스팅 뱅크', 커뮤니티 및 콘텐츠 제작자를 지원하는 '포레스팅랩'으로 구성된 서비스이다. 블록체인을 통해 가치 있는 콘텐츠를 제공하고 보상한다.

블록체인 기반 소셜 네트워크 서비스들은 부분, 전체의 분산 아키텍처를 활용하고 네트워크 내 콘텐츠의 사회적 영향을 고려하여 토큰으로 보상하는 의미 있고 흥미로운 콘텐츠를 제공하나, 여전히 불특정인들과 주제에 맞지 않는 커뮤니티의 구성은 데이터의 신뢰성과 투명성을 보장해 주지 않는다. 이러한 문제로 인해 신뢰성 있는 커뮤니티를 구성하고 이를 활용하는 것이 필요하다고 판단된다.

Ⅲ. 제안하는 시스템

본 연구는 소셜 네트워크에 블록체인을 활용하는 방안으로 "블록체인 기반 분산 소셜 네트워크 시스템"을 제안한다. 제안하는 시스템은 소셜 네트워크로부터 친구 링크 및 주제별 데이터를 수집하고, 주제별 분산 오버레이 네트워크 구성을 통해 중앙 서버의 통제로부터 분리하며, 주제 기반 커뮤니티 내에서 합의와 검증을 통해 데이터를 블록화함으로써 데이터 주권 확보와 루머/허위정보·가짜뉴스를 필터링 하여 투명성 및 신뢰성 높은 데이터를 제공하는 시스템이다. 분산 소셜 오버레이 네트워크는 각각의 데이터의 주제별로 클러스터링을 하고 데이터와 사용자의 이계층으로 나누어 주제간 커뮤니티 멤버 구성, 파일 검색은 친구 링크를 통해 접근을 할 수 있는 오버레이된 네트워크를 말한다.

그림 1은 최종연구목표로써 제안하는 시스템이다. 그림의 하단부에서처럼 기존 시스템은 주제와 상관없이 친구 기반으로 네트워크가 구축이 되어있었다면, 제안하는 시스템은 블록체인을 적용하여 주제 기반으로 클러스터링 되어 유사 주제의 사용자들을 통해 커뮤니티를 형성하고 커뮤니티 기반으로 합의와 검증을 진행하며, 원 소유자의 데이터를 주권을 강화하였으며, 새로 생성된 분산 오버레이 네트워크의 기존에 사용하던 친구링크를 통하여 원하는 주제를 검색하여 보다 전문성이 있고 신뢰성이 높은 데이터에 접근을 가능하게 한다. 기존 시스템의 경우 중앙 서버가 데이터 관리를 함으로써 사용자의 데이터가 어디서 어떻게 활용되어지는지 사용자가 확인할 수 없고, 중복으로 품질이 낮은 데이터들이 즐비하였으며, 검증되지 않은 각종 루머 및 가짜 뉴스들이 범람하였다.

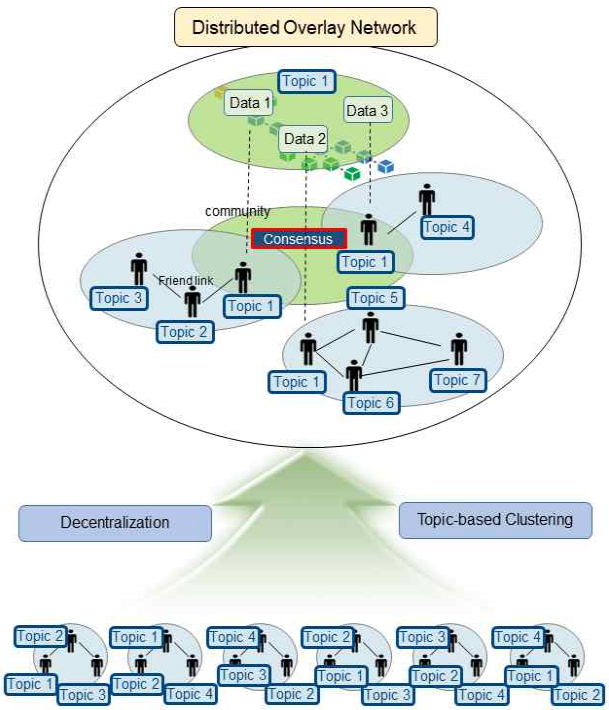

그림 1. 제안하는 시스템
Fig. 1. Proposed system

제안하는 시스템은 이 블록체인을 통해 데이터 주권을 확보하고 커뮤니티 멤버들간의 합의 및 검증으로 인한 데이터의 신뢰성 및 투명성을 확보할 수 있게 된다.

해당 시스템이 가능한 이유는 첫 번째로 제안하는 시스템을 구성하는 분산 오버레이 네트워크는 커뮤니티와 친구 링크를 통해 구성된 네트워크에 접속하고 있는 모든 사용자에게 원하는 파일을 공정하게 분배 받을 수 있도록 하는데 큰 역할을 한다. 또한 블록체인 기술을 이용하여 원 소유자의 데이터가 어디서, 어떻게 사용되어지고 있는지를 파악하고, 어떠한 가치를 창출하게 되는지를 확인함으로써 원 소유자 본인들의 데이터를 통제 가능케 한다. 마지막으로 주제별로 구성된 커뮤니티는 의견의 다양성, 독립성, 분권화, 통합화의 과정을 거치므로써 집단지성에 기반한 전문성을 띤 커뮤니티 기반의 합의와 검증이 가능하다 [12].

그림 2는 본 사용자가 소셜 데이터를 업로드하면서 데이터의 주제에 기반한 오버레이 네트워크를 생성하는 과정을 나타낸 것이다. 네트워크 구성은 초기에 미리 시스템에서 완성된 커뮤니티 구성을 제외하고 데이터를 업로드시에 동시에 이루어진다. 초기에 기본 주제별 커뮤니티가 존재하고, 해당 주제에 관한 단어 가방(Bags of words)가 있다고 가정한다. 사용자는 소셜 데이터를 웹에 올리게 된다. 시스템은 해당 데이터의 태그로부터 주요 키워드를 추출하고 이를 기존 주제에 포함되는 단어가방으로부터 존재하는지 파악하고, 존재할 경우에 해당 단어가방의 단어에 관한 주제를 확인하여 해당 커뮤니티에 포함시킨다.

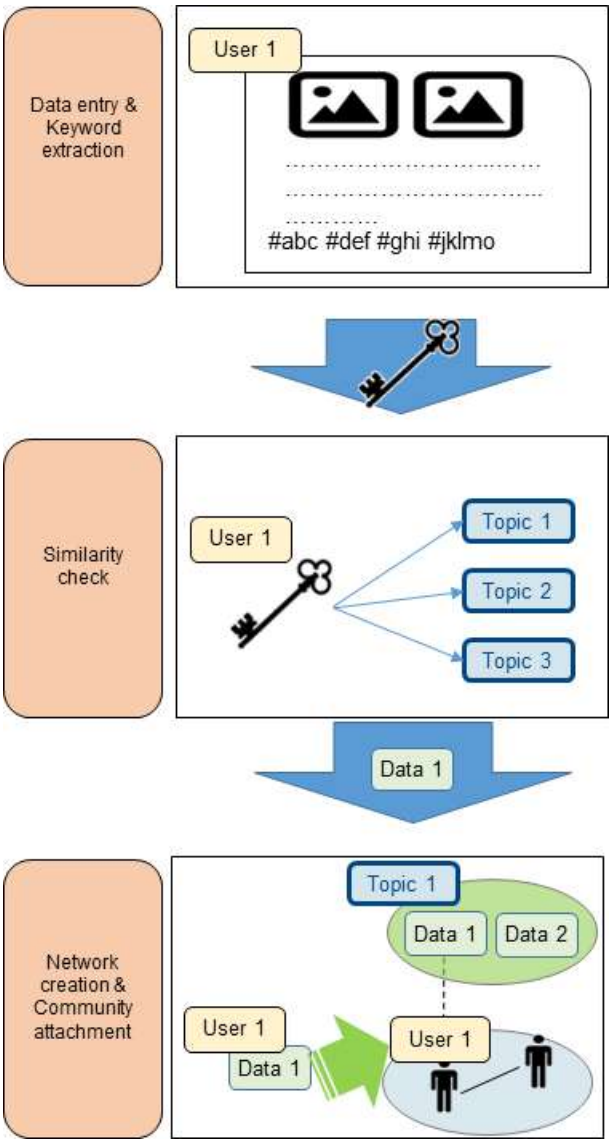

그림 2. 네트워크 생성
Fig. 2. Network creation

만약 단어가방이 존재하지 않는다면, 데이터의 키워드들과 단어가방의 주제들과의 유사도 검사를 통해 유사하다고 판단되면 유사한 주제 커뮤니티에 포함시킨다. 모두 해당이 안되면 가장 최초의 태그키워드를 통해 주제 커뮤니티를 새로 만든다. 사용자가 데이터 올릴 시에 반복하게 되며, 주제별로 확장해 나간다.

Ⅳ. 프로토타입 구현

본 연구에서는 제안하는 시스템이 실제로 동작여부를 파악하기 위해 프로토타입을 만든다. 기존 소셜 네트워크 시스템의 데이터를 추출하여 하이퍼렛저 패브릭 기반의 블록체인을 활용한다. 본 프로토타입은 주제 기반 클러스터링을 통한 기본 블록체인 오버레이 네트워크가 구성을 제외하고 사용자의 입력부터 합의 및 검색까지 구현한다.

4-1 하이퍼렛저 패브릭 기반 시스템 구조도

본 연구에서 개발한 프로토타입은 리눅스 재단에서 만든 하이퍼렛저 패브릭(Hyperledger Fabric) 블록체인 프레임워크를 활용하였다. 그림 3은 본 프로토타입에 사용한 하이퍼렛저 패브릭 기반의 시스템 구조도를 도식화 한 것이다. 제안하는 시스템은 애플리케이션(Applicaton), 블록체인 API 서버(Blockchain API Server), MongoDB, 블록체인 코어(Blockchain core)로 구성되어 있으며 본 시스템의 설정 및 테스팅을 위한 블록체인 빌딩 & 테스팅 툴(Blockchain Budiling & Testing Tool)이 있고 데이터 관리를 위해서 외부의 IPFS [13]와 연동하기 위한 IPFS 클라이언트(IPFS Client)가 있다. 애플리케이션은 개발에 용이한 Node.js, 나머지는 뷰기능을 쉽게 다룰 수 있는 웹 애플리케이션 프레임워크인 Pug, 블록체인 트랜잭션의 동작을 위한 내부의 체인코드(Chaincode)는 GoLang[14]으로 개발한다. 기본적으로 웹에서 실행할 수 있으며, 애플리케이션은 서버의 기능을 담당하고 시스템 동작의 총괄을 한다. 블록체인 API 서버는 블록체인의 스마트 계약을 통해 블록체인에 원장을 읽고 쓰는 작업을 하며, 이를 애플리케이션으로 관리한다. 블록체인 코어는 하이퍼렛저 패브릭 1.4.4로 구성되어 있으며, 트랜잭션 처리와 데이터의 검증 및 Raft 알고리즘 [15]을 활용한 합의 기능을 수행한다. MongDB는 블록화 되기위한 소셜 데이터들을 관리하며, 블록체인 빌딩 & 테스팅 툴은 블록체인 네트워크를 설정하고 테스트 한다.

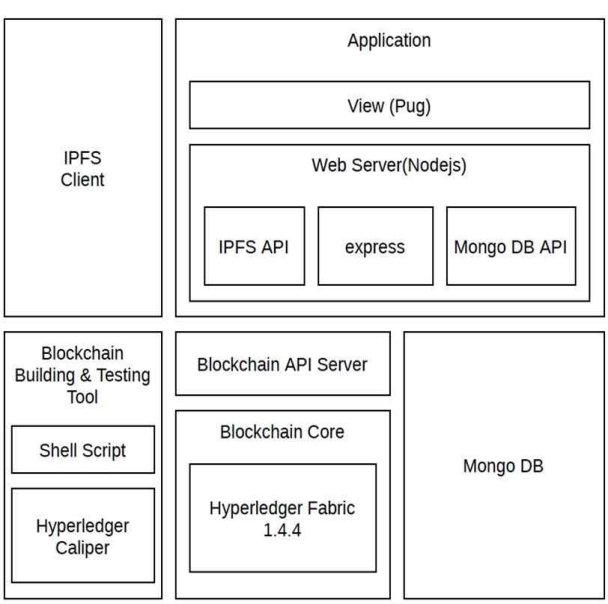

그림 3. 시스템 구조도
Fig. 3. System Architecture

4-2 프로토타입 시나리오

그림 4는 프로토타입의 동작 시나리오이며, 표 1는 개별 객체들의 설명을 보여준다. 데이터의 사용자(User)가 웹 페이지(Web page)에 소셜 데이터를 입력을 하면 웹 서버(Web server)에서는 IPFS에 소셜 데이터 파일을 저장 요청한다. IPFS는 분산화된 네트워크에 파일을 저장하고, 파일의 원본 파일에 대한 해쉬값을 생성해서 웹 서버로 해쉬값을 넘겨준다. 웹 서버는 넘겨받은 해쉬값 및 메타데이터 정보(e.g., 사용자, 생성 일시 등)를 분산원장에 저장한다. 저장된 트랜잭션 정보는 다시 MongoDB에 저장하여 추후에 데이터를 읽어올 때의 효율성을 증가시킨다. MongoDB에 저장된 데이터를 웹 페이지에 보여주면서 사용자가 소셜 데이터를 입력했을 때 소셜 데이터 정보가 저장되고 웹 페이지에 저장된 정보가 출력되고 사용자는 출력된 데이터를 확인할 수 있으며, 다른 사용자들도 이 정보에 접근할 수 있게 된다. 궁극적으로 본 시스템은 블록체인을 활용하여 IPFS의 분산 peer에 저장되는 파일들은 파일의 해쉬 값을 통하여 파일의 위변조 탐지가 가능하게 하여 데이터 주권을 확보하고 신뢰성을 높일 수 있다.

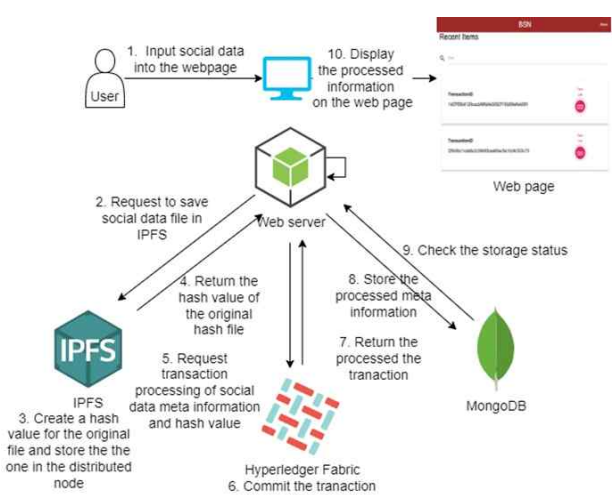

그림 4. 프로토타입 동작 시나리오
Fig. 4. Prototype operation scenario

표 1. 프로토타입 객체 역할
Table 1. Prototype object role

Role	Definition
Client(User)	Data management, release (On-chain submission), retrieval
Web server	Saving social data into IFPS, Keeping the original hash value
IPFS	Creation of a hash value
Hyperledger Fabric	Committing transactions to distributed ledgers
MongDB	Saving the meta information
Web page	Checking the storage status

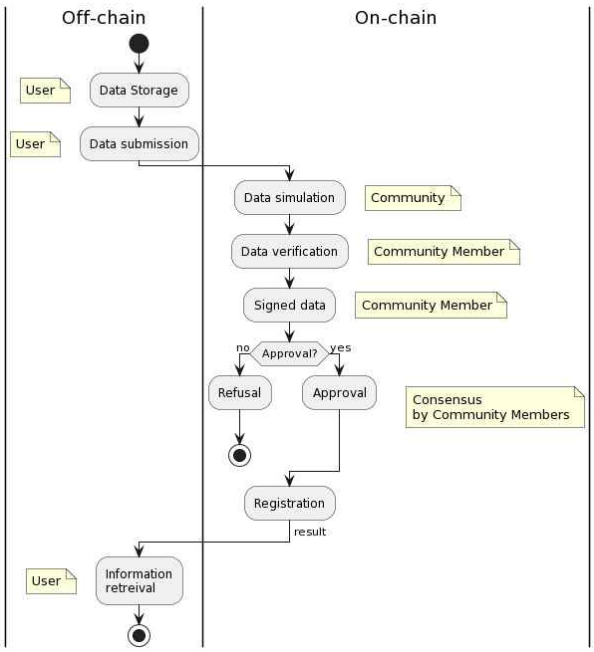

그림 5. on-chain, off-chain 동작 흐름
Fig. 5. on-chain, off-chain operation flow

4-3 프로토타입 모델링

프로토타입은 Docker 기반의 peer 형태로 구성되며 검증 노드는 Docker 컨테이너에 체인코드를 배포하고 실행한다. 표 2는 본 구성에 따른 Docker 컨테이너이며, 그림 7은 컨테이너간 관계도를 나타낸다.

사용자가 직접 접근할 수 있는 Web Server와 이와 연계되는 IPFS Client, Mongo DB, Hyperledger Fabric API Server를 비롯하여 주요 컨테이너로는 메인 네트워크를 구성하는 3개의 orderer, 각 orderer와 연계하는 4개의 peer, 각 조직이 관리하는 2개의 CA가 있다. API Server는 각 peer와 http로 연계된다. Web Server의 경우 사용자게에게 본 시스템을 활용할 수 있도록 웹페이지를 제공하며, 사용자는 웹페이지를 통해 Web Server에 다양한 명령을 내린다. Web Server는 사용자의 명령에 따라 각 클라이언트를 적극 활용하여 서비스를 제공한다. Web Server에서 활용하는 IPFS Client는 전세계의 IPFS Server와 연계되어 있으며, Web Server와 연계하여 본 시스템에서 관리하는 파일을 서버에 upload, read하는 기능을 수행한다. 또한 Web Server에서 활용하는 MongoDB의 경우 본 시스템이 관리하는 데이터들을 캐싱하여 더욱 빠르게 listing, query등의 데이터를 처리할 수 있도록 도와주는 역할을 한다. 각 블록체인 네트워크의 분산화, 성능, 안정성을 위해 5개의 물리적인 서버 또는 peer에서, 2개의 조직에 네트워크를 관리하고 있으며, Orderer는 각 서버에 할당되어 있다.

표 2. 사용자별 Docker container
Table 2. Docker container by users

User	Docker container
orderer	orderer0.kict.re.kr, orderer1.kict.re.kr, orderer2.kict.re.kr
peer0.org1.kict.re.kr	peer0.org1.kict.re.kr, ca.org1.kict.re.kr
peer1.org1.kict.re.kr	peer1.org1.kict.re.kr
peer0.org2.kict.re.kr	peer0.org2.kict.re.kr, ca.org1.kict.re.kr
peer1.org2.kict.re.kr	peer1.org2.kict.re.kr

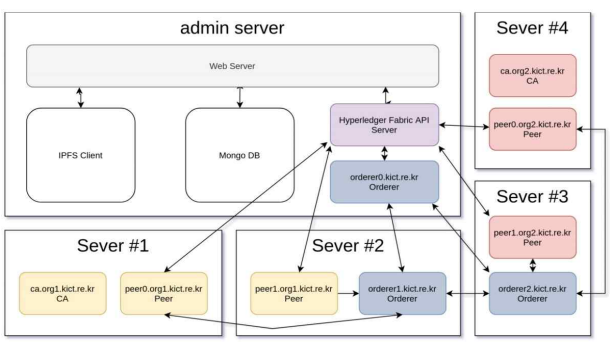

그림 6. Docker 컨테이너간 관계도
Fig. 6. Relationship of docker containers

이를 통해 하나의 peer 또는 Orderer에 문제가 발생하더라도 네트워크 전체적으로는 문제 없도록 설계되어 있다. 그리고 2개의 조직은 각각 2개의 peer를 각 서버에 가지고 있으며 이 또한 한, 두개의 Peer 에 장애가 발생하더라고 문제없도록 구성하였다. 각 블록체인의 요소들은 gRPC를 통해 연동이 된다.

그림 7은 프로그램상 실제로 동작하는 네트워크의 개념적 구성도이다. 본 시스템을 구성하는 블록체인 네트워크의 경우 네트워크 및 구성 요소들을 관리하는 Orderer Channel과 본 시스템에서 활용하는 네트워크인 kict Channel이 있다. 각 peer들은 Orderer Channel 및 kict Channel에 연계되어 있으며, 각 Peer들은 본 네트워크의 endpoint인 Hyperledger Fabric API Server와 연계되어 있어서, 외부의 사용자는 Hyperledger Fabric API Server 를 통해서 본 네트워크를 활용하게 된다. 그리고 각 조직은 하나의 CA를 가지고 있으며, CA를 활용하여 각 피어의 접근, 서명 등을 관리한다. Orderer Channel의 경우 3개의 Orderer가 관리하고 있으며, 다른 채널과 peer 등을 등록하여 관리하는 역할을 한다. 그리고 kict Channel의 경우 org1, org2 두 조직이 관리 및 활용하고 있다. 그래서 본 채널에서 발생한 데이터는 본 채널의 가입자만 접근할 수 있다. 이를 통해 네트워크는 private 한 데이터는 kict Channel에서 관리하고 그 외의 시스템 적은 부분은 orderer Channel이 관리하여 데이터의 기밀이 유지될 수 있도록 구성한다. 각 peer는 네트워크에서 활용되는 체인코드 및 데이터를 저장하는 Ledger를 가지고 있다.

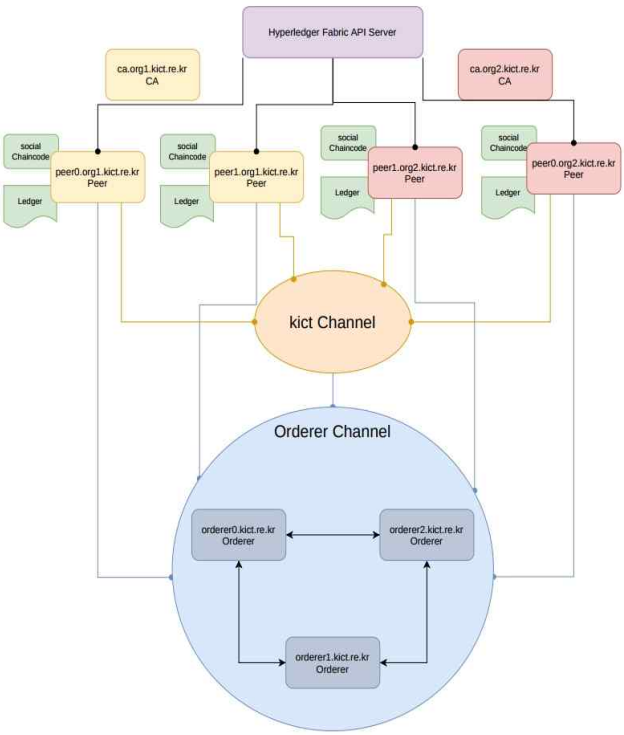

그림 7. 프로토타입 블록체인 네트워크 구성도
Fig. 7. Prototype Blockchain Network Diagram

체인코드의 경우 블록체인을 활용하는 비즈니스 로직이며, 모든 peer가 같은 체인코드를 가지고 있다. 이는 피어 간의 합의를 통해 보안/신뢰를 얻는 신뢰할 수 있는 분산 응용 프로그램의 기능을 한다. Ledger의 경우 합의된 데이터를 관리하고, 블록체인 내의 채널에서 쌓였던 모든 데이터를 가지고 있고 필요시 query, listing등의 기능을 제공해 준다.

4-4 프로토타입 동작

본 프로토타입은 그림 4의 시나리오에 기반하여 작성한 chaincode에 따라 그림 8과 같이 동작한다. IFPS와 블록체인은 REST API서버를 통해서 통신을 수행하며, 수행절차마다 함수기반으로 호출 및 응답한다.

주요 구성요소로는 사용자가 접근할 수 있는 Web, 제안을 확인하고 서명하는 Community, 메타데이터를 관리하는 IFPS, 하이퍼렛저 패브릭에 접근할 수 있는 Web server, 제안을 시뮬레이션을 통한 유효성을 확인하는 Endorser peer, peer와 연동하여 블록을 배포하는 Orderer, 데이터가 담긴 블록을 저장하고 관리하는 Committing Peer가 있다. 표 3의 각 peer들은 모두 Community member, Endorser peer, Committing peer로 행동한다. 사용자는 Web을 통하여 제안 데이터를 Web Server로 보낸다. Web Server는 메타 데이터를 IPFS를 통하여 저장하고 Endorser Peer에 보내 데이터의 유효성을 검사한다.

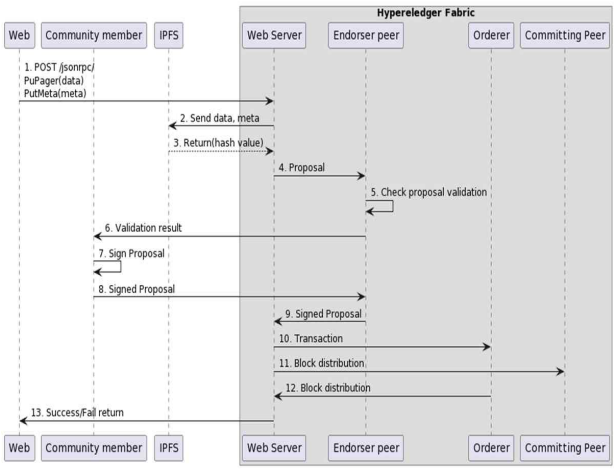

그림 8. 코드 동작
Fig. 8. How codes work

검사된 결과는 Community member인 조직들이 확인하고 서명을 하게 된다. 서명된 정보는 다시 Web Server를 통하여 Orderer로 가게된다. 최종적으로 Orderer에서 각 Peer로 배포된다. 그리고 Orderer로 데이터를 보낸 결과를 Web서버를 통해 사용자에게 알려준다.

V. 결 론

본 연구는 블록체인을 활용하여 소셜 네트워크 상에서 주권이 확보되지 않아 출처가 모호하고 데이터의 무분별함을 방지하기 위해 친구 링크와 주제 클러스터링을 통해 분산 오버레이 네트워크를 구축하고 주제 커뮤니티의 커뮤니티 멤버들의 합의와 검증을 통해 소셜 데이터를 블록화함으로써 데이터 주권 확보를 하고 신뢰성 높은 데이터를 공유하는 시스템을 제안하였다. 또한 하이퍼렛저 패브릭과 IPFS를 활용해 사용자가 데이터를 입력하고 이 데이터가 블록체인 네트워크가 구성되는 프로토타입을 개발을 함으로써 해당 시스템의 활용 가능성을 확인할 수 있었다.

본 연구는 프로토타입의 개발이기 때문에 향후에는 이를 보완하여 다수 사용자의 본격적인 참여를 통해 합의 알고리즘을 강화하고 인센티브를 제공하는 강화된 블록체인 시스템을 연구할 예정이다.

감사의 글

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업 연구로서, 관계부처에 감사드립니다.

참고문헌

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." *Decentralized Business Review*, 21260. 2008. https://www.debr.io/article/21260.pdf

[2] H. Kang and S. Jeon, “The Current Issues on Domestic e-Commerce Regulations and Global Competitions: Market Dominance, Data Sovereignty, and Amazon Effects”, *Korea Law & Economics Association*, Vol. 15, No. 3, pp. 355-374, December, 2018. https://scholarworks.bwise.kr/gachon/handle/2020.sw.gachon/4540

[3] A. Kiayias, B. Livshits, A.M. Mosteiro, and O.S.T. Litos, “A puff of steem: Security analysis of decentralized content curation”, arXiv preprint, pp. 1-35, October, 2018. https://doi.org/10.48550/arXiv.1810.01719

[4] B. Guidi, and A. Michienzi, “Users and bots behaviour analysis in blockchain social media”, in *Proceedings of 2020 Seventh International Conference on Social Networks Analysis, Management and Security*, pp. 1-8, December, 2020. https://ieeexplore.ieee.org/document/9336553

[5] M. Huetsch and C. Wang, Hyperspace: Fast, Cheap, and Private Storage, Coinpaprika, Technical Report, pp. 1-8, December, 2018. https://static.coinpaprika.com/storage/cdn/whitepapers/10557423.pdf

[6] A. Bhatia, R. Giometti, and A. Nicolas, Decentralized social news platform, Technical Report, pp. 1-52, March, 2018. https://neironix.io/documents/whitepaper/094dc71f08804f544dcf947982789f30.pdf

[7] SocialX Pte. Ltd., The socialx ecosystem takes the social media experience to the next level, Technical Report, pp. 1-48, July, 2018. https://socialx.network/wp-content/uploads/2018/09/Whitepaper-SocialX-v1.1.pdf

[8] Foresting HQ Ltd., Foresting, Technical Report, pp. 1-130, August, 2019. https://www.allcryptowhitepapers.com/pton-foresting-whitepaper/

[9] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin,vK. Christidis, A. De Caro, ... and J. Yellick, “Hyperledger fabric: a distributed operating system for permissioned blockchains”, in *Proceedings of the thirteenth EuroSys conference*, pp. 1-15, April, 2018. https://doi.org/10.1145/3190508.3190538

[10] V. Buterin, What Proof of Stake Is And Why It Matters, Bitcoin Magazine[Internet], pp. 1-1, August, 2013. Available:https://bitcoinmagazine.com/culture/what-proof-

of-stake-is-and-why-it-matters-1377531463

[11] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance”, *Third Symposium on Operating Systems Design and Implementation*, Vol. 99, No. 1999, pp.173-186, February, 1999. https://dl.acm.org/doi/10.5555/296806.296824

[12] J. Hwang, S. Choi, and S. Kim, A Study on the Mechanism of Social Production of Collective Intelligence in a Social Computing Environment, *Korea Information Society Development Institute*, Technical Report, pp. 1-169, December, 2019.

[13] A.A. Donovan and B.W. Kernighan, The Go programming language, *Addison-Wesley Professional*, pp. 1-380, September, 2015.

[14] J. Benet, “Ipfs-content addressed, versioned, p2p file system”, arXiv preprint, pp. 1-11, July, 2014. https://doi.org/10.48550/arXiv.1407.3561

[15] D. Ongaro and J. Ousterhout, J, “In search of an understandable consensus algorithm”, in *Proceeding of 2014 USENIX Annual Technical Conference* , pp. 305-319, June, 2015.

김선겸(Sun-Kyum Kim)

2012년 : 연세대학교 대학원 컴퓨터과학과(공학석사)
2016년 : 연세대학교 대학원 컴퓨터과학과(공학박사-모바일컴퓨팅)

2016년～2017년: 한국건설기술연구원
2017년～2019년: 한국과학기술정보연구원
2019년～2020년: 차세대융합기술연구원
2020년～현 재: 한국건설기술연구원 미래스마트건설연구본부
※관심분야 : 모바일 컴퓨팅(Mobile Computing), 데이터 분석(Data Analysis), 블록체인(Blockchain)